Valentin Mulder
Alain Mermoud
Vincent Lenders
Bernhard Tellenbach *Editors*

Trends in Data Protection and Encryption Technologies

OPEN ACCESS

Springer

Trends in Data Protection and Encryption Technologies

Valentin Mulder • Alain Mermoud •
Vincent Lenders • Bernhard Tellenbach
Editors

Trends in Data Protection and Encryption Technologies

Springer

Editors
Valentin Mulder
Cyber-Defence Campus
armasuisse Science and Technology
Thun, Switzerland

Alain Mermoud
Cyber-Defence Campus
armasuisse Science and Technology
Thun, Switzerland

Vincent Lenders
Cyber-Defence Campus
armasuisse Science and Technology
Thun, Switzerland

Bernhard Tellenbach
Cyber-Defence Campus
armasuisse Science and Technology
Thun, Switzerland

This work was supported by armasuisse.

ISBN 978-3-031-33385-9 ISBN 978-3-031-33386-6 (eBook)
https://doi.org/10.1007/978-3-031-33386-6

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Foreword by Quentin Ladetto

Being invited to provide a foresight perspective on data protection and encryption technologies is quite challenging. The data we need to protect today is significant, not neglecting the numerous risks and forms of attacks we need to anticipate. Are we looking to protect access to the data, its transfer, its computation, or its commercial exploitation? How long should the data be protected or resist attacks? Any answer to those questions will undoubtedly lead to different design choices and technological challenges.

Historically, protection to prohibit access to data and information has always existed, as well as different forms of encryption. However, the digitalization of our society has increased its importance. Phrases like "software is eating the world" and "data is the new gold" reflect the crucial importance of data in our modern society. Via all the connected devices and the various digital applications, the ultimate goal via the production of data is the complete and permanent anticipation of all desires and needs of the individuals. Unfortunately, the main driving force behind those developments is not the individual's well-being per se but the leveraging of the collected data for commercial purposes. Therefore, data protection related to privacy became essential to fulfill that goal and comply with new regulations, leading to specific research and innovation.

The digitalization trend illustrates the importance of society in developing and accepting data protection and encryption technologies. The past years' economic, political, and research environment has allowed the emergence of our technological level in this area. However, values and lifestyles are being challenged today and, as such, shall be our priorities for the upcoming years.

The development run of areas such as quantum computing, artificial intelligence, and biometrics, to take only a few trends addressed in this book, is driving the developments of the future of data protection and encryption technologies. This book provides a valuable overview of the upcoming challenges and trends with

practical recommendations. It is a must-read for any decision-maker who must protect their data against current and emerging cyber threats.

Thun, Switzerland
November 2022

Quentin Ladetto
Head of Technology Foresight,
armasuisse Science and Technology

Foreword by Florian Schütz

Data fuels our modern economy and is at the heart of our digital lifestyle. Its protection is, therefore, not only important but crucial for modern societies to function. When discussing the protection of data, quite often, the public discussion focuses on confidentiality. However, with increasing dependence on technology for everyday services, the understanding that availability and integrity are just as important spreads fast beyond expert circles. Data protection is a topic that has been discussed previously. For example, the Spartans already used cryptography, the best-known means to protect data. However, modern, interconnected large-scale systems have very different requirements, not only on the robustness of protection mechanisms but also on their scalability and maintainability. To protect ourselves, an organization, or even a nation, it is, therefore, crucial to maintain an overview of available technologies and innovations that have the potential to fill gaps or improve current solutions. The National strategy for the protection of Switzerland against cyber risks 2018–2022[1] has, therefore, as its first measure the "early identification of trends and technologies and knowledge building." This book is a significant contribution toward our national strategy—and beyond. Today's and future information and industrial control systems often face data protection challenges that still need to be met satisfactorily. For example, a significant enabler in e-commerce is machine learning, which can enable better customer experiences through targeted recommendations. At the same time, the combination of data to extrapolate knowledge about customer preferences and requirements might allow profiling beyond reason. Further, accumulating data in a data lake benefits machine learning but, without proper protection, gives access to data beyond what a single entity would need. Challenges like these can be met using technologies such as, for example, searchable symmetric encryption revealing a subset of data that the person or algorithm searching is allowed to see without revealing the entire dataset. In this book, the authors introduce encryption fundamentals, discuss critical technologies for data protection, and present specific use cases. This makes the book

[1] National strategy for the protection of Switzerland against cyber risks (NCS) 2018–2022.

a valuable guide for decision-making within the Swiss Federal administration and administrations of other nations. Nevertheless, limiting the view on governments only would not do the book justice. This book will also serve the industry well. While its primary audience will be Chief Information Security Officers (CISO) and Chief Technology Officers (CTO), it will also be interesting for the tech-savvy board members or engineers looking to get an entry point into data protection topics. Last but not least, the book will be interesting for anyone interested in data protection and encryption. I am happy that this significant contribution by the Cyber-Defence Campus toward our strategic goals has been made available for everyone – as true resilience against cyber threats requires all of us to properly understand protective technology and its applicability to today's challenges.

Bern, Switzerland
February 2023

Florian Schütz
Federal Cyber Security Delegate

Preface

Militaries and governments have long used encryption technologies to facilitate secret communication. However, today, encryption technologies are equally crucial in protecting our economy and civil society. Moreover, encryption technologies are critical enablers of the ongoing transformation in the digital economy and online society. For example, encryption technologies are widely used to secure financial transactions over blockchains, authenticate users, or secure cloud and personal computing environments.

The present study was conducted in Switzerland in 2022 to provide an overview of the changing landscape of encryption and data protection technologies and their global usage trends. The Swiss Confederation tasked the Cyber-Defence Campus to identify the 38 most relevant encryption and data protection technologies, analyze their expected evolution until 2025, and derive implications for the military, civil society, and economy sectors.

Fifty experts from academia, the government, and the industry have contributed to this study and provided their viewpoints on the different technologies and trends. This comprehensive collection of factsheets provides a reference for organizations and individuals that need to elaborate coherent and efficient data protection and encryption strategies in the coming years. The 38 technologies have been sorted into 5 categories. First, encryption foundations represent the technologies used to create other encryption applications. Second, low-level applications represent the technologies that focus on micro functionalities. Third, high-level applications represent the technologies that focus on more abstract and macro functionalities. Fourth, data protection represents the technologies used to protect data without encrypting these data. Finally, use cases represent concrete ways the different technologies can be used together to create a working solution.

Each factsheet contains an introduction of the technology, a trend analysis, the consequences for Switzerland, and a conclusion. At the end of the book,

we compare the trends of the different technologies using a scientometric and Wikipedia pageview analysis as well as data from open source code collected from GitHub.

We wish you a pleasant and insightful read.

Thun, Switzerland
November 2022

Valentin Mulder
Alain Mermoud
Vincent Lenders
Bernhard Tellenbach

Acknowledgements

This book is the result of a study conducted during the year 2022 for the National Cyber Security Centre (NCSC) by the Cyber-Defence Campus of armasuisse Science and Technology (S+T). In this respect, this book contributes to measure 1 (Technology Monitoring) of the National strategy for the protection of Switzerland against cyber risks (NCS) 2018–2022. In this sense, this publication can be considered as co-branding success.

Contents

List of Contributors

Authors		
Name	Affiliation	Chapter(s)
Thomas Lugrin	Swiss Confederation, Bern, Switzerland	One-time Pad, Symmetric Cryptography, Asymmetric Encryption, Hash Functions, and Random Number Generator
François Weissbaum	Swiss Confederation, Bern, Switzerland	Symmetric Cryptography
Christian Stohrer	Swiss Confederation, Bern, Switzerland	Asymmetric Encryption
Cyrill Krähenbühl	Swiss Federal Institute of Technology in Zurich, Zurich, Switzerland	Key Management, and Searchable Symmetric Encryption
Adrian Perrig	Swiss Federal Institute of Technology in Zurich, Zurich, Switzerland	Key Management, and Searchable Symmetric Encryption
Urs Wagner	Swiss Confederation, Bern, Switzerland	Hash Functions
Imad Aad	EPFL, Lausanne, Switzerland	Zero-knowledge Proof, and Disk, File and Database Encryption
Jean-Pierre Hubaux	EPFL, Lausanne, Switzerland	Homomorphic Encryption, and Blockchain
Jasper Rödiger	Rohde und Schwarz, Cologne, Germany	Quantum Key Distribution
Linus Gasser	EPFL, Lausanne, Switzerland	Post-quantum Cryptography, Blockchain, Disk, File and Database Encryption, and WEB3

Romain Gay	IBM Switzerland, Zurich, Switzerland	Functional Encryption
Bernhard Tellenbach	Cyber-Defence Campus, Thun, Switzerland	Identity-based Cryptography, and Secure Operating System
Christian Cachin	University of Bern, Bern, Switzerland	Multi-party Threshold Cryptography
Weyde Lin	Eraneos Switzerland AG, Zurich, Switzerland	Digital Signature, Biometrics, Tunneling and VPN, and 5G
Maria Sommerhalder	Eraneos Switzerland AG, Zurich, Switzerland	Hardware Security Module, Trusted Execution Environment
Louis-Henri Merino	EPFL, Lausanne, Switzerland	Secure Multi-Party Computation, and Electronic Voting
José Cabrero-Holgueras	European Organization for Nuclear Research, Geneva, Switzerland	Secure Multi-Party Computation
Yacine Felk	CYSEC, Lausanne, Switzerland	Confidential Computing
Dina Mahmoud	EPFL, Lausanne, Switzerland	Hardware Acceleration
Llorenç Romá	Cyber-Defence Campus, Thun, Switzerland	Secure Operating System
Sophia Ding	Eraneos Switzerland AG, Zurich, Switzerland	Biometrics, Digital Rights Management, and Secure Payment
Emilia Nunes	Eraneos Switzerland AG, Zurich, Switzerland	Biometrics, Email Security, Secure Messaging
Pascal Bettendorff	Eraneos Switzerland AG, Zurich, Switzerland	Biometrics
Roland Meier	Cyber-Defence Campus, Thun, Switzerland	Data in Transit Security
Valentin Mulder	Cyber-Defence Campus, Thun, Switzerland	Differential Privacy
Mathias Humbert	University of Lausanne, Lausanne, Switzerland	Differential Privacy
Belinda Müller	Eraneos Switzerland AG, Zurich, Switzerland	Authentication
Touradj Ebrahimi	EPFL, Lausanne, Switzerland	Secure Media
Martin Strohmeier	Cyber-Defence Campus, Thun, Switzerland	Secure Positioning and Localization
Yann Donon	RUAG, Emmen, Switzerland	Secure Smartphone
Fabien Künzler	RUAG, Emmen, Switzerland	Secure Smartphone
Pawel Jasinski	RUAG, Emmen, Switzerland	Secure Smartphone
Carl Piening	RUAG, Emmen, Switzerland	Secure Smartphone

Arnaud Savary	RUAG, Emmen, Switzerland	Secure Smartphone
Alexander Glavackij	Cyber-Defence Campus, Thun, Switzerland	Scientometric and Wikipedia Pageview Analysis
Sarah Ismail	Cyber-Defence Campus, Thun, Switzerland	Scientometric and Wikipedia Pageview Analysis
Percia David Dimitri	HES-SO Valais-Wallis, Sion, Switzerland	Scientometric and Wikipedia Pageview Analysis
Lucía Gómez Teijeiro	University of Geneva, Geneva, Switzerland	Trends in Open Source Software for Data Protection and Encryption Technologies
Thomas Maillart	University of Geneva, Geneva, Switzerland	Trends in Open Source Software for Data Protection and Encryption Technologies

Reviewers		
Name	Affiliation	Chapter(s)
Joachim Rosenthal	University of Zurich, Zurich, Switzerland	Post-quantum Cryptography
Stefan Röhrich	Rohde und Schwarz, Cologne, Germany	Post-quantum Cryptography, Disk, File and Database Encryption, and Tunneling and VPN
Katerina Mitrokotsa	University of St. Gallen, St. Gallen, Switzerland	Multi-party Threshold Cryptography
Kévin Huguenin	University of Lausanne, Lausanne, Switzerland	Differential Privacy
Nikos Karapanos	Futurae, Zurich, Switzerland	Authentication, and Biometrics
William Blonay	Cyber-Defence Campus, Thun, Switzerland	5G
Loic Maréchal	University of Lausanne, Lausanne, Switzerland	Scientometric and Wikipedia Pageview Analysis
Andrei Kucharavy	HES-SO Valais-Wallis, Sion, Switzerland	Scientometric and Wikipedia Pageview Analysis

Part I
Encryption Foundations

Chapter 1
One-Time Pad

Thomas Lugrin

1.1 Introduction

The one-time pad is a simple cipher. It ensures a perfect form of confidentiality known as *perfect secrecy* by combining a plaintext and a key of the same length with the exclusive-or (XOR) operator to produce a ciphertext. However, it lacks basic security properties shared by standard ciphers, namely authentication, and integrity. The central issue of the critical exchange between communication partners must be solved by other means. Some modern stream ciphers derive from the one-time pad in that they simulate its mechanism.

1.2 Analysis

The invention of the one-time pad can be attributed to Gilbert S. Vernam, who developed an automated system for teletypewriters using punched paper tapes in 1917 [1]. Together with Joseph O. Mauborgne, he realized that if the keystream, i.e. the distribution of the punches on the tape, was uniformly random and independent such as an infinite non-periodic tape, the cipher would be unbreakable. An earlier mention of the one-time pad can be found in an 1882 publication by Frank Miller [2] and could have been a source of inspiration for Vernam [3]. A famous implementation of the one-time pad is the hotline between the United States and the USSR that was established in 1963 [4].

T. Lugrin (✉)
Federal Administration, Bern, Switzerland
e-mail: thomas.lugrin@vtg.admin.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_1

1.2.1 Definition

The one-time pad takes a plaintext message and a random key of the same length as inputs. The message and key are represented in bits in a modern setup. Encryption consists of adding the message to the key using the XOR operator. The result is the ciphertext. The one-time pad decryption process is similar, as the ciphertext is XOR-ed with the same key to recover the plaintext. The simplicity of the encryption and decryption process makes it a very fast cipher, but the length of the key makes it difficult to use in practice.

In 1949, Claude E. Shannon formally showed that the one-time pad has *perfect secrecy* in an information-theoretic sense [5]. Any ciphertext of a given length can be the encryption of any plaintext of the same length with equal probability. Moreover, adversaries with arbitrarily considerable computing power cannot break it, which means it is also quantum-computer resistant.

The one-time pad is, however, not perfect in a broader sense, as it does not provide authentication of the sender, nor does it ensure the integrity of the ciphertext; a malicious intermediary can modify the ciphertext without any of the communicating parties noticing it. Even worse, if parts of the plaintext are known, as is typical in e-mail headers, the corresponding ciphertext parts can be altered to yield precisely any malicious plaintext of the same length. Re-using the key completely breaks the one-time pad security: XOR-ing two ciphertexts gives the XOR-ed plaintexts. If there is enough redundancy in text encoding, e.g., ASCII, one can recover the two plaintexts. More generally, this means that the keystream used by the one-time pad must be free of any dependence patterns, i.e., it must be truly random, see Chap. 7.

1.2.2 Trends

The concept of the one-time pad offers an excellent pedagogical introduction to modern ciphers. However, in practice, its usage is rare and limited to circumstances where perfect secrecy is of utmost importance and integrity and authenticity can be guaranteed by other means.

Most current stream ciphers are simulations of the one-time pad: a random seed, e.g., a 256-bit sequence, is first defined, from which a deterministic pseudo-random keystream is then generated.

1.3 Consequences for Switzerland

The one-time pad should generally not be used, and standardized symmetric encryption algorithms should be preferred and used with the appropriate parameters

and the correct implementation, see Chap. 2. Its usage is costly, and its setup is complicated. Nevertheless, its use could be envisaged in particular government applications where perfect secrecy is a must. The key exchange shall be performed reliably, the keys securely stored until their use and systematically destroyed after encryption. Further measures are required to guarantee the communicating parties' authenticity and the encrypted messages' integrity.

The development of Quantum Key Distribution (QKD, see Chap. 9) renewed interest in the one-time pad [6], as keys could be shared on an interception-aware channel. In practice, however, attacks exist that take advantage of the redundancy of the signal [7], meaning that the one-time pad using QKD would not guarantee perfect secrecy.

1.3.1 Implementation Possibilities

A critical aspect in the application of the one-time pad is the quality of the source of randomness used to feed the keystream. It should be investigated and verified before use. The correctness of its implementation should be verifiable. In particular, the same key should never be re-used. The reliability of the key exchange mechanism should undergo a thorough investigation, and authenticity and integrity should be guaranteed to hold using different mechanisms.

The length of the key is a hindrance to using the one-time pad; if a secure channel exists to communicate a key of the same length as the message to be sent, this same channel could also serve to send that same message. Nevertheless, in the standard one-time pad setup, the secret key exchange would typically happen before the exchange of the message, thus providing a shift of secrecy through time. The one-time pad offers, however, neither authentication nor integrity.

The properties of the one-time pad make it hardly usable in practice, except in particular circumstances, typically in the government, and must be complemented by authentication procedures and integrity protocols.

1.4 Conclusion

The one-time pad is interesting from a theoretical point of view, but it could be more complex and questionable to use in practice. It is very appealing because of its perfect secrecy property. However, it lacks basic security properties shared by standard ciphers, namely authentication, and integrity. It needs to solve the central issue of the critical exchange between communication partners. Some secure stream ciphers simulations of the one-time pad should be preferred.

References

1. D. Kahn. *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. Scribner, New York, 2nd edition, 1996.
2. F. Miller. *Telegraphic Code to Insure Privacy and Secrecy in the Transmission of Telegrams*. Charles M. Cornwell, New York, 1882.
3. Steven M. Bellovin. Frank Miller: Inventor of the one-time pad. *Cryptologia*, 35:203–2222, 2011.
4. Mariusz Borowski and Marek Leśniewicz. Modern usage of "old" one-time pad. In *Military Communications and Information Systems Conference (MCC)*, pages 1–5. IEEE, 2012.
5. C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28:656–715, 1949.
6. C. H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of International Conference on Computers, Systems and Signal Processing*, pages 175–179, Bangalore, 1984.
7. Miloslav Dušek, Ondřej Haderkaab, and Martin Hendrych. Generalized beam-splitting attack in quantum cryptography with dim coherent state. *Optics Communication*, 169:103–108, 1999.

Chapter 2
Symmetric Cryptography

François Weissbaum and Thomas Lugrin

2.1 Introduction

To guarantee the confidentiality of a message or information, different encryption methods are used. In almost all applications, data is encrypted symmetrically. In most cases, it is advised to encrypt data using symmetric methods. The key length for symmetric encryption must be at least 256 bits to guarantee a sufficient level of protection against the possible arrival of quantum computers. The use of standard methods such as AES with 256 bits should be promoted.

2.2 Analysis

Different encryption methods can be used to guarantee the confidentiality of a message or information. Symmetric encryption is the most common method, for example, for file encryption, messaging and data transfer, as it is fast and secure, provided the length of the encryption key is large enough. The encryption key is exchanged through a secure channel or asymmetric encryption methods.

2.2.1 Definition

Encryption is a cryptographic process that makes it impossible to gain knowledge of plaintext for anyone who does not have the decryption key. Encryption is called

F. Weissbaum · T. Lugrin (✉)
Federal Administration, Bern, Switzerland
e-mail: thomas.lugrin@vtg.admin.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_2

symmetric when it uses the same key for encryption and decryption. See Chap. 3 for details on asymmetric cryptography.

Symmetric ciphers are generally grouped into two sub-categories: stream and block ciphers. Stream ciphers generate a continuous keystream and combine it bit by bit with the plaintext to produce the ciphertext, typically using the exclusive-or (XOR) operator; block ciphers divide the plaintext into fixed-size sequences of bits called blocks, potentially applying some padding. They then run the same encryption procedure on each block. Various procedures have been standardized, also known as *modes of operation* [1, 2]. In order to ensure a good level of security, each block should have a length of at least 128 bits. The distinction between the two cipher types is loose since block ciphers applied to 1-bit blocks are essentially stream ciphers. Block ciphers operating in counter mode (CTR) provide a good example, where a block-counter appended to a fixed random nonce is encrypted, *de facto* providing a keystream, which is then XOR-ed with the blocks of plaintext. The output feedback mode (OFB) is another example with a similar structure.

It is essential to verify that an encrypted message has not been modified during its transport. This is why the authenticity—or at least the integrity—of the encrypted message should be verified before decrypting it. This requirement can be satisfied by using, e.g., Authenticated Encryption or Authenticated Encryption with Associated Data (AEAD) [3, 4], which ensure data confidentiality as well as authenticity.

2.2.2 Trends

It is advised to encrypt data using symmetric methods in the future. However, the required key length for symmetric encryption must be at least 256 bits to guarantee a sufficient level of protection against brute force attacks and the possible arrival of quantum computers. Therefore, standard methods such as AES [5] with 256 bits should be promoted.

When symmetric encryption is used, it is recommended to complement it with methods that guarantee the encrypted message's authenticity—or at least integrity.

2.3 Consequences for Switzerland

Switzerland should continue to use symmetric encryption methods with an appropriate level of security, as detailed in Sect. 2.2.2.

2.3.1 Implementation Possibilities

In general, one should not develop symmetric encryption algorithms on one's own, as the standard methods are secure and efficient. Instead, well-established cryptographic libraries that implement those standard algorithms should be preferred over homemade implementations. Moreover, when buying a product, one should check that its parameter setup corresponds to symmetric security of at least 256 bits, e.g., standard symmetric encryption algorithms such as AES [5] with 256 bits. The AES Algorithm is also known as Rijndael's Algorithm. The four other algorithms (Serpent, Twofish, RC6, and MARS) that were selected for the final round of the competition conducted by NIST in 2001 [6] can also be used in addition to the standard AES.

2.4 Conclusion

Over the last decades, the use of methods guaranteeing the confidentiality of a message has exploded, and symmetrical methods have been proven secure in this domain. If the proper implementations and parameters are used, these algorithms will remain secure even with the arrival of the quantum computer—see, for example, Section 2.5 of [7]. Therefore, the choice of secure algorithms and the size of the parameters proposed in this document is expected to stay the same over the next decade.

References

1. Morris J. Dworkin. Recommendation for Block Cipher Modes of Operation: Methods and Techniques. Technical Report SP 800-38A, National Institute of Standards and Technology, December 2001.
2. Morris J. Dworkin. Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode. Technical Report SP 800-38A Addendum, National Institute of Standards and Technology, October 2010.
3. Mihir Bellare, Phillip Rogaway, and David Wagner. The EAX mode of operation. In *International Workshop on Fast Software Encryption*, pages 389–407. Springer, 2004.
4. Morris J. Dworkin. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. Technical Report SP 800-38D, National Institute of Standards and Technology, November 2007.
5. Morris J. Dworkin, Elaine B. Barker, James R. Nechvatal, James Foti, Lawrence E. Bassham, E. Roback, and James F. Dray Jr. Advanced Encryption Standard (AES). Technical report, National Institute of Standards and Technology, November 2001.
6. James Nechvatal, Elaine Barker, Donna Dodson, Morris J. Dworkin, James Foti, and Edward Roback. Status report on the first round of the development of the advanced encryption standard. *Journal of Research of the National Institute of Standards and Technology*, 104(5):435, September 1999.

7. European Telecommunications Satandards Institute. Quantum Safe Cryptography and Security - An introduction, benefits, enablers and challenges. https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf, 2015.

Chapter 3
Asymmetric Encryption

Christian Stohrer and Thomas Lugrin

3.1 Introduction

While symmetric encryption uses the same key to encrypt and decrypt data, public key cryptography uses a pair of keys. One of these keys is used for encryption and the other one for decryption. For the security of the public key cryptosystem, only the decryption key must be kept secret. For this reason, it is often referred to as the private key. On the other hand, the encryption key, or public key, can be made publicly available without harming the security of the cryptosystem.

3.2 Analysis

For a public key cryptosystem to be secure, it must be computationally infeasible to compute the private key from the public key [1]. As the processes for encryption and decryption differ from each other and rely on different keys, another name for public key encryption is asymmetric encryption.

Generally, one does not use public key cryptography to encrypt large amounts of data directly, as this is generally computationally more expensive than symmetric encryption. However, it is common to use public key cryptography to encrypt and securely exchange keys of symmetric encryption schemes (see Chap. 2). The symmetric keys are then used for bulk data encryption [1, 2]. This combination of public key cryptography and symmetric encryption is called hybrid encryption.

C. Stohrer · T. Lugrin (✉)
Federal Administration, Bern, Switzerland
e-mail: thomas.lugrin@vtg.admin.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_3

To ensure that only the intended recipient can decrypt a cipher text, the public key must be authenticated through other means, e.g., a Public Key Infrastructure (PKI) [3]. For more information on key management, see Chap. 4.

Asymmetric encryption is not the only application for public key cryptography. Digital signatures, see Chap. 15, used to verify the authenticity of a document, are another important example. Another application is homomorphic encryption, see Chap. 8.

3.2.1 Definition

An asymmetric encryption scheme uses two different keys, a private one and a public one. While the public key is used for encryption and may be known by others, the private key is used for decryption and must be kept secret. Like most public cryptosystems, asymmetric encryption relies on one-way mathematical functions. This means that while it is easy to compute the result from given input data, it is hard to recover the input data from the result. Moreover, the corresponding mathematical problems are conjectured to be hard, such that it is computationally infeasible to decrypt a message without knowing the private key.

3.2.2 Trends

The widespread public critical systems are based on the integer factorization problem or the discrete logarithm problem over finite fields and elliptic curves. In a seminal paper, Peter W. Shor showed that it is possible to solve these problems efficiently using a sufficiently powerful quantum computer [4]. This triggered the search for replacement schemes. Several standardization agencies are now evaluating new proposals for this. In 2022, NIST announced the winners of their corresponding competition. For further details, we refer to Chap. 10 dedicated to post-quantum cryptography.

3.3 Consequences for Switzerland

The advent of the quantum computer threatens public key cryptosystems considered secure today. A strategy should therefore be developed that considers the implications of this threat on the security of current systems and proposes appropriate measures to ensure the preservation of security.

3.3.1 Implementation Possibilities: Make or Buy

Generally, one should not develop proprietary public cryptosystems, as the standardized algorithms have been thoroughly tested and deeply analyzed. Furthermore, any proprietary design will likely fail and expose weaknesses that may corrupt the entire system's security. Therefore, when procuring products involving public key cryptography, only those that have been standardized and verified for correctness by an appropriate specialized authority should be considered.

3.3.2 Variation and Recommendation

We recommend to continue using well-established public cryptosystems, e.g., RSA (Rivest-Shamir-Adleman cryptosystem [5]) with OAEP (Optimal Asymmetric Encryption Padding), Elgamal over a finite field, and Elgamal over appropriate elliptic curves. The minimal key length and the required size of the involved parameters should be chosen according to the current regulation or best practice advice. With today's knowledge, these algorithms are considered secure, although they are known to be vulnerable to future powerful quantum computers. Cryptosystems based on elliptic curves (ECC) can use shorter keys and are thus more efficient to achieve the same security level against attacks with classical, i.e., non-quantum computers. They should therefore be preferred over RSA and classical Elgamal. However, the above reasoning does not hold when considering attacks *against* a future large-scale quantum computer. In this scenario, one should not try to enhance security by using larger keys; one should instead use alternative quantum-safe cryptosystems, see Chap. 10.

In addition, one should follow the various standardization initiatives for new quantum-safe alternative public vital algorithms and integrate them accordingly to mitigate the threat posed by quantum computers. For this, a deep understanding of algorithms and a close inspection of possible solutions are necessary.

3.4 Conclusion

Asymmetric cryptography is a core part of many cryptographic applications. For example, it allows for encrypting messages, exchanging secret keys over an insecure channel, and establishing authenticity using digital signatures.

Current public cryptosystems are considered secure against classical computers (operating with bits), but the large majority of those commonly used today will be broken by attacks from not yet existing powerful quantum computers. Therefore, a corresponding strategy should be developed and implemented to counter this risk.

References

1. Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, Boca Raton, October 1996.
2. Wikipedia, Public-key cryptography. https://en.wikipedia.org/w/index.php?title=Public-key_cryptography&oldid=1099221204, July 2022.
3. Carlisle Adams and Steve Lloyd. *Understanding Public-Key Infrastructure*. Addison–Wesley Professional, Boston, 2nd edition, 2003.
4. Peter W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, 26(5):1484–1509, October 1997. arXiv:quant-ph/9508027.
5. R. L. Rivest, A. Shamir, and L. Adleman. a method for obtaining digital signatures and public-key cryptosystems. 21(2):120–126, feb 1978.

Chapter 4
Key Management

Cyrill Krähenbühl and Adrian Perrig

4.1 Introduction

Key management describes how cryptographic keys are created, securely stored, distributed to the respective key holders, and used in accordance with protocol specifications. It is thus a cornerstone of most cryptographic systems and must be handled with care. Advances in hardware security modules (HSM) used in key storage and high-end as well as low-cost random number generator used in key generation show a promising future for secure and affordable key management. However, future challenges, such as quantum resilience have to be overcome by new key management systems. For the military, existing experience in handling cryptographic keys could help in the development of a key management system, and the reputation of Switzerland could help promote key management systems developed in Switzerland.

4.2 Analysis

Key management comprises all steps in creating, storing, distributing, recovering, and using cryptographic keys. Key management is a vital part of any cryptographic system since the security guarantees often depend on correctly performed key management.

C. Krähenbühl (✉) · A. Perrig
Swiss Federal Institute of Technology, Zurich, Switzerland
e-mail: cyrill.kraehenbuehl@inf.ethz.ch; adrian.perrig@inf.ethz.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_4

4.2.1 Definition

Key management can be split into four stages: creation, storage, distribution, and usage of keys.

4.2.1.1 Key Creation

Key creation typically consists of deriving a cryptographic key from a source of randomness. In the case of the public-key cryptosystem RSA, key generation creates large prime numbers by randomly choosing large numbers until the number is prime. For the elliptic curve cryptosystem Ed25519 and symmetric cipher AES see Chap. 2, the private keys are randomly drawn 256 or 128 bit numbers. Apart from common pitfalls, such as improper use of key derivation functions, the most crucial property of key creation is a good source of randomness (see Chap. 7) with sufficient entropy [1].

4.2.1.2 Key Storage

Once keys are generated, they must be stored securely. Hardware security modules (HSM) are commonly used to protect the confidentiality of keys (see Chap. 16). This is essential, especially in the case of key hierarchies, where one key can be used to generate or issue other keys, and a compromised key (especially the root key) would invalidate all security properties. While key creation and storage are difficult to implement correctly, there are widely accepted solutions, such as hardware random number generators (HRNG) and HSMs from well-established vendors.

4.2.1.3 Key Distribution

Key distribution is typically the most challenging part of key management, as multiple systems must correctly interact over potentially insecure channels. Key distribution works differently depending on the type of keys. Symmetric keys are typically pre-shared out-of-band, for example, by storing them in physical smart cards or distributing them via a trusted channel, such as a secure connection over the Internet. Asymmetric keys can be pre-shared or generated by the user and authorized through delegation via digital certificates, including the corresponding public key. This public key infrastructure (PKI) approach is widely used to authenticate web traffic through the web PKI, domain names through the DNS PKI (DNSSEC), and network resources through the resource PKI (RPKI). Delegation in a PKI typically involves proof of the ownership of a resource, such as domain names or IP prefix ranges. A challenge in key distribution is the revocation of keys that are no

longer valid, for example, because the key was compromised or the resource owner changed.

4.2.1.4 Key Usage

Once keys are distributed to the respective users, keys must be used according to the protocol specifications. Depending on the protocol, keys can be reused without implications, or key reuse can potentially compromise the security properties of the protocol. Therefore, a protocol must define policies, for example, whether the key is stored in memory or on a trusted platform module (TPM), how often a key is replaced (key rollover), or for which operation a key can be used.

4.2.2 Trends

Regarding key creation, hardware components such as HRNGs are becoming more accessible. Specialized HRNG, for example, optical quantum random number generators, can generate randomness at high bandwidth [2], while low-cost HRNGs, for example, based on timing jitter in Field Programmable Gate Arrays (FPGAs), can generate randomness at reasonable rates while only consuming limited resources [3]. The cost of hardware security modules for storing keys varies significantly depending on their security guarantees and performance. However, with several competitors in this market (including Swiss HSM producers [4]), the cost may continue to decrease over time. In addition, recent advances in verifying the correct operation of HSMs show a promising trend for the security of HSMs [5].

Apart from HSMs, key management systems geared towards personal use, for example, based on smart cards distributed to citizens or on capabilities of ubiquitous devices, such as smartphones, can be envisioned in the future to provide digital identities for Swiss citizens.

There are several improvements in the field of public key infrastructures. Free certificates are issued by certificate authorities such as Let's Encrypt through automatic certificate issuance, which increases the coverage of the web PKI [6]. After a relatively slow adoption in the first few years since its inception in 2012, the deployment of RPKI protecting IP address resources has been steadily increasing over the last three years, reaching 40% coverage today [7]. In addition to the increasing adoption of existing PKI systems, we observe advances in solving the problems of revocation [8], lack of flexibility of relying parties [9], and efficient distribution of symmetric keys [10].

4.3 Consequences for Switzerland

For the military, secure key management is essential to maintain autonomy and protect against foreign and domestic adversaries. Single entities that can impact the operation or security of the key management system are potential threats that must be assessed carefully. An example of such an entity is a kill switch that can shut down a large portion of the (Internet) communication [11]. In the commercial sector, depending on the sensitivity of data, separate key management systems are already in use today, as shown by the SCION-based secure swiss finance network (SSFN), which provides high availability and security for communication between Swiss banks.

4.3.1 Implementation Possibilities: Make or Buy

For the military, buying a key management system or developing a custom one represents a fundamental choice. The main reason for developing a system is that in the military, there is a large amount of knowledge and experience in key management on various aspects, such as key storage and distribution. On the other hand, purchasing a standard key management protocol from a trusted vendor might facilitate collaboration with foreign entities while not absorbing the limited development resources of the military.

Civil society and businesses need more incentives to develop their key management system due to the lack of know-how and high cost. The exception could be a security-affine IT company using the reputation of Switzerland as a "safe" country to market the developed product (see Securosys [4]). For both sectors, buying is the natural choice as it allows for easier interoperability with other organizations, typically at a lower cost (Table 4.1).

4.3.2 Variations and Recommendation

The adversary model is an important aspect to consider when investing in a key management system. For example, the system may need to provide quantum resilience to remain confidential for an extended period, or it may be sufficient to consider state-of-the-art adversaries. For the former, a hybrid approach combining symmetric and asymmetric keys, such as TLS hybrid key exchange [12], can be a good solution. Such an approach benefits from the quantum resilience of symmetric cryptosystems [13] and the valuable properties of public-key cryptosystems.

Table 4.1 Implementation possibilities for different sectors

	Make		Buy	
	Pros	Cons	Pros	Cons
Military	Ample existing experience and knowledge	None	Easier collaboration with foreign armed forces	Risk of backdoors that are difficult to detect
Civil Society	None	Costs and difficulty to get it right	Beneficial for compatibility between various organizations	None
Economy	Use global reputation of Switzerland as a safe country to market the key management product	Costs and difficulty to get it right	Many commercial key management systems available	Risk of backdoors that enable industrial espionage

4.4 Conclusion

There are well-established standards for key management, e.g., FIPS 140-3 [14] for hardware security modules or random number generators which provide a measurable quality for key management systems. Furthermore, although many commercial key management systems exist from reputable vendors, Swiss IT security companies can potentially enter the key management market by leveraging the trust placed in Switzerland as a safe country. Finally, recent research on PKI explores ways to have more flexible notions of trust without the reliance on globally trusted entities, solves the revocation problem, and efficiently provides symmetric keys between users.

References

1. Nadia Heninger, Zakir Durumeric, Eric Wustrow, and J. Alex Halderman. Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices. pages 205–220, 2012.
2. Ziyong Zheng, Yichen Zhang, Weinan Huang, Song Yu, and Hong Guo. 6 Gbps real-time optical quantum random number generator based on vacuum fluctuation. *Review of Scientific Instruments*, 90(4):043105, April 2019. Publisher: American Institute of Physics.
3. Gaoliang Ma, Huaguo Liang, Liang Yao, Zhengfeng Huang, Maoxiang Yi, Xiumin Xu, and Kai Zhou. A Low-Cost High-Efficiency True Random Number Generator on FPGAs. In *2018 IEEE 27th Asian Test Symposium (ATS)*, pages 54–58, October 2018. ISSN: 2377-5386.
4. Securosys SA. Securosys | Hardware Security Ready For the Challenges of Tomorrow. https://www.securosys.com/en/.

5. Anish Athalye, M Frans Kaashoek, and Nickolai Zeldovich. Verifying Hardware Security Modules with Information-Preserving Refinement. page 18.
6. Internet Security Research Group (ISRG). Let's Encrypt stats. https://letsencrypt.org/stats/, September 2022.
7. National Institute of Standards and Technology (NIST). NIST RPKI monitor. https://rpki-monitor.antd.nist.gov/, September 2022.
8. Trevor Smith, Luke Dickinson, and Kent Seamons. Let's Revoke: Scalable Global Certificate Revocation. In *Proceedings 2020 Network and Distributed System Security Symposium*, San Diego, CA, 2020. Internet Society.
9. Laurent Chuat, Cyrill Krähenbühl, Prateek Mittal, and Adrian Perrig. F-PKI: Enabling Innovation and Trust Flexibility in the HTTPS Public-Key Infrastructure. In *Proceedings 2022 Network and Distributed System Security Symposium*, San Diego, CA, USA, 2022. Internet Society.
10. Benjamin Rothenberger, Dominik Roos, Markus Legner, and Adrian Perrig. PISKES: Pragmatic Internet-Scale Key-Establishment System. In *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security*, ASIA CCS '20, pages 73–86, New York, NY, USA, October 2020. Association for Computing Machinery.
11. Benjamin Rothenberger, Daniele E. Asoni, David Barrera, and Adrian Perrig. Internet Kill Switches Demystified. In *Proceedings of the 10th European Workshop on Systems Security*, EuroSec'17, pages 1–6, New York, NY, USA, April 2017. Association for Computing Machinery.
12. Douglas Stebila, Scott Fluhrer, and Shay Gueron. Hybrid key exchange in tls 1.3. Internet-Draft draft-ietf-tls-hybrid-design-05, IETF Secretariat, August 2022.
13. Vasileios Mavroeidis, Kamer Vishi, Mateusz D., and Audun Jøsang. The impact of quantum computing on present cryptography. *International Journal of Advanced Computer Science and Applications*, 9(3), 2018.
14. National Institute of Standards and Technology. Security requirements for cryptographic modules. Technical Report NIST FIPS 140-3, National Institute of Standards and Technology, Gaithersburg, MD, April 2019.

Chapter 5
Hash Functions

Urs Wagner and Thomas Lugrin

5.1 Introduction

Hash functions are one-way functions that map arbitrary-length input to fixed-length output. Cryptographic hash functions enjoy additional properties, making them suitable for many cryptographic applications. Established hash functions are considered secure, and no significant development is expected in this area. Insecure hash functions should be discarded, and existing secure hash functions should be promoted and adequately used.

5.2 Analysis

Hash functions have a wide range of cryptographic applications, such as:

- Integrity check: Files having the same hash value are supposedly equal. Hence, an unchanged hash value indicates an unchanged file.
- Password storage: The hash value of a password does not reveal any information on the password. Hence, passwords should be stored suitably hashed on the server side.
- Signatures: In digital signatures, message hashes are signed rather than the whole message itself (see Chap. 15).
- MACs: By carefully combining a secret key with the input data, hash functions can be used to compute Message Authentication Codes (MACs) that guarantee the authenticity of the data, e.g., in HMACs [1].

U. Wagner · T. Lugrin (✉)
Federal Administration, Bern, Switzerland
e-mail: thomas.lugrin@vtg.admin.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_5

- Key derivation: Small changes in the input lead to a random-looking change in the output (diffusion property). That makes them useful in key derivation functions [2].

There exist standardized hash functions that are considered secure, i.e., they satisfy the required properties. We are unaware of a quantum algorithm that poses a general risk for standard hash functions. For example, the asymptotically quadratic speedup of Grover's quantum search algorithm [3] can be countered using hash functions of sufficient length.

5.2.1 Definition

Cryptographic hash functions are functions mapping input of arbitrary length to a fixed-size output and having some additional properties that can be formulated as hard problems [4] :

- Pre-image resistance: It is hard to find an input that maps to a given hash value.
- Second pre-image resistance: It is hard to find an input that maps to the same value as a given different input.
- Collision resistance: It is hard to find two input values that map to the same value.

Hash functions having these properties are considered secure and are suitable for a wide range of cryptographic applications. On the contrary, the hash function is considered broken as soon as one of the above three problems can be solved by brute force or significantly faster than by brute force.

5.2.2 Trends

The last competition to find and standardize a new Secure Hash Algorithm (SHA-3) ended in 2012 [5] with the winner's announcement, namely Keccak. However, both SHA-3 (FIPS PUB 202, [6]) and its predecessor SHA-2 (FIPS PUB 180-4, [7]) with a minimal length of 256 bits are considered secure (concerning the properties mentioned in Sect. 5.2.1) and we see no indication that this will change in the next few years. Furthermore, other hash functions are considered secure (e.g., BLAKE) [8]. We, therefore, consider a significant development in this area unlikely.

5.3 Consequences for Switzerland

Switzerland should continue to use and promote the use of cryptographically secure and standardized hash functions.

5.3.1 Implementation Possibilities

Standardized hash functions considered secure in Sect. 5.2.1 exist, and open-source implementations thereof can be used at no cost. There is hence no need for Switzerland to develop its hash functions.

The security properties required from hash functions depend on the intended purpose. For example, a collision attack on the used hash functions has catastrophic consequences when it is used in signature schemes (see [9] for an attack scenario), whereas this is not necessarily problematic when it is used in HMACs. Nevertheless, insecure hash functions should not be used anymore, independently of their area of application.

Numerous hash functions are considered secure concerning the properties mentioned in 5.2.1; their design and properties differ. For example, SHA-2 is vulnerable to length extension attacks, whereas SHA-3 is not [8]. This is why hash functions cannot be used interchangeably and should be chosen carefully depending on the intended purpose.

There exist a wide range of cryptographic applications that make use of hash functions. The US National Institute of Standards and Technology (NIST) publishes standards for hash functions (FIPS 180-4 in [7], FIPS 202 in [6]) as well as methods making use of hash functions (e.g., HMAC in FIPS 198-1, HKDF in SP 800-56A/B, digital signatures in FIPS 186-5).

5.4 Conclusion

Hash functions have been in use in cryptographic applications for a long time. There exist established hash functions, and their pitfalls are known and documented. The development in computing power, including Quantum Computers, is not expected to yield a general problem with hash functions in the foreseeable future. As a consequence, not much development in this area is expected. Insecure hash functions should be discarded and existing secure hash functions adequately used.

References

1. James M Turner. The Keyed-Hash Message Authentication Code (HMAC), 2008. Federal Inf. Process. Stds. (NIST FIPS), National Institute of Standards and Technology, Gaithersburg, MD.
2. Lily Chen. Recommendation for Key Derivation Using Pseudorandom Functions, 2022. Federal Inf. Process. Stds. (NIST FIPS), National Institute of Standards and Technology, Gaithersburg, MD.
3. Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219, 1996.
4. Bart Preneel. Cryptographic hash functions. *European Transactions on Telecommunications*, 5(4):431–448, 1994.

5. Crypto competitions: SHA-3: a secure hash algorithm. https://competitions.cr.yp.to/sha3.html, June 2022.
6. Morris J. Dworkin. Sha-3 standard: Permutation-based hash and extendable-output functions, August 2015. Federal Inf. Process. Stds. (NIST FIPS), National Institute of Standards and Technology, Gaithersburg, MD.
7. Quynh Dang. Secure Hash Standard (SHS). March 2012. Federal Inf. Process. Stds. (NIST FIPS), National Institute of Standards and Technology, Gaithersburg, MD.
8. Wikipedia, Hash function security summary. https://en.wikipedia.org/w/index.php?title=Hash_function_security_summary&oldid=1054598969, November 2021.
9. Marc Stevens, Arjen Lenstra, and Benne de Weger. Chosen-prefix collisions for MD5 and colliding X. 509 certificates for different identities. In M. Naor, editor, *Annual International Conference on the Theory and Applications of Cryptographic Techniques — EUROCRYPT 2007*, volume 4515, pages 1–22. Springer, 2007.

Chapter 6
Zero-Knowledge Proof

Imad Aad

6.1 Introduction

Zero-knowledge proofs (ZKPs) are techniques to verify claims without revealing the information itself. In this process, a "prover" shares proof of their claim with a "verifier," who then verifies the accuracy of the proof without learning any additional information. ZKPs can be either interactive, where multiple interactions are needed to reach near-certainty, or non-interactive, where the proof can be verified in a single shot. One example of a non-interactive ZKP is zkSNARK, which is succinct and efficient for storage cost and allows the result of a computation to be used as a statement. The key difference between interactive and non-interactive ZKPs is that the latter replaces the verifier's random challenges with a common reference value, allowing the proof to be transferred to third parties.

6.2 Analysis

A conventional verification paradigm typically involves a "verifier" and a "prover," where the former does not trust the latter prior to the verification process (for example, a user proving his age to a service provider). However, it is assumed that the user trusts that the service provider will not misuse the shared data, which often shows to be a flawed assumption (e.g. the service provider selling user data to third parties) [1–3]. With the massive proliferation of online services, and their providers tending to diversify their businesses and monetizing the data assets at hand, there is

I. Aad (✉)
EPFL, Lausanne, Switzerland
e-mail: imad.aad@epfl.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_6

a need to rethink the trust the user puts in the service provider (i.e., how much the prover trusts the verifier). Optimally, the prover should share the proof of his claim with the verifier without revealing any additional information (e.g., sharing proof of adulthood instead of the date of birth).

6.2.1 Definition

Conceived in 1985, Zero-Knowledge Proofs (ZKP) are techniques to verify claims regarding some given information without revealing the information itself. Various "basic" examples can be found in the literature [1, 4]:

- Alice needs to prove to Bob, who is color-blind, that two balls have different colors:
  Bob conceals whether he should swap the balls before showing them to Alice. Alice then tells whether they were swapped or not. After repeating the experiment several times, Bob can get almost sure whether Alice is telling the truth (i.e., the balls have different colors) without learning any extra information (e.g., the colors of the balls)
- Alice proves to Bob that she knows the code to open a hidden door connecting two tunnels without revealing the code itself:
  Bob instructs Alice on which tunnel to go out from outside the tunnels. Then, after repeating the experiment several times, Bob can get almost sure whether Alice knows the code of the door connecting the tunnels without learning the code itself.

Note that ZKPs do not prove things with certainty. Instead, the process is repeated as often as needed, eventually reaching near-certainty [2].

A ZKP method must satisfy three criteria [2]:

- Completeness: If the information provided by the prover is accurate, then a ZKP method must enable the verifier to verify that the prover is telling the truth.
- Soundness: If the information provided by the prover is false, then a ZKP method must allow the verifier to refute that the prover is telling the truth.
- Zero-knowledge: The method must reveal to the verifier nothing other than whether the prover is telling the truth.

Types of ZKPs: The "basic" examples described above are called "Interactive ZKPs". They share two common properties:

- Numerous interactions are needed between the prover and the verifier until the latter gets convinced.
- The proof cannot be transferred to third parties (e.g. by recording) who would not trust that the verifier did not coordinate his choices with the prover [4].

Non-interactive ZKPs also exist where the proof delivered by the prover can be verified in a single shot [5]. This type of ZKPs requires more computational power

than interactive ZKPs. Unlike interactive ZKPs, non-interactive ZKPs apply to large groups of verifiers since the proof can be transferred to third parties, which is a big advantage w.r.t. interactive ZKP solutions.

One non-interactive ZKP solution is called zkSNARK (zero-knowledge Succinct Non-interactive Argument of Knowledge) [4, 6, 7]. It has, besides zero-knowledge and non-interactiveness, the following properties:

- Succinct: Regardless of the problem size, the proof is 288 bytes, which is convenient for storage cost (e.g., on a blockchain)
- Argument (i.e., claim of the prover): The result of any execution of a computation can be used as a statement/argument.

In order to move from interactive to non-interactive, zkSNARK replaces the verifier's random challenges to the prover with a "common reference value," such as a random string commonly agreed upon and accessible to all. At the same time, no party influences the actual random choice. Based on the "common reference value," the prover simulates the challenges and constructs the proof. The verifier then re-runs the experiment for verification.

6.2.2 Trends

ZKPs are still in their early days. Open initiatives and standardization efforts involve industry, academia, and technical and non-technical specialists. The potential impact is well beyond 2025.

6.3 Consequences for Switzerland

6.3.1 Public Sector

ZKPs also bring promising research in "zero knowledge treaty verification". The most famous example is "nuclear warhead verification", where ZKPs can give information about the nuclear warheads without revealing closed secret designs. The details of "nuclear warhead verification" are based on the comparison of physical properties of objects (thus the term "physical ZKP") which is out of the scope of this article. However, this opens the door for a wide range of other applications in international treaties, controls, and mediations.

Being very active on the international level in treaties and mediations, Switzerland can benefit from ZKPs for specific checks without revealing additional secret information, which often hinders negotiations between opposing parties. Identifying the specific use cases and the corresponding ZKP solutions can be a potential collaboration between authorities and academia.

6.3.2 Private Sector

ZKP can have an impact in different areas:

- ZKPs could revolutionize the current web usage in favor of Web3 projects [8]. Web3 (see Chap. 34) is the new iteration of the World Wide Web where decentralization and blockchain technologies are vital factors, compared to Web 2.0, where content is centralized in a small group of big tech companies [9]. In addition, Web3 is argued to provide more data security, user privacy, and scalability. However, Web3 is another debatable question [9].
- SSI: in the context of electronic identities, Self-Sovereign IDs is a concept where the end-user is in control of what attributes (e.g the age) are shared and how (e.g. > 18, not the exact age nor date of birth), and where trust is decentralized. Many electronic identifiers and eWallets worldwide, including Switzerland, are planned to follow the SSI concept. Furthermore, one of the SSI principles is data minimization, which implicitly includes ZKPs where applicable. Therefore, we should expect to see ZKP increasingly used in specific use-cases [3].
- PETs: ZKPs can be seen as privacy-enhancing technologies (PETs) applicable to various use cases, as previously described. However, they require personnel with good knowledge of the technology and non-negligible overhead for implementing them. Therefore, the incentive for using ZKPs must be strong enough to overcome the overhead. In addition, it is still early to say which factors would push for their adoption: security consideration (e.g, No data breaches because no data have been shared), marketing/reputation, and regulations (e.g., GDPR, which requires data minimization).

Internationally, the adoption of PETs in the private sector is often slower than desired and used as a marketing argument: differential privacy at Google and Apple, end-to-end encryption in messaging applications. ZKPs can be expected to have similar adoptions.

In the Swiss market, a couple of enterprises offer privacy-based digital services. For instance, Threema for messaging and Proton for a broader range of services. With the emergence of eID and eWallets, we can expect a similar small adoption of ZKPs, in the use cases where they apply. Similarly, with the emergence of new ZKPs use-cases, we can expect more privacy-based services. However, the market share of these privacy-based services is relatively small, with occasional boosts due to data leaks and scandals. This trend is likely to remain the same.

6.3.3 Civil Society

Like with end-to-end encrypted messaging or privacy-preserving Covid tracing, PETs help increase the trustworthiness of the applications, the companies, or the governments collecting the data, which benefits the economy and administrative

efficiencies. ZKPs will play a similar role. However, as mentioned before, the market share of these privacy-based services is relatively small, with occasional boosts due to data leaks and scandals. This trend is likely to remain the same.

6.3.4 Implementation Possibilities: Make or Buy

There are different ZKPs for different use cases, and most of these are either being researched or open-source implementations. So far, Buying is not an option.

6.3.5 Variation and Recommendation

The most prominent implementation of ZKPs is Zcash for anonymous cryptocurrencies. However, there is a slight advantage for Switzerland to play a role there. However, the basic idea of ZKP, which is sharing the minimum necessary provable information without revealing anything else, can have high utility in the banking sector and in the mediation activities between conflicting parties, where Switzerland is well placed. Therefore, an interdisciplinary working group to investigate these potentials is worth establishing.

6.4 Conclusion

ZKPs are in their early stages, and research is still widening their application range and use cases.

For the industry (swiss or worldwide), this may bring new opportunities to:

- Using the (new) PET as a differentiation factor (like Threema and Proton do for messaging and email)
- Adopting ZKP where applicable, therefore improving the security of data sharing

For civil society, where ever ZKPs apply, this is an additional way to secure personal data, reducing the impacts of data breaches.

For the Swiss government and military, ZKPs may help improve controls and mediation between conflicting parties. Therefore it is recommended to investigate the potentials further here and keep observing the evolution of ZKPs.

References

1. Gwyneth Iredale. Example of A Good Zero Knowledge Proof, March 2021. 101 Blockchains.
2. 14 ZKP Clare Nelson. https://docs.google.com/presentation/d/19v3jjK0bMM_nYshblWbR8UBr0k8wNWSU2pGeQtM7Fn0, August 2022.
3. Vincent Tabora. Self-Sovereign Identity With Zero Knowledge Proof. https://medium.datadriveninvestor.com/self-sovereign-identity-with-zero-knowledge-proof-9a05f36f16da, December 2018. Medium.
4. Hasib Anwar. Zero Knowledge Proof: A Introductory Guide. https://101blockchains.com/zero-knowledge-proof/, November 2021. 101 Blockchains.
5. Zero-Knowledge Proof: How it Works, Use Cases & Applications. https://research.aimultiple.com/zero-knowledge-proofs/, August 2022.
6. Demonstrate how Zero-Knowledge Proofs work without using math. https://www.linkedin.com/pulse/demonstrate-how-zero-knowledge-proofs-work-without-using-chalkias, August 2022.
7. Introduction to zk-SNARKs (Part 1). https://blog.decentriq.com/zk-snarks-primer-part-one/, September 2018. Decentriq.
8. CoinYuppie. 2022 predictions: Zero-knowledge proofs (ZKPs) key to Web3 - CoinYuppie: Bitcoin, Ethereum, Metaverse, NFT, DAO, DeFi, Dogecoin, Crypto News. https://coinyuppie.com/2022-predictions-zero-knowledge-proofs-zkps-key-to-web3/, https://coinyuppie.com/2022-predictions-zero-knowledge-proofs-zkps-key-to-web3/, March 2022.
9. Wikipedia, Web3. https://en.wikipedia.org/w/index.php?title=Web3&oldid=1103656598, August 2022.

Chapter 7
Random Number Generator

Thomas Lugrin

7.1 Introduction

Most modern encryption and authentication methods rely on the generation of random numbers [1], such as for key generation, initial vectors, or nonces. Therefore, a reliable source of entropy is fundamental in making encryption and authentication methods secure—weak sources of randomness can compromise otherwise secure encryption and authentication schemes.

7.2 Analysis

7.2.1 Definition

A Random Number Generator (RNG) is cryptographically secure if the sequences of numbers that it generates are unpredictable (Section 3.3.1 of [2]). RNGs are typically grouped in two categories: Pseudo-Random Number Generators (PRNG) and True Random Number Generators (TRNG).

PRNGs depend on a seed value, from which a seemingly erratic albeit deterministic sequence is produced; it is a quick and debug-friendly version of RNGs often used in statistical applications. They are not suitable for cryptographic applications in isolation. However, they may be used when correctly combined (seeded) with a reliable entropy source.

T. Lugrin (✉)
Federal Administration, Bern, Switzerland
e-mail: thomas.lugrin@vtg.admin.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_7

TRNGs rely on physical phenomena, e.g., radioactive decay, thermal noise, small-scale hardware activity, or particular hardware based on quantum physics (abbreviated QRNG; see for example, Chapter 2 of [3]). As it is hard to balance physical processes such that the probability of 0's and 1's is exactly ½, the output of TRNGs must be adequately post-processed. Secure mixing functions such as hash functions or symmetric encryption schemes may produce unbiased output [4]. These mixing functions also remove serial dependence between bits. An excellent example of such an implementation is the Linux kernel RNG `/dev/urandom` [5].

Quantum RNGs are often presented as the only means to protect infrastructure against future powerful quantum computers. However, this is misleading, as any reliable source of randomness remains unpredictable against any adversary with arbitrary computing power.

7.2.2 Trends

Small-size, low-cost QRNGs have already been integrated into off-the-shelf devices such as smartphones, computers, and hardware security modules.

7.3 Consequences for Switzerland

People, businesses, and authorities in Switzerland should continue using and promoting research on secure random hardware number generators. This will ensure that they can benefit from the newest technological advances when they become available.

7.3.1 Implementation Possibilities: Make or Buy

Using secure RNGs that cannot be manipulated or tampered with and whose output is not predictable is fundamental as a basis for encryption methods. Applications involving particularly sensitive data can combine the output from two or more independent sources of randomness for improved security. PRNGs, which produce deterministic outcomes, must not be used in cryptography in isolation and must at least blend in TRNG's randomness.

Open-source solutions such as the Linux kernel RNG `/dev/urandom` are considered reliable [6]. Hardware products dedicated to producing randomness from reliable and reputable producers can be used as a complement after appropriate verification and approval.

Several companies are operating in the TRNG market, e.g., developing QRNG chips that can be integrated into hardware. A few companies selling QRNG chips

Table 7.1 Different companies active in the QRNG field

Company	Description	Technology	Country
ID Quantique	Technology pioneers, well established, integrated into a chip, promote cost-effectiveness.	Photonic (Optical)	Switzerland (Linked to South Korea through SK Telecom)
Quintessence Labs	Well established, fastest generators, not chip integrated	Barrier Tunneling.	Australia
RandomPower	Newcomers, growing, qualification and MVP in place, offers new technology. RUAG Switzerland ran tests on their products.	In-silico	Italy

or systems are listed in Table 7.1. These QRNG chips do not offer stronger guarantees than other TRNGs; they are just another means of potentially generating cryptographically secure randomness.

7.3.2 Variation and Recommendation

RNGs should be appropriately isolated and integrity protected to prevent tampering or access to internal states that could leak information about the random sequence. Combining the output of several RNGs (e.g., using XOR) can mitigate the potential weaknesses of individual RNGs.

The US National Institute of Standards and Technology (NIST) published a range of hypothesis tests [7] that can provide evidence of potentially complex dependence patterns. Its German equivalent (Bundesamt für Sicherheit in der Informationstechnik, BSI) also suggests a suite of tests [8]. These tests do not provide proof of randomness; they can, at best, reject the null hypothesis that a specific dependence pattern occurs in a sequence at a given confidence level. The longer the test sequence, the more confidence can be placed in the test results. A good understanding of the inner workings of a TRNG is key to assuring the unpredictability of its output.

7.4 Conclusion

A reliable source of randomness is critical to ensuring the security of most modern encryption and authentication systems. Unfortunately, pseudo-random number

generators are not suited in such a context, except if suitably combined with a reliable entropy source.

Proving that a source of bits is truly random is impossible on finite sequences, but statistical test suites exist that provide evidence against non-randomness. Good physical sources of entropy must be chained with robust post-processing techniques to remove biases and serial dependencies.

Standard tools like `/dev/urandom` on Linux systems provide a good source of random numbers based on multiple hardware-based entropy sources. Additional security can be achieved by combining independent RNGs, typically based on physical processes of different types, e.g., quantum physics.

References

1. Kinga Marton, Alin Suciu, and Iosif Ignat. Randomness in Digital Cryptography: A Survey. *Romanian Journal of Information Science and Technology*, 13:219–240, 2010.
2. Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography*. CRC Press, Boca Raton, 3rd edition, 2021.
3. David Johnston. *Random Number Generators—Principles and Practices: A Guide for Engineeers and Programmers*. Walter de Gruyter GmbH, Berlin/Boston, 2018.
4. Steve Crocker, Donald E. Eastlake 3rd, and Jeffrey I. Schiller. Randomness Recommendations for Security. Request for Comments RFC 1750, Internet Engineering Task Force, December 1994.
5. random(4) - Linux manual page. https://man7.org/linux/man-pages/man4/random.4.html, August 2022.
6. Stephan Müller. Documentation and Analysis of the Linux Random Number Generator. Technical report, Bundesamt für Sicherheit in der Informationstechnik, April 2020.
7. Andrew Rukhin, Juan Soto, James Nechvatal, Elaine Barker, Stefan Leigh, Mark Levenson, David Banks, Alan Heckert, and James Dray. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Technical report, National Institute of Standards and Technology, April 2010.
8. Wolfgang Killmann and Werner Schindler. A proposal for: Functionality classes for random number generators. Technical report, Bundesamt für Sicherheit in der Informationstechnik, September 2011.

Chapter 8
Homomorphic Encryption

Jean-Pierre Hubaux

8.1 Introduction

Homomorphic Encryption (HE) is a technique in cryptography that allows for performing operations on encrypted data. The encrypted result can then be decrypted to obtain the result of the operation, making it possible to perform computations on sensitive data without revealing it. However, with recent advancements and the increasing demand for data protection, HE is expected to become more relevant soon and be used in many industries. In Switzerland, IBM, Inpher, and Tune Insight are among the companies that have developed HE libraries and offer solutions for secure computation. These solutions can provide better protection and reduce the vulnerability of data entrusted to Swiss companies.

8.2 Definition and Analysis

In some application areas, performing operations (additions, multiplications, etc.) on the encrypted form of data is desirable. This is precisely what homomorphic encryption does. The encrypted result can then be decrypted to obtain the result of the operation. The obtained result will be the same as if the computation had been performed in cleartext. This technique makes it possible to ask a third party, such as a cloud service provider, to perform operations on data that it hosts on behalf of a customer, but without seeing this data.

J.-P. Hubaux (✉)
EPFL, Lausanne, Switzerland
e-mail: jean-pierre.hubaux@epfl.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_8

The basic idea is several decades old, and partial solutions were already proposed in the late twentieth century. In 2009, Craig Gentry proved that it was possible to operate under fully homomorphic encryption (FHE) to support any computation [1]. Since then, many improvements were made, notably to increase performance.

For sensitive data, such as healthcare information, homomorphic encryption can enable new services by removing privacy barriers inhibiting data sharing, or increasing the security of existing services. For example, due to medical data privacy concerns, predictive analytics in healthcare can be hard to apply via a third-party service provider. However, these privacy concerns are diminished if the predictive analytics service provider can operate on encrypted data instead. Moreover, even if the service provider's system is compromised, the data would remain secure [2].

For many years, homomorphic encryption has suffered from two significant weaknesses: Limitations on the nature of the computations that could be performed and high computational costs (and thus higher energy consumption and slower execution). The former has been addressed by the advent of the already mentioned FHE and the subsequent enhancements brought after that; polynomials of the appropriate degree can approximate non-polynomial functions. In addition, several software optimizations have mitigated the latter. Nevertheless, many additional improvements (several orders of magnitude) are expected by deploying specialized hardware accelerators that should become available by 2025.

8.2.1 Trends

Well-established cryptographic algorithms and security protocols provide vital data protection at rest and in transit. Homomorphic encryption fills the critical data gap in processing, a need that will become more relevant in the future. This trend will be fueled by an increasing demand for data protection (motivated notably by numerous and recent data leakage scandals, including in Switzerland), increased performance of the software libraries, remarkable progress on the front of fully homomorphic encryption, hardware accelerators, better development tools, and progress on standardization [3, 4].

In particular, homomorphic encryption can be competitive compared to hardware-based solutions (enclaves or Trusted Execution Environments as described in Chap. 18). Indeed, the latter suffer from (i) the need to trust a hardware vendor, (ii) side-channel attacks, and (iii) high costs when systems need to be retrofitted after the discovery of a vulnerability. However, the equivalent problems are less salient with HE. Indeed, (i) trusting a software vendor is easier to achieve because its code can be scrutinized; moreover, (ii) the absence of side-channel attacks can be demonstrated by mathematical proofs; finally, (iii) hardware accelerators are meant to be replaced only rarely.

8.3 Consequences for Switzerland

On the business side, considering how heavily Switzerland is involved in the service sector, including data-intense activities, it is expected that homomorphic encryption can be of high relevance. In particular, better protection can reduce the vulnerability of data entrusted to Swiss companies.

In Switzerland, the three main industry-level activities related to HE are as follows. In its Zurich Research Lab, IBM has developed an HE library called HElib. HElib is a free and open-source cross-platform software. It implements various forms of homomorphic encryption. It is based on the Brakerski-Gentry-Vaikuntanathan (BGV) fully homomorphic encryption scheme. It also includes several optimizations, such as Smart-Vercauteren ciphertext packing techniques. It is written in C++.

The US-Swiss company Inpher has developed an open-source HE library called TFHE [5]. It is written in C/C++ and based on the ring variant of the Gentry, Sahai, and Waters (GSW) cryptosystem. TFHE is distinct from the company's flagship product, XOR, a software product providing secure multi-party computation features. However, XOR and TFHE can be used jointly in some cases. The company is funded mainly by US banks and operates primarily in that sector, but it also invests in the health sector.

Finally, the EPFL spin-off Tune Insight SA that was founded in 2021 has developed a HE library called Lattigo, written in GoLang [6]. The library is based on the Cheon-Kim-Kim-Song (CKKS) crypto scheme and thus provides floating point operations and supports fast bootstrapping.

For cloud computing, homomorphic encryption can respond to the legal uncertainty generated by the Schrems II ruling of the European Court of Justice. Indeed, Schrems II has challenged the agreement that was previously set up between the US and EU authorities in terms of processing of data related to EU citizens by US companies [7]. Homomorphic encryption is a response to this concern because, with HE, Swiss-based users can use US-operated cloud services while retaining the exclusive knowledge of their decryption keys and, therefore, all their data.

For an overview of HE libraries (including those unrelated to Switzerland), the reader is referred to the Wikipedia article on HE [2]. For applications aiming at building intelligence out of siloed data, homomorphic encryption can be combined with secure multi-party computation (SMC) which is described in Chap. 17.

8.3.1 Implementation Possibilities: Make or Buy

As with cryptographic solutions in general, it is not recommended to develop proprietary HE implementations, but rather to rely on well-established and standardized solutions.

8.3.2 Variations and Recommendation

At the time of this writing (November 2022), HE is still in a maturation phase, and much more information can be found about the HE tools themselves than about real-world applications. Nevertheless, we briefly provide three real-world examples related to the three companies mentioned above with Swiss-based technical activities on HE.

Organizations can use IBM's HElib to scale their stream processing applications into the infrastructure-as-a-service clouds elastically. Moreover, the proposed solution not only elastically scales data stream processing applications into public clouds but also preserves the privacy of such applications [8].

Inpher's technical solutions, XOR and TFHE, can be used to support privacy-preserving techniques in financial services. More specifically, these tools can be instrumental in fighting financial crime such as money laundering and enable enforcement use cases [9].

Finally, armasuisse and Tune Insight SA are collaborating on sharing cybersecurity intelligence [10]. Tune Insight has already deployed its privacy-preserving distributed data analysis solution among several university hospitals.

8.4 Conclusion

Homomorphic encryption can be a transformative technology to reinforce digital trust. The availability of domestic research and solutions is a competitive advantage for Switzerland.

References

1. Craig Gentry. A fully homomorphic encryption scheme. *Stanford PhD thesis*, 2009.
2. Wikipedia, Homomorphic encryption. https://en.wikipedia.org/w/index.php?title=Homomorphic_encryption&oldid=1099292061, July 2022.
3. Homomorphic Encryption Standardization – An Open Industry / Government / Academic Consortium to Advance Secure Computation. https://homomorphicencryption.org/, August 2022.
4. Abbas Acar, Hidayet Aksu, Selcuk Uluagac, and Mauro Conti. A survey on homomorphic encryption schemes: Theory and implementation. *ACM Computing Surveys*, 2019.
5. TFHE Fast Fully Homomorphic Encryption over the Torus. https://tfhe.github.io/tfhe/, August 2022.
6. Lattigo: lattice-based multiparty homomorphic encryption library in Go. https://github.com/tuneinsight/lattigo, August 2022.
7. Mildebrath Hendrik. The CJEU judgment in the Schrems II case, September 2020.
8. Rodrigo Arosha, Dayarathna Miyuru, and Sanath Jayasena. Latency-aware secure elastic stream processing with homomorphic encryption. *Data Science and Engineering*, 2020.

9. Inpher's privacy-preserving cross-border analytics case study published in global ffis report. https://inpher.io/news/inphers-privacy-preserving-cross-border-analytics-case-study-published-in-global-ffis-report/.
10. Strengthening collective cyber resilience. https://www.ar.admin.ch/en/armasuisse-wissenschaft-und-technologie-w-t/cyber-defence_campus.detail.news.html/ar-internet/news-2022/news-w-t/staerkung-der-kollektiven-cyber-resilienz.html.

Chapter 9
Quantum Key Distribution

Jasper Rödiger

9.1 Introduction

A new class of computers, so-called quantum computers, will soon be able to crack common encryption algorithms. Quantum Key Distribution (QKD) is a promising solution to stay secure in the quantum computer age, which is progressively getting industrialized in recent years. Worldwide, point-to-point QKD links are combined into larger and larger testbed networks, which approach more commercially usable networks. Topics like certification and standardization have become increasingly important for QKD. Since Switzerland is strong in the field of QKD in terms of academia and industry, it has the opportunity to produce QKD technology within the country successfully.

9.2 Analysis

9.2.1 Definition

Quantum computers will soon thus endanger secure data traffic. Entirely new methods will therefore be needed to secure data transmission in the future. Nowadays, two leading families of cryptographic techniques are used to protect telecommunications. The first is symmetric encryption, see Chap. 2, such as AES, and the other is public-key cryptography, also known as asymmetric cryptography. The asymmetric cryptographic methods are often used to distribute the symmetric

J. Rödiger (✉)
Rohde und Schwarz, Cologne, Germany
e-mail: jasper.roediger@rohde-schwarz.com

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_9

keys needed for symmetric cryptographic methods to the communication partners. The sender and receiver each use different keys in these methods: a public key and a private key. With conventional computers, it takes much effort to deduce the private key from the public key and thus break the encryption. However, as soon as quantum computers with the necessary computing power are available, the Shor algorithm can calculate the private key quickly for many methods used today [1].

QKD uses the quantum states of individual photons, i.e., light particles, to send so-called qubits from one communication partner to the other and thus generate a symmetric and secure key [2]. This exploits the fact that individual photons cannot be copied due to the no-cloning theorem of quantum physics and that the measurement of photons leads to measurement errors due to the quantum mechanical uncertainty principle. By cleverly applying these laws and if an authenticated communication channel exists between the communication parties, they can gain an information-theoretic advantage over potential attackers. Furthermore, by suitable post-processing of the measured qubits, they can generate a sequence of coinciding bits only known to them, which they can then use as a key, e.g., in symmetric cryptography methods.

Since the quantum key exchange is based on physical laws and not on the complexity of specific mathematical problems, the keys generated in this way can be used securely regardless of the computing power of quantum or classical computers and are thus future-proof.

9.2.2 Trends

There are many different QKD protocols in existence, which, based on the above-described principles, use different degrees of freedom and state preparation and measurement mechanisms. The maturity of the implementation and theoretical assessment of the different QKD protocols are vastly different. Some implementations of those protocols are already quite mature, can be purchased as QKD solutions for point-to-point secure communication by different vendors, or are close to being purchasable. Worldwide, those point-to-point solutions are combined to testbed networks, which approach more commercially usable networks.

The largest of those QKD networks is the quantum backbone network built in China from 2013 to 2017, which spans over 2000 km of fiber between Beijing and Shanghai, including the satellite Micius offering satellite-based QKD links [3]. It is being expanded in 2017 to cover China by 2025. In the EU, since 2019, the EuroQCI initiative aims to build a secure quantum communication infrastructure (QCI) that will span the whole EU, including its overseas territories through fiber and satellite links [4]. All 27 EU member states have signed the EuroQCI declaration, committing themselves to the EuroQCI initiative. EuroQCI's goal is to have a fully operational QCI by 2027. The US company Battelle and the swiss company IDQuantique implemented a QKD network in the US in 2013 between

Columbus and Dublin in Ohio, namely the Battelle Quantum Network (BQN) [5]. It is their declared goal to extend the BQN to span 700 km.

Another sign that QKD is progressively getting industrialized can be observed by examining standardization endeavors. The most critical standardization organizations regarding QKD are ETSI and ITU. The first standardization activity was already started in 2008 by the ETSI by establishing the Industry Specification Group on QKD. Later, the ITU started in the realm of QKD and remained very active. Additionally, cybersecurity authorities, like, e.g., the German BSI or the French ANSSI, will play an essential role in the certification of QKD products [6]. However, governmental agencies still point out the lack of scalability [7] or even oppose its use for business-critical networks [8].

9.3 Consequences for Switzerland

Academically, Switzerland is one of the leading countries worldwide in the QKD [9]. This also affects the know-how transfer into the industry. One prominent example is the company IDQuantique, one of the first companies to bring QKD products to the market in 2004 and has remained an essential company in this area.

9.3.1 Implementation Possibilities: Make or Buy

Since there is already much know-how in Switzerland, both academically and in the private industry, Switzerland is in an excellent position to produce QKD technology within the country if QKD technology is further fostered. Due to the expected demand, the QKD market is currently massively growing. Therefore, it is reasonable to expect more QKD vendors to emerge, exploring the different possible technologies including continuous-variable (CV) and discrete-variable (DV) QKD modules. The best technologies may be depending on the exact use case (Table 9.1).

9.3.2 Variations and Recommendation

Since the QKD market is growing, Switzerland can keep its advantages in the field of QKD if the field is further supported [10].

Table 9.1 Implementations possibilities for different sectors

	Make		Buy	
	Pros	Cons	Pros	Cons
Military	Full control over development	The Market is still developing and changing	A lot of different vendors and technologies expect to emerge in the next five years	Less control over products
Civil Society	Switzerland is in a good position, academically and industry-wise	None	A lot of different vendors and technologies expect to emerge in the next five years	None
Economy	Switzerland is in a good position, academically and industry-wise	None	Switzerland is in a good position already	None

9.4 Conclusion

The QKD market is developing. Industrialization takes place in terms of publicly funded projects and private actors. Since Switzerland is vital in the field of QKD in terms of academia and industry, it has the opportunity to produce and export QKD technology. However, it is necessary to know that influential cybersecurity authorities do not recommend using this technology at a broader level as there are cheaper alternatives for the mass market.

References

1. Craig Gidney and Martin Ekerå. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum*, 5:433, April 2021. arXiv:1905.09749 [quant-ph].
2. S. Pirandola, S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, J. Shamsul Shaari, M. Tomamichel, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden. Advances in quantum cryptography. *Advances in Optics and Photonics*, 12(4):1012–1236, December 2020. Publisher: Optica Publishing Group.
3. *An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology*. RAND Corporation, 2022.

4. The European Quantum Communication Infrastructure (EuroQCI) Initiative | Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci.
5. Alex Morrow and Matthieu Legré. Battelle QKD Test Bed. In *2012 IEEE Conference on Technologies for Homeland Security (HST)*, Waltham, MA, USA, November 2012. IEEE.
6. Marius Loeffler, Christian Goroncy, Thomas Länger, Andreas Poppe, Alexander Neumann, Matthieu Legré, Imran Khan, Christopher Chunnilall, Diego López, Marco Lucamarini, Andrew Shields, Elisabetta Spigone, Martin Ward, and Vicente Martin. Current Standardisation Landscape and existing Gaps in the Area of Quantum Key Distribution. page 31.
7. Should Quantum Key Distribution be Used for Secure Communications? https://www.ssi.gouv.fr/publication/should-quantum-key-distribution-be-used-for-secure-communications/, November 2022. ANSSI.
8. Quantum security technologies. https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies, November.
9. Lutz Bornmann, Robin Haunschild, Thomas Scheidsteger, and Christoph Ettl. Quantum technology – a bibliometric analysis of a maturing research field, August 2019.
10. Cathal J. Mahon and SSC secretariat. White Paper: Quantentechnologie in der Schweiz, 2020.

Chapter 10
Post-quantum Cryptography

Linus Gasser

10.1 Introduction

The chapter about Post-quantum Cryptography discusses the need for a new generation of cryptography to protect against future quantum computers. These computers will likely reverse many of the one-way functions used in current asymmetric encryption methods, making encrypted data vulnerable. The US government advocates vigorously to implement post-quantum algorithms by 2035, as an enemy could decrypt encrypted data or messages copied today. Symmetric encryption is not significantly faster for quantum computers to break, but asymmetric encryption, which relies on one-way functions, is vulnerable. NIST started a Post-Quantum Cryptography (PQC) challenge in 2016, with four algorithms selected as safe against quantum computers in 2022. The first implementations have started to appear, combining PQC with classical algorithms for added security. The research will continue to find faster and more secure algorithms, but no known cryptographic algorithm is *provably* secure against quantum computers and allows homomorphic encryption. Hybrid encryption is becoming more common, but protocols without a fallback must be considered carefully, as some quantum-safe algorithms may be attackable.

L. Gasser (✉)
EPFL, Lausanne, Switzerland
e-mail: linus.gasser@epfl.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_10

10.2 Analysis

Cryptography is widely used to encrypt (hide) and sign (prove the source) electronic documents and internet traffic. The underlying mathematical concept is a one-way function [1] that makes it easy to encrypt but challenging to decrypt without a secret. However, future quantum computers will likely be able to reverse many of these one-way functions that are widely used and allow the calculation of the secret needed to decrypt the data.

The US government urges its services to implement post-quantum algorithms by 2035 [2]. The urgency comes from the fact that even if quantum computers are expected to be available after that date, an enemy who copied encrypted data or encrypted messages might decrypt them at this point. For data with a long secrecy requirement, it is thus crucial to start using quantum-safe encryption well before such quantum computers exist.

10.2.1 Definition

Current encryption algorithms can be separated into two groups: symmetric encryption (see Chap. 2) and asymmetric encryption (see Chap. 3).

As of 2022, quantum computers are not significantly faster at breaking symmetric cryptography [3]. However, asymmetric encryption is based on one-way functions which can take a random, secret key and create a corresponding public key. The inverse function, taking a public key, and finding the secret key, is supposed to be hard for the two most commonly used algorithms, namely RSA and Elliptic Curves.

Future quantum computers should be able to speed up this reversing operation and make it possible to use a public key to find the corresponding private key within minutes instead of eons. They will use the Shor algorithm to break the one-way functions of RSA and Elliptic Curves. However, as seen in [4], there are still exponential advancements in terms of the number of qubits and their quality (error rate) required until quantum computers are powerful enough to run the Shor algorithm for today's asymmetric encryption algorithms.

Various propositions exist for one-way functions where quantum computers do not have an advantage. There are a couple of challenges: similar to one-way functions in widespread use today, these new ones need to be secure against any type of attack. It is not because nobody found an attack that would break an algorithm that the algorithm is secure as it often takes years to find such attacks, as seen in the example of two entries in the NIST post-quantum standardization effort [5]. Another problem is the encryption's speed, the keys' size, and the corresponding messages.

10.2.2 Trends

NIST started a Post-Quantum Cryptography (PQC) challenge in 2016, intending to find suitable algorithms for Public-key Encryption and Key-establishment as well as Digital Signature Algorithms. All cryptographers can participate in both proposing new algorithms, as well as in attacking existing algorithms. In July 2022, NIST published four algorithms that it believes to be safe against quantum computers [6].

Now that the winners of the NIST PQC challenge are known, the first implementations have started to appear. Because these algorithms are still very new, most implementations combine a PQC algorithm with a classical one. This is done so that even if one of the two turns out to be broken, the security of the other algorithm remains. One downside of the NIST PQC winners is that there is only one encryption algorithm but three signature algorithms. This means that if the encryption algorithm is broken, no alternative exists.

Google already tested quantum-safe encryption [7], and the SSH application, used to connect a user to a remote computer securely, proposes a hybrid encryption scheme as of April '22 [8].

Of course, research will continue with the goal of finding faster, more compact, and more versatile algorithms than the ones being submitted to NIST. Nevertheless, most importantly, there is currently no known cryptographic algorithm that is provably secure against attacks from quantum computers that allows homomorphic encryption.

More and more protocols will propose hybrid encryption, like SSH in [8], and later quantum-safe protocols only. However, the protocols that do not offer a fallback will have to be taken into account carefully, as there is a high probability that some of the currently proposed quantum-safe algorithms will turn out to be attackable either by quantum computers or even by classical computers.

10.3 Consequences for Switzerland

To understand why it is important to speed up the development and usage of quantum-safe algorithms, one has to look at Fig. 10.1:

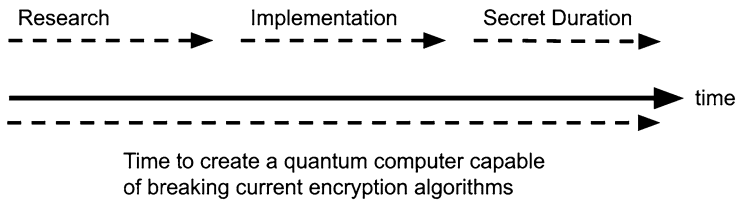

Fig. 10.1 Timelines of development of new algorithms and development of quantum computers

Even if we do not know whether or when a quantum computer capable of breaking today's encryption algorithms will be available, this does not mean we should wait until we know to switch to quantum-safe algorithms. This is because we need to add the time for research on quantum-safe algorithms, transitioning to them (updating old software and replacing non-upgradable legacy systems), and most importantly, the duration for which something encrypted today needs to stay secret. If an adversary stores encrypted messages in the hope of being able to decrypt them later using a quantum computer, the usefulness of these secrets must have expired by the time a quantum computer gets available.

This is true for both stored secrets and secret communications. As has been shown by the Snowden revelations, the NSA (and probably other secret services as well) is storing encrypted secrets and communications in the hope of being able to decrypt them at a later time [9]. For Switzerland, this means that it is of utmost importance for the banking and the military sector to drive the move to quantum-safe encryption. Otherwise, copies of the current safe data will be decrypted by third parties once quantum computers that can do so should become available. Stories about a quantum computer breaking a well-known algorithm like RAS-2048 will continue to emerge. But, they still do not achieve a scientific consensus [10].

For governments, one consequence is that future e-voting systems (see Chap. 23) need to be evaluated regarding their quantum-safe operations. If, for example, all encrypted votes are publicly available for verification, a future quantum computer might breach voting secrecy. On the other hand, businesses will mostly want to follow regulations and ensure that they implement the necessary and available technology. Otherwise, they might be penalized because they needed to implement better practices.

10.3.1 Implementation Possibilities: Make or Buy

Make: developing custom cryptographic algorithms is strongly discouraged since they are likely to be insecure. Custom implementations of existing algorithms (e.g., NIST candidates) might be considered, but usage (and review/analysis) of existing and well-tested implementations should be preferred.

Buy: use an existing library—NIST candidates are supposed to be patent-free, and most are available as Open Source implementations (Table 10.1).

10.3.2 Variations and Recommendation

There are different options for quantum-safe implementations. The first one would be to implement the probable best algorithm available. The second would be a hybrid combination of classical and quantum-safe algorithms to get the most secure option. Moreover, to wait until a consensus emerges on the best algorithm existing (Table 10.2).

Table 10.1 Implementation possibilities for different sectors

	Make		Buy	
	Pros	Cons	Pros	Cons
Military	Augment legacy systems, protection against backdoors	Potential error in implementation adding attack surface will leak	Access to peer-reviewed library	Might contain accidental or purposeful backdoors
Civil Society	None	None	Use library compatible with other services	None
Economy	Sell hardened library	Liability in case the library has an error	Faster development of quantum-secure products	Less advantage over competition

Table 10.2 Variation and recommendation for different sectors

	Military		Civil Society		Economy	
	Pros	Cons	Pros	Cons	Pros	Cons
Wait	No expense	Secrets will leak	Most easy solution	No e-voting	No cost	Liability issues
Hybrid	Maximum protection	Only feasible for the most sensitive data	More security	Only feasible for very few use-cases	Security and PR	Cost and need to follow development
Quantume-safe	Easier than hybrid	Might be broken	None	Hassle because it will need to change	None	Need to be updated

10.4 Conclusion

For the time being, symmetric encryption is secure and a quantum computer will not be able to create a significant speedup over classical computers for decrypting messages. However, the estimations of if and when a quantum computer capable of breaking RSA and Elliptic Curves will become available differ significantly between experts. As Fig. 10.1 indicates, not switching to quantum-safe algorithms would mean that long-term secrets might get compromised. For this reason, switching to quantum-safe algorithms is critical for data that must remain secret for years (e.g., military secrets or e-voting data). For all other data, it is crucial to ensure that systems are at least crypto-agile (migration path exists) or already come with support for hybrid algorithms, primarily when they are widely used like SSH [8].

While a complete migration to quantum-safe algorithms will only happen after 2035 [11], the start for tests and migrating critical systems should start much earlier. For example, the military should start testing systems now and move systems requiring long-term security to quantum-safe algorithms well before 2035. The economy, more specifically banks, should start with testing at the latest in 2025 and also consider having done most of the adaption by 2035.

References

1. Erica Klarreich. Researchers Identify 'Master Problem' Underlying All Cryptography. https://www.quantamagazine.org/researchers-identify-master-problem-underlying-all-cryptography-20220406/, April 2022. Quanta Magazine.
2. National security memorandum on promoting united states leadership in quantum computing while mitigating risks to vulnerable cryptographic systems.
3. Quantum computing: Progress and prospects (2019) - chapter:4 quantum computing's implications for cryptography. https://nap.nationalacademies.org/read/25196/chapter/6#98, January 2019. Washington, DC: The National Academies Press.
4. Samuel Jaques. Landscape of Quantum Computing in 2021. https://sam-jaques.appspot.com/quantum_landscape, May 2021.
5. Post-quantum encryption algorithms under rigorous scrutiny: expect more hacks.
6. Post-quantum cryptography pqc - selected algorithms 2022. https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022, July 2022. NIST.
7. TLS Post-Quantum Experiment. https://blog.cloudflare.com/the-tls-post-quantum-experiment/, October 2019. The Cloudflare Blog.
8. Openssh 9.0 release. https://www.openssh.com/txt/release-9.0, August 2022.
9. Leaked nsa doc says it can collect and keep your encrypted data as long as it takes to crack it.
10. admin. Researchers' Quantum Threat Debunked, RSA Safe for Now. https://thenetworkcompany.net/researchers-quantum-threat-debunked-rsa-safe-for-now/, January 2023.
11. National Security Agency. Announcing the Commercial National Security Algorithm Suite 2.0, 2022.

Part II
Low-Level Applications

Chapter 11
Functional Encryption

Romain Gay

11.1 Introduction

Functional encryption is a cryptographic tool that gives users fine-grained access to encrypted data. Applications include situations where privacy and confidentiality conflict with practical data usage and aggregation, such as medical data or smart grid electricity consumption patterns. The benefits of functional encryption include built-in verifiability and the ability for the server to perform computations "blindly" on encrypted data while retaining the confidentiality of the plaintexts. The Swiss company Kudelsky Security is developing an open-source library for functional encryption. While developing a solution from scratch can improve performance, the more compelling case is to use existing technology for faster product development and a solution less prone to bugs.

11.2 Analysis

11.2.1 Definition

Functional encryption provides users with fine-grained access to the encrypted data and permits the computation of specific functions on the protected plaintexts. Namely, data is encrypted using a public key, while restricted keys that correspond to particular functions are generated. Decryption recovers only the function evaluated on the plaintext. It is possible to fine-tune which information is revealed during

R. Gay (✉)
IBM Switzerland, Zurich, Switzerland
e-mail: RGA@zurich.ibm.com

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_11

decryption, as opposed to the all-or-nothing access that standard encryption provides [1].

Consider the simple example of private spam filtering. Incoming emails are encrypted using the recipient's public key. At the same time, the server has only a restricted key revealing whether such an email is spam without revealing the actual content of the email. Applications of Functional Encryption include many use cases where privacy and confidentiality conflict with practical data usage and aggregation, such as medical data or electric consumption patterns in smart grids.

Like Homomorphic Encryption (see Chap. 8), Functional Encryption allows the server to compute "blindly" on the encrypted data retaining the confidentiality of the plaintexts. Unlike Homomorphic Encryption, however, Functional Encryption gives the server some well-chosen, partial information of the plaintexts in the clear, thanks to the restricted decrypting keys, which relieves the server from the need to interact with the user to extract useful information such as in the example of spam filtering. Moreover, Functional Encryption has a built-in verifiability property. This prevents the server from computing anything else than the function specified by the restricted decrypting key.

11.2.2 Trends

Traditional encryption schemes already address the need for confidential point-to-point communication. However, only advanced encryption schemes such as Functional Encryption can handle more sophisticated data sharing involving an untrusted cloud. Several technological trends are likely to accelerate the deployment of this new tool:

- recent progress regarding the building of general purpose Functional Encryption that supports rich and complex classes of functions, performing advanced analytics of the encrypted plaintexts
- efficiency improvement for schemes supporting simple functions, with the implementation of libraries and the application to real-life use cases, such as Privacy-preserving and auditable Digital Currency, Motion Detection and Local Decision Making, and Privacy-Preserving Statistical Analysis [2–5].
- rise of new decentralized schemes where no trusted setup is required, removing the single point of failure that plagues conventional encryption schemes.

Just as Homomorphic Encryption, Functional Encryption protects data in use—as opposed to standard encryption that only protects data in transit or at rest—with the additional advantage that the computation performed by the cloud is trusted by design and requires less interaction with the clients since the server can directly recover partial information from the encrypted data.

11.3 Consequences for Switzerland

A large share of Swiss businesses, such as the medical, banking, and insurance sectors, rely heavily on users' data, which is often confidential and sensitive. Besides solid privacy laws, these businesses can build trust with the consumers by using cryptographic tools such as Functional Encryption to build a product that is private by design. On the other hand, many data sets deemed too sensitive to share could be securely aggregated and put to practical use, for instance, medical data used for research.

11.3.1 Implementation Possibilities: Make or Buy

The fact that the Fentec project [2], whose sponsors include the Swiss company Kudelsky Security [6], is currently developing an open-source library for Functional Encryption makes a case for buy. As typical for cryptographic schemes, and especially for recent technologies such as Functional Encryption, it is riskier to develop a homemade solution than using a tried and tested implementation. Using existing technology implies a faster development of products and a solution that is less prone to bugs.

On the other hand, making a scheme from scratch would avoid using a scheme that potentially has a (purposeful or accidental) trapdoor. It could also permit a tailored scheme for a particular application, improving performance.

Overall the case for buying is more compelling than making because it would require significant efforts to build a security scheme that is on par with the existing open-source solutions.

11.3.2 Variations and Recommendation

Functional Encryption schemes come in many forms. First, the general purpose schemes that can handle arbitrarily complex functions and satisfy strong security notions are versatile tools but need more concrete efficiency. Second, another class of Functional Encryption schemes handles complex functions but only supports a somewhat limited security notion where keys only have a short life span (technically speaking, the attackers' capability of corrupting keys needs to be bounded and known in advance so that the security parameters can be scaled accordingly). These schemes may be well suited for applications that require performing sophisticated computation on the encrypted data and where the attackers' capabilities are relatively limited in scope.

Finally, the third type of Functional Encryption scheme focuses on smaller classes of simple functions, such as a weighted average on encrypted data. These

schemes are the most efficient, and the simple functions they handle are sufficient for applications such as private inference. In some applications, simplicity is beneficial since it allows the classifier to justify itself easily. For instance, if a bank refuses a loan based on data analysis from a client, it should be able to justify its choice and make sure the decision is fair (e.g., not based on discriminatory attributes). This is easier to do if the classifier is a simple function. There are a variety of schemes and underlying cryptographic assumptions available. The schemes based on elliptic curves enjoy the smallest ciphertext and key sizes. In contrast, the lattice-based options have the advantage of post-quantum security but are currently less efficient (especially size-wise) than their counterparts.

11.4 Conclusion

Functional encryption is to become an increasingly valuable tool in the context of growing concern for privacy and the ubiquitous use of data. Switzerland is involved in open-source projects such as Fentec sponsored in part by Kudelsky Security [6], which will facilitate the deployment of this technology for promising applications.

References

1. Wikipedia, Functional encryption. https://en.wikipedia.org/w/index.php?title=Functional_encryption&oldid=1096161660, July 2022.
2. Fentec | Functional Encryption Technologies. https://fentec.eu/, August 2022.
3. Technology. https://cosmian.com/technology/, August 2022. Cosmian.
4. Ruby Protocol - Web3 Privacy-Centric Infrastructure. https://www.ruby.xyz/, August 2022.
5. Picolo Labs. https://www.picolo.network/, August 2022.
6. Kudelski Security | Cybersecurity & Managed Security Company. https://kudelskisecurity.com, August 2022.

Chapter 12
Identity-Based Cryptography

Bernhard Tellenbach

12.1 Introduction

In identity-based cryptosystems (IBC), identity is also the public key. This has two clear advantages over traditional public-key cryptosystems. First, certificates are not needed to bind the two independent information units, identity and public key. Second, key management is simplified because users can easily remember public keys for identities such as email addresses or domain names. There exists a wide variety of IBCs with widely differing properties and application domains. However, since most of them need a trusted third party that can derive the private keys of participants, those systems are not suitable for applications where this is a problem. This might contribute to the fact that, in practice, applications of IBC are still relatively rare, although there are various standards for IBC. Examples are ISO/IEC 18033-5:2015, IEEE 1363.3-2013, or the MIKEY-SAKKE protocol for securing communication links, which is being actively pushed by the UK's National Cyber Security Centre. In Switzerland, the use of technology in the public and private sectors, unlike research on it at universities, has yet to receive much attention. Changing this could lead to more effective solutions to several problems that it can address.

B. Tellenbach (✉)
Cyber-Defence Campus, Thun, Switzerland
e-mail: bernhard.tellenbach@ar.admin.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_12

12.2 Analysis

Asymmetric cryptosystems form the foundation for establishing a secure connection with another party, for example, also with those where no secure channel has existed at any time before. This is possible because, unlike with symmetric cryptosystems, no secret key material needs to be exchanged between the interacting parties beforehand. Instead, it is sufficient for the interacting parties to publish the public part of their key material, and for a trusted third party to confirm that this is indeed the public key of that party.

The public part of a party's key can then be used to encrypt data for that party or verify a digital signature created by that party with the private part of the key. Certificates are typically used for third-party confirmation. Certificates contain at least the identity (e.g., the email address), a party's public key, and the digital signature of this association created by the trusted third party—also called Certification Authority (CA). Suppose the public keys of such CAs are already present on the parties' systems, for example, because they were delivered with the operating system or browser or placed on the system by hand. In that case, the digital signature of the CA on the certificate can be verified.

12.2.1 Definition

In identity-based cryptosystems, the public key is also the identity. This has two clear advantages over traditional public-key cryptosystems: first, there is no need for certificates to bind the two independent information units, identity and public key, and second, key management is simplified because users can easily remember public keys, at least for identities such as email addresses or domain names. These two properties were the primary motivation of Adi Shamir when he introduced this type of cryptography in 1984 [1].

12.2.2 Trends

In addition to the advantages already mentioned, identity-based cryptography (IBC)—at least in its simplest form—also has to contend with some challenges. These include, in particular, the fact that it requires a trusted third party that knows all the private keys of the identities as stated in the key escrow problem [2]. Other challenges are that no revocation of compromised keys is possible without changing the identity, and that the trusted third party poses a problem in terms of scalability, availability, and risk distribution.

Solutions to these challenges are partially available, for example, Hierarchical Identity Based Encryption (HIBE) [3–6] can be used to distribute risk and load

across a system of hierarchical PKGs (private key generators). There are also proposed solutions for the key-escrow problem [7–9]. However, in many cases, these solutions still need to be well-tested or have limitations of their own. Finally, resistance to quantum computing is likely to be an issue since many of today's solutions are based on assumptions about difficult-to-solve problems on elliptic curves. Approaches that rely on believed-to-be quantum computing-resistant lattice-based cryptography have existed since 2008. However, these need to be prepared for practical use because of various open questions and factors such as too large public keys [10]. It is therefore expected that this technology will continue to be actively researched and improved in the coming years. Additional application areas and forms will be proposed and tested.

In practice, applications of IBC are still relatively rare, although there are now various standards for IBC procedures and their application, e.g. ISO/IEC 18033-5:2015 or IEEE 1363.3-2013. Examples of products where IBC can already be used today are FortiMail from Fortinet or Voltage SecureMail Cloud. Another example where IBC is used is the MIKEY-SAKKE protocol for securing communication links, which is standardized in IETF RFCs 6507, 6508, and 6509 and is being actively pushed by the UK's National Cyber Security Centre (NCSC). While isolated solutions currently exist in individual companies and sectors, the use of MIKEY-SAKKE should later allow seamless cross-government and industry communication. This is why the NCSC only certifies secure Voice-Over-IP (VoIP) clients for official use by the UK government that supports this protocol. A good overview of the topic and possible application areas is provided by the ETSI Technical Report 103 719 from March 2022, which is also suitable for non-experts [11]. ETSI sees, in particular, government and enterprise applications, public safety and mission-critical applications, the Internet of Things, and Intelligent Transport Systems as promising application areas.

12.3 Consequences for Switzerland

Regarding knowledge and research, Switzerland is in a good spot with researchers at ETH Zurich, EPFL, IBM Rüschlikon, and other institutions that work on or have worked on identity-based cryptosystems. Switzerland should continue to invest in research in that domain, as it is an active research field with many open issues and room for improvement. In contrast to research, it seems that the technology did not get much attention in Switzerland's public and private sectors yet, despite being a viable solution for several application domains. Suppose this technology was better known among companies and individuals building solutions with cryptographic building blocks. In that case, the available range of solutions and the innovation potential could be better exploited.

Table 12.1 Implementation possibilities for different sectors.

	Private		Public	
	Pros	Cons	Pros	Cons
Military	Strategic and operational independence	Cost and interoperability	Products might have been analyzed for their security by different cryptographers and researchers	Dependence on (proprietary) solutions from actors not under your control and Supply-Chain risks
Civil Society	Expertise can be utilized in many areas, trust in Swiss-made solutions and full transparency is possible	Cost and interoperability	Cheaper, faster in the short term, more trust in the long term if large user-base	Dependence on foreign actors and enterprises, no Swiss finish (customizations) and less transparency
Economy	Expertise can be utilized in many areas, business opportunities	Cost and interoperability	Better time to market, more trust in the long term (if larger user-base)	Less or no flexibility if custom features and extensions are needed to innovate

12.3.1 Implementation Possibilities: Make or Buy

This section presents the pros and cons of buying or making identity-based cryptography solutions (Table 12.1).

12.3.2 Variations and Recommendation

Many identity-based cryptosystems with widely differing properties and application domains exist. We can name the closed IBE cryptosystem, the open IBE cryptosystem, or the Intelligent Transport System. Therefore, it is out of this study's scope to discuss the different variations of such systems. We refer the reader to ETSI's technical report [12] as a good starting point for a general discussion. For the same reason, it is also difficult to give any recommendation other than that IBC should not be used whenever the existence of a trusted third party that knows the private keys is considered a problem, as this property is needed for the functioning of the system. Unless one uses research-grade IBC that at least partially addresses this issue. For

other recommendations, [12] contains some and serves as a starting point for more in-depth investigation.

12.4 Conclusion

Identity-based encryption systems are characterized by the fact that the public key is easy to remember, and the implementations skip the step of linking the public key to a specific identity. However, they also have some disadvantages. In particular, the trust that must be placed in the trusted third party is significantly higher than in traditional public key systems.

Whether these and other potentially disadvantageous properties, such as the lack of well-tested quantum-safe solutions, are relevant depends on the specific use case. Moreover, the lively research activity in the field can potentially mitigate or eliminate undesirable properties.

References

1. Adi Shamir. Identity-Based Cryptosystems and Signature Schemes. In George Robert Blakley and David Chaum, editors, *Advances in Cryptology*, Lecture Notes in Computer Science, pages 47–53, Berlin, Heidelberg, 1985. Springer.
2. Wikipedia, key escrow. https://en.wikipedia.org/w/index.php?title=Key_escrow&oldid=1100458218, July 2022.
3. Craig Gentry and Alice Silverberg. Hierarchical ID-Based Cryptography. 2002. Cryptology ePrint Archive.
4. Jeremy Horwitz and Ben Lynn. Toward Hierarchical Identity-Based Encryption. In Gerhard Goos, Juris Hartmanis, Jan van Leeuwen, and Lars R. Knudsen, editors, *Advances in Cryptology — EUROCRYPT 2002*, volume 2332, pages 466–481. Springer Berlin Heidelberg, Berlin, Heidelberg, 2002. Series Title: Lecture Notes in Computer Science.
5. Dan Boneh, Xavier Boyen, and Eu-Jin Goh. Hierarchical Identity Based Encryption with Constant Size Ciphertext. In Ronald Cramer, editor, *Advances in Cryptology – EUROCRYPT 2005*, Lecture Notes in Computer Science, pages 440–456, Berlin, Heidelberg, 2005. Springer.
6. Roman Langrehr and Jiaxin Pan. Tightly Secure Hierarchical Identity-Based Encryption. *Journal of Cryptology*, 33(4):1787–1821, October 2020.
7. Keita Emura, Shuichi Katsumata, and Yohei Watanabe. Identity-based encryption with security against the KGC: A formal model and its instantiations. *Theoretical Computer Science*, 900(C):97–119, January 2022.
8. Rikke Bendlin, Sara Krehbiel, and Chris Peikert. How to Share a Lattice Trapdoor: Threshold Protocols for Signatures and (H)IBE. *Cryptology ePrint Archive*, 2013.
9. Mahender Kumar and Satish Chand. ESKI-IBE: Efficient and secure key issuing identity-based encryption with cloud privacy centers. *Multimedia Tools and Applications*, 78(14):19753–19786, July 2019.
10. Goichiro Hanaoka and Shota Yamada. A Survey on Identity-Based Encryption from Lattices. In Tsuyoshi Takagi, Masato Wakayama, Keisuke Tanaka, Noboru Kunihiro, Kazufumi Kimoto, and Dung Hoang Duong, editors, *Mathematical Modelling for Next-Generation Cryptography: CREST Crypto-Math Project*, Mathematics for Industry, pages 349–365. Springer, Singapore, 2018.

11. www.etsi.org-/deliver/etsi_tr/103700_103799/103719/. https://www.etsi.org/deliver/etsi_tr/103700_103799/103719/, February 2023.
12. European Telecommunications Standards Institute. Guide to Identity-Based Cryptography. Technical report, March 2022.

Chapter 13
Multi-Party Threshold Cryptography

Christian Cachin

13.1 Introduction

Multi-party threshold cryptography (MPC) is a type of cryptography that enables secure computations to be performed jointly by multiple parties. It allows multiple parties to collaborate and perform sensitive operations such as decryption or signing without revealing their private keys. Threshold cryptography (TC) uses secret sharing to split secret information into pieces and distribute them among several parties. To perform a computation, a threshold of the parties must come together and combine their shares, creating a new piece of information. The minimum number of parties needed to perform the computation is called the threshold, which can be set in advance. TC can be used to protect privacy in cloud computing, secure financial transactions, and other sensitive applications where multiple parties are involved. It ensures that the secret information remains secure even if some of the parties involved are compromised, as long as the threshold is not reached.

13.2 Analysis

13.2.1 Definition

Cryptographic techniques, such as public-key encryption and digital signatures, are ubiquitous in today's security infrastructures. However, recent years have seen a move towards building resilient distributed systems (such as blockchains [1]), which

C. Cachin (✉)
University of Bern, Bern, Switzerland
e-mail: cachin@inf.unibe.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_13

gain security by drawing on replication and redundancy and rely on multiple parties to operate. Threshold cryptography is the technology that lets such systems execute cryptographic operations. As no single party must store any secret material (such as the private key) because the party may leak when it is corrupted, the cryptographic operations must also be distributed.

In a threshold cryptosystem, the private key is typically distributed among the N parties that constitute the system using cryptographically secure secret sharing. Up to F of the parties might be faulty and leak their key shares, but $F+1$ must cooperate in executing a cryptographic operation. From the outside, the cryptographic result (such as the digital signature or the decryption of a ciphertext) is the same as if the operation had been executed on a single party. It is crucial that the operation reveals nothing about the private key to the faulty parties and that it is robust. That is, it cannot be disrupted by faulty parties that may act maliciously. Threshold cryptosystems require at least $N > 2 * F$, which means that any minority of the parties could become corrupted.

Threshold cryptosystems have been developed for most public-key cryptosystems in use today. This includes digital signatures (RSA, DSA, ECDSA, BLS, and more), encryption (RSA, variants of ElGamal encryption, including pairing-based ones.), and coin-tossing for producing unbiased randomness. However, the efficiency of implementations differs widely depending on the mathematical structure of the underlying cryptosystem; for example, threshold implementations of BLS-based schemes are easy to build and relatively efficient, but the operations of DSA and ECDSA are challenging to distribute.

Particular focus must be placed on generating the private key held jointly by the parties. The simplest method would be to generate the key material on a single node, but this introduces more centralization than is generally accepted. The reason is that this node itself could become corrupted, contradicting the motto that no single party can be trusted. Protocols for distributed key generation (DKG) have therefore been developed. However, they are often more complex than the standard operation of the public-key schemes, and they require integration with a distributed communication platform.

Notably, threshold cryptosystems differ widely according to their needs for interaction among the parties. The most efficient schemes are non-interactive: when producing a digital signature, every party generates a “share” of such a signature and disseminates it. Upon receiving $F + 1$ such shares, every party can obtain the digital signature. Many other schemes, however, require multiple rounds of interaction among the parties and some steps in which they reach a consensus on which parties have been potentially faulty during the key-generation process. These are more difficult to implement and are not widely available or deployed today. A typical example from the latter category is DKG protocols: they require more than one rounds of communication and some “agreement” on which parties terminated the protocol correctly.

13.2.2 Trends

Threshold cryptosystems have been explored in the cryptographic literature and prototype systems exist for a long time, starting around 1990 [2]. However, they have only seen industrial applications in the last 10 years. This trend has resulted from the appeal of blockchain platforms, which have demonstrated the advantage of building secure, resilient systems from multiple and less trustworthy components. As a result, the system remains intact even if some components fail or become corrupted.

Most practical blockchain networks today do not support threshold cryptography for applications nor exploit it internally, although several have proposed using the technology. A notable exception is perhaps the Internet Computer (built by DFINITY, [3]), which uses threshold-cryptography schemes at its core. The reasons for this are manifold: Lack of cryptographic expertise among developers, no standards, and the complexity of implementations.

Nevertheless, the trend toward implementing and deploying threshold cryptosystems is clear and will accelerate. Most practical secure distributed platforms will be enhanced with this capability. Furthermore, several standardization efforts are underway: NIST in the United States has initiated an effort to standardize multi-party threshold cryptography [4], which is currently underway. The IETF/IRTF, through their Crypto Forum Research Group (CFRG), is also pushing the development and standardization of specific threshold cryptosystems for use on the Internet.

Most efforts until 2025 will come from the "blockchain ecosystem", producing implementations that are available as open source. As a result, one may expect multiple libraries for specific platforms and generic services to become available.

The NIST effort has yet to gain much momentum. As a result, NIST is likely to focus on standardization first. Nevertheless, the field offers considerable complexity, ranging from data formats over protocol interactions to security aspects, like cryptographic parameters. This makes it unlikely that the effort will lead to concrete standards and widely available implementations until 2025. Nevertheless, over a longer time, this is likely to happen.

13.3 Consequences for Switzerland

13.3.1 Implementation Possibilities: Make or Buy

Cryptographic algorithms must be standardized globally, and their security needs broad public analysis. These processes are typically multi-year efforts driven by governmental or private-sector standardization agencies. The key players of the IT industry are often represented or participating actively in this development. Other active drivers are startups and smaller companies with deep expertise in the algorithms and their implementation that place a bet on the technology itself.

It is therefore expected that standards for threshold cryptography and the corresponding open-source implementations will also emerge without concrete steps taken by the Swiss government. Instead, cryptographic libraries suitable for standardized wide deployment will become available from public and commercial sources. To obtain the expertise necessary to autonomously build applications that rely on threshold cryptography and exploit it, investment and education will be needed. Switzerland is positioned well in this space since multiple universities (ETHZ, EPFL, University of Bern) and many private companies, especially in the blockchain environment, have deep expertise in the domain.

13.3.2 Variations and Recommendation

Like blockchain platforms, threshold cryptosystems realize secure applications from partially untrusted components. They exist in many forms, such the suitability for every concrete deployment has to be analyzed in detail. However, if used in a matching application scenario, they greatly enhance the security and resilience of the application.

It is recommended that Switzerland closely watches the development of threshold cryptography and invests moderately in it. In this sense, the technology seems related to post-quantum cryptography and its positioning; this is another area of active worldwide technology development in cryptography research. Switzerland is one of many active players in this field, but the technology still needs to be mature for industrial deployment, which merits a direct commercial investment.

13.4 Conclusion

For building secure distributed systems that can survive a partial corruption of their components, multi-party threshold cryptography plays an important role. It is related to secure multi-party computation because both use the same trust model, also found in many blockchain platforms. However, MPC systems are more general than threshold cryptosystems and may compute arbitrary functions, whereas threshold cryptosystems are limited to operations with cryptographic keys. In addition, MPC protocols are several orders of magnitude less efficient than the typical threshold cryptosystems. Therefore, threshold cryptosystems are expected to be deployed earlier than MPC-based systems.

References

1. Luca Gambazzi, Patrick Schaller, Alain Mermoud, and Vincent Lenders. Blockchain in Cyberdefence: A Technology Review from a Swiss Perspective, March 2021. arXiv:2103.02606 [cs].
2. Yvo G. Desmedt. Threshold cryptography. *European Transactions on Telecommunications*, 5(4), 1994.
3. The dfinity foundation is a major contributor to the internet computer blockchain. https://dfinity.org, July 2022.
4. Information Technology Laboratory Computer Security Division. Multi-Party Threshold Cryptography | CSRC | CSRC. https://csrc.nist.gov/Projects/threshold-cryptography, July 2018. CSRC | NIST.

Chapter 14
Searchable Symmetric Encryption

Cyrill Krähenbühl and Adrian Perrig

14.1 Introduction

Searchable symmetric encryption (SSE) allows operating on encrypted data, in particular keyword- based search on documents and range-based search on spatial data. Various methods can be used in SSE, such as order-preserving encryption or fully homomorphic encryption for different levels of information leakage. New schemes with more efficient search operation and reduced access and search pattern leakage that support novel settings, such as dynamic data sets and multiple users, have been proposed in the last few years. Especially with the emergence of cloud storage, encrypting sensitive remote data while preserving the ability to efficiently operate on it is an ample opportunity for the military and industry. However, there are risks when deploying SSE that must be taken into account since some SSE schemes proposed in the past have been (completely) broken by the research community.

14.2 Analysis

14.2.1 Definition

In the searchable symmetric encryption (SSE) setting, there is a collection of files where keywords are associated with each file. A user searches for all files in the collection associated with a specific keyword. Neither the content of files nor the

C. Krähenbühl (✉) · A. Perrig
Swiss Federal Institute of Technology, Zurich, Switzerland
e-mail: cyrill.kraehenbuehl@inf.ethz.ch; adrian.perrig@inf.ethz.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_14

associated keywords should be revealed to an unauthorized entity. To achieve this, files and keywords are encrypted, and only users with the respective keys can search the collection and decrypt files. Depending on the SSE protocol, files can be added and removed (dynamic), files can be added but not removed (semi-dynamic), or all files must be present when the system is set up and cannot change over time (static).

SSE should not be confused with Public Key Encryption with Keyword Search (PEKS), a related technique that allows holders of a public key to add encrypted files to the collection and the private key holder to search for and decrypt files.

The security of an SSE protocol is defined by its privacy leakage, i.e., how much information is leaked in addition to necessarily leaked information such as the file sizes, access patterns, and search patterns under different attacker models (adaptive and non-adaptive attackers) [1].

Fully homomorphic encryption (FHE) is another cryptographic primitive to operate on encrypted data without revealing the results. Although FHE can provide stronger privacy guarantees than SSE, it is computationally more expensive and requires data in homogeneous form, while SSE can operate on any heterogeneous data.

There are several variations on the SSE model. For example, some SSEs consider searches for data ranges instead of searches for specific keywords. Such SSEs are useful for outsourcing encrypted spatial data, e.g., collecting location-indexed data. However, early constructs, such as order preserving encryption [2], are vulnerable to database reconstruction attacks [3].

Traditional SSEs operate in a single-user setting, but some SSE also considers a multi-user setting, where users can be added and removed, which brings additional challenges, such as colluding users.

14.2.2 Trends

There is a long history of research on SSE, starting with early work in 2000 by Song et al. [4]. Over the last 20 years, SSEs have improved functionality, security, and efficiency. First, the functionality of SSE schemes was improved, e.g., by allowing modifications to the dictionaries [5]. The attacker model was extended to provide forward privacy (previous search queries cannot be associated with future updates) and backward privacy (search queries cannot be associated with deleted documents). Finally, SSE schemes become increasingly efficient (e.g., Aura [6], which has a sub-millisecond index insertion time and a sub-microsecond deletion time). State-of-the-art SSE schemes have become practical to be used in real-world settings while providing strong security properties [6, 7].

With the emergence of cloud-based services and storage, parties in various sectors have decided to move their data to cloud storage, significantly reducing operational costs. In most cases, the cloud infrastructure is not hosted by the party but by an independent provider. In such cases, it is often preferential or even required by law or policy to only store encrypted data in the cloud. Unfortunately, storing

encrypted data makes searching the database impossible for the provider that does not possess the decryption keys. SSE allows parties to combine the benefits of encrypted cloud storage while retaining the ability to search this data. Since the trend of increasingly using cloud storage is not expected to slow down in the near future, efficient SSE approaches are likely to be increasingly used.

However, it is essential to note that correctly designing and implementing SSE is difficult. Many proposed systems have become insecure as they leak access patterns or even allow reconstructing the complete database [8, 9]. The risk of storing sensitive data on remote storage using SSE must thus be carefully evaluated case-by-case.

14.3 Consequences for Switzerland

There is ample opportunity to move more sensitive data to the cloud to reduce hardware and management costs and facilitate information sharing. At the same time, privacy regulations or company-specific policies that require sensitive data to be encrypted fuel the need for SSE.

14.3.1 Implementation Possibilities: Make or Buy

For the military, public cloud solutions are likely not up to their standard in terms of security and reliability. However, the military must collaborate with foreign armed forces, police forces, or between different divisions. Therefore, custom-built SSE solutions running on trustworthy cloud infrastructures could be attractive, especially for sharing data within Switzerland. Furthermore, a solution offered by a trustworthy international source could also be an exciting option for collaboration with foreign entities.

For the civil society and economy sector, custom-built solutions may be prohibitive in terms of cost and complicate collaboration with other entities. Public cloud SSE solutions are also attractive due to their low cost and simple management. A straightforward use case for SSE in civil society is storing privacy-sensitive healthcare data on a public cloud for collaboration between health insurance providers, hospitals, and clinics (Table 14.1).

14.3.2 Variations and Recommendation

There is typically a trade-off between the low cost, straightforward management, and ease of collaboration of (public) cloud-based SSE solutions and the stronger security guarantees of self-hosted storage (which can be further improved through

Table 14.1 Implementation possibilities for different sectors

	Make		Buy	
	Pros	Cons	Pros	Cons
Military	Custom solutions could provide stronger assurances for storing highly sensitive data	None	Use SSE technology from trusted sources for sharing data with other armed forces	risk of tampered software introducing backdoors
Civil Society	Create Swiss-wide solution for specific sectors, i.e., health care	Costs	Useful for sharing data between a larger number of collaborating entities	Potential legal hurdles if proprietary code is used for sensitive citizen data
Economy	For large companies relying on cloud storage, a custom approach can enhance the privacy of cloud data	Costs	Can use existing service offered by cloud providers	None

SSE). In general, which type of SSE should be used depends on the application (e.g., keyword search or geometric range search on spatial data), the efficiency, and the security requirements.

14.4 Conclusion

SSE provides the necessary tools to ensure privacy for the transitions of different sectors from local storage to cloud-based remote storage. The benefits of cloud-based services have been shown over the last decade for virtually all sectors. Moreover, this trend of moving data to the cloud does not show any signs of slowing down, making efficient and secure SSE solutions a vital tool for Switzerland in the coming years. However, the secure usage of SSE approaches is very challenging; thus, data security needs to be carefully assessed, especially in the case of highly sensitive information.

References

1. Reza Curtmola, Juan Garay, Seny Kamara, and Rafail Ostrovsky. Searchable symmetric encryption: Improved definitions and efficient constructions. *Journal of Computer Security*, 19(5):895–934, November 2011.
2. Rakesh Agrawal, Jerry Kiernan, Ramakrishnan Srikant, and Yirong Xu. Order preserving encryption for numeric data. In *Proceedings of the ACM international conference on Management of data*, SIGMOD '04. ACM Press, 2004.
3. Georgios Kellaris, George Kollios, Kobbi Nissim, and Adam O'Neill. Generic attacks on secure outsourced databases. CCS '16. ACM, oct 2016.
4. Dawn Xiaoding Song, D. Wagner, and A. Perrig. Practical techniques for searches on encrypted data. In *Proceeding 2000 IEEE Symposium on Security and Privacy. S&P 2000*, pages 44–55, May 2000. ISSN: 1081-6011.
5. Seny Kamara, Charalampos Papamanthou, and Tom Roeder. Dynamic searchable symmetric encryption. In *Proceedings of the 2012 ACM conference on Computer and communications security - CCS '12*, page 965, Raleigh, North Carolina, USA, 2012. ACM Press.
6. Shi-Feng Sun, Ron Steinfeld, Shangqi Lai, Xingliang Yuan, Amin Sakzad, Joseph Liu, Surya Nepal, and Dawu Gu. Practical Non-Interactive Searchable Encryption with Forward and Backward Privacy. In *Proceedings 2021 Network and Distributed System Security Symposium*, Virtual, 2021. Internet Society.
7. Tianyang Chen, Peng Xu, Wei Wang, Yubo Zheng, Willy Susilo, and Hai Jin. Bestie: Very Practical Searchable Encryption with Forward and Backward Security. In *Computer Security – ESORICS 2021: 26th European Symposium on Research in Computer Security, Darmstadt, Germany, October 4–8, 2021, Proceedings, Part II*, pages 3–23, Berlin, Heidelberg, October 2021. Springer-Verlag.
8. Paul Grubbs, Richard McPherson, Muhammad Naveed, Thomas Ristenpart, and Vitaly Shmatikov. Breaking Web Applications Built On Top of Encrypted Data. pages 1353–1364, October 2016.
9. Francesca Falzon, Evangelia Anna Markatou, Akshima, David Cash, Adam Rivkin, Jesse Stern, and Roberto Tamassia. Full Database Reconstruction in Two Dimensions. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, CCS '20, pages 443–460, New York, NY, USA, October 2020. Association for Computing Machinery.

Chapter 15
Digital Signature

Weyde Lin

15.1 Introduction

The chapter "Digital Signature" covers the use of cryptographic methods and asymmetric cryptography to sign data and provide origin authentication, data integrity, and signer non-repudiation. The signing process involves generating a hash of the data using a cryptographic hashing function, encrypting the hash with the signing party's private key, and sending the data and encrypted hash to the verifying party. The verifying party can determine the validity of the signature by generating a hash of the data and comparing it to the decrypted hash. The digital signature market is expected to grow by around 30% annually over the next few years, with a focus on reducing friction for users and ensuring security. In Switzerland, organizations can either make their digital signature solution for internal use or buy a solution from established companies offering digital signature services.

15.2 Analysis

A digital signature uses cryptographic hashing functions and asymmetric cryptography to sign data. It also provides origin authentication (attribution to a particular individual), data integrity (proof that data has not been tampered with in transit or otherwise), and signer non-repudiation (signers cannot deny that they signed data). It is possible to apply a digital signature to any data, including emails, contracts (e.g., in PDF format), and messages. A qualified electronic signature (QES) is based on a

W. Lin (✉)
Eraneos Switzerland AG, Zurich, Switzerland
e-mail: Weyde.Lin@eraneos.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_15

digital signature. In many legislative frameworks, a QES is the digital equivalent of a handwritten signature.

15.2.1 Definition

Figure 15.1 illustrates the signing and verifying of a digital signature. To digitally sign data, two cryptography functions are used [1, 2]. The first step is to generate a hash (fingerprint) of the data using a cryptographic hashing function (see Hash Functions in Chap. 5). The hash is then encrypted by the signing party using its private key. This encrypted hash is the data's digital signature. Finally, the data and the signature are sent to the verifying party as separate files in a container or embedded in the data (e.g., signed PDF). As part of the verification process, the verifying party generates the hash of the data using the same cryptographic hashing function. Additionally, the verifying party decrypts the signature using the signing party's public key, resulting in a decrypted hash that the signer can only generate. The verifying party can determine whether the digital signature is valid by comparing the decrypted hash with the calculated hash [3]. When a public key is used with a public key certificate (i.e., a certificate that confirms the validity of a public key and contains information about the key owner), it can be identified who signed the document, or it can be proved that it was signed by a specific individual (see Public Key Infrastructure in Chap. 10).

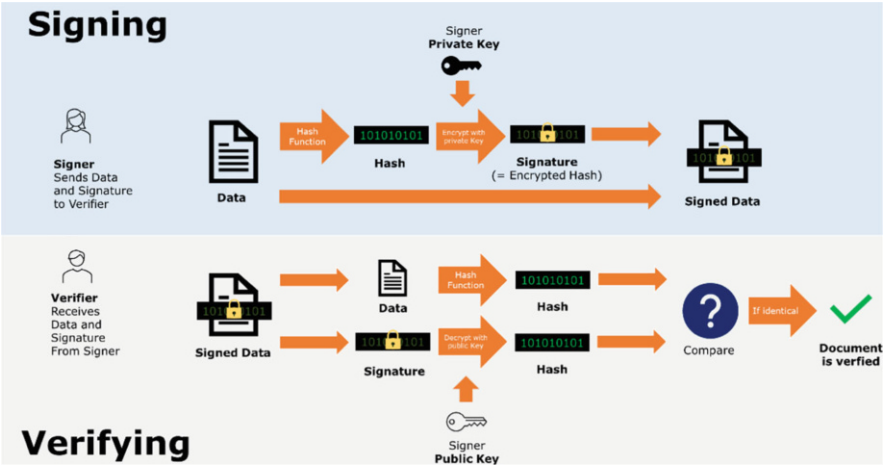

Fig. 15.1 Schematic depiction of digital data signing and verifying process

15.2.2 Trends

With the increasing digitalization of business processes and other processes in general, the ability to apply and verify digital signatures will become increasingly important: the digital signature market size is expected to grow by approximately 30% annually over the next few years [4]. However, it is essential to note that although the EU and Switzerland both have laws regarding qualified electronic signatures (QES), and they are technically compatible, the issue of mutual legal recognition still needs to be fully resolved [5].

Through the use of digital signatures, current paper-based processes will not only be replaced, but they will also be improved, e.g, through audit trails (i.e., tracking documents from beginning to end by digitally signing each process step and saving them alongside the document, ensuring document integrity at each stage and providing legal protection as admissibility in court). For digital and electronic signatures to reach widespread adoption, it is necessary to reduce the friction for the user, for example, by making it possible to generate signatures on mobile devices. The wide acceptance of the digital signature also requires it to be secure. Digital signatures, however, are only as secure as the cryptographical methods (e.g., hash functions) they are based upon. As computation power increases and quantum computing becomes feasible, attacks on underlying cryptographic methods become more effective [6], thereby endangering the security of digital signatures as well (see Post-Quantum Cryptography in Chap. 10).

15.3 Consequences for Switzerland

15.3.1 Implementation Possibilities: Make or Buy

Make: It is important to note that a digital signature is only helpful if all parties use the same standard. As a result, making your digital signature products is only suitable for internal use within an organization which is rarely the case—as such, creating your solution for signing data allows you to control all aspects of the signing process. Military applications may benefit from this technology.

Buy: Many other use cases, especially those in which data is shared with third parties, could benefit from buying from one of the established companies offering digital signature services (e.g., DocuSign, Connective, Adobe Sign, One Span, Evidos, Signicat, Signing Hub, Cryptomathic) or electronic signatures (accredited by ZertES (Federal law on electronic signatures): Swisscom (Schweiz) AG, QuoVadis Trustlink Schweiz AG, SwissSign AG, Bundesamt für Informatik und Telekommunikation BIT [7]). Furthermore, in civil society and the economy, purchasing commercial off-the-shelf (COTS) products from accredited companies is beneficial since they are already certified, meet the legal framework, and should be compatible with other products.

15.3.1.1 Distinction from Electronic Signature

Electronic signatures are sometimes used as synonyms for digital signatures [8]. Despite this, in many legislations (e.g., eIDAS in the European Union or ZertES in Switzerland), the term electronic signature (or e-signature) has a particular meaning. It refers to signing data with the same legal status as a handwritten signature. Electronic signatures are often based on a digital signature. In the EU (eIDAS Regulation [9]) and Switzerland (ZertES [10] and VzertES [11]), this is codified in the law. Electronic signatures can be classified into the following types:

- Qualified electronic signature (QES): QESs is recognized as equivalent to handwritten signatures in Switzerland and the European Union. A QES is based on a digital signature and can be used for documents that require a legal form (e.g., employment contracts)
- Advanced electronic signature (AES): An advanced electronic signature is also based on a digital signature but does not provide liability protection. It defines specific technical requirements for electronic signatures and allows for the signer's identification. AES can be used for documents that do not require a legal form (e.g., rental agreement)
- Basic electronic signature: A handwritten or scanned signature can be used, as well as a signature recorded with a stylus on a tablet. There is no legal or technical requirement for this type of signature.

Everything regarding the usage of the electronic signature can be found in the Federal Act on certification services in the field of electronic signatures and other applications of digital certificates [12].

15.3.1.2 Code Signing

A particular case of the digital signature is code signing, which entails digitally signing executables and scripts. By doing so, it is possible to verify the code's author and ensure that it has not been altered or compromised since it was signed.

15.4 Conclusion

As (business) processes become more digitalized, digital and qualified electronic signatures will play an increasingly important role. As part of these processes, verifying the authorship of some data and whether the data was altered during transport will be necessary. However, a digital signature is only as secure as the cryptographic mechanism underlying it (e.g., hash functions, public key encryption), so the developments in those fields must be studied and adapted for use in digital signatures.

References

1. CSRC Content Editor. digital signature - Glossary | CSRC. https://csrc.nist.gov/glossary/term/digital_signature, July 2022.
2. Kazue Sako. Digital Signature Schemes. In Henk C. A. van Tilborg and Sushil Jajodia, editors, *Encyclopedia of Cryptography and Security*, pages 343–344. Springer US, Boston, MA, 2011.
3. Ravneet Kaur and Amandeep Kaur. Digital Signature. In *2012 International Conference on Computing Sciences*, pages 295–301, September 2012.
4. Spiller, Patrik and Hirs, Daniel and Vanhaecht, Jan and Frik, Joran and Maager, Patrick. E-signing. https://www2.deloitte.com/ch/en/pages/strategy-operations/articles/e-signing-market-size-and-vendor-landscape.html.
5. Warum eine Unterschriftenpanne Stadler Milliarden kosten könnte. *SRF 4 News*, September 2021.
6. COMPUTER SECURITY RESOURCE CENTER at NIST. Post-Quantum Cryptography. https://csrc.nist.gov/Projects/post-quantum-cryptography.
7. Swiss Accreditation Service SAS. Electronic signature. https://www.sas.admin.ch/sas/en/home/akkreditiertestellen/akkrstellensuchesas/pki1.html.
8. COMPUTER SECURITY RESOURCE CENTER at NIST. electronic signature. https://csrc.nist.gov/glossary/term/electronic_signature.
9. European Commission. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG.
10. Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate. https://www.fedlex.admin.ch/eli/cc/2016/752/de.
11. Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate. https://www.fedlex.admin.ch/eli/cc/2016/753/de.
12. SR 943.03 - Bundesgesetz vom 18. März 2016 über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur). https://www.fedlex.admin.ch/eli/cc/2016/752/de.

Chapter 16
Hardware Security Module

Maria Sommerhalder

16.1 Introduction

This chapter provides an analysis of hardware security modules (HSMs). HSMs are specialized devices that perform cryptographic operations and store private-public key pairs and their associated secret values. They are widely used in various industries, such as banking, insurance, digital identity, and blockchain, to secure data. The chapter begins with defining HSMs and explaining their function and use in the cryptographic process. It also discusses trends in the use of HSMs until 2025, including the rise of cloud computing, double-key encryption, and the increasing demand for HSMs in the banking, financial services, and insurance industries. The chapter concludes by mentioning some of the key players in the global HSM market.

16.2 Analysis

Various industries use hardware security modules (HSMs) to secure data, including banking, insurance, digital identity, and blockchain applications. Their functions include key generation, key management, encryption, decryption, and hashing.

M. Sommerhalder (✉)
Eraneos Switzerland AG, Zurich, Switzerland
e-mail: Maria.Sommerhalder@eraneos.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_16

16.2.1 Definition

A vital component of the cryptographic process is collecting and storing private-public key pairs and their associated secret values. HSMs are typically used in critical infrastructure such as payment solutions, encryption systems on the Internet, and certificate management systems [1]. HSMs are specialized devices used to conduct cryptographic operations and use a random number source to generate public-private key pairs and subsequently store them. Most HSM systems are designed to store information on the device itself. However, some systems can back up secret values outside the HSM perimeter, such as on USB storage devices, hard disks, smart cards, or other digital media [2]. In addition to providing logical protection for keys, HSMs also provide physical protection. For example, some devices are equipped with tamper-proofing features such as logging and alerting mechanisms and more intrusive features such as wiping the entire contents when tampering is detected, making it inoperable [3]. In addition, HSMs have the advantage of isolating cryptographic processes from other operations, resulting in more efficient processing and additional security [3].

16.2.2 Trends

For over 20 years, HSMs have been used to protect cryptographic material in multiple applications [4]. However, a Ponemon Institute survey of 580 IT and security practitioners worldwide (55% from organizations with 1000 or more employees) found that HSMs are primarily used for key management or payment. A survey made in 2014 found that Organizations typically utilize 13 modules for key management, followed by eight for payment purposes [5].

The advent of cloud computing has increased the complexity of securing critical data. Data is now stored in the cloud: the percentage of corporate data stored in the cloud in organizations worldwide has doubled from 30% in 2015 to 60% by 2022 [6]. Many companies are concerned that their data will be unprotected from unauthorized access by the cloud provider or the US government in case of a subpoena, as most of the renowned cloud providers operate from the United States. As a result, double-key encryption has become increasingly popular, which encrypts data using two keys. A copy is stored on an HSM, and a copy is stored in the cloud. Before storing the data in the cloud, the owner of the data or the HSM vendor encrypts it so that the cloud provider cannot decrypt it. Parties can only access the data with both keys [7]. The use of double key encryption is widespread in highly regulated industries such as banking, health, and the public sector to comply with privacy and data protection laws [7].

Global payment markets are expanding, resulting in a higher demand for HSM machines to secure payment-related cryptographic operations. Many other factors are driving the growth of the HSM market, including the rise of cybersecurity

threats and the need for confidentiality in the banking, financial services, and insurance industries [8]. There is also an increase in demand for HSMs from other sources, such as the automotive industry, where they are used to enable secure communication, verify and authenticate software updates [9].

Several key players in the global HSM market include Gemalto, Inc., IBM Corporation, Ultra Electronics Group Holdings, Utimaco GmbH, Futurex L.P., Thales e-Security, Inc., Hewlett Packard Enterprise Development L.P., SWIFT C.S., and Yubico, Inc. [8].

In EPFL's School of Computer and Communication Sciences, there is a research domain entitled "Security and Privacy", which publishes papers on the topic [10]. The area of research involving the development of post-quantum hardware security modules is also present. The possibility of seeing some of them be available shortly, combined with embedded hardware accelerators, see Chap. 20 [11]. The area of combining Iot devices and Hardware Security modules is also explored. For example, the HSM can achieve the integrity of the key injection [12].

16.3 Consequences for Switzerland

Due to the political stability and the availability of skilled labor, a specialist ecosystem has developed in Switzerland, with many HSM providers having branch offices here and Swiss providers establishing themselves on the international stage. The Swiss branch of Securosys SA and the Swiss branch of Thales Suisse SA are examples of this.

16.3.1 Maturity

Due to the maturity of the HSM market, it is possible to find machines suitable for a wide range of applications. However, HSMs should be purchased from reputable vendors, preferably ones that have already been certified (see below).

16.3.2 Recommendation and Options

Three recommendations are presented in this section regarding the use of HSMs.

- Geo-redundant setup and Clustering

  HSMs must be stored in secure data centers, but even then, hardware failures, natural disasters, or human error can destroy an HSM. This would result in the irreversible loss of all key material. Typically, a company has two to three devices with the same build and data (i.e., replicated) located geographically. Therefore,

there must be operational failover procedures (switching operations to a backup recovery facility in case of primary system failure) between these devices [4].

- Key ceremony auditability

  Companies in regulated industries may be required to audit the generation of asymmetric key material [13]. The auditor must be able to obtain evidence of the entire process, including the hardware used, as well as verify the location and ownership of all key components during key generation and management. As a result, additional policies regarding access and change management must be prepared, as well as documents relating to the transport, storage, and management of keys, tokens, smart cards, and any related hardware. In light of the number of steps that could potentially compromise the private key, it is essential to have a solid runbook. The runbook describes the step-by-step process and the roles of all personnel involved in key generation. This ensures that auditors and all involved parties understand the process and serves as an audit trail [13].
- HSM Security Certification

  Generally, HSMs are certified following internationally recognized standards, such as FIPS-PUB 140-2 [3], 140-3 [14], or Common Criteria (CC) [15]. In addition, four security levels are defined by the FIPS certification [16]. An HSM certificate is issued only for the HSM device itself. It does not automatically guarantee secure keys since the operation of a key management system is equally critical to security. Regardless of certification, a system must address the single point of failure problem. It is a legal and compliance requirement that custodial services in the financial sector must be enforced to implement governance and policy regulation throughout the entire key lifecycle.

16.4 Conclusion

HSMs provide adequate cryptographic key protection throughout their lifecycles by enabling the secure generation of keys within an isolated hardware environment without revealing their identity. Furthermore, as HSMs can manage keys and enable users to manage keys, they provide significant security benefits to applications utilizing cryptography.

References

1. Norbert Pohlmann. Hardware-Sicherheitsmodule zum Schutz von sicherheitsrelevanten Informationen. page 5, 2012. Datenschutz und Datensicherheit.
2. William Mehuron. SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES. page 69, May 2001.
3. National Institute of Standards and Technology. Security Requirements for Cryptographic Modules. Technical Report Federal Information Processing Standard (FIPS) 140-2, U.S. Department of Commerce, December 2002.

4. Michael Suby. An Anchor of Trust in a Digital World: Risk Management Strategies for Digital Processes - Whitepaper. March 2020.
5. Ponemon Institute LLC. HSM Global Market Study. July 2014.
6. Statista. Share of corporate data stored in the cloud in organizations worldwide from 2015 to 2022. https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data/, March 2022.
7. Mustapha Hedabou. Cloud Key Management Based on Verifiable Secret Sharing. In Min Yang, Chao Chen, and Yang Liu, editors, *Network and System Security*, volume 13041, pages 289–303. Springer International Publishing, Cham, 2021. Series Title: Lecture Notes in Computer Science.
8. Bloomberg. Hardware Security Modules Market size worth $ 7.9 Billion, Globally, by 2028 at 12.4% CAGR: Verified Market Research. February 2022.
9. Claudius Pott, Philipp Jungklass, David Jacek Csejka, Thomas Eisenbarth, and Marco Siebert. Firmware Security Module: A Framework for Trusted Computing in Automotive Multiprocessors. *Journal of Hardware and Systems Security*, 5(2):103–113, June 2021.
10. EPFL. Security & Privacy. https://www.epfl.ch/schools/ic/research/security-privacy/, August 2022.
11. Wen Wang and Marc Stöttinger. Post-Quantum Secure Architectures for Automotive Hardware Secure Modules, 2020. Report Number: 026.
12. Simranjeet Sidhu, Bassam J. Mohd, and Thaier Hayajneh. Hardware Security in IoT Devices with Emphasis on Hardware Trojans. *Journal of Sensor and Actuator Networks*, 8(3):42, September 2019. Number: 3 Publisher: Multidisciplinary Digital Publishing Institute.
13. Capital Markets and Technology Association. Digital Assets Custody Standard. https://cmta.ch/content/77ea8b352579fd35f28e246cec6c4c46/cmta-digital-assets-custody-standard-v-12-final-october-2020-1.pdf, October 2020.
14. National Institute of Standards and Technology. Security requirements for cryptographic modules. Technical Report NIST FIPS 140-3, National Institute of Standards and Technology, Gaithersburg, MD, April 2019.
15. Common Criteria Portal. Certified Products. https://www.commoncriteriaportal.org/products/, August 2022.
16. NIST. FIPS General Information. https://www.nist.gov/itl/fips-general-information, May 2018.

Chapter 17
Secure Multi-Party Computation

Louis-Henri Merino and José Cabrero-Holgueras

17.1 Introduction

Secure Multi-Party Computation enables a group of parties to compute a function while jointly keeping their private inputs secret. The chapter discusses the definition of secure multi-party computation, its benefits and drawbacks, and its potential applications. It also discuss the trends in the field until 2025 and the challenges that need to be addressed for widespread adoption. Finally, the implementation possibilities for secure multi-party computation in Switzerland and the different deployment variations are discussed. The author provides recommendations for different markets and the need to consider deployment options.

17.2 Analysis

17.2.1 Definition

Secure Multi-Party Computation (MPC) enables a group of m mutually distrusting parties to jointly compute the outputs of a function $f(x_1, x_2, ..., x_m)$ where x_i is the ith party's private inputs without disclosing their private inputs [1]. The term "secure" indicates the latter property where the private inputs used for computation

L.-H. Merino (✉)
EPFL, Lausanne, Switzerland
e-mail: louis-henri.merino@epfl.ch

J. Cabrero-Holgueras
European Organization for Nuclear Research, Geneva, Switzerland
e-mail: jose@cabreroholgueras.com

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_17

are kept secret from all other parties. Some MPC protocols allow for auditable computation allowing any party, including a party who did not participate in the computation, to verify the correctness of the result [2, 3].

A significant benefit of using MPC is that many of the constructed MPC protocols are information-theoretically secure, avoiding many of the problems involved with using cryptographic hardness assumptions. However, using MPC comes at the cost of performance (several orders of magnitudes slower), primarily due to MPC's high bandwidth requirements. Nonetheless, specialized MPC protocols can significantly enhance performance compared to generic MPC protocols; one prominent example is private set intersection [4]. A drawback of information-theoretic MPC protocols in comparison to MPC protocols that rely on hardness assumptions that their security guarantees are violated in the presence of a dishonest majority [5].

One particular case of multi-party computation is private set intersection (PSI). In this case, each party has a set of items, and the goal is to learn the intersection of those sets while revealing nothing else about those sets [6].

17.2.2 Trends

Virtually all organizations could see benefits from utilizing MPC as it enables mutually distrustful parties to cooperatively compute the output of a function that they all agree on without revealing their input. These parties may be distinct. (e.g., different healthcare providers aiming to collaborate to improve patient care but do not want to disclose patient data) or the same (e.g., an organization aiming to protect sensitive information by splitting this information across its multiple data centers, where each data center is a party to the MPC protocol).

Some notable MPC use cases are secure auctions [7], privacy-preserving network security monitoring [8], spam filtering on encrypted emails [9] and secure machine learning [10]. Another notable MPC application is distributed authentication where MPC can strengthen an organization's key server by splitting the critical server's functionalities across multiple servers; an adversary capable of compromising one or a threshold of critical servers will not be able to reconstruct the organizations' keys. Please refer to Chap. 13 for additional information on multi-party threshold systems. Unfortunately, factors such as a steep learning curve, unfamiliar mathematical notions, and a rapidly growing and evolving environment prevent easy exploitation of the technology by programmers and end users. To reach a widespread adoption of MPC, these issues must be addressed [11]. Application Programming interfaces (APIs) for secure multiparty computations are a promising technology to overcome these challenges. Another one are compilers.

17.3 Consequences for Switzerland

17.3.1 Implementation Possibilities: Make or Buy

An MPC solution consists of two major disciplines (distributed systems & cryptography), each with its challenges and it would thus require extensive efforts to design and implement a homemade MPC solution. The author then recommends purchasing an existing MPC solution for all markets (military, civil society, and economy) Nevertheless, he recommends different deployments as discussed in Sect. 17.3.2.

17.3.2 Variations and Recommendation

There are three MPC deployment variations: on-premise, hybrid, and cloud. For the military and maybe for civil society, the preferable setup is on-premise to prevent distributing private inputs to the software provider. To achieve the promises of MPC, an on-premise setup should require two or more independent data centers where each data center is considered a party to the MPC protocol. For civil society and the economy, the likely preferable option is a hybrid setup where the client's IT infrastructure and the software provider's IT infrastructure are each a party to the MPC protocol. The bandwidth between these two parties could be significant but may save the client from compartmentalizing their IT infrastructure. Cloud deployment allows for the complete outsourcing of the MPC solution where it is operated only on the software provider's IT infrastructure. This cloud deployment is likely the least expensive option.

17.4 Conclusion

In conclusion, MPC enables a group of mutually distrusting parties to compute an agreed-upon function using their own private inputs without revealing their private inputs to other parties. MPC can be used to secure and enable privacy-preserving applications from privacy-preserving network security to secure machine learning. Given the complexity of designing and implementing MPC protocols, enlisting an MPC provider is preferable, but clients should have flexibility over the type of MPC deployment: on-premise, hybrid, and cloud.

References

1. David Evans, Vladimir Kolesnikov, and Mike Rosulek. A Pragmatic Introduction to Secure Multi-Party Computation. April 2020.
2. Carsten Baum, Ivan Damgård, and Claudio Orlandi. Publicly Auditable Secure Multi-Party Computation. In Michel Abdalla and Roberto De Prisco, editors, *Security and Cryptography for Networks*, pages 175–196, Cham, 2014. Springer International Publishing.
3. Sanket Kanjalkar, Ye Zhang, Shreyas Gandlur, and Andrew Miller. Publicly Auditable MPC-as-a-Service with succinct verification and universal setup. *arXiv:2107.04248 [cs]*, July 2021.
4. Vladimir Kolesnikov, Ranjit Kumaresan, Mike Rosulek, and Ni Trieu. Efficient Batched Oblivious PRF with Applications to Private Set Intersection. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, pages 818–829, New York, NY, USA, October 2016. Association for Computing Machinery.
5. Shai Halevi, Yuval Ishai, Eyal Kushilevitz, and Tal Rabin. Best Possible Information-Theoretic MPC. In *Theory of Cryptography: 16th International Conference, TCC 2018, Panaji, India, November 11–14, 2018, Proceedings, Part II*, pages 255–281, Berlin, Heidelberg, November 2018. Springer-Verlag.
6. CSRC Presentation: A Brief Overview of Private Set Intersection | CSRC. https://csrc.nist.gov/presentations/2021/a-brief-overview-of-private-set-intersection, April 2021. CSRC | NIST.
7. Peter Bogetoft, Dan Lund Christensen, Ivan Damgård, Martin Geisler, Thomas Jakobsen, Mikkel Krøigaard, Janus Dam Nielsen, Jesper Buus Nielsen, Kurt Nielsen, Jakob Pagter, Michael Schwartzbach, and Tomas Toft. Secure Multiparty Computation Goes Live. In Roger Dingledine and Philippe Golle, editors, *Financial Cryptography and Data Security*, pages 325–343, Berlin, Heidelberg, 2009. Springer.
8. Martin Burkhart, Mario Strasser, Dilip Many, and Xenofontas Dimitropoulos. SEPIA: Privacy-Preserving aggregation of Multi-Domain network events and statistics. In *19th USENIX Security Symposium (USENIX Security 10)*, Washington, DC, August 2010. USENIX Association.
9. Trinabh Gupta, Henrique Fingler, Lorenzo Alvisi, and Michael Walfish. Pretzel: Email encryption and provider-supplied functions are compatible. In *Proceedings of the Conference of the ACM Special Interest Group on Data Communication*, SIGCOMM '17, page 169–182, New York, NY, USA, 2017. Association for Computing Machinery.
10. Jian Liu, Mika Juuti, Yao Lu, and N. Asokan. Oblivious neural network predictions via minionn transformations. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, CCS '17, page 619–631, New York, NY, USA, 2017. Association for Computing Machinery.
11. José Cabrero-Holgueras and Sergio Pastrana. Sok: Privacy-preserving computation techniques for deep learning. *Proceedings on Privacy Enhancing Technologies*, 2021(4):139–162, 2021.

Part III
High-Level Applications

Chapter 18
Trusted Execution Environment

Maria Sommerhalder

18.1 Introduction

Trusted Execution Environments (TEEs) are secure areas of central processors or devices that execute code with higher security than the rest of the device. They provide confidentiality and integrity for sensitive data in all its states. TEEs are similar to hardware security modules but are a component of the typical chipset rather than a separate dedicated device. Moreover, TEEs aim to provide verifiable launch, run-time isolation, trusted input/output, and secure storage for TEE data. TEEs are widely used in mobile phones, cloud computing environments, and other embedded hardware platforms. Using TEEs in cloud environments enables companies to securely migrate sensitive data to the cloud. The regulation of TEEs will play an essential role in driving companies to adopt cloud computing, especially in highly regulated industries such as healthcare and banking.

18.2 Analysis

Trusted execution environments (TEEs) ensure the confidentiality and integrity of highly sensitive data in all its states (i.e., at rest, in transit, and use). Using TEE on-premises, in the cloud, or within embedded hardware platforms is possible. For example, smartphones and Internet of Things (IoT) devices used in automotive and healthcare applications often incorporate TEEs [1].

M. Sommerhalder (✉)
Eraneos Switzerland AG, Zurich, Switzerland
e-mail: Maria.Sommerhalder@eraneos.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_18

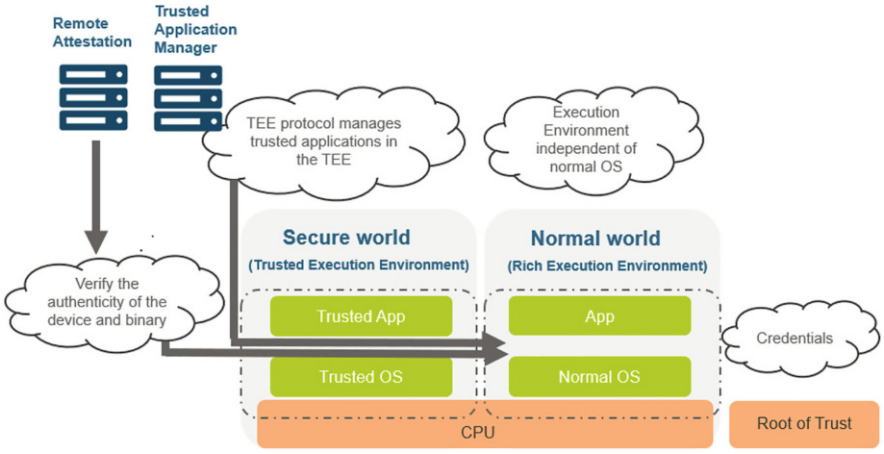

Fig. 18.1 Depiction of a TEE compared with a "normal" environment. The root of Trust and Remote Attestation is used to authenticate the device and the executed applications. The Trusted Application Manager is used to install applications, which can then be consumed in the TEE

18.2.1 Definition

TEEs are areas on a central processor or device that execute code with higher levels of security than the rest of the device. Security is provided by encrypted memory regions called enclaves. Because the environment is isolated from the rest of the device, it is not affected by infection or compromise of the device. The code or applications that run on the TEE are referred to as trusted applications (TAs) [2] (see Fig. 18.1).

In principle, TEEs are similar to hardware security modules (HSMs), which are dedicated devices that allow the creation of keys protected by hardware and perform everyday cryptographic operations such as encryption, decryption, and signing. It is a separate module that is connected to the main CPU and motherboard via a PCI bus or a network [3] (see HSM in Chap. 16). On the other hand, the TEE is a component of the typical chipset and does not require any additional hardware.

TEEs often vary in terms of their exact security goals. However, most of them aim to provide four high-level security protections. The first one is the verifiable launch of the execution environment for the sensitive code and data so that a remote entity can assure that it was set up correctly. The second is the run-time isolation to protect the confidentiality and integrity of sensitive code and data. The third is the trusted IO to enable secure access to peripherals and accelerators. The fourth one is the secure storage for TEE data that must be stored persistently and made available only to authorized entities at a later time [4].

18.2.2 Trends

18.2.2.1 Application on Mobile Phones

The mobile phone is capable of downloading and using a wide variety of applications. As a result of this increased complexity of code bases running on mobile operating systems, vulnerabilities and compromises are more likely to be exploited. Malicious code from one application can access information from another application and leak the information. Using TEEs, application space can be separated from each other, and sensitive applications can be restricted to running within the TEE. Data that requires high levels of security can be designated to be stored and processed exclusively within the TEE and nowhere else [1]. In most modern smartphones and tablets, the ARM TrustZone implements a TEE [5].

18.2.2.2 Security in Cloud Data Processing

The use of hardware-based TEEs within cloud environments is referred to as "confidential computing" by various vendors, including AMD, Intel, and ARM, and on various platforms, including Microsoft Azure or Internet of Things applications [2, 6]. TEEs have historically stored small amounts of data, such as passwords or encryption keys. Nowadays, they are available on a larger scale in cloud environments and can therefore be offered as part of secure database services that allow data only to be decrypted in the TEE of the respective servers. In other words, the data is encrypted both in transit and at rest. Even though it is not encrypted during use, it is still protected since it can only be used within the isolated enclave [7]. Using TEEs in cloud environments enables companies to migrate highly sensitive data to the cloud. According to an exploratory study [8], understanding the regulatory impact of TEEs is essential in driving companies' cloud adoption, especially in industries such as healthcare, life sciences, and banking that are more conservative and slow to adapt.

18.2.2.3 Data Protection Laws

Today's computer and mobile systems are becoming increasingly complex, hosting a variety of untrusted software components, such as multiple applications interacting with user data on a single smartphone or multiple tenants sharing a single cloud platform [4]. Thus, systems must protect sensitive data from unauthorized access over networks and physical attacks. In addition to storing encryption keys [9], TEE is capable of isolating private data, such as contacts, messages, photos, or sensitive data, such as credentials, passwords, or medical information. In the event of a loss, theft, or malware infection, data is not exposed [10].

18.2.2.4 Cryptocurrency Usage

TEEs are used to protect cryptocurrency wallets. One example is the ARM TrustZone-based Secure Blockchain Lightweight Wallet (SBLWT) [11]. In SBLWT, the private key associated with the digital assets is isolated. By using this method, retail investors can replace the common practice of backing up private keys on paper or insecurely storing them in the cloud [12].

18.2.2.5 Demand

Currently, hardware tokens are used in many aspects of our lives, including one-time tokens for multi-factor authentication and tokens for opening cars or buildings. In the future, TEEs in our mobile phones may replace these, improving the user experience and reducing the costs for service providers [1]. With the many possible applications of TEEs in mobile phones, it can be inferred that demand for such devices will increase. As of 2021, almost 15 billion mobile devices were operating worldwide. The previous year, just over 14 billion mobile devices were operating worldwide. By 2025, the number of mobile devices is expected to reach 18 billion. The demand for TEE systems is likely to increase as these devices become increasingly available and related apps become increasingly popular on a global scale [13].

18.2.2.6 Actors

There are many key players in the global TEE market, including IBM Corporation, Intel Corporation, Fortanix, Inc., Alibaba Group Holdings, Microsoft Corporation, Advanced Micro Devices, Inc., and Edgeless Systems GmbH. Securosys SA, CYSEC SA, Legic Identsystems SA, and Fortinet Switzerland GmbH are the market leaders in the Swiss market.

18.2.2.7 Research

The Secure & Trustworthy Systems Group at ETH Zurich has released an Open Framework for Architecting Trusted Execution Environments as a reference for creating large systems [14, 15]. On the other hand, Zurich University of Applied Sciences (ZHAW) is focused on developing privacy-preserving applications of TEE [16].

The Linux Foundation's Confidential Computing Consortium is a community dedicated to defining and accelerating the adoption of confidential computing [17]. TEE Committee members are members of GlobalPlatform [18]. The project aims to define an open security architecture for consumers and connected devices using a TEE and to enable the development and deployment of services by multiple service

providers. In particular, they address API specifications and security evaluation frameworks [19].

18.3 Consequences for Switzerland

Swiss providers have established themselves internationally due to the country's stability and availability of skilled labor. Many TEE providers have branch offices here, and Swiss providers have established themselves in other countries. Examples include Securosys SA, Global Platform Services GmbH, and CYSEC SA.

18.3.1 Maturity

As noted above, most mobile phones are equipped with TEE functionality [1]. Furthermore, TEE has achieved a high level of maturity due to the almost 15 billion mobile phones in circulation [13].

18.3.1.1 Recommendations and Options

- Open-source hardware security
  Hardware vulnerabilities are a real threat, which has been exploited most recently in 2018, when it was revealed that a wide range of attacks might be possible, including Foreshadow, Spectre, and Meltdown. As these vulnerabilities affected closed-source hardware, open-source projects aim to close these vulnerabilities by making their code base available to a variety of specialists [20–22].
- Potential security and/or trust issues
  Cerdeira et al. [23] studied the vulnerabilities and limitations affecting existing TrustZone-assisted TEE systems. They found three different categories of issues:
  - Critical implementation bugs
    There are continuous bugs found in trusted applications as well as trusted OS.
  - Architectural deficiencies
    TEEs have large attack surfaces due to the lack of standard protection mechanisms generally found in modern OSes.
  - Overlooked hardware properties
    In most TrustZone systems, there are overlooked properties on the architectural and microarchitectural levels that can be exploited and/or used to exfiltrate sensitive data.

- Lack of standards

  The development of TEE has been siloed by a small number of companies, which has led to the need for well-established standards. Unfortunately, this resulted in proprietary designs (SGX, SEV, TrustZone) with interoperability issues. However, a few research groups are committed to developing industry standards (see research section above).

18.4 Conclusion

With TEE, sensitive data is protected in an isolated enclave, and other applications are prevented from accessing the reserved memory enclave. Furthermore, since TEEs are part of a standard chipset, this inexpensive technology can be leveraged across many devices, resulting in increased security, especially in the mobile sector and IoT products.

References

1. Jan-Erik Ekberg, Kari Kostiainen, and N. Asokan. The Untapped Potential of Trusted Execution Environments on Mobile Devices. *IEEE Security & Privacy*, 12(4):29–37, July 2014.
2. Victor Costan and Srinivas Devadas. Intel SGX Explained. https://eprint.iacr.org/2016/086, 2016. Published: Cryptology ePrint Archive, Paper 2016/086.
3. A. M. Parker. HSMs and Key Management: Effective Key Security. https://www.cryptomathic.com/news-events/blog/hsms-and-key-management-effective-key-security, August 2022.
4. Moritz Schneider, Ramya Jayaram Masti, Shweta Shinde, Srdjan Capkun, and Ronald Perez. SoK: Hardware-supported Trusted Execution Environments. 2022. Publisher: arXiv Version Number: 1.
5. ARM. ARM Security Technology Building a Secure System using TrustZone Technology. https://developer.arm.com/documentation/PRD29-GENC-009492/c/?lang=en, April 2009.
6. Christian Priebe. Protecting applications using trusted execution environments. April 2020. Publisher: Imperial College London.
7. Arseny Kurnikov. *Trusted Execution Environments in Cloud Computing*. Doctoral thesis, School of Science, 2021. ISBN: 978-952-64-0619-0 (electronic), 978-952-64-0618-3 (printed) ISSN: 1799-4942 (electronic), 1799-4934 (printed), 1799-4934 (ISSN-L) Series: Aalto University publication series DOCTORAL DISSERTATIONS; 171/2021.
8. Tim Geppert, Jan Anderegg, Leoncio Frei, Simon Moeller, Stefan Deml, David Sturzenegger, and Nico Ebert. Overcoming Cloud Concerns with Trusted Execution Environments? Exploring the Organizational Perception of a Novel Security Technology in Regulated Swiss Companies. 2022.
9. Kalmer Keerup, Dan Bogdanov, Baldur Kubo, and Per Gunnar Auran. Privacy-Preserving Analytics, Processing and Data Management. In Caj Södergård, Tomas Mildorf, Ephrem Habyarimana, Arne J. Berre, Jose A. Fernandes, and Christian Zinke-Wehlmann, editors, *Big Data in Bioeconomy*, pages 157–168. Springer International Publishing, Cham, 2021.
10. GlobalPlatform. The Trusted Execution Environment: Delivering Enhanced Security at a Lower Cost to the Mobile Market. https://globalplatform.org/wp-content/uploads/2018/04/GlobalPlatform_TEE_Whitepaper_2015.pdf, 2015.

11. Weiqi Dai, Jun Deng, Qinyuan Wang, Changze Cui, Deqing Zou, and Hai Jin. SBLWT: A Secure Blockchain Lightweight Wallet Based on Trustzone. *IEEE Access*, 6:40638–40648, 2018.
12. Karanjai Rabimba, Shi Weidong, Xu Lei, Chen Lin, Zhang Fengwei, and Gao Zhimin. Lessons Learned from Blockchain Applications of Trusted Execution Environments and Implications for Future Research. In *Workshop on Hardware and Architectural Support for Security and Privacy*, pages 1–8, Virtual CT USA, October 2021. ACM.
13. S. O'Dea. Forecast number of mobile devices worldwide from 2020 to 2025 (in billions)*. Technical report, Statista, September 2021.
14. ETH Zurich. Research. https://sectrs.ethz.ch/research.html, August 2022.
15. Dayeol Lee, David Kohlbrenner, Shweta Shinde, Krste Asanović, and Dawn Song. Keystone: an open framework for architecting trusted execution environments. In *Proceedings of the Fifteenth European Conference on Computer Systems*, pages 1–16, Heraklion Greece, April 2020. ACM.
16. ZHAW. Privacy-preserving confidential computing with trusted execution environments. https://www.zhaw.ch/en/research/research-database/project-detailview/projektid/3698/, August 2022.
17. The Linux Foundationő. What is the Confidential Computing Consortium? https://confidentialcomputing.io/, August 2022.
18. GlobalPlatform, Inc. GlobalPlatform, Inc. https://globalplatform.org/.
19. GlobalPlatform. Trusted Execution Environment (TEE) Committee. https://globalplatform.org/technical-committees/trusted-execution-environment-tee-committee/.
20. Jo Van Bulck, Marina Minkin, Ofir Weisse, Daniel Genkin, Baris Kasikci, Frank Piessens, Mark Silberstein, Thomas F. Wenisch, Yuval Yarom, and Raoul Strackx. Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution. In *27th USENIX Security Symposium (USENIX Security 18)*, pages 991–1008, Baltimore, MD, August 2018. USENIX Association.
21. Paul Kocher, Jann Horn, Anders Fogh, and Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, and Yuval Yarom. Spectre Attacks: Exploiting Speculative Execution. In *40th IEEE Symposium on Security and Privacy (S&P'19)*, 2019.
22. Moritz Lipp, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Anders Fogh, Jann Horn, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, and Mike Hamburg. Meltdown: Reading Kernel Memory from User Space. In *27th USENIX Security Symposium (USENIX Security 18)*, 2018.
23. David Cerdeira, Nuno Santos, Pedro Fonseca, and Sandro Pinto. Sok: Understanding the prevailing security vulnerabilities in trustzone-assisted tee systems. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 1416–1432, 2020.

Chapter 19
Confidential Computing

Yacine Felk

19.1 Introduction

Confidential computing protects data during processing by performing computations in a Trusted Execution Environment (TEE) and/or through Secure Multi-Party Computation. The goal is to encrypt data in the system's main memory without sacrificing performance. There are two approaches to protect the data in memory: full system memory encryption and individual virtual machine (VM) memory encryption, isolated from the hypervisor. This protects data from cold boot and physical attacks and attacks originating from other VMs or the hypervisor. CPU providers, such as AMD, Intel, and Arm, offer confidential computing technology, and it can be applied anywhere, including public and private clouds, edge deployments, and user devices. Encryption is the most common technique, but other solutions are also possible.

19.2 Analysis

In classical computing, data exists in three states: in transit, at rest, and in use. Data traversing the network is "in transit," data in storage is "at rest," and data being processed is "in use." In a world where we are constantly storing, consuming, and sharing sensitive data—from credit card data to medical records, from firewall configurations to our geolocation data—protecting sensitive data in all of its states is more critical than ever. While techniques to protect data in transit and at rest are

Y. Felk (✉)
CYSEC, Lausanne, Switzerland
e-mail: yacine.felk@cysec.com

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_19

now commonly deployed, the third state - protecting data in use—is the new frontier being addressed by the Confidential Computing Consortium [1].

19.2.1 Definition

Confidential computing protects data in use by performing the computation in a hardware-based Trusted Execution Environment (see Chap. 18). It may also use the Secure Multi-Party Computation (see Chap. 17) technology for some of its tasks. The goal of confidential computing technology is to encrypt data in use in the main memory of the system without compromising performance. There are two aspects to protecting the data in memory:

- Encrypting full system memory
- Encrypting individual virtual machine (VM) memory and isolating the VM memory from the hypervisor (hypervisor is a type of computer software, firmware, or hardware that creates and runs virtual machines)

Whole system memory encryption helps defend data against cold boot and physical attacks. Encrypting individual VM memory helps defend data against attacks that originate in other VMs on the same physical host and from the hypervisor itself. Encrypting individual VM memory and isolating it from the hypervisor is critical in today's highly virtualized, multi-tenant environment. There are many CPU providers with confidential computing technology; among them, AMD (including SEV and its derivatives such as SEV-SNP), Intel SGX or TDX, and Arm (with its Trust zone enclave), to name a few. The definition is not limited to "cloud" uses but can be applied anywhere, including public cloud servers, on-premises servers, gateways, IoT devices, Edge deployments, user devices, etc. It is also not limited to such trusted execution being done by any particular processor since trusted processing might be in various places, such as a GPU or a network interface card. Neither is it limited to encryption solutions, though this is the most common technique employed.

19.2.2 Trends

Although the adoption of confidential computing is nascent, its potential is tremendous, not only for the enterprises consuming it but also for the technology and service providers enabling it. The Total Addressable Market (TAM) for confidential computing in 2021 is 1.9–2.0 billion US Dollars, with expected growth at a compound annual growth rate (CAGR) of 90–95% in the best-case scenario, and 40–45% in the worst-case scenario through 2026. Exponential increases in cyber risks, regulations, and avenues for incremental revenue position confidential computing for hyper-growth. Regulated industries like banking, finance, insurance, healthcare,

life sciences, the public sector, and defense will drive over 75% of demand [2]. Awareness of the benefits of confidential computing and willingness to invest in exploration is expected to double across crucial regulated industries through 2026.

One can wonder about the drivers for use cases in confidential computing. Confidential computing encompasses different use cases across many critical industries, to name a few:

- Cloud Key Management Services (KMS).
- Improve application security on the public cloud and prevent data compromise from malicious actors.
- Scalable replacement for dedicated Hardware Security Modules (HSMs).
- Sharing sensitive data with third parties for analytics and other multi-party computing scenarios.
- Smart Contracts and Blockchain.
- Secure data during AI/ML modeling.
- Secure the intellectual property and data generated or utilized in edge and IoT devices from malicious elements.

19.3 Consequences for Switzerland

In 2020, the Federal Council established Switzerland's strategy for Public Cloud and elaborated an analysis of its impacts on public and administrative data governance and protection [3]. Interestingly, the conclusions emphasize the importance of hyperscalers (such as GCP, AWS, Oracle, Alibaba, etc.) infrastructure exploitation to guarantee reliable and resilient services. This can only be done with the exploitation of confidential computing technologies, ensuring that the application deployment environment is isolated from the infrastructure provider environment, thus ensuring data confidentiality and integrity. When looking at confidential computing consortium members, three players are Swiss-based:

- Swisscom: national telco operator providing the IT infrastructure.
- Decentriq: providing trusted collaboration application exploiting technologies
- CYSEC: providing a complete set of confidential computing software creating secure private environments and enabling to turn of Public Cloud into Private Clouds for any application or workload.

19.3.1 Implementation Possibilities: Make or Buy

Competitors of the three Swiss companies mentioned above are insistent with their state-owned organizations and delegations. To mention two actual examples:

- In March 2022, Fortanix announced the adoption of its Data Security Manager (DSM) platform by federal agencies to safeguard sensitive data and mitigate

future cyberattacks. Fortanix's DSM platform uses confidential computing to help government agencies protect data and IP within Trusted Execution Environments and provide them the ability to move and process encrypted data in cloud environments [4].

- In February 2022, Anjuna announced that Israel's Ministry of Defense (MOD) has entered into the public cloud for the first time with Anjuna's software, which offers the most robust data security available. With Anjuna Confidential Cloud software, the MOD can leverage confidential computing features available in cloud servers that eliminate exposure of data in use to insiders, malicious software, and bad actors. In addition, sensitive data and applications remain fully encrypted with Anjuna—without any software modifications—and stay isolated and in complete control of the MOD [5].

This section presents the pros and cons of buying or making confidential computing technologies. For confidential computing, Make is interpreted as exploiting Swiss-based solutions enabling the protection of Data in use. In contrast, Buy is interpreted as using a foreign solution enabling to turn Public clouds into Private ones (Table 19.1).

Table 19.1 Implementation possibilities for different sectors

	Swiss Solutions		**Foreign Solutions**	
	Pros	Cons	Pros	Cons
Military	More secure against partner attacks and control	May rely on small actors and start-ups	Easy integration with other armies and international organizations	System might malfunction and transfer trusted layer to foreign entities (companies or governments)
Civil Society	Added value and Trust to critical services running on Hyperscalers and Public Cloud	Difficult to interact with others or ensure that it is easily implemented	Exchange with a larger group of people	More expensive and increased risk of attacks
Economy	More innovation and know-how and Strengthening of cybersecurity skills	Less dependency on foreign providers	Innovation through external actors (might enhance international collaborations)	Need to assess the maturity of foreign solutions

19.4 Conclusion

Given the broad applicability of confidential computing, enterprises are starting to experiment with the technologies for their use cases. This also helps to understand potential areas of adoption. For the military, one of the most exciting problems to solve with confidential computing is the data integrity and code integrity problem.

In civil society, confidential computing currently benefits several critical parts of the economy (enabling compliance with privacy and security regulations), primarily banks, and some parts of critical infrastructure, which can take advantage of this technology by providing new services/business while exploiting hyper scalers infrastructure. Nevertheless, the maturity of technical solutions must still be deployed at scale.

References

1. Confidential Computing Consortium - Open Source Community. https://confidentialcomputing.io/, August 2022.
2. Confidential computing TAM by segment 2021-2026. https://www.statista.com/statistics/1290939/confidential-computing-tam-share-technology-segment/, February 2023.
3. Federal Chancellery FCh. SB020 - federal cloud strategy. https://www.bk.admin.ch/bk/en/home/digitale-transformation-ikt-lenkung/ikt-vorgaben/strategien-teilstrategien/sb020-cloud-strategie_der_bundesverwaltung.html, August 2022.
4. Fortanix Helps Federal Clients Protect Data With Integrated Security Platform; Ambuj Kumar Quoted - ExecutiveBiz. https://blog.executivebiz.com/2022/03/fortanix-announces-federal-adoption-of-data-security-platform/, March 2022.
5. ZDNet: Why Israel's Ministry of Defense is Moving to the Public Cloud. https://www.anjuna.io/in-the-news/why-israeli-ministry-of-defense-is-moving-to-the-public-cloud, August 2022.

Chapter 20
Hardware Acceleration

Dina Mahmoud

20.1 Introduction

With Moore's law and Dennard's scaling no longer fueling the improvement in computing performance, new avenues for increasing performance are needed. Hardware acceleration is one avenue where many researchers and industrial parties work and invest. This is because accelerators can allow for high levels of parallelism not supported by general-purpose central processing units. These high levels of parallelism are particularly well-suited for many modern applications. Therefore, research on and use of hardware acceleration is expected to continue soon. However, various parties should consider various aspects when deciding whether to invest in hardware acceleration by making their accelerators or buying them from a third party. This factsheet presents an analysis of hardware acceleration and the trends until 2025. It also discusses the aspects to consider and how specific considerations are more important for some actors.

20.2 Analysis

With the slowdown of Moore's law, system developers are examining potential avenues for performance improvement of computing systems. As simply increasing the frequency or the number of transistors on the chip is no longer feasible, IT infrastructure operators have adopted hardware acceleration. Various platforms and levels of hardware acceleration exist.

D. Mahmoud (✉)
EPFL, Lausanne, Switzerland
e-mail: dina.mahmoud@epfl.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_20

20.2.1 Definition

Hardware acceleration is the use of specialized hardware within a computing system designed to handle specific tasks in an optimized way [1]. Central processing units (CPUs) are typically responsible for most tasks within a computing system. However, tasks requiring high levels of parallelism do not run efficiently on general-purpose CPUs. Moreover, many tasks need to be run, and if one of them is slower than the rest, it can affect the system's performance. This is where hardware acceleration comes in. When a task possesses properties making its execution on a CPU suboptimal, system designers include specialized hardware in the system to which the task is offloaded. Graphics processing units (GPUs) are among the most famous hardware accelerators designed for rendering graphics. Their support for parallelism has also made them suitable for other tasks, including machine learning acceleration [2]. To avoid long execution times due to the sequential nature of CPUs and to avoid software-based exploits, cryptographic algorithms are also among the notable applications benefiting from hardware acceleration [3]. Other examples of hardware accelerators include application-specific integrated circuits (ASICs), which can implement specialized cryptographic accelerators on modern systems-on-chip (SoCs), and field-programmable gate arrays (FPGAs).

20.2.2 Trends

There has been a steady growth in research on hardware acceleration (as shown in Fig. 20.1) and in the adoption of specialized hardware. For instance, specialized accelerators like the Apple Neural Engine are making their way into consumer

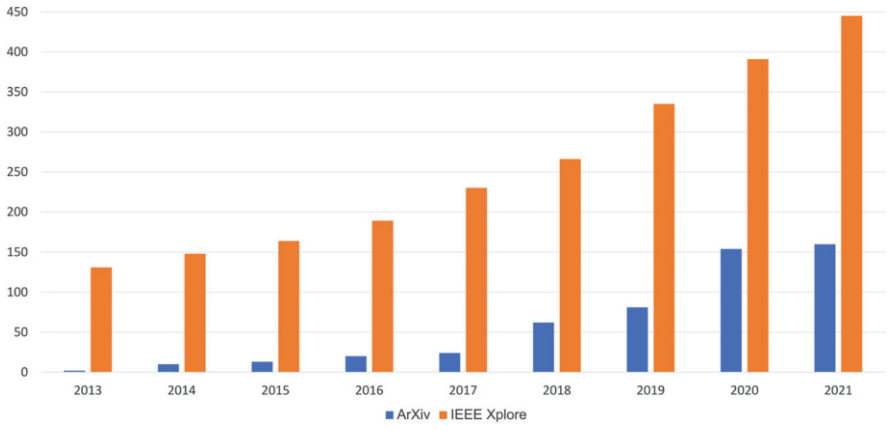

Fig. 20.1 Describes arXiv and IEEE Xplore publications containing the keywords "Hardware acceleration" OR "Hardware accelerator"

electronics [4]. ARM also offers security algorithm accelerators to support the Armv8-A cryptography extensions [5]. Due to the inability of CPUs to meet the increasing computing demand, the use of specialized hardware is expected to keep increasing until 2025. The increased interest in using hardware accelerators has also increased the research on their security in terms of attacks and countermeasures.

20.3 Consequences for Switzerland

Hardware acceleration is helpful for more efficient computing. Nevertheless, there are many considerations when investing in a hardware accelerator, especially when using it for security. If the specialized computing core is to be highly utilized, it is helpful to invest in it [2]. This is a likely case for a cryptographic accelerator in a system that encrypts and decrypts all outgoing and incoming data, for example. However, one needs to consider that the security of hardware accelerators may be questionable. Hardware Trojans, fault injection attacks, and side-channel attacks are significant threats to hardware cryptographic accelerators.

20.3.1 Implementation Possibilities: Make or Buy

This section presents the pros and cons of buying or making secure hardware accelerators (Table 20.1).

Depending on the type of hardware accelerator, many risks and opportunities are associated with making or buying it. Making the hardware accelerator from scratch gives higher security guarantees as there is no possibility for third-party-implanted hardware Trojans. Furthermore, specific countermeasures can be implemented to protect against various exploits, such as redundancy, masking, and hiding. However, there is significant engineering effort in building a correct, highly performant, secure hardware accelerator. If not correctly designed and built, bugs can result in misbehavior, reducing the system's performance or reliability. Furthermore, the interoperability of hardware accelerators with other components in the system is a critical aspect to consider. Buying accelerators usually guarantees that they will have standard interfaces, but it is possible to design a specialized core with standard interfaces.

For specialized military applications, where security is of the utmost concern, and if accelerators are unlikely to already be in existence, making the accelerators is better. Making the hardware eliminates the possibility of hardware Trojans, but not of bugs in the design nor potential leakage of information. Coupled with proper testing (for security and reliability), making the accelerator would guarantee secure and reliable hardware. If the accelerator can be bought, design effort can be saved, but guaranteeing the security would come at the cost of extensive security testing to guarantee that there are no (intentional or unintentional) backdoors. Making

Table 20.1 Implementation possibilities for different sectors

	Make		**Buy**	
	Pros	Cons	Pros	Cons
Military	No hardware Trojans/More specialized hardware	Potential error in implementation adding attack surface	Reuse available tested accelerators, no design effort and accelerator interoperable with other platforms	Might contain accidental or purposeful backdoors and increased need for security testing
Civil Society	None	None	Accelerator interoperable with other platforms, reuse available tested accelerators	Potential security vulnerabilities
Economy	Sell for profit	Liability in case the accelerator has an error or a security vulnerability	Faster development of products	Less advantage over competition features and extensions are needed to innovate

accelerators that target widely used applications can have a significant economic benefit for businesses. Such accelerators can be sold to many parties resulting in high profits. For example, many hardware accelerator designs can be bought and used on Amazon Web Services Marketplace [6]. However, this is only the case for widely used applications. For more specialized accelerators, making them may still prove helpful to the business if the accelerator significantly improves their workloads' performance. However, there may be no direct profit from selling the accelerators. Buying pre-existing accelerators will allow for faster end-product development if the business entity is not accustomed to building hardware. For the remaining actors, buying the accelerators is a good solution. Again, some testing would need to be done to guarantee a minimum level of security for the purchased hardware.

20.3.2 Variations and Recommendation

Hardware accelerators have varying levels of specialization (and flexibility). They can also be integrated using a variety of methods in existing systems. The choice of which variation to opt for depends on the application and the actor looking to use the

specialized hardware. The highest level of specialization is achievable when using application-specific integrated circuits (ASICs). However, this translates to higher costs in engineering efforts and reduced flexibility. Field programmable gate arrays (FPGAs) require less effort to design the accelerator and offer more flexibility at the price of remaining within the constraints of the FPGA resources and slightly reduced performance. Finally, graphics processing units (GPUs) offer high flexibility and parallelism. However, they are not as customizable to the application as FPGAs and ASICs and can therefore have lower performance. If the application for which the custom hardware is being purchased will be fully utilizing the hardware, and one in which performance is of the utmost importance, then an ASIC is the best choice. The lower the utilization is expected to be, the better it is to opt for a more flexible option.

Deploying any chosen accelerator still requires considering its security. With attacks constantly being demonstrated against ASIC-, FPGA-, and GPU-based accelerators, designs should be appropriately secured before deployment. The main security risks arise if the device is physically accessible to a remote party. However, software access can also be leveraged for a variety of exploits. According to the deployment model of the device and the desired security level, various protection mechanisms (e.g., redundancy, radiation-hardening, leakage detection) can be implemented.

20.4 Conclusion

The use of specialized hardware to accelerate applications not performing well on modern CPUs will likely continue in the coming years. Consequently, they are likely to be used by all actors in various applications. For example, we already see many hardware accelerators for cryptographic applications and security. Each actor needs to decide on the variation of customized hardware to invest in based on the expected usage and the application. Furthermore, security should be essential when designing or buying the hardware accelerator. The tradeoff between security and design cost must be studied to decide whether to make or buy the accelerator and the amount of testing necessary to guarantee the desired level of security and reliability.

References

1. Wen-mei Hwu and Sanjay Patel. Accelerator Architectures – A Ten-Year Retrospective. *IEEE Micro*, 38(6):56–62, November 2018. Conference Name: IEEE Micro.
2. IRDS™ 2021: Executive Summary - IEEE IRDS™. https://irds.ieee.org/editions/2021/executive-summary, August 2022.
3. Mohamed Gafsi, Mohamed Ali Hajjaji, Jihene Malek, and Abdellatif Mtibaa. FPGA hardware acceleration of an improved chaos-based cryptosystem for real-time image encryption and decryption. *Journal of Ambient Intelligence and Humanized Computing*, October 2021.

4. Apple unleashes M1, November 2020. Apple Newsroom.
5. Arm Ltd. Security algorithm accelerators. https://developer.arm.com/downloads/-/security-algorithm-accelerators.
6. AWS Marketplace: Homepage. https://aws.amazon.com/marketplace, August 2022.

Chapter 21
Secure Operating System

Llorenç Romá and Bernard Tellenbach

21.1 Introduction

The operating system (OS) is the backbone of every modern computer system, managing the system's resources and executing applications. Its security is critical as a vulnerability in the OS or any applications running on it can expose the entire system to risk. Different types of OS can be considered security-wise: (1) security-focused OS and (2) security-evaluated OS. A security-focused OS aims to provide a higher level of security by protecting the rest of the system from modules that an attacker might exploit. In contrast, a security-evaluated OS is certified by an external security-auditing organization. Hardening measures will vary as different use cases have different requirements for a secure OS. In addition, different technologies are used to complement the security provided by the OS. The trend for secure OSes is, among others, the use in container-focused OSes and intelligent vehicles where digital features are increasing, as well as in mobile phones.

21.2 Analysis

21.2.1 Definition

Every modern computer system runs a core piece of software executed on top of the hardware. This software is the operating system (OS). It is responsible for allocating the primary resources of the system (e.g., CPU, memory, communication ports) and

L. Romá (✉) · B. Tellenbach
Cyber-Defence Campus, Thun, Switzerland
e-mail: llorenc.roma@ar.admin.ch; bernhard.tellenbach@ar.admin.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_21

supervising the execution of all the applications within the system. Given the crucial role of the OS, its security (or the lack of security) might have a significant impact on the whole system: a vulnerability in the OS, or any applications running in it, exposes a danger to all the other applications running in the system as well as to all the data stored in it. This situation becomes highly problematic when the system stores important (confidential) data or runs critical applications in high-risk facilities (e.g., satellite communications, power plants, banking systems, aircraft systems, and SCADA systems). Therefore, it is essential to improve OS security to ensure data integrity, confidentiality and availability.

When discussing secure operating systems, we generally refer to (1) security-focused OS and (2) security-evaluated OS. In any case, such operating systems are designed to provide a higher level of security.

(1) Security-Focused OS

A security-focused operating system should guarantee the secure or trusted execution of components that might not be secure (programs). That is, the OS should protect the rest of the system from modules that an attacker might exploit to get control of the system, for instance, using sandboxing, compartmentalization or by isolating cryptography functions and key management. QubeOS is one such OS, which is especially valuable in industries where sensitive data has to be securely segregated. Other examples include Tails OS and ReactOS.

In addition, to provide an extra level of security at different layers, OSes may leverage other software and hardware technologies and mechanisms, described in more detail in other chapters, such as Secure Boot, Trusted Platform Modules (TPM), Hardware Security Modules (HSM), disk encryption, network protection and other security-related features such as access control lists (ACLs), event auditing.

One example of such hardware-based technology is HSM (Chap. 16). An HSM can improve the security of an operating system by providing secure storage for cryptographic keys and other sensitive data, such as passwords and certificates. This makes it much more difficult for attackers to access the keys and other sensitive data, even if they have successfully compromised the operating system or other software on the computer. In addition, an HSM can also perform cryptographic operations, such as encryption, decryption, and signing. By offloading these operations to the HSM, the operating system can reduce its exposure to security threats, as the keys and sensitive data are not accessible to the operating system or other software.

Similarly to an HSM, a Trusted Execution Environment, or TEE (Chap. 18) is a secure area of a computing device, typically implemented on the chip itself, that provides a secure environment for executing sensitive operations. The TEE is also used to provide secure storage for cryptographic keys and other sensitive data, such as passwords and certificates, which would protect such assets in a scenario where the OS is compromised. For example, iOS uses a dedicated, isolated and hardware-backed subsystem called secure enclave to isolate important cryptographic tasks. And on Android smartphones, it depends on the manufacturer of the smartphone

whether and which type of TEE is present (e.g., Google Pixel smartphones contain the Titan M chip for this purpose).

An example of a software-based solution that improves the security of an operating system is SELinux [1]: a security feature built into the Linux operating system that provides enhanced security through the use of mandatory access control (MAC) policies. SELinux defines access control policies that restrict processes and users' actions on files, processes, and network resources. The policies are implemented in software and are enforced by the Linux kernel

(2) Security-Evaluated OS

A security-evaluated OS is an OS that has achieved certification from an external security-auditing organization. However, they still need to implement more security mechanisms to make certain system areas more secure (e.g., cryptographic modules, fine-grained access control) according to the criteria. Some of the most popular evaluation criteria are Common Criteria [2], FIPS 140-2 [3], and ITSEC [4]. Examples of such OSs are SUSE Linux or some Red Hat Linux Enterprise versions, Windows 10 Enterprise, etc.

Even though a baseline exists for achieving a minimum level of security, the ultimate set of requirements to make a secure OS depends on the specific use case. For instance, a mobile OS has different requirements than a container-focused OS. Therefore, different measures can be taken to harden the underneath operating system for each specific use case.

21.2.2 Trends

One envisioned trend of secure OSes is their use in container-focused OSes. Over the last five years, many enterprises have moved their primary business activities and deployed their applications in container environments. However, those environments present particular risks since multiple applications/services run on containers on the underlying OS, sharing the same set of resources. Therefore, if an attacker manages to compromise the host OS, the rest of the system could be affected. For instance, they disrupt the applications running on the top or steal critical business information. On the other hand, if an attacker compromises an application running inside a container, he/she could try to escape the container and gain access to the host OS and/or pivot to other containers, achieving the same results as in the previous example. With that in mind, it seems reasonable that a container-focused OS might also be security-focused, including features such as those mentioned in Sect. 21.2.1. That is why recently, the first standards on container security are emerging [5]. Examples of well-known container-focused OSes are FlatCar Container Linux [6] or Bottlerocket [7]. However, those are not considered secure OSes since some of the features mentioned in previous sections are not implemented. Another example of such an OS that focuses on security is ARCA OS, from CySec [8], a Swiss startup launched in 2018 in Lausanne, EPFL.

Another trend comes with the increasing development of intelligent vehicles. Modern vehicle industries (i.e., automotive, aeronautic) deploy more and more digital features; therefore, the attack surface widens significantly. A compromised component should not be able to endanger the rest of the system. For example, a car's Bluetooth vulnerability should not allow an attacker to control the brakes. Several efforts are being carried out to improve the development of vehicle-secure OSes. For instance, Automotive Grade Linux [8] or Red-Hat In-Vehicle OS [9] and the tendency should move to increase the safety of future intelligent vehicles.

Finally, in the last years, a trend toward more hardware security components, especially for separation of cryptographic functions and implementation of critical operations has emerged. Examples of technologies that are part of this trend have been mentioned above, namely HSM, TEEs and SELinux. These components are being used widely in critical infrastructures but also in smartphones to improve the security provided by the operating system.

21.3 Consequences for Switzerland

The use of secure operating systems is beneficial not only for high-risk systems but also for individuals who want to protect their assets.

In more critical environments, such as governments and military systems that typically have higher security restrictions, security-evaluated OSes are a convenient option used in other countries, ensuring those systems fulfill a set of security requirements. In addition, these OSes ensure a minimum level of trustworthiness and security by limiting access to specific resources and isolating components.

For Switzerland, a movement toward more secure operating systems is required to improve the security of sectors such as the banking and the military sectors.

Individuals and businesses are also the targets of cyber attackers. While individuals often opt for functionality over security, it is crucial to raise the importance of using security-focused OSes with extra security features to reduce the attack surface and protect their assets.

21.3.1 Implementation Possibilities: Make or Buy

Large amounts of knowledge, human resources, and time is required to create an OS from scratch. An OS is a piece of software responsible for controlling a device's hardware and providing an interface whereby an operator can use it. However, most OSes are much more sophisticated and perform many tasks: manage multitasking, memory management, multiple processor cores, networking support, and drivers for all standard hardware. For instance, the Linux kernel (i.e., one part of an OS) consists of several millions of lines of code. Therefore, if the development of an OS were already a complex task, adding security concerns on top of that would require

Table 21.1 Implementation possibilities for different sectors

	Make		Buy	
	Pros	Cons	Pros	Cons
Military	Full control over implemented modules	Error in implementation and lack of compatibility with existing modules and libraries	Working solution	Might contain accidental or purposeful backdoors
Civil Society	None	Lot of resources needed to implement a functioning solution	Easy adoption	Associated cost
Economy	In-house solution	Liability in case of security holes	Cost of development is zero and choose solution according to to needs.	Not as flexible as self-developed solution

even more resources. For instance, the vulnerability management system is typically the most critical and time-consuming part of an OS conception. In addition, one of the most significant shortcomings of OSes built from scratch is the limited support for existing software, which could limit the functionalities of a given system.

On the other hand, given the availability of existing solutions buying appears to be a preferable option, especially regarding the maturity of the existing solutions compared to an OS developed from zero and given the complexity of such a task. When building an OS from scratch, many bugs might be introduced, and the time to reach a certain level of stability and maturity might require several years. Operating systems in the market have been developed for decades, and security has been considered a significant concern to all of them. In addition, one could implement additional security features on top of an existing OS to fill the needs (e.g., some specific cryptographic functions or authentication mechanisms) (Table 21.1).

21.4 Conclusion

Although the use of secure operating systems is not a definitive solution to protect against all the dangers of current cyberspace, it is clear that it can reduce the impact of individual vulnerable applications or modules being exploited on the whole system. Moreover, improving the security of the operating system is only one measure that can be adopted to reduce the attack surface: the combination of several other technologies, such as the ones discussed in other chapters, might

increase the protection against cyber attacks and limit the ability of an attacker to exploit our systems. In addition, the human factor is still a significant factor concerning the overall security of a system. A secure OS will reduce the attack surface. Nevertheless, training teams of users is essential for security.

References

1. Stephen Smalley Walsh and Greg. Selinux: Nsa's open source security enhanced linux, 2003.
2. Common Criteria: New CC Portal. https://www.commoncriteriaportal.org/, August 2022.
3. National Institute of Standards and Technology. Security Requirements for Cryptographic Modules. Technical Report Federal Information Processing Standard (FIPS) 140-2, U.S. Department of Commerce, December 2002.
4. C. Jahl. The information technology security evaluation criteria. pages 306 – 312. IEEE Computer Society, January 1991.
5. Murugiah Souppaya, John Morello, and Karen Scarfone. Application Container Security Guide. Technical Report NIST Special Publication (SP) 800-190, National Institute of Standards and Technology, September 2017.
6. Flatcar Container Linux. https://flatcar-linux.org/, August 2022. Flatcar.
7. Bottlerocket OS. https://github.com/bottlerocket-os/bottlerocket, August 2022. original-date: 2019-04-03T23:28:55Z.
8. ARCA | Confidential Computing | Container Workload. https://www.cysec.com/arca/.
9. What is automotive grade linux? https://www.automotivelinux.org/, August 2022. Automotive Grade Linux.

Chapter 22
Biometrics

Sophia Ding, Emilia Nunes, Pascal Bettendorff, and Weyde Lin

22.1 Introduction

This chapter provides an overview of biometrics's current state and future trends, a technology that measures physiological characteristics for individual identification. The technology is based on three types of biometrics: biological, morphological, and behavioral. The data collected from a biometric sample is stored on a storage medium and is compared with a database during authentication. The biometrics market is growing globally and is expected to reach $68.6 billion by 2025. Future trends in biometrics include increased usage in the sharing economy and unstaffed shops, technical advancements in real-time biometric authentication and increased privacy concerns.

22.2 Analysis

Recent years have seen a surge in the use of biometric authentication methods. Technological progress, especially in the Internet of Things (IoT) and Artificial Intelligence (AI), makes it possible to measure biometrics quickly within a reasonable amount of time and with high-quality results. As a result, it is possible to solve several challenges in existing security concepts by using biometrics. However, their use also raises ethical and regulatory concerns.

S. Ding · E. Nunes · P. Bettendorff · W. Lin (✉)
Eraneos Switzerland AG, Zurich, Switzerland
e-mail: Sophia.Ding@eraneos.ch; Emilia.Nunes@eraneos.ch; pascal@bettendorff.net; Weyde.Lin@eraneos.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_22

22.2.1 Definition

In biometrics, physiological characteristics (e.g., fingerprints, facial features, voices) are measured so individuals can be identified [1]. It is important to note that biometrics are unique biological characteristics, which means that no two individuals, not even twins, possess the same biometrics. Biometrics are used for various purposes, including fighting crimes, screening people at borders, combating fraud, and protecting access to a secured asset (such as computer networks, hardware, or software) [1, 2].

Biometric security is divided into three groups [3]:

- Biological biometrics analyze characteristics at the genetic and molecular level (e.g., DNA or blood).
- Morphological biometrics is based on the body's structure (such as the iris or fingerprint).
- Behavioral biometrics are based on patterns unique to each individual (e.g., how people walk or speak).

A biometric sample is obtained from an individual (e.g., a fingerprint or iris scan). Data is extracted from the sample and stored on a storage medium (e.g., a smart card). If a person requests authentication, the system compares the person's biometrics with the data in the database. The system authenticates a person if there is a match [4].

Since biometry does not share the same characteristics of other authentication techniques, such as passwords or PIN codes, it is widely used as a second-factor authentication. In addition, on mobile phones and laptops, biometric-based encryption is widely used.

There has been a steady increase in the importance of data protection. It has been reported that users are reluctant to entrust biometric data, particularly fingerprints, to solution providers [5]. Some authentication systems try to address this issue by storing a user's biometric data locally on the device itself instead of storing it remotely on a server. For example, Apple's Touch ID technology stores a mathematical representation of the user's fingerprint locally in a secure enclave, which is inaccessible by the device's operating system [6]. This makes it more privacy-friendly, leading to higher adoption rates.

22.2.2 Trends

Globally, the biometrics market is proliferating. The global biometric market is expected to reach $68.6 billion by 2025, from $36.6 billion in 2020 [7]. Furthermore, due to the increasing number of terrorist activities and the increased theft of sensitive data, the biometrics market is expected to grow at a significant rate [5].

Future trends in biometrics include (Table 22.1):

Table 22.1 Future trends in biometrics

Trend Category	Trend	Description	
Use Cases	Sharing Economy	During the next few years, biometrics will become increasingly prevalent in the sharing economy (e.g., car sharing, apartment sharing), enabling organizations to offer trustworthy services and improve customer satisfaction.	[8, 9]
	Unstaffed Shops	In these stores, customers must download a mobile app that must be scanned before entering the store. A facial recognition device verifies the identity of customers and a digital camera records all actions taken by customers. The number of pilot shops is anticipated to increase in the coming years (e.g., the "VOI Cube" by Migros).	[10, 11]
Technical Development	Real-time Biometric Authentication	By using real-time biometric authentication systems, criminal acts, such as hacking and database breaches, are reduced while data privacy is maintained. Progress in the development of existing techniques (Biometric Encryption, Behavioral Biometrics) combined with the Internet of Things (IoT) and artificial intelligence (AI) has increased their applicability. For example, the global market for behavioral biometrics is expected to reach $3.9 billion by 2025.	[12, 13]
	Cloud-based Biometrics	A cloud-based biometric solution enables companies to use and scale search and enrollment capabilities quickly and efficiently. Using biometrics as a Service (BaaS) solutions, companies can prevent identity theft and data breaches without building their own biometric systems. The global market for biometrics-as-a-service is forecasted to grow by 16% a year, reaching $10.4 billion by 2030.	[14, 15]

	Multimodal Authentication	Multimodal authentication systems use two or more biometric features to provide an additional layer of security for organizations. As fraud attempts increase, biometric anti-counterfeiting technologies are being developed to detect them.	[16]
Risks	Cyberattacks in the Age of AI	There is a close connection between biometric technology and artificial intelligence. As a result, cybercriminals have new opportunities for more sophisticated cyberattacks. By mimicking victims' facial features, deep fakes can be used to exploit identification systems. Similarly, adversarial attacks manipulate sensory data. Other attacks include morphing (the manipulation of reference data) and backdoor attacks (the manipulation of training data). In the future, these attacks are expected to increase in frequency. Another issue relates to the immutable nature of biometrics [17]. While a breached password is easily changed, most biometrics are not spontaneously malleable (e.g., fingerprints remain the same throughout life, the facial change would require surgical intervention). This poses a significant post-breach risk for users and highlights one of the large drawbacks of biometric authentication.	[18]
	Ethical and Regulatory Risks in the Age of AI	Several countries are currently working on regulating artificial intelligence. For example, the proposed EU AI Act prohibits using AI systems classified as unacceptable risk systems, such as real-time, remote biometric identification systems used in public spaces for law enforcement purposes.	[19]

22.3 Consequences for Switzerland

The Swiss private sector already uses biometric identification and authentication extensively (e.g., for school canteen access, attendance, and access to IT systems). However, aligning these use cases with data protection laws takes time and effort. According to the Swiss Federal Data Protection and Information Commissioner (FDPIC), biometric systems should be used with caution, and many recommendations are provided on how to use them effectively [20].

Using biometric fingerprints has been a part of Swiss law enforcement for over a century [21]. In recent years, more advanced biometric methods have been considered (especially facial recognition). There is a legal basis for their use in criminal investigations, but some legal experts argue that they are insufficient [22, 23]. In particular, facial recognition is opposed by several groups due to privacy concerns,

violations of human rights, and fears of mass surveillance [24–26]. While Swiss law enforcement agencies are aware of the risks associated with facial recognition technology, they closely monitor the development of frameworks for the responsible use of this technology. Although some high-level frameworks exist, they need to include concrete recommendations for implementation [27].

Biometric technology is a subject of active research in Switzerland. For example, the Swiss Center for Biometrics Research and Testing at IDIAP, https://www.biometrics-center.ch, or the Center for Security Studies at ETH Zurich, https://css.ethz.ch. In addition to conducting commercial research on identity and data governance, IBM Research Zurich researches biometrics. Also, many companies sell biometric products and solutions, such as Touchless Biometric Systems AG (Pfäffikon SZ), Tech5 (Geneva, GE), as well as research spinoffs, such as PXL Vision (Zürich, ZH), and BWO Systems (Schenkon, LU).

22.3.1 Implementation Possibilities: Make or Buy

A biometric system is vulnerable to various attacks, from faking input (for example, copying fingerprints) to attacking the technology itself. As a result, designing and implementing secure biometric authentication methods requires highly specialized technical expertise and experience. According to the British National Cyber Security Centre, buyers should ask vendors to conduct a detailed security analysis of their product [28].

A fully integrated solution offers significant advantages as it aligns biometric hardware, key generation, validation, and storage with the cryptographic provider, providing a coherent control environment. A well-established example is IBM's Trusted Platform Module and Fingerprint Reader ecosystem [29].

In recent years, there has been a push for the creation of open-source solutions [30]. While their performance may be comparable to commercial solutions, they usually need a more in-depth security analysis.

Organizations must choose both hardware and software when sourcing biometric technology. For fingerprinting, for instance, the choice of hardware is influenced by factors such as the company's industry, the age range of users, and the climate. In addition, the choice of hardware and software can impact the computational workload of the biometric system [31].

22.3.2 Variation and Recommendation

There are several military applications:

- Biometric identification friend or foe: It is essential to distinguish between friends and foes on the battlefield and at borders and checkpoints [32].

- Weapons with fingerprint lock: Weapons with fingerprint lock. A signature gun (smart gun) is a firearm that an authorized individual can only fire. A security function such as this can prevent third parties from misusing the weapon [33].

22.4 Conclusion

The trend in biometrics is toward faster, more secure, and more convenient solutions. As a result, there is an increasing market share of integrated systems, which integrate hardware, key generation, validation, and storage, as well as cryptographic providers. As biometrics become more prevalent and their integration with AI systems increases, ethical and regulatory questions become more pressing.

References

1. National Institute of Standards and Technology. Biometrics. https://www.nist.gov/programs-projects/biometrics.
2. Ann Cavoukian and Alex Stoianov. Biometric Encryption. In Henk C. A. van Tilborg and Sushil Jajodia, editors, *Encyclopedia of Cryptography and Security*, pages 90–98. Springer US, Boston, MA, 2011.
3. Kaspersky Lab. What is Biometrics? How is it used in security? https://www.kaspersky.com/resource-center/definitions/biometrics.
4. Ann Cavoukian and Alex Stoianov. Biometric Encryption. Technical report, Information and Privacy Commissioner of Ontario, March 2007.
5. GLOBALER MARKT FÜR BIOMETRIE – WACHSTUM, TRENDS, AUSWIRKUNGEN VON COVID-19 UND PROGNOSEN (2022–2027). Technical report.
6. Apple. About Touch ID advanced security technology. https://support.apple.com/en-us/HT204587.
7. Justina Alexandra Sava. Global biometric system market revenue from 2020 to 2027. Technical report, Statista, May 2022.
8. Yubo Chen and Liantao (Tarry) Wang. Commentary: Marketing and the Sharing Economy: Digital Economy and Emerging Market Challenges. *Journal of Marketing*, 83(5):28–31, September 2019.
9. Sami Dakhlia, Andrés Davila, and Barry Cumbie. Trust, but Verify: The Role of ICTs in the Sharing Economy. In Francesca Ricciardi and Antoine Harfouche, editors, *Information and Communication Technologies in Organizations and Society*, volume 15, pages 303–311. Springer International Publishing, Cham, 2016. Series Title: Lecture Notes in Information Systems and Organisation.
10. Marc Bürgi. Ohne Personal: Die Migros lanciert den Selbstbedienungsladen "Voi Cube". *Handelszeitung*, January 2021.
11. Lizheng Liu, Bo Zhou, Zhuo Zou, Shih-Ching Yeh, and Lirong Zheng. A Smart Unstaffed Retail Shop Based on Artificial Intelligence and IoT. In *2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, pages 1–4, Barcelona, September 2018. IEEE.
12. RecFaces. Part 1. Biometricisation of the planet: Key market trends and upcoming plans. https://recfaces.com/articles/biometricisation-of-the-planet, March 2022.

13. Yunji Liang, Sagar Samtani, Bin Guo, and Zhiwen Yu. Behavioral Biometrics for Continuous Authentication in the Internet-of-Things Era: An Artificial Intelligence Perspective. *IEEE Internet of Things Journal*, 7(9):9128–9143, September 2020.
14. Silvio Barra, Aniello Castiglione, Maria De Marsico, Michele Nappi, and Kim-Kwang Raymond Choo. Cloud-Based Biometrics (Biometrics as a Service) for Smart Cities, Nations, and Beyond. *IEEE Cloud Computing*, 5(5):92–100, September 2018.
15. Inc. Aware. The Rise of Biometrics in the Cloud. https://www.aware.com/blog-biometrics-in-the-cloud/#, July 2021.
16. Riseul Ryu, Soonja Yeom, Soo-Hyung Kim, and David Herbert. Continuous Multimodal Biometric Authentication Schemes: A Systematic Review. *IEEE Access*, 9:34541–34557, 2021.
17. Andy Greenberg. OPM now admits 5.6m Feds' Fingerprints were stolen by hackers. https://www.wired.com/2015/09/opm-now-admits-5-6m-feds-fingerprints-stolen-hackers/.
18. Christian Berghoff, Matthias Neu, and Arndt von Twickel. The Interplay of AI and Biometrics: Challenges and Opportunities. 54(9):80–85, September 2021. Computer.
19. European Union. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206, April 2021.
20. Federal Data Protection and Information Commissioner (FDPIC). Some data protection considerations with regard to the use of biometric data in the private sector. Annual Report 12 - 2004/2005, July 2005.
21. Bundesamt für Polizei fedpol. Der FingerabDruck.
22. Denis De la Reusille. Police use of prohibited Software. https://www.parlament.ch/en/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20223113, March 2022.
23. Franziska Ramser. Verbrecherjagd mit umstrittenen Mitteln. January 2022. SRF News Clip.
24. Katharina Jochum. Stadt Zürich will biometrische Überwachung verbieten. *INSIDE IT*, June 2022.
25. Regulierung der Gesichtserkennung im öffentlichen Raum. https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20213580,author=Glttli,Balthasar,.
26. Angela Müller. Gesichtserkennung im öffentlichen Raum gehört verboten. July 2022. Neue Zürcher Zeitung.
27. WEF. A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations. October 2021.
28. National Cyber Security Centre. Biometric recognition and authentication systems. https://www.ncsc.gov.uk/collection/biometrics/how-biometrics-are-attacked.
29. Reiner Sailer, Leendert Van Doorn, and James P Ward. IBM Research Report RC23368. 2004.
30. S. Marcel, A. Anjo, and R. Lessmann. OPEN SOURCE SOFTWARE. https://eab.org/information/software.html?ts=1651622400052.
31. Pawel Drozdowski, Christian Rathgeb, and Christoph Busch. Computational workload in biometric identification systems: an overview. *IET Biometrics*, 8(6):351–368, November 2019.
32. National Institute of Standards and Technology. FY07: Biometrics—Identifying Friend or Foe. https://www.nist.gov/director/congressional-and-legislative-affairs/fy07-biometrics-identifying-friend-or-foe, January 2017.
33. Woodie Kessel. Smart Guns Don't Kill People. In Marie Crandall, Stephanie Bonne, Jennifer Bronson, and Woodie Kessel, editors, *Why We Are Losing the War on Gun Violence in the United States*, pages 249–254. Springer International Publishing, Cham, 2021.

Chapter 23
Electronic Voting

Louis-Henri Merino

23.1 Introduction

Remote electronic voting, where eligible voters can cast votes from anywhere in the world on their device, promises to increase voter turnout, improve accessibility, and reduce costs. However, building a secure online voting system is complex, involving four essential requirements: integrity, privacy, coercion-resistance, and availability. Moreover, the successful deployment of a secure online voting system would require close collaboration among the public and private sectors and academia. The military and intelligence agencies could play an essential role in supporting the e-voting operator against cyberattacks meant to deteriorate public trust in the voting outcome.

23.2 Analysis

23.2.1 Definition

Online voting promises to increase voter turnout, improve accessibility (e.g., support for multiple languages) and reduce cost for voters [1, 2]. For organizations, online voting can help increase productivity and decrease costs [2].

However, the outcome of an election event will usually have real-world impact, making security paramount [3, 4]. At the moment, the approaches to securing an election are still being debated, evolving since at least 1987 [3, 5–8].

L.-H. Merino (✉)
EPFL, Lausanne, Switzerland
e-mail: louis-henri.merino@epfl.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_23

Table 23.1 Necessary security requirements for an online voting system

Property	Requirement	Definition
Vote Compliance	Integrity	Invalid votes must be discarded.
Vote Secrecy	Privacy	Voter's votes must be confidential.
Voter Intention	Coercion-Resistance	Voters can cast their intended vote.
Individual Verifiability	Integrity	Voters are capable of checking the inclusion and the correctness of their votes
Universal Verifiability	Integrity	Anyone can verify the outcome of a voting event.
Resiliency	Availability	E-voting authority registers votes and reveals outcomes promptly.
Transparency	Integrity	Anyone can audit the e-voting platform and the deployed infrastructure.

In Table 23.1, compiled from a variety of academic, industry, and government sources [8–11], we present, to our knowledge, the necessary security requirements for an online voting system suitable for high-stakes voting events. There are namely four crucial requirements: integrity, privacy, coercion-resistance, and availability. Integrity ensures that every participating eligible voter can cast their vote and that the outcome of the voting event has not been altered; privacy ensures that the vote of any given voter is not revealed; coercion-resistance ensures that the voter can cast their intended vote; and availability ensures that the e-voting authority accepts and tallies votes promptly.

23.2.2 Trends

Market and Application The most apparent market for remote e-voting systems is government electoral agencies. However, many other actors could benefit from remote e-voting, some of which include a government's judicial branch (e.g., jury voting), a government's legislative branch (e.g., voting on legislative proposals), corporations (e.g., boardroom voting), and academic institutions (e.g., student representative elections). Each use case may have it is own subtle specialized requirements; for example, for boardroom voting and jury voting, where the number of voters is small, it is preferable to release the outcome without releasing the number of votes per option since it could deter voters from voting their actual preference [12].

Actors The design of an e-voting system for a high-stakes use case will likely require the involvement (and close collaboration) of actors from all sectors: academia for research, industry for technology transfer and support, and government

for regulations. This collaboration is observed with the development of the Swiss Post E-Voting system with the intent for use in Swiss elections and referendums [10, 11, 13]. Academics have proposed various electronic voting schemes, found critical vulnerabilities in the Swiss Post E-Voting System, and given feedback on proposed Swiss regulations.

23.3 Consequences for Switzerland

23.3.1 Implementation Possibilities: Make or Buy

See Table 23.2.

23.3.2 Variations and Recommendation

While online voting does not have direct military usage, the military could have an impact on online voting in the public sector. A successful cyber-attack on the nation's e-voting platform may cause significant consequences to society (e.g., reducing public trust in the outcome) [14, 15]. A denial of service attack, for example, could cause votes to be rejected, alternatively, cause a delay in the results. In such circumstances, the support of the military may help e-voting operators remain available and secure despite the most sophisticated attacks.

Table 23.2 Implementation possibilities for different sectors

	Make		**Buy**	
	Pros	Cons	Pros	Cons
Civil Society	Collaboration between academia, industry and government	High costs	Potentially lower cost	May lack transparency in its security requirements
Economy	Tailored for the use case in question	Primarily a cost reduction strategy with high costs to develop	Lower cost (no dedicated internal resources)	May require adapting to the abilities of the purchased system

23.4 Conclusion

Remote E-Voting systems promise substantial benefits from an increase in convenience, productivity, and accessibility to a decrease in costs. However, these systems must satisfy various security requirements to become eligible for high-stakes voting events (e.g., governmental elections). The author believes that the military and intelligence agencies could play an essential role in ensuring the uptime of a deployed e-voting system, helping to achieve the availability security requirement. In the meantime, remote e-voting systems can already be deployed in a variety of environments that require less stringent security requirements: Academia and industry (e.g., student elections, boardroom voting).

References

1. European Commission. Directorate General for Justice and Consumers. *Study on the benefits and drawbacks of remote voting: final report.* Publications Office, LU, 2018.
2. David Chaum, Richard T. Carback III, Jeremy Clark, Chao Liu, Mahdi Nejadgholi, Bart Preneel, Alan T. Sherman, Mario Yaksetig, and Filip Zagorski. VoteXX: A Remote Voting System that is Coercion Resistant. October 2020. Accepted: 2020-11-30T17:36:37Z.
3. Josh Benaloh. Verifiable Secret-Ballot Elections. September 1987.
4. Alex Moyher. The Challenges of Online Voting. *Diversity: the art of thinking independently, together*, 2015.
5. Josh Benaloh and Dwight Tuinstra. Receipt-free secret-ballot elections (extended abstract). In *Proceedings of the twenty-sixth annual ACM symposium on Theory of Computing*, STOC '94, pages 544–553, New York, NY, USA, May 1994. Association for Computing Machinery.
6. Ari Juels, Dario Catalano, and Markus Jakobsson. Coercion-Resistant Electronic Elections. In David Chaum, Markus Jakobsson, Ronald L. Rivest, Peter Y. A. Ryan, Josh Benaloh, Miroslaw Kutylowski, and Ben Adida, editors, *Towards Trustworthy Elections: New Directions in Electronic Voting*, Lecture Notes in Computer Science, pages 37–63. Springer, Berlin, Heidelberg, 2010.
7. Ralf Küsters, Tomasz Truderung, and Andreas Vogt. A Game-Based Definition of Coercion-Resistance and Its Applications. *IACR Cryptology ePrint Archive*, 2009:582, January 2009.
8. Ralf Küsters, Tomasz Truderung, and Andreas Vogt. Verifiability, Privacy, and Coercion-Resistance: New Insights from a Case Study. In *2011 IEEE Symposium on Security and Privacy*, pages 538–553, May 2011. ISSN: 2375-1207.
9. Huangyi Ge, Sze Yiu Chau, Victor E Gonsalves, Huian Li, Tianhao Wang, Xukai Zou, and Ninghui Li. Koinonia: verifiable e-voting with long-term privacy. In *Proceedings of the 35th Annual Computer Security Applications Conference*, ACSAC '19, pages 270–285, New York, NY, USA, December 2019. Association for Computing Machinery.
10. SR 161.116 - Federal Chancellery Ordinance of 13 December 2013 on Electronic Voting (VEleS). https://www.fedlex.admin.ch/eli/cc/2013/859/en, August 2022.
11. Die Schweizerische Post. E-voting. https://www.post.ch/en/business-solutions/e-voting, August 2022.
12. Johannes Mueller. Ordinos: A Verifiable Tally-Hiding E-Voting System. 2020.
13. Véronique Cortier, Alexandre Debant, and Pierrick Gaudry. A privacy attack on the Swiss Post e-voting system. page 4.

14. Trust in public institutions: Trends and implications for economic security | DISD. https://www.un.org/development/desa/dspd/2021/07/trust-public-institutions/, August 2022.
15. Fabio Rugge. "MIND HACKING": INFORMATION WARFARE IN THE CYBER AGE. page 8.

Chapter 24
Data in Transit Security

Roland Meier

24.1 Introduction

Data in transit, or network traffic, can be eavesdropped on and potentially leak sensitive information. This information can be in the form of the payload (the message being transmitted), headers (which contain information about the sender and receiver), or metadata (protocol information about the packet). To prevent information leakage, various technologies exist that encrypt the payload and headers, such as MACsec, IPsec, and TLS. However, it is more challenging to protect metadata, as it involves hiding more than just the contents of the packet. Techniques to hide metadata include obfuscating packet sizes, timing, and path, but these methods often come with trade-offs, such as increased latency or decreased network performance. Therefore, it is essential to consider data security in transit and implement appropriate measures to prevent unauthorized access and information leaks.

24.2 Analysis

24.2.1 Definition

Data in transit (i.e., network traffic) is susceptible to eavesdropping and can leak information through the following channels:

- Payload: The packet payload contains the message transmitted (e.g., parts of a website or email).

R. Meier (✉)
Cyber-Defence Campus, Thun, Switzerland
e-mail: roland.meier@ar.admin.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_24

- Headers: The packet headers contain the information required to deliver the packet to the correct destination and parse it correctly by the receiving application. Packet headers, therefore, contain information about the sender and receiver of a packet (e.g., their IP and MAC addresses) and information about the user application and protocol.
- Metadata: Metadata in network traffic is normally considered as the protocol information including the packet headers They are not contained in the packet directly but can be observed when recording the packet (e.g., the packet size or the time when it was received). If a packet is received at multiple locations, this reveals additional information (e.g., the path a packet takes through the network).

For an eavesdropper, extracting information from unprotected headers and payloads is easy. Nevertheless, even if headers and payloads are protected (i.e., encrypted), several so-called traffic-analysis attacks can infer sensitive information based on traffic metadata.

For each type of information channels, there exist technologies to prevent the leakage:

Protecting Payload and Headers The usual approach to protecting the payload and packet headers is to encrypt them. To do so, various encrypted protocols exist that encrypt data on various layers (not only the payload but also some headers). Widely used protocols include MACsec, IPsec, and TLS, which are explained in more detail below.

- MACsec (Medium Access Control security) [1]: Operates on the link layer and encrypts packets between (layer 2) switches. MACsec encrypts the entire packet, including all headers except the source and destination addresses in the link layer (i.e., the source and destination MAC address). MACsec is typically used to protect individual links in a local area network (LAN) or wide area network (WAN) against eavesdropping.
- IPsec (Internet Protocol Security) [2]: Operates on the network layer and can be used in two modes: transport mode and tunnel mode. In transport mode, IPsec encrypts the payload of the IP layer (i.e., the headers of the transport-layer protocol and packet payloads). In tunnel mode, IPsec creates a tunnel from the sender to a destination and encrypts the IP header and its payload. To do so, it encapsulates the original IP packet within a new IP packet whose destination address is the tunnel's endpoint, thereby revealing the IP addresses of both ends of the tunnel. IPsec is typically used to create tunnels between locations connected over an untrusted network (e.g., the Internet). For more information about tunnels and so-called Virtual Private Networks (VPNs), see Chap. 26.
- TLS (Transport Layer Security) [3]: Operates on the transport layer and encrypts only its payload. Therefore, it does not hide other packet headers such as the source and destination IP addresses. TLS is used for many applications, but its most well-known use case is web browsing over HTTPS.

Protecting Metadata Hiding packet metadata is more difficult compared to hiding packet contents because hiding metadata involves more than just encrypting the actual traffic. Completely hiding metadata is often impossible because packets need to be sent at some point. There exists various options:

- Obfuscating packet sizes: Obfuscating the size of packets or flows can be achieved by adding padding to the original contents of a packet or by splitting one packet into multiple fragments. For example, IPsec and TLS allow adding a random amount of padding to each packet before encrypting it to conceal its real size. However, it has been shown that this padding is too little to prevent traffic-analysis attacks [4].
- Obfuscating packet timing: Obfuscating the timing of packets can be achieved by delaying the sending time of a packet. However, this inevitably leads to an increase in latency and, therefore, a decrease in network performance. Therefore, systems to hide the timing mainly exist as prototypes presented in research papers (e.g., [4–6]), and are rarely used in practice.
- Obfuscating packet's path: Obfuscating the path of packets can be achieved by re-encrypting the packet multiple times while it crosses the network. The most well-known technique to do this is Onion Routing and its implementation in the TOR network. However, more than re-encrypting packets is needed; packet timings and sizes need to be concealed, too, in order to prevent correlation attacks such as the ones discussed in [7].

Reliably preventing traffic analysis attacks based on metadata requires making the traffic that crosses the network independent of the actual production traffic in terms of packet size, timing, and contents. This can be achieved by reshaping and encrypting production traffic such that it is sent at a fixed rate, and the encryption makes packets indistinguishable from each other.

Unfortunately, preventing traffic analysis attacks typically adds large amounts of overhead in terms of additional delays, packet padding, and cover traffic and, therefore, often comes at the cost of throughput decrease or latency increase.

24.2.2 Trends

The percentage of encrypted network traffic has risen continuously in the past years, and we expect this trend to continue in the following years.

A major driving factor for this is that the "Let's Encrypt" certification authority [8] allows everyone to obtain TLS certificates for free. This led to a rapid increase in the websites reachable over encrypted connections, i.e., over HTTPS. In addition, website operators are further incentivized to deploy TLS because it leads to a better ranking in the Google search results [9].

In addition, QUIC, a new transport-layer protocol, was standardized in 2021 [10]. In contrast to TCP and UDP, QUIC is encrypted by default and provides better

performance and reliability than TCP and UDP. Google initially introduced it and supports it in its products, but other platforms and services now support it as well.

TLS and QUIC are increasingly used to encrypt traffic that was traditionally not encrypted. For example, DNS queries are now sent over encrypted channels.

24.3 Consequences for Switzerland

Popular websites and services in Switzerland enforce encrypted connections leads to most web network traffic in Switzerland being encrypted. In addition, the major Swiss web hosting providers support TLS encryption for their customers' websites free of charge and with an easy setup, further increasing the percentage of encrypted traffic.

On the other hand, measures to protect metadata are not widespread in Switzerland, leaving network traffic vulnerable to traffic-analysis attacks. However, these attacks primarily exist as research prototypes only.

24.3.1 Implementation Possibilities: Make or Buy

Buy: The widely available secure transport protocols and their implementations in popular libraries should be used for encryption.

Make: For sensitive environments, benefits outweigh metadata protection schemes' potential costs (e.g., additional overhead). Unfortunately, there is no widespread solution here, and it would be necessary to develop a new solution for Switzerland's use case (e.g., based on research projects from Swiss universities [5, 6, 11, 12]).

24.4 Conclusion

Unprotected traffic allows an eavesdropper to learn sensitive information about ongoing communication. To mitigate this, there exist many communication protocols that encrypt traffic on different layers. These protocols (MACsec, IPsec, and TLS) are widely used today and achieve good security for network traffic. However, even if traffic is encrypted, it leaks information through its metadata. Preventing this is more challenging, leads to more communication overhead, and is rarely done today.

References

1. 802.1AE: MAC Security (MACsec) 1.ieee802.org. https://1.ieee802.org/security/802-1ae/. [Accessed 04-Nov-2022].
2. RFC 4301: Security Architecture for the Internet Protocol – rfc-editor.org. https://www.rfc-editor.org/rfc/rfc4301. [Accessed 04-Nov-2022].
3. RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3 — rfc-editor.org. https://www.rfc-editor.org/rfc/rfc8446. [Accessed 04-Nov-2022].
4. Kevin P. Dyer, Scott E. Coull, Thomas Ristenpart, and Thomas Shrimpton. Peek-a-boo, i still see you: Why efficient traffic analysis countermeasures fail. In *2012 IEEE Symposium on Security and Privacy*, pages 332–346, 2012.
5. Ludovic Barman, Italo Dacosta, Mahdi Zamani, Ennan Zhai, Bryan Ford, Jean-Pierre Hubaux, and Joan Feigenbaum. Prifi: A low-latency local-area anonymous communication network. *arXiv preprint arXiv:1710.10237*, 2017.
6. Roland Meier, Vincent Lenders, and Laurent Vanbever. ditto: Wan traffic obfuscation at line rate. In *NDSS Symposium 2022*, 2022.
7. Ishan Karunanayake, Nadeem Ahmed, Robert Malaney, Rafiqul Islam, and Sanjay K. Jha. De-anonymisation attacks on tor: A survey. *IEEE Communications Surveys & Tutorials*, 23(4):2324–2350, 2021.
8. Lets Encrypt—letsencrypt.org. https://letsencrypt.org/. [Accessed 04-Nov-2022].
9. HTTPS as a ranking signal — Google Search Central Blog — Google Developers — developers.google.com. https://developers.google.com/search/blog/2014/08/https-as-ranking-signal. [Accessed 04-Nov-2022].
10. Martin Thomson. RFC 9000: QUIC: A UDP-Based Multiplexed and Secure Transport – rfc-editor.org. https://www.rfc-editor.org/rfc/rfc9000. [Accessed 04-Nov-2022].
11. Chen Chen, Daniele E Asoni, Adrian Perrig, David Barrera, George Danezis, and Carmela Troncoso. TARANET: Traffic-Analysis Resistant Anonymity at the Network Layer. *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, 2018.
12. Chen Chen, Daniele E Asoni, David Barrera, George Danezis, and Adrain Perrig. Hornet: High-speed onion routing at the network layer. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015.

Chapter 25
Blockchain

Linus Gasser and Jean-Pierre Hubaux

25.1 Introduction

A blockchain is a decentralized system for managing a block-based data structure. Unlike centralized systems that rely on honest operators, blockchains can function even when some participants act maliciously, as long as more than half of the entities in the network are honest. Digital Ledger Technologies (DLT) encompass systems like blockchains, which offer decentralized data management. Blockchains differ from databases in that they are entirely decentralized, while DLTs have some decentralized components and rely on the majority of participants for trust. Blockchains vary in data structure, content, visibility, node onboarding, consensus algorithm, wallets, and second-layer services. The use of blockchains in finance, under the name of cryptocurrencies, is currently the most visible application, but the industry is still heavily debated and subject to speculation.

25.2 Analysis

25.2.1 Definition

In 2008, in his seminal work on Bitcoin, Satoshi Nakamoto introduced a data structure ("a chain of blocks") as well as a consensus mechanism that enables a set of entities to maintain the general ledger of a currency in a distributed manner [1]. Furthermore, the construction provides security guarantees as long as

L. Gasser (✉) · J.-P. Hubaux
EPFL, Lausanne, Switzerland
e-mail: linus.gasser@epfl.ch; jean-pierre.hubaux@epfl.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_25

more than half of the entities participating in the distributed network are honest. Parts of the difficulty and confusion when talking about "Blockchains" stems from the fact that there is no precise definition of a "Blockchain". Some consider the whole ecosystem, including all its components, the consensus mechanism, and the execution environment for a scripting language running on the participating nodes as "the Blockchain". In contrast, others restrict the focus on the underlying data structure that consists of blocks containing data that build a chain.

A broader term for blockchains is Digital Ledger Technologies (DLT). This includes systems that do not rely on linked blocks but offer decentralized data management. The difference between blockchains, DLTs, and databases can be summarized as follows:

- Database: allows to store, retrieve, and update data according to a set of rules (access control); the trust relies on the administrators
- DLT: like a database, but some of the system components are decentralized; the trust relies on the majority of participants
- Blockchain: a special type of DLT where all of the system components are decentralized

Thousands of blockchain systems have already been implemented. Here are the main concepts differentiating their various kinds:

- Data structure—how the data is stored: this is either a single chain of blocks or blocks that link to more than one other block to create a Directed Acyclic Graph (DAG)
- Data content—what is stored: only asset transactions, or scripting possibilities (smart contracts)
- Data visibility—who can view the data: global blockchains offer full access to the data (public), while some local blockchains have a restriction at the network level (private). Some newer global systems protect the data using a zero-knowledge proof system [2, 3].
- Node onboarding—how new nodes are accepted in the system: Bitcoin uses Proof of work (PoW), where new nodes spend energy to join. Newer blockchains use Proof of Stake (PoS), where new nodes need to stake money to join. More centralized DLTs use Proof of Authority (PoA) and have a centrally managed list of nodes. One can add that PoW systems are also called *Permissionless* systems, while PoA systems are called *Permissioned* systems. PoS is in between those two.
- Consensus algorithm—how conflicting data gets stored: the simplest system is to accept only a linear list of non-conflicting blocks, but this can take time. PBFT systems vote on every new block and do not have to wait. Other systems exist like Avalanche [4] or Narwhal/Tusk [5]
- Wallets—storage of user data: most DLTs use an access control system based on private keys. As there is no central service to restore access in case of loss of this private key, the wallets are of utmost importance in DLT systems

- 2nd layer—services on top of the DLT: as DLTs in 2022 are too slow for worldwide usage. Some offer external protocols which use the underlying DLT to synchronize in regular intervals

25.2.2 Trends

Market It is still very much debated where the money in DLT investment comes from and how it is used. While some people promote blockchains as the ultimate tool for a libertarian lifestyle [1], others think that blockchains only serve as an opaque technical background for investment fraud. For example, Alvin [6] thinks that Bitcoin is a unique asset in history and can best be compared with a zero-coupon perpetual bond or an indefinite call option. This is an ironic way to say that investing in blockchains is the same as high-risk speculation.

Applications In 2022, most of the visible applications of blockchains are in the financial sector under the name of cryptocurrencies [7]. This includes investment/speculation in the form of assets like Non-Fungible Tokens (NFTs), Decentralized Finance (DeFi), e.g. Uniswap. However, contrary to its name, only a few cryptocurrencies are currently used for digital payment. If blockchains get regulated, they might also be used for day-to-day payment services, where they will have to compete with VISA, PayPal, Stripe, and others.

DeFi currently allows the exchange of tokens from one blockchain into tokens from another. In the future, this will also include trading fiat money, lending, and receivables management.

NFTs bind a public key to a digital token and can be used by artists to sell their art. Depending on the license, the current holder of the digital token has some rights toward the piece of art [8]. The opinion on NFTs is also very split between Ponzi Schemes and a fairer way for artists to make money. They will undoubtedly continue to be used for brand-aware marketing, but real-world use cases are difficult to find.

Finally, Decentralized Autonomous Organizations (DAOs) want to allow more direct investments into innovative systems in the blockchain space. However, most attempts have been crippled by wrong programming and subsequent loss of investments. Another fact that makes DAOs difficult is missing legislation, which makes it difficult to trust the investment.

A growing list of applications is produced around blockchains' tracking and logging capabilities: due to their underlying data structure, all history is available forever. It is also easy to onboard new actors if the wallets are implemented in a user-friendly way. This makes supply chain management easier for all involved partners while removing the need for a central actor [9]. This supply chain management can be helpful for civil purposes like determining where all ingredients for a medical drug come from. However, also the military must know where the different parts come from and whether they are trustworthy. An example is the *detached labels*, where the parts are identified by a QRcode, which refers to the data on a blockchain.

A third application that is being pushed is identity management. Several actors started to push Self-Sovereign Identities to increase users' confidence in this topic. The users manage these identities, which can be stored on a blockchain. This decreases the risk of a single actor behaving maliciously.

Actors On the research front, the Web3 foundation, the Ethereum Foundation, and Protocol Labs are three significant sources of grants for new technology in the blockchain space. They are responsible for many new protocols and algorithms in that space.

Even though cryptocurrencies are supposed to be decentralized, there are two prominent companies helping users buy and sell those coins: Binance and Coinbase. In 2022, Binance alone traded more than all other exchanges combined!

Upcoming prominent actors include countries starting to regulate blockchain technology and, more specifically, cryptocurrencies. While China has already passed legislation to regulate blockchains strictly, India and Europe have several laws in preparation. The USA law proposals are more geared toward integrating cryptocurrencies into the rest of the financial system.

Research For blockchain systems to be helpful globally, much research still needs to be done. The road is long to fulfill the goal of having a global, fully decentralized ledger that allows the transaction of assets and handling personal data like self-sovereign identity.

Starting from the current blockchain's performance problems, the governance model most appropriate for these systems needs to be more transparent. Then there is a need to be able to exchange between different blockchains, and current solutions still fail too often. New algorithms are needed to handle private data on a public ledger for privacy reasons. To include outside information in blockchains, like stock markets or other data, so-called Oracles will be needed. Furthermore, much research must be done to ensure secure operation even once powerful quantum computers exist.

Smart Contracts Instead of storing transactions in the block, most modern blockchains can also store pieces of a program in a block. These programs are called "smart contracts". "Smart", because users can interact with these programs by sending new transactions to the blockchain. "Contract", not in a legal sense, but because they are immutable and represent all possible interactions of the user with this program. The following list in "Applications" gives some examples, as does the chapter about Web3 (Chap. 34).

25.3 Consequences for Switzerland

While in the beginning, cryptocurrencies have been hailed as the new banks and the downfall of the traditional financial system has been proclaimed, current expectations are much lower. So far, cryptocurrencies have been used as an

Table 25.1 Implementation possibilities for different sectors

	Private		Public	
	Pros	Cons	Pros	Cons
Military	More secure against partner attacks	Difficult to interact with others	Easy integration with other armies	System might malfunction if majority of participants misbehave
Civil Society	Easier to set up for small groups	Difficult to interact with others	Exchange with a larger group of people	More expensive, increased risk of attacks
Economy	Control the system	Less innovation	Innovation through new disruptive ideas	Need to create new business models

investment/speculation vehicle. Other uses in the financial sector will complement traditional services but probably not disrupt them on a large scale. This is due to missing regulations, which makes investing and using DLT technologies very risky.

Contrary to most other countries, Switzerland has clear regulations regarding blockchains that allow building such systems without legal risks [10]. The crypto-valley in Switzerland, centered around Zug but also in Geneva and Neuchatel, has a thriving ecosystem of blockchain-related companies.

25.3.1 Implementation Possibilities: Make or Buy

This section presents the pros and cons of buying or making a blockchain. For blockchains, "Instead of evaluating between 'Make' or 'Buy' like for the other entries, we chose to differentiate between using a 'private' or 'public' blockchain. This is because blockchains are a very complex technology, and nobody should 'Make' their own, new blockchain (Table 25.1).

25.3.2 Use Cases

In this section, three use cases are presented (Table 25.2).

Table 25.2 Use cases

	Military		Civil Society		Economy	
	Pros	Cons	Pros	Cons	Pros	Cons
Supply chain for logistics and procurement	Decentralized and secure	None	Decentralized and secure	None	Decentralized and secure	None
Detached labels and proof of ownership	Resilience and scalable	Ecology	Resilience and scalable	Ecology	Resilience and scalable	Ecology
Self Sovereign Identity Management	Durable and stable	Anonymisation and privacy	Durable and stable	Anonymisation and privacy	Durable and stable	Anonymisation and privacy

25.4 Conclusion

One of the most exciting problems for the military to solve with blockchains is the supply chain management problem. For this task, a public blockchain spanning several armies plus their suppliers might reduce costs, increase security, and reduce delivery times [11]. In civil society, blockchains and cryptocurrencies will remain an investment/speculation vehicle for quite some time. However, there are no real advantages to using a blockchain for most applications proposed. Several parts of the economy, primarily banks and some parts of retail, can take advantage of current and future blockchains to reduce their business running costs. Nevertheless, the complexity of blockchain systems still has to be tamed before it makes economic sense [12].

References

1. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. page 9.
2. Privacy-protecting digital currency. https://z.cash/, August 2022. Zcash.
3. Mina protocol. https://minaprotocol.com/, August 2022.
4. Avalanche: Blazingly Fast, Low Cost, & Eco-Friendly | Dapps Platform. https://www.avax.network/, August 2022.
5. George Danezis, Eleftherios Kokoris Kogias, Alberto Sonnino, and Alexander Spiegelman. Narwhal and Tusk: A DAG-based Mempool and Efficient BFT Consensus, March 2022. arXiv:2105.11827 [cs].
6. Alvin T. Calling Bitcoin a Ponzi Scheme is Lazy Thinking. https://medium.datadriveninvestor.com/why-simply-calling-bitcoin-a-ponzi-scheme-is-lazy-thinking-a3dfc67c25e, June 2022.
7. 51 Critical Blockchain Statistics: 2022 Data Analysis & Market Share. https://financesonline.com/blockchain-statistics/, April 2021. Financesonline.com.

8. Nft NFT Blockchain Intellectual Property: Nfts and intellectual property rights. https://www.nortonrosefulbright.com/de-de/wissen/publications/1a1abb9f/nfts-and-intellectual-property-rights, October 2021. nortonrosefulbright.
9. TradeLens | Supply chain data and docs. https://www.tradelens.com/, August 2022.
10. Digitalisation of the financial sector: Blockchain/DLT. https://www.sif.admin.ch/sif/en/home/finanzmarktpolitik/digitalisation-financial-sector/blockchain.html, January 2022.
11. Blockchain for military logistics. https://www.army.mil/article/227943/blockchain_for_military_logistics.
12. Nils Braun-Dubler, Hans-Peter Gier, Bulatnikova Tetiana, Manuel Langhart, Manuela Merki, and Florian Roth. The Technical Capabilities of Blockchain and its Economic Viability, 2020.

Chapter 26
Tunneling and VPN

Weyde Lin

26.1 Introduction

Tunneling is a technique used to transport data packets over a network. The original data packets, with a protocol not supported by the host network, are encapsulated within another packet and then transported through the network. This technique is helpful for encrypted networks and can be used in virtual private networks (VPNs). Tunneling can be either full, where all network traffic is routed through the tunnel, or split, where only part of the network traffic is routed. The trend in tunneling is shifting from VPN access to a zero trust model, where the focus is on protecting data and ensuring privacy rather than remote access.

26.2 Analysis

26.2.1 Definition

To transport data through a network, the data is divided into packets. In tunneling, packets from one network are sent via another network's connections. The packets are encapsulated within packets and then transported by the second network [1]. This means that data with a protocol not supported by a given network can be sent over that network. In tunneling, the original packet is encapsulated inside another packet (see Fig. 26.1).

There are two types of tunnels:

W. Lin (✉)
Eraneos Switzerland AG, Zurich, Switzerland
e-mail: Weyde.Lin@eraneos.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_26

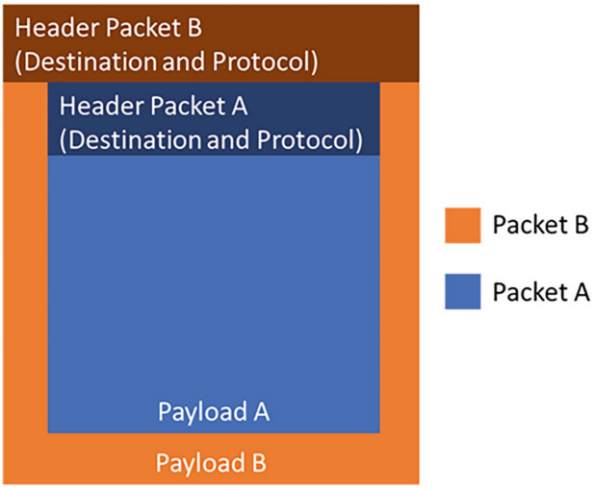

Fig. 26.1 Each packet has a header and a payload. The header lists the packet's destination and protocol. Packet A is encapsulated by Packet B and becomes its payload

- In **full tunneling** all network traffic goes through the tunnel [2].
- In **split tunneling**, only part of the network traffic is routed through the tunnel. This allows the user or device to simultaneously access resources in different networks [3].

Tunneling is very useful in encrypted networks. To create an encrypted tunnel, a network packet, including the header, is completely encrypted and encapsulated as a payload inside another packet for transport across a network. The payload is decrypted at the destination, and the original packet is restored.

While tunneling is often used in virtual private networks[1] (VPNs), VPN and tunneling are technically not the same, and there are VPNs without tunneling. E.g., the VPN implementation, IPsec supports transport modes where not the complete packets are encrypted and encapsulated. Instead, the packet retains its original packets header [5], and only the packet payload is encrypted.

26.2.2 Trends

The internet protocol version 6 (IPv6) is a replacement for IPv4 that, due to its limited number of available IP address space, will be phased out. However, as there

[1] "A virtual network built on top of existing networks that can provide a secure communications mechanism for data and IP information transmitted between networks" [4].

are still IPv4-only networks that do not support IPv6, the tunneling protocol 6in4 [6] allows sending IPv6 packets over an IPv4 network [7].

Another prominent use case of tunnels is VPNs. The global VPN market is expected to grow from US$ 44bn in 2022 to US$ 77.1bn in 2026 [8]. However, at the same time, there is also a shift from VPN access to a zero trust model (e.g., Zero Trust Network Access (ZTNA) and/or Zero Trust Architectures (ZTA)). For example, Google [9] and the US Government [10] both announced shifts from VPN solutions to a zero trust model (See Zero Trust factsheet), and a 2021 study found that 72% of all companies were adopting or planning to adopt zero trust [11].

26.3 Consequences for Switzerland

There is no Swiss-specific need for tunneling, and the demand is expected to be similar to other industrial countries. The exception is VPN providers. Thanks to the strict Swiss laws regarding data protection and privacy, the two VPN providers VyprVPN and Proton VPN are located in Switzerland. Proton explicitly states: "Weil wir in der Schweiz angesiedelt sind, ist Proton VPN durch einige der strengsten Datenschutzgesetze der Welt geschützt und bleibt ausserhalb der Gerichtsbarkeit der USA und der EU." [Because we are based in Switzerland, Proton VPN is protected by some of the strictest privacy laws in the world and remains outside the jurisdiction of the US and EU.] [12].

26.3.1 Implementation Possibilities: Make or Buy

Most tunneling protocols are defined in Request for Comments (RFC) documents (see also below in 2.2 Variations and Recommendation for examples) and then implemented by network equipment or software vendors. For VPNs, the most common closed-source solutions used globally [13] are Cisco VPN, Cisco AnyConnect, Juniper VPN, and Citrix Gateway. There are also two widespread open-source VPN solutions:

- OpenVPN [14] is an open-source (GNU GPLv2) VPN system that uses the OpenSSL library to encrypt the data as well as the control channels. It was first released in 2001. The throughput over an OpenVPN tunnel is somewhat limited, but the software runs on any operating system and platform and makes it widely used.
- WireGuard [15] is an open source (GNU GPLv2) VPN implementation to be easy to use and with improved performance compared to other VPN implementations and a low attack surface.

26.3.2 Variation and Recommendation

There are many tunneling protocols in use today; a few are listed below:

- **GRE Tunneling [16]**: Generic Routing Encapsulation (GRE) is a protocol where packets are encapsulated inside other packets. It can connect separate networks and allows protocols on a network that does not support said protocols.
- **IP-in-IP [17]**: Here, IP packets are encapsulated inside other IP packets. There is no encryption, and the encapsulated packets remain unmodified.
- **SSH tunneling [18]**: SSH is typically used for the terminal access of a remote machine, but it can also be used to establish a secure tunnel between two computers.
- **Point-to-Point Tunneling Protocol (PPTP) [19]**: PPTP is an obsolete VPN Protocol that uses a GRE tunnel
- **Secure Socket Tunneling Protocol (SSTP) [20]**: SSTP is a replacement and improvement of PPTP, which encrypts the transfer with SSL/TLS.
- **Layer 2 Tunneling Protocol (L2TP) [21]**: L2TP is a tunnel protocol mainly used in VPNs. It provides a tunnel for Layer 2.[2]
- **Virtual Extensible Local Area Network (VXLAN) [24]**: VXLAN is a network virtualization technique that allows Layer 2 connection over a Layer 3 [3] network.
- **IPv6 in IPv4 Tunnel (or IPv4 in IPv6 Tunnel)**: In 6in4, IPv6 packets are encapsulated in IPv4 packets. This allows the transport of IPv6 packets over an IPv4 network. Vice versa is true for the opposite (4in6: IPv4 over an IPv6 network [6]).

26.4 Conclusion

Tunneling is essential for the secure access of a remote resource as an integral part of most VPN implementations. Without such encrypted tunnels, the traffic to this remote resource would be unencrypted and potentially taped by a malicious third party. In addition, tunneling allows connection networks (e.g., VXLAN) or enables the use of communications protocol on unsupported networks (e.g., 6in4).

[2] "Layer 2, also known as the Data Link Layer, is the second level in the seven-layer OSI [Open Systems Interconnection, see [22] reference model for network protocol design" [23].

[3] Layer 3 is the Network Layer and the third level in the seven-layer OSI reference model [25].

References

1. CSRC Content Editor. tunneling - Glossary | CSRC. https://csrc.nist.gov/glossary/term/tunneling, September 2022.
2. CSRC Content Editor. Full Tunneling - Glossary | CSRC. https://csrc.nist.gov/glossary/term/full_tunneling, September 2022.
3. CSRC Content Editor. split tunneling - Glossary | CSRC. https://csrc.nist.gov/glossary/term/split_tunneling, September 2022.
4. CSRC Content Editor. VPN - Glossary | CSRC. https://csrc.nist.gov/glossary/term/vpn, September 2022.
5. Juniper Networks. Understanding IPsec VPN Modes. https://www.juniper.net/documentation/en_US/junos-space18.4/topics/concept/junos-space-ipsec-vpn-mode-understanding.html, September 2022.
6. Steve E. Deering and Alex Conta. Generic Packet Tunneling in IPv6 Specification. Request for Comments RFC 2473, Internet Engineering Task Force, December 1998. Num Pages: 36.
7. Robert E. Gilligan and Erik Nordmark. Basic Transition Mechanisms for IPv6 Hosts and Routers. Request for Comments RFC 4213, Internet Engineering Task Force, October 2005. Num Pages: 27.
8. Justina Alexandra Sava. VPN market size worldwide 2027. https://www.statista.com/statistics/542817/worldwide-virtual-private-network-market/, September 2022.
9. Zero Trust and BeyondCorp Google Cloud. https://cloud.google.com/blog/topics/developers-practitioners/zero-trust-and-beyondcorp-google-cloud/, September 2022.
10. Shalanda D. Young. M-22-09.pdf. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf, January 2022.
11. Cybersecurity Insiders. 2021 VPN RISK REPORT. Technical report, September 2022.
12. Swiss IT Magazine. VPNs aus der Schweiz im Vergleich. https://www.itmagazine.ch/artikel/77534/VPNs_aus_der_Schweiz_im_Vergleich.html, September 2022.
13. Top global VPN market share by technology 2021.
14. OpenVPN. Business VPN | Next-Gen VPN. https://openvpn.net/, September 2022.
15. Jason A. Donenfeld. WireGuard: Next Generation Kernel Network Tunnel. In *Proceedings 2017 Network and Distributed System Security Symposium*, San Diego, CA, 2017. Internet Society.
16. Tony Li, Dino Farinacci, Stanley P. Hanks, David Meyer, and Paul S. Traina. Generic Routing Encapsulation (GRE). Request for Comments RFC 2784, Internet Engineering Task Force, March 2000. Num Pages: 9.
17. IP in IP Tunneling. Request for Comments RFC 1853, Internet Engineering Task Force, October 1995. Num Pages: 8.
18. Berkeley Information Security Office. Securing Network Traffic With SSH Tunnels. https://security.berkeley.edu/education-awareness/securing-network-traffic-ssh-tunnels, September 2022.
19. Glen Zorn, Gurdeep-Singh Pall, and Kory Hamzeh. Point-to-Point Tunneling Protocol (PPTP). Request for Comments RFC 2637, Internet Engineering Task Force, July 1999. Num Pages: 57.
20. [MS-SSTP]: Secure Socket Tunneling Protocol (SSTP). https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-sstp/c50ed240-56f3-4309-8e0c-1644898f0ea8, September 2022.
21. Anew J. Valencia, Glen Zorn, William Palter, Gurdeep-Singh Pall, Mark Townsley, and Allan Rubens. Layer Two Tunneling Protocol "L2TP". Request for Comments RFC 2661, Internet Engineering Task Force, August 1999. Num Pages: 80.
22. ITU. X.225: Information technology – Open Systems Interconnection – Connection-oriented Session protocol: Protocol specification. https://www.itu.int/rec/T-REC-X.225-199511-I/en, September 2022.

23. Juniper Networks. Layer 2 Networking. https://www.juniper.net/documentation/us/en/software/junos/multicast-l2/topics/topic-map/layer-2-understanding.html, September 2022.
24. Juniper. What is VXLAN? https://www.juniper.net/us/en/research-topics/what-is-vxlan.html.
25. What is Network layer? - Definition from WhatIs.com. https://www.techtarget.com/searchnetworking/definition/Network-layer, September 2022. SearchNetworking.

Part IV
Data Protection

Chapter 27
Differential Privacy

Valentin Mulder and Mathias Humbert

27.1 Introduction

Differential privacy is a technology that allows for sharing information about a dataset while ensuring the protection of individual privacy by adding noise to the results. This results in a constraint on the algorithms used to publish information about a statistical database, limiting the disclosure of private information. Differential privacy is becoming increasingly important as a tool for companies to collect information while controlling the visibility of sensitive data. The field is rapidly advancing with the development of accessible tools and the focus on the usability of open-source differential privacy systems. The technology could benefit Switzerland with the upcoming federal act on data protection, as companies such as Apple and Google have already utilized it to comply with privacy regulations. The implementation of differential privacy can either be done in-house or by purchasing tools.

27.2 Analysis

The literature on privacy protection abounds in various methods whose guarantees are not robust to the auxiliary information a strong adversary may have. Differential privacy provides new means to achieve generic and robust privacy guarantees that

V. Mulder (✉)
Cyber-Defence Campus, Thun, Switzerland
e-mail: valentin.mulder@ar.admin.ch

M. Humbert
University of Lausanne, Lausanne, Switzerland
e-mail: mathias.humbert@unil.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_27

do not depend on the adversary's auxiliary information. It has applications in myriads of settings: census, labor statistics, health records, security, genome-wide association studies, monitoring of education quality, analysis of business strategies, and so on [1].

27.2.1 Definition

Differential privacy is a technology for sharing information about a dataset by describing the patterns of groups within the dataset while withholding information about individuals. This is mainly achieved by adding noise to the results. It will have the following effect: if the arbitrary single substitution in the database is small enough, then the query result cannot be used to infer much about any single individual. Differential privacy, therefore, provides formal privacy guarantees. Another way to describe differential privacy is as a constraint on the algorithms used to publish aggregate information about a statistical database. This limits the disclosure of private information of records whose information is in the database. For example, differentially private algorithms are used by some government agencies to publish demographic information or other statistical aggregates while ensuring the confidentiality of survey responses and by companies to collect information about user behavior while controlling what is visible even to internal analysts [2]. It is also important to note that adding noise to a data set may render it less valuable.

Roughly speaking, an algorithm is differentially private if an observer seeing its output cannot tell if a particular individual's information was used in the algorithm's computation. Differential privacy is often discussed in identifying individuals whose information may be in a database. Although it does not directly refer to the identification and reidentification attacks, differentially private algorithms probably resist such attacks [3].

27.2.2 Trends

In the cases of counting, summation, or average queries over a large, single table of data, DP is ready to be used effectively. However, some other settings still have problems. For example, one key drawback of differential privacy is that it often trades data accuracy for privacy. Typically, suppose the database size on which statistics are computed is too small. In that case, the amount of noise that needs to be added to the statistics is often too high to keep some statistical accuracy. Moreover, the DP guarantees decrease proportionally to the number of statistical queries made to the database. Similarly, implementations of queries on multiple tables, synthetic data generation, and deep learning exist, but they may only sometimes be accurate enough [4]. These drawbacks are due to the solid adversarial assumptions that are key to providing formal privacy guarantees against an adversary.

Progress on tools for differential privacy has accelerated rapidly in the past several years, and we look forward to the availability of accessible tools for these tasks shortly. Indeed, companies like Apple or Google already use differential to anonymize their customer data [5, 6]. This is completed by different open-source libraries, like the one from Google and IBM [7, 8].

The academic field also works on challenges like ensuring correctness and automatic proofs. Nevertheless, the solutions remain primarily theoretical. Finally, open-source differential privacy systems have recently started focusing on usability. The OpenDP [9] and diffprivlib [10] projects both provide notebook-based programming interfaces that will be familiar to many data scientists, as well as extensive documentation. Researchers are beginning to study the usability of systems like these, which will likely lead to further improvements [11].

27.3 Consequences for Switzerland

The federal act on data protection should come into effect in September 2023 [12]. Differential privacy could be a great tool to help the government and large companies better comply with this new law. Big tech companies, like Apple, Google, Uber, and Facebook, have used different applications of this technology that could be a source of inspiration for Switzerland [13]. The primary example remains the United States Census which takes place every ten year [14].

27.3.1 Implementation Possibilities: Make or Buy

See Table 27.1.

27.4 Conclusion

Organizations should consider differentially private approaches to increase data protection. While differential privacy is not a field that is widely commercially developed, it can provide beneficial results when properly applied.

Differential privacy is a powerful tool for quantifying and solving practical problems related to privacy. Its flexible definition allows it to be applied in a wide range of applications, including machine learning applications [4, 15]. The technology is at its starting point. However, it holds the promise of benefiting big data analysis without compromising on privacy [16].

Table 27.1 Implementation possibilities for different sectors

	Make		Buy	
	Pros	Cons	Pros	Cons
Military	Full control over implementation	Error in implementation and lack of compatibility	Working solution	Might contain accidental or purposeful backdoors
Civil Society	None	Many resources needed to implement a functioning solution	Easy adoption	Associated cost and lack of technical knowledge
Economy	In-house solution	Liability in case of security holes	Easy implementation and no liability in case of security holes	

References

1. Cynthia Dwork. Differential Privacy. In Henk C. A. van Tilborg and Sushil Jajodia, editors, *Encyclopedia of Cryptography and Security*, pages 338–340. Springer US, Boston, MA, 2011.
2. Wikipedia, Differential privacy. https://en.wikipedia.org/w/index.php?title=Differential_privacy&oldid=1098798710, July 2022.
3. Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. Calibrating Noise to Sensitivity in Private Data Analysis. In Shai Halevi and Tal Rabin, editors, *Theory of Cryptography*, Lecture Notes in Computer Science, pages 265–284, Berlin, Heidelberg, 2006. Springer.
4. Implémenter la confidentialité différentielle avec TensorFlow Privacy | Responsible AI Toolkit.
5. How Google anonymizes data – Privacy & Terms – Google. https://policies.google.com/technologies/anonymization?hl=en, November 2022.
6. Apple. Apple Differential Privacy Technical Overview. https://www.apple.com/privacy/docs/Differential_Privacy_Overview.pdf, November 2022.
7. Differential Privacy. https://github.com/google/differential-privacy, November 2022. original-date: 2019-09-04T13:04:15Z.
8. Diffprivlib v0.6. https://github.com/IBM/differential-privacy-library, November 2022. original-date: 2019-06-18T13:36:41Z.
9. OpenDP. ulrhttps://privacytools.seas.harvard.edu/opendp, October 2022.
10. Naoise Holohan, Stefano Braghin, Pól Mac Aonghusa, and Killian Levacher. Diffprivlib: The IBM Differential Privacy Library, July 2019. arXiv:1907.02444 [cs].
11. Joseph Near. Differential Privacy: Future Work & Open Challenges. *NIST*, January 2022. Last Modified: 2022-01-24T12:00-05:00 Publisher: Joseph Near.
12. La nouvelle Loi sur la protection des données arrivera plus tard que prévu.
13. Alexandra Wood, Micah Altman, Aaron Bembenek, Mark Bun, Marco Gaboardi, James Honaker, Kobbi Nissim, David O'Brien, Thomas Steinke, and Salil Vadhan. Differential Privacy: A Primer for a Non-Technical Audience. *SSRN Electronic Journal*, 2018.

14. US Census Bureau. Statistical Safeguards. https://www.census.gov/about/policies/privacy/statistical_safeguards.html, August 2022. Census.gov.
15. Confidentialité différentielle dans TFF | TensorFlow Federated.
16. An Nguyen. Understanding Differential Privacy. https://towardsdatascience.com/understanding-differential-privacy-85ce191e198a, August 2022. Medium.

Chapter 28
Digital Rights Management

Sophia Ding

28.1 Introduction

Digital Rights Management (DRM) systems have been used for decades to protect companies' intellectual property and ensure the trusted exchange of digital information over the internet. DRM systems serve multiple functions, such as access control, usage control, billing, and the pursuit of legal infringements. These functions are achieved through various technologies, such as encryption, digital signatures, digital watermarks, secure authentication, rights expression languages, and product keys. The section provides a comprehensive overview of the various DRM functions and technologies, making it an essential resource for anyone interested in understanding the workings of DRM systems.

28.2 Analysis

Digital Rights Management has been around for decades. However, traditional systems were designed for something other than the highly interconnected world where content such as music, movies, and eBooks are just a click away. In addition, new technologies such as blockchain have the potential to revolutionize the DRM system. As a result, the importance of DRM is decreasing in some industries, but it remains an essential part of modern business models in the streaming economy.

S. Ding (✉)
Eraneos Switzerland AG, Zurich, Switzerland
e-mail: Sophia.Ding@eraneos.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_28

28.2.1 Definition

Essentially, Digital Rights Management refers to "trusted exchange of digital information over the Internet in which the user is granted only those privileges granted by the document sender" [1]. A Digital Rights Management system is designed to protect companies' intellectual property, i.e., their intellectual creations and the underlying business models. The first DRMs were used in the 1980s as copy protection for pay television. In recent decades, and the aftermath of the digitalization era, use cases in the music and gaming industries have been identified [2].

DRM systems protect a copyright holder's interests in the following ways:

- Access control (AC): Using DRM, only authenticated and identified users can access legal content. It is possible, for example, that the content is encrypted and that only authorized users are permitted access [3]. In addition, it is possible to restrict access to content based on specific criteria. For example, content is available only to individuals within a particular geographical area (regional lockout) [4].
- Usage control (UC): It is determined by DRM systems how much users can consume. Depending on the user group and the type of subscription, this might vary [2]. In addition, it is possible to apply other types of restrictions, such as activation limits, which limit the number of devices on which content can be installed and consumed [3].
- Billing (BI): Various billing models can be implemented within DRM systems [2].
- Pursuit of legal infringements (LI): The use of DRM systems allows the ex-post verification of the authenticity and integrity of the content. Watermarks and tags may indicate that a piece of content is protected by a copyright. Copy protection is an everyday use case for this function [5].

Each of the above functions relies on a different technology. Table 28.1 provides examples.

In recent years, DRM systems have been controversial due to privacy concerns, their potential negative impact on open-source software, and their incompatibility with fair use principles [3]. It is based on the belief that the public is entitled to freely and impartially access portions of copyrighted materials to comment and critique [9].

28.2.2 Trends

It is important to note that the importance of DRM varies across industries: although it is diminishing the traditional music industry. Numerous business models for streaming platforms and eBook providers are based on their role [2]. Key DRM trends in the coming years are listed in Table 28.2.

Table 28.1 Technologies on which different digital rights management functions rely

	Description	AC	UC	BI	LI	
Encryption	Encrypted information is used to protect the confidentiality of information from unauthorized access.	++	++		+	[2, 5]
Digital Signature	Authenticates documents using the creator's private key, which represents a digital fingerprint. See also Digital Signature (see Chapter 15).				++	[2, 5]
Digital Watermark	Ensures the authenticity and integrity of a digital work by containing hidden steganographic meta-information within the digital work, which allows a unique identification of the work	+	+		++	[2, 5, 6]
Secure Authentication	In light of trends such as the Internet of Things and wearable devices, biometric authentication is becoming increasingly relevant. The term refers to identifying individuals based on their physical characteristics or behavior. A smartcard can authenticate all parties within a DRM environment and is an alternative to encryption-based authentication. See also Biometrics (see Chapter 22) and Authentication (see Chapter 29).	++		++		[2, 5, 7]
Rights Expression Language	Representation of the licensing conditions in a machine-readable format to limit access to the content.	++	++	++		[2]
Product Keys	Used to prevent the unauthorized access of a particular copy of the software.	++	++		+	[8]

Table 28.2 Key digital rights management trends

Trend Category	Trend	Description	
Use Cases	Online education platforms	Online education platforms (e.g., Coursera) are becoming increasingly popular. They pose several challenges in DRM, such as the infringement of the course's copyright and the verification of online certificates. Recently, blockchain-based DRM solutions have been suggested for this application.	[10]
	Music streaming platforms	Music streaming platforms (such as Spotify) with millions of users have created new challenges for digital rights management since DRM was created when streaming was not an option. A chain of contracts is generated whenever a user streams a song, and rights are transferred. Consequently, streaming platforms have begun experimenting with blockchain technology to eliminate the "middleman" and simplify the transaction process.	[11]
Technical Development	DRM based on blockchain	The traditional DRM systems pose several challenges, which new digital business models, such as streaming platforms, exacerbate. These include 1) the centralization of protected information, which makes it more susceptible to cyberattacks, and 2) the opaque nature of copyright and transaction information, negatively impacting the user experience. On the other hand, blockchain technology, especially non-fungible tokens (NFT), is a decentralized, secure, and reliable technology that can be maintained collectively. Therefore, it offers an interesting alternative to existing DRM systems.	[11, 12, 13, 14, 15]
	DRM based on biometrics	The Internet of Things (IoT), for example, has created numerous possibilities for accessing content from mobile devices. DRM systems that utilize biometrics provide a good user experience. However, biometric-based authentication schemes are susceptible to device theft. These risks may be addressed by authentication protocols that use several factors, including biometrics	[16, 17]
Risks	Chip Shortage	Several DRM systems make use of computer chips as watermarks: In 2022, Canon, the manufacturer of printers and copy machines, was forced to disable its DRM system for office printers due to a shortage of the chips required to ensure that only original Canon toner cartridges are inserted into Canon products. As a result of the semiconductor crisis and its impacts on global value chains, DRM systems have also been adversely affected.	[18]

28.3 Consequences for Switzerland

The World Intellectual Property Organization (WIPO) published two Internet treaties in 1996 ([19, 20]), which govern copyright issues, such as those related to music records. As a result of these treaties, intellectual property is legally protected, and those who infringe on this property are sanctioned. In 2008, Switzerland ratified these treaties by amending its federal copyright law (Copyright Act, CopA) [21, 22]. Following the Copyright Act, users are prohibited from circumventing DRM unless there are legal requirements, such as prosecution. In addition, a Swiss Monitoring Office for Technological Measures (OTM) was established after the revision of the Copyright Act to continuously evaluate the impacts of technological measures on the consumption of copyrighted content.

Several Swiss research groups work on DRM, ranging from consumer acceptance of protected digital content to blockchain technology and collective rights management [23, 24]. ETH Zurich's Intellectual Property Group (Bechtold), part of the Center for Law & Economics, focuses specifically on DRM [25]. A project on innovative rights and access management inter-platform was also co-funded by the federal government in the past [26]. Sharedien (Wallisellen, ZH) offers cloud-based DRM services in the private sector.

28.3.1 Implementation Possibilities: Make or Buy

As far back as the 1980s, the first commercial DRM software was known as DigiBox. It had its origins in library software. Xerox and IBM were among the first large commercial providers of DRM [27]. Intending to create a royalty-free DRM standard in 2005, Sun Microsystems launched an open-source project (DRM everywhere/available). Unfortunately, the project was discontinued in 2008 due to inactivity [28].

28.3.2 Variation and Recommendation

Concepts related to DRM include:

- Digital Asset Management (DAM): A DAM is a system used by organizations to manage (e.g., store, retrieve, organize, or share) content in an asset library. Therefore, DAM is a component of DRM. To avoid legal penalties, DRM utilizes technical means to ensure that a company does not infringe copyright when using content from its asset library [2, 29].
- Enterprise DRM (EDRM): As a pillar of data-oriented security and an integral part of security concepts, EDRM is becoming increasingly important. As with DRM systems, EDRM systems offer various functionalities, including access

control and identity management. Access rights to data are defined by EDRM systems independent of the application, device, or access point used by the user or users. Users must authenticate themselves in order to access restricted content. A typical use case would be to protect highly confidential documents and emails being exchanged between several parties to which several parties have access. The rights of access to data can expire or be revoked by the owner of the data [30].

28.4 Conclusion

Although DRM systems have been widely used to protect the copyright of multimedia content, organizations also use DRM systems for security purposes. In an increasingly interconnected world, DRM systems will become increasingly important overall, but they will lose their influence in specific industries, such as the traditional music industry.

References

1. DRM (Digital Rights Management). https://www.gartner.com/en/information-technology/glossary/drm-digital-rights-management, August 2022. Gartner Glossary.
2. Tassilo Pellegrini. Digital Rights Management - Technologien, Anwendungsbereiche und Entwicklungsperspektiven. In Jan Krone and Tassilo Pellegrini, editors, *Handbuch Medienökonomie*, pages 329–346. Springer Fachmedien Wiesbaden, Wiesbaden, 2020.
3. Electronic Privacy Information Center. Digital Rights Management and Privacy. https://archive.epic.org/privacy/drm/, March 2004.
4. Introduction: Regional Lockout as Technology, Distribution, and Culture. In *Locked Out*, pages 1–22. New York University Press, December 2020.
5. *Encyclopedia of Cryptography and Security*.
6. JNTUH, Kavitha Soppari, and N.Subhash Chandra. Study of Digital Watermarking Algorithms for Digital Rights Management and their Attacks. 67(1):16–24, January 2019. International Journal of Computer Trends and Technology.
7. Hung-Wen Yang, Chou-Chen Yang, and Woei Lin. Enhanced digital rights management authentication scheme based on smart card. 7(3):189–194, September 2013. IET Information Security.
8. Douglas E. Phillips. *The software license unveiled: how legislation by license controls software access*. Oxford Univ. Press, Oxford, 2009.
9. Stanford Libraries. Fair Use. https://fairuse.stanford.edu/overview/fair-use/#:~:text=Fair%20use%20is%20a%20copyright,novelist's%20work%20without%20asking%20permission., August 2022.
10. Junqi Guo, Chuyang Li, Guangzhi Zhang, Yunchuan Sun, and Rongfang Bie. Blockchain-enabled digital rights management for multimedia resources of online education. *Multimedia Tools and Applications*, 79(15-16):9735–9755, April 2020.
11. Tatiana Koffman. How Blockchain Will Transform Media & Entertainment. February 2020. Forbes.
12. Michèle Finck and Valentina Moscon. Copyright Law on Blockchains: Between New Forms of Rights Administration and Digital Rights Management 2.0. *IIC - International Review of Intellectual Property and Competition Law*, 50(1):77–108, January 2019.

13. Abba Garba, Ashutosh Dhar Dwivedi, Mohsin Kamal, Gautam Srivastava, Muhammad Tariq, M. Anwar Hasan, and Zhong Chen. A digital rights management system based on a scalable blockchain. *Peer-to-Peer Networking and Applications*, 14(5):2665–2680, September 2021.
14. Andrew Guadamuz. What do you actually own when you buy an NFT? https://www.weforum.org/agenda/2022/02/non-fungible-tokens-nfts-and-copyright/, February 2022.
15. Everything You Need to Know About NFT for Digital Rights Management.
16. Cheng-Chi Lee, Chun-Ta Li, Zhi-Wei Chen, and Yan-Ming Lai. A Biometric-Based Authentication and Anonymity Scheme for Digital Rights Management System. *Information Technology And Control*, 47(2):262 – 274, June 2018.
17. SungJin Yu, KiSung Park, YoHan Park, HyungPyo Kim, and YoungHo Park. A lightweight three-factor authentication protocol for digital rights management system. *Peer-to-Peer Networking and Applications*, 13(5):1340–1356, September 2020.
18. Halbleiterkrise: Canon entfernt Kopierschutz, aber nur auf Bürodruckern.
19. World Intellectual Property Organization. WIPO Copyright Treaty. https://wipolex.wipo.int/en/text/295166, urldate = 2022-08-05, December 1996.
20. World Intellectual Property Organization. WIPO Performances and Phonograms Treaty (WPPT). https://www.wipo.int/treaties/en/ip/wppt/summary_wppt.html, 1996.
21. Federal Assembly of the Swiss Conferedation. Federal Act on Copyright and Related Rights. https://www.fedlex.admin.ch/eli/cc/1993/1798_1798_1798/en, October 1992.
22. Droit d'auteur: La gestion numérique des droits (DRM). https://libguides.graduateinstitute.ch/droit-dauteur/DRM, June 2022.
23. Dana Mareckova. Blockchain and Collective Rights Management of Copyright and Related Rights at the Global Level. https://p3.snf.ch/project-187702, August 2022.
24. Marc Fetscherin. Digital Rights Management - Modeling Consumer Acceptance of Protected Digital Content. https://p3.snf.ch/project-104449, August 2022.
25. ETH Zurich. Intellectual Property Group (Bechtold). https://ip.ethz.ch/, August 2022.
26. ARAMIS. TIRAMISU: The innovative rights and access management inter-platform solution. https://www.aramis.admin.ch/Texte/?ProjectID=18999&Sprache=en-US.
27. Ernie Smith. The Incredibly Technical History of Digital Rights Management. https://www.vice.com/en/article/evbgkn/the-incredibly-technical-history-of-digital-rights-management, October 2017. Vice.
28. John Leyden. Sun pushes open-source DRM scheme. August 2005.
29. *Encyclopedia of library and information sciences.* 2009. OCLC: 1082244237.
30. Mario de Boer. Deploying Enterprise Digital Rights Management to Control and Monitor Unstructured Data. August 2017. Gartner Research.

Chapter 29
Authentication

Belinda Müller

29.1 Introduction

The purpose of authentication is to verify the identity of an entity. The number of factors required to authenticate an entity determines the type of authentication—single-factor, two-factor, or multi-factor. The section delves into the trends and advancements in the field of authentication, with a focus on security and usability. The section covers topics such as the current state of password security, the emergence of passwordless authentication, and the future potential of biometric authentication. The section also discusses current authentication trends, including adaptive and continuous authentication.

29.2 Analysis

29.2.1 Definition

An authentication process is a process of verifying an entity's identity based on one or multiple factors [1]. A factor can be something the entity is (e.g., device fingerprinting for devices or biometrics such as a retina, face, or behavior for a person), possesses (e.g., a token or a bank or ID card), or knows (e.g., a password or algorithm) [2]. Sometimes a location factor is listed as a fourth category [3]: Location and/or time of the entity's login, e.g. GPS coordinates, IP address, or cellular triangulation. An entity may be, for instance, a computer or smartphone

B. Müller (✉)
Eraneos Switzerland AG, Zurich, Switzerland
e-mail: Belinda.Mueller@eraneos.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_29

or a user using such a device. Depending on the number of credentials (or factors) required, the authentication process is referred to as single-factor authentication (SFA), two-factor authentication (2FA), or multifactor authentication (MFA). Note that MFA includes two-factor authentication. Behavior can also be a factor in behavior-based authentication and continuous authentication systems.

29.2.2 Trends

Security Factors

Password security has inherent weaknesses [4], particularly sensitivity to social engineering (for example, phishing) and dictionary attacks. However, passwords remain the most popular authentication method worldwide, according to an Okta Inc. study conducted in 2021 [5]. According to this study, 5% of organizations worldwide use passwords as their primary security measure. Moreover, the password management market revenue is expected to increase from 1.25 billion U.S. dollars in 2020 to 3.07 billion U.S. dollars by 2025 [6].

Although the knowledge factor is still omnipresent, the opposite trend of passwordless authentication is emerging. Passwordless authentication eliminates the knowledge factor and relies on more substantial security factors such as ownership and biometrics. In 2020, the worldwide market revenue for passwordless authentication was approximately 10.3 billion U.S. dollars and was expected to reach 25.2 billion U.S. dollars by 2025 [7]. However, biometrics is often just an add-on for better usability, especially in the mobile domain. For example, Android and iPhones still rely on a pin or strong password in the background. A promising approach to passwordless authentication is the authentication standard *FIDO2*, which was developed by the FIDO alliance, an open industry association. FIDO2 is based on public key cryptography, stores credentials on a user's device, and uses unique credentials for every website [8]. This makes it not only resistant to replay attacks and password theft but also against some phishing attacks [8], to which other forms of MFA are still susceptible. However, this does not prevent online-phishing attacks where the attacker is the proxy to the actual service.

With the surge of wearables and other IoT devices, biometric factors in the future as wearables could be the only workable solution. This might be problematic because these new devices will need a strong password. By 2027, the worldwide biometric authentication and identification market is expected to reach almost 100 billion U.S. dollars, up from 33 billion U.S. dollars in 2019 [9]. The significant barriers to large-scale use of passwordless authentication are considered to be legacy systems and applications: 61% of IT staff and 58% of IT security leaders worldwide in 2022 reported that legacy systems and applications did not support the technology as one of the main barriers to using passwordless [10].

Authentication Approaches
Current trends attempt to enhance security and usability. These include:

- Adaptive authentication [11]: The authentication procedure in adaptive or risk-based authentication is determined by an entity's context. Contextual factors, such as a device's location or the data sensitivity a user requests, are considered during authentication. Following this, an authentication risk score is calculated, often utilizing machine-learning techniques. This risk score determines how many security measures are required. We are staying on top of security by using adaptive authentication when increasing usability. This approach was recommended in the NIST Digital Identity Guidelines from 2017 [12].
- Continuous authentication [3]: During continuous or active authentication, the identity of an entity is recurrently verified based on patterns derived from continuous monitoring of the entity. This is achieved primarily by using behavioral or biometric factors such as keystroke patterns, mouse movements, or gait patterns (see also Real-time Biometric Authentication in Chap. 22). With this approach, impersonation attacks can be prevented more effectively than static authentication: the perpetrator must continuously mimic the entity's behavior. Otherwise, they would be blocked when an untypical behavior is detected [13]. However, the continuous collection of biometric and behavioral data has raised concerns regarding privacy, which must be addressed.
- Authentication technology for the approval of sensitive user actions: Authentication technology is commonly used to approve financial transactions: the transaction details are sent to the payer via an independent channel to be confirmed via a security factor, for example, via *3D Secure* (see Chap. 32.1 for details). This can help secure transactions against the compromise of operating systems or browsers through malware. However, using authentication technology to approve sensitive user actions is not limited to financial transactions but can also be implemented, for example, for changing one's online account details.

29.3 Consequences for Switzerland

According to a study conducted by ESET in 2022, most Swiss smartphone users use a PIN to access their smartphones [14], and Swiss people need to manage their passwords better. In the study, 12% of the participants used identical passwords for multiple accounts, but only 5.8% did so in Germany [15]. According to the study, 14% of Swiss participants always use 2FA for online services, which is in line with the recommendation by the Swiss National Cyber Security Centre to use MFA whenever possible [16]. In Germany, however, 27.8% reported always using two-factor authentication. This is still significantly less. Regarding biometric authentication, there seems to be a general interest and openness to this technology among the Swiss people: As of 2019, 85% of Swiss citizens indicated that

fingerprint authentication was the most secure method for making credit card payments [17].

Also, authentication is generally well represented in research in Switzerland, e.g., at the Idiap Research Institute ([18], biometric authentication), IBM Zurich ([19] password cryptography). Also, this research has been successfully transferred, leading to spin-offs like Token2 Sàrl (University of Geneva) and Futurae Technologies AG (ETH Zurich).

29.3.1 Implementation Possibilities: Make or Buy

In choosing a particular authentication solution for organizations, it is crucial to balance security, usability, cost, and privacy considerations. The authentication solution for a particular service can be predetermined for the private individual, although stronger authentication can be enabled if desired. It can also increase security by purchasing additional solutions, such as a password manager or hardware security keys. The following are some considerations for the different security factors:

- Knowledge factor: Passwords are still prevalent, so it is essential to maintain a secure password management system. A variety of commercial password managers can assist in breaking habits like reusing passwords or writing them down. There are also free options, such as open-source password managers, and numerous options integrated into many browsers and smartphones. According to Grauer and Klosowski [20] 1Password [21] is the best password manager, whereas Bitwarden [22] is the best free solution.
- Ownership factor: There is an abundance of authenticator applications to choose from, including Authy [23], the Microsoft Authenticator [24], or Duo [25]. The Yubico Security Key series [26] and the Google Titan Security Key [27] can also be purchased as hardware tokens. It is essential to consider whether such devices meet industry standards such as FIDO2 and whether they are compatible with future trends such as passwordless authentication. In addition to hardware tokens, Swiss providers offer software tokens, including Swiss SafeLab, Token2 Sàrl, or Futurae Technologies AG.
- Biometric factor: The sourcing of biometric authentication solutions can be challenging due to the highly specialized technology required. Furthermore, privacy regulations and data protection regulations need to be considered. One option to address privacy for biometric authentication is to store biometric data only on a user's device instead of remotely on servers. For more privacy and information about commercial and open-source solutions, please see Chap. 22.

29.4 Conclusion

Though knowledge-based authentication has been known to have shortcomings, it remains the most popular method for entity authentication. The shortcomings are currently addressed through sophisticated password management and multifactor authentication. Nevertheless, concurrently with the increase in IoT devices and advances in machine learning, there is a trend towards passwordless authentication utilizing biometrics and new authentication approaches such as continuous and adaptive authentication. While these trends suggest a more secure and user-friendly authentication process, they may also introduce new privacy concerns that must be addressed in the future.

References

1. EbruCelikel Cankaya. Authentication. In Henk C. A. van Tilborg and Sushil Jajodia, editors, *Encyclopedia of Cryptography and Security*, pages 61–62. Springer US, Boston, MA, 2011.
2. Aleksandr Ometov, Sergey Bezzateev, Niko Mäkitalo, Sergey Andreev, Tommi Mikkonen, and Yevgeni Koucheryavy. Multi-factor authentication: A survey. *Cryptography*, 2(1):1, 2018. Publisher: MDPI.
3. Dipankar Dasgupta, Arunava Roy, and Abhijit Nag. *Advances in User Authentication*. Infosys Science Foundation Series. Springer International Publishing, Cham, 2017.
4. Passwords — Strengths and Weaknesses. https://www.garykessler.net/library/password.html.
5. Okta Inc. The State of Zero Trust Security 2021. Technical report, June 2021.
6. Justina Alexandra Sava. Password management market revenue worldwide in 2020 and 2027. https://www.statista.com/statistics/1300988/global-password-management-market-revenue/, June 2022. Statista.
7. Justina Alexandra Sava. Passwordless authentication global market size 2030. https://www.statista.com/statistics/1290586/passwordless-authentication-global-market-size/, August 2022. Statista.
8. FIDO Alliance. FIDO2. https://fidoalliance.org/fido2/, August 2022.
9. Justina Alexandra Sava. Biometric authentication and identification market revenue worldwide in 2019 and 2027. https://www.statista.com/statistics/1012215/worldwide-biometric-authentication-and-identification-market-value/, February 2022. Statista.
10. Justina Alexandra Sava. Main barriers to adopting passwordless authentication worldwide 2022. https://www.statista.com/statistics/1305837/global-barriers-to-adopting-passwordless-authentication/, May 2022. Statista.
11. Patricia Arias-Cabarcos, Christian Krupitzer, and Christian Becker. A survey on adaptive authentication. *ACM Computing Surveys (CSUR)*, 52(4):1–30, 2019. Publisher: ACM New York, NY, USA.
12. P.A. Grassi, J. L. Fenton, E. M. Newton, R. A. Perlner, A. R. Regenscheid, W. E. Burr, and M. F. Therfanos. Nist special publication 800-63b. digital identity guidelines: authentication and lifecycle management. Technical report, NIST, 2017.
13. Lorena Gonzalez-Manzano, Jose M. De Fuentes, and Arturo Ribagorda. Leveraging User-related Internet of Things for Continuous Authentication: A Survey. *ACM Computing Surveys*, 52(3):1–38, May 2020.
14. Studie: Die Schweizer Bevölkerung verwaltet ihre digitalen Zugänge und Passwörter ziemlich schlecht.

15. ESET. Deutschland holt auf: Passwort wird für Online-Nutzer zum alten Eisen. https://www.eset.com/de/about/presse/pressemitteilungen/pressemitteilungen/deutschland-holt-auf-passwort-wird-fuer-online-nutzer-zum-alten-eisen-2/, August 2022.
16. National Cyber Security Centre NCSC. Protect your accounts. https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-private/aktuelle-themen/schuetzen-sie-ihre-konten.html, February 2021.
17. Visa Studie: Biometrische Authentifizierungsmethoden werden bei Schweizer Karteninhabern immer beliebter.
18. idiap Research Institute. Biometrics Security & Privacy. https://www.idiap.ch:/en/scientific-research/biometrics-security-and-privacy/index_html, August 2022.
19. Jan Camenisch, Anja Lehmann, Gregory Neven, and Kai Samelin. Virtual smart cards: How to sign with a password and a server. In *International Conference on Security and Cryptography for Networks*, pages 353–371. Springer, 2016.
20. Yael Grauer and Thorin Klosowski. The Best Security Key for Multi-Factor Authentication. July 2022. The New York Times.
21. 1Password. 1Password. https://1password.com/, August 2022.
22. Bitwarden. Bitwarden Open Source Password Manager. https://bitwarden.com/, August 2022.
23. Twilio Authy. Authy | Two-factor Authentication (2FA) App & Guides. https://authy.com/, August 2022.
24. Microsoft. Microsoft authenticator. https://www.microsoft.com/en/security/mobile-authenticator-app?rtc=1, August 2022.
25. Cisco. Duo. https://duo.com/product/multi-factor-authentication-mfa/duo-mobile-app, August 2022.
26. Yubico. Yubico | YubiKey Strong Two Factor Authentication. https://www.yubico.com/, August 2022.
27. Titan Security Key - FIDO U2F USB-C NFC Bluetooth - Google Store. https://store.google.com/us/product/titan_security_key?hl=en-US, August.

Part V
Use-Cases

Chapter 30
Secure Media

Touradj Ebrahimi

30.1 Introduction

Technological advancements make it easy to capture, process and distribute multimedia content such as sound, picture, and video. This has been made possible through the widespread use of mobile multimedia devices, access to cloud computing infrastructure, broadband communication, and social networks. However, this paradigm also brings new security challenges, particularly in media security. Media security is a subset of information security and is concerned with protecting the semantic information behind multimedia assets, such as images, instead of just representing the information. Media security problems can be divided into two main clusters: creator-centric and content-centric. The former is about problems related to the content creator, such as copyright protection and source authentication. The latter concerns the content, such as conditional access and integrity verification. Media security solutions include labeling, monitoring, fingerprinting, forensics, and watermarking.

30.2 Analysis

With advances in information and communication technologies, it is now easy to capture, process (including manipulate), and widely distribute content seamlessly. The past practices where the content was produced by just a few professionals (e.g. press and media outlets) and distributed through a limited number of channels (e.g.

T. Ebrahimi (✉)
EPFL, Lausanne, Switzerland
e-mail: touradj.ebrahimi@epfl.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_30

Radio and TV) have been replaced by social media or user-generated content where not only professionals but also consumers can now generate content of all sorts in the form of sound, picture and video and to distribute them widely.

This change has been, in particular, triggered by the wide adoption of mobile multimedia (e.g. smartphones with high-performance cameras and microphones, powerful processors, and wideband networks), a growing number of Internet of Multimedia Things (e.g. security cameras, smart glasses, wearable cameras), access to affordable cloud computing infrastructure (e.g. ample capacity storage and processing power and associated software), broadband communication (e.g. high-speed Internet and 5G), social networks (e.g. Instagram, Snapchat, and TikTok) and computational imaging and computer vision based on artificial intelligence.

This new paradigm brings considerable advantages and challenges, particularly regarding security.

Media security is a subset of information security where the information exhibits several specificities, among which the most important are:

- The information in media has a perceptual dimension, in the sense that it is destined to be perceived either by humans (in a large majority of cases today) or analyzed by machines (a growing trend).
- The information in media exhibits a particular underlying structure that can be leveraged both to secure and attack them.
- The information in media often represents high-value assets either from monetary (e.g. music and movies) or affective (photos of essential persons or events) viewpoints.

Many tools and solutions developed in generic information security can be directly applied to media. For example, one could digitally sign (see Chap. 15) an image to enable viewers to check its authenticity. This is of limited use to secure media because media security is about protecting information, not a specific representation of it. Consequently, to protect the integrity of information in an image, one would need a technology that is indifferent to converting the image to a different format or slight change to its resolution. It should also be able to cope with image artifacts caused by such conversions, such as compression artifacts.

One of the significant differences and the main objective of media security is to protect the semantic information representing assets in multimedia as opposed to the protection of the specific representation of such content. For example, when protecting the integrity of a picture in JPEG format, a good media security solution will not merely protect the integrity of the bits that represent that picture in that format but the semantic content behind those bits. This can be done in such a way that the integrity would still be protected if those bits change (for example, in the picture is converted to PNG format) without changing the content behind the bits (as far as the content of the picture has not changed and it is perceived the same).

In addition, several security concepts, such as integrity protection, are different in the context of media than in generic information. Others, such as watermarking, have no direct counterparts.

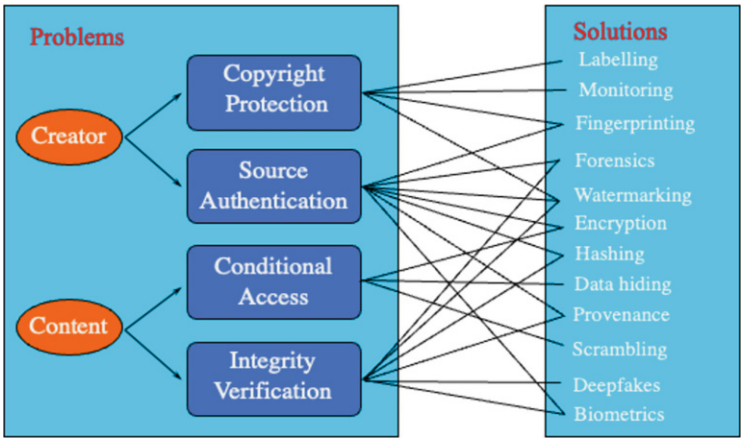

Fig. 30.1 Media security problems and related solutions

Media security problems can be divided into two main clusters, creator-centric and content-centric. The first one is about the problems generated by the content creator. These also can be divided into two categories: copyright protection, ensuring that the creator has the rights related to the content, and source authentication, which ensures that the content is related to its creator. The second cluster is about the content itself. It also can be divided into two categories: conditional access, which can be linked to digital right management (see Chap. 28), and integrity verification which is about verifying that the content has not been modified (Fig. 30.1).

30.2.1 Definition

Labeling [1]: Annotation of multimedia content by taking advantage of its metadata insertion mechanism by providing information about the condition of use and ownership. The label can be put in a pre-defined location in the file format and accessed or in the form of a visible mark, logo, or label, mainly when the content is of visual form.

Monitoring [2]: Tracing the ownership changes of a digital asset (content) by keeping a record of it in a ledger (e.g. in a blockchain).

Fingerprinting [3]: Inclusion of information about interactions between users and content into a media asset.

Forensics [4]: General terminology refers to all analytical techniques to detect if a digital asset has been tampered with or is coming from the claimed source.

Watermarking [5]: Insertion of imperceptible information (e.g. an identifier) through a secret code within a digital asset.

Encryption [6]: An algorithm to convert a piece of clear information into a cipher text and vice versa through a secret key.

Hashing [7]: An algorithm that cryptographically maps a digital asset into a predefined number of bits in a hard-to-reverse manner to create a unique fingerprint of the content that will be changed with the slightest modifications. A perceptual hash is an algorithm like a cryptographic hash, but the signature is modified only when the semantic content of the digital asset is modified.

Data hiding [8]: Refers to all techniques which aim at obfuscating the existence of a covert message. Often the hidden message is represented in a container of the same or other modality of information as opposed to the modality of the message itself. Information hiding techniques such as steganography extensively use multimedia content for data hiding.

Provenance [9]: Refers to algorithms and procedures that produce a log of the history of a digital asset from creation to the moment it is being accessed or consumed.

Scrambling [10]: Refers to algorithms similar to encryption but targeted to media assets and preserve the nature of the content after they have been applied (e.g. a scrambled JPEG image will remain a JPEG image and can be displayed as such). The degree of modification in scrambling can often be set to make the content more or less intelligible. For example, scrambling could be applied to a specific portion of the media asset.

Deepfake detection [11]: Generally, it refers to digital assets in the form of audio, image, or video (often containing people) where artificial intelligence techniques are used to change the content. Shallowfakes and cheapfakes are variations of the latter where either the techniques could be more efficient or when they are not based on artificial intelligence. However, the objective of the manipulation is the same. Artificial intelligence can also be used to detect such manipulations through training with examples. However, these techniques only work on transformed digital assets rather than the ones generated from scratch.

30.2.2 Trends

With the growing reliance on multimedia content in the daily lives of citizens, both professionally and in their private lives, media security is becoming an essential technology to include in many applications. The following presents some of the immediate challenges and trends:

- Privacy protection in pictures and video, particularly for video surveillance and social networks and especially in the context of GDPR [12].
- Countermeasures to fight the growing use of deepfakes to spread misinformation.
- Media security standardization to create interoperable, secure ecosystems, particularly those developed by International Standardization Organizations such as JPEG [13].

30.3 Consequences for Switzerland

Historically, Switzerland has been considered a country of stability, trust, and security. Several standard-setting organizations dealing with information and communication technologies, including those defining security mechanisms, are also based in Switzerland, and it is easier for Swiss actors in media security to play an essential role in the definition of media security standards that will be the backbone of information and communication technologies in the new world order. Furthermore, like any other country, Switzerland is also vulnerable to misinformation which can result in unrest and instability and hurt its so-far impeccable image.

30.3.1 Implementation Possibilities: Make or Buy

It is only possible to decide abstractly and by knowing the precise application and context, if media security tools should be made, tailored, or bought from third parties. However, some guidelines can provide help to find the answer on a case-by-case basis:

- Proprietary and closed solutions in media security should be avoided. In a security context, it has been demonstrated multiple times that security tools and systems whose specifications are kept secret are weaker and more vulnerable to attacks when compared to open and publicly accessible specifications [14].
- Media security tools and solutions based on international standards where multiple suppliers can be identified as providers of tools and solutions are mainly preferable.
- In mission-sensitive contexts, including in applications relevant to national security, design, and validation, in particular, the security analysis of tools and solutions should be performed internally and externally by relying on trusted third parties.

30.3.2 Variations and Recommendation

Media security is no longer a niche; many applications need media security tools and solutions in addition to more general security tools and solutions such as symmetric or asymmetric encryption. Therefore, Switzerland needs to strengthen its skills and know-how in media security through initiatives to encourage education and public-private collaborations. In most cases, media security tools and solutions can result in successful business opportunities for those involved.

30.4 Conclusion

Media security refers to a large spectrum of tools and solutions that often need to be sufficiently and optimally addressed through generic information security tools and solutions. At the same time, media security tools and solutions are increasingly essential elements in many professional and private applications that have become multimedia-rich. Breach of security in applications where multimedia information is used can have devastating and irreversible consequences. This can go from impact on the privacy of citizens to manipulation of public opinion through misinformation, which is particularly dangerous in the Swiss context where direct democracy is a foundational principle, requiring well-informed citizens who need to depend on reliable information. Because of these reasons, media security must have a prominent position in the Swiss strategy in cybersecurity in the years to come.

References

1. Xiao Jin, Yuting Su, Liang Zou, Chengqian Zhang, Peiguang Jing, and Xuemeng Song. Video logo removal detection based on sparse representation. *Multimedia Tools and Applications*, 77(22):29303–29322, November 2018.
2. Lijun Xiao, Weihong Huang, Yong Xie, Weidong Xiao, and Kuan-Ching Li. A Blockchain-Based Traceable IP Copyright Protection Algorithm. *IEEE Access*, 8:49532–49542, 2020.
3. Xiushan Nie, Xiaoyu Li, Yane Chai, Chaoran Cui, Xiaoming Xi, and Yilong Yin. Robust Image Fingerprinting Based on Feature Point Relationship Mining. *IEEE Transactions on Information Forensics and Security*, 13(6):1509–1523, June 2018.
4. Kratika Bhagtani, Amit Kumar Singh Yadav, Emily R. Bartusiak, Ziyue Xiang, Ruiting Shao, Sriram Baireddy, and Edward J. Delp. An Overview of Recent Work in Media Forensics: Methods and Threats, May 2022. arXiv:2204.12067 [cs].
5. Wenbo Wan, Jun Wang, Yunming Zhang, Jing Li, Hui Yu, and Jiande Sun. A comprehensive survey on robust image watermarking. *Neurocomputing*, 488:226–247, June 2022.
6. Mandeep Kaur, Surender Singh, and Manjit Kaur. Computational Image Encryption Techniques: A Comprehensive Review. *Mathematical Problems in Engineering*, 2021:e5012496, July 2021. Publisher: Hindawi.
7. Hany Farid. An Overview of Perceptual Hashing. *Journal of Online Trust and Safety*, 1(1), October 2021. Number: 1.
8. Inas Jawad Kadhim, Prashan Premaratne, Peter Vial, and Brendan Halloran. Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. *Faculty of Engineering and Information Sciences - Papers: Part B*, pages 299–326, January 2019.
9. Imani N. Sherman, J. W. Stokes, and Elissa M. Redmiles. Designing Media Provenance Indicators to Combat Fake Media. *RAID*, 2021.
10. Alia Madain, Abdel Abu Dalhoum, Hazem Hiary, Alfonso De la Puente, and Manuel Alfonseca. Audio scrambling technique based on cellular automata. *Multimedia Tools and Applications*, 71, August 2012.
11. Md Shohel Rana, Mohammad Nur Nobi, Beddhu Murali, and Andrew H. Sung. Deepfake Detection: A Systematic Literature Review. *IEEE Access*, 10:25494–25513, 2022.
12. General Data Protection Regulation (GDPR) Compliance Guidelines. https://gdpr.eu/, August 2022.

13. JPEG. https://jpeg.org/, August 2022.
14. Kyndall Elliott. Impact Of Using Open Source Software On Cybersecurity. https://www.cybersaint.io/blog/impact-of-using-open-source-software-on-cybersecurity, 2022.

Chapter 31
Secure Positioning and Localization

Martin Strohmeier

31.1 Introduction

Secure positioning and localization refer to the use of technology to accurately determine the location of an object or person in a secure and trustworthy manner. It involves GPS, Bluetooth, Wi-Fi, and other wireless technologies to determine location. The goal is to ensure the privacy and security of users while providing accurate location information.

31.2 Analysis

31.2.1 Definition

Localization and broadcast positioning techniques (e.g., Global Navigation Satellite Systems or GNSS) are crucial to many applications in the military, business, and society. However, the analysis of their security over the past two decades has shown that an attacker who controls the signals at the antenna of a receiver can spoof the positioning results. Several methods have been proposed to address this problem by securing the content of the signals cryptographically. Distance bounding [1, 2] and TESLA (Timed Efficient Stream Loss-Tolerant Authentication) [3] are two leading examples.

Distance bounding helps to enable secure positioning systems. It allows so-called verifiers to bound the distance of a prover node. As a concrete use case,

M. Strohmeier (✉)
Cyber-Defence Campus, Thun, Switzerland
e-mail: martin.strohmeier@ar.admin.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_31

one can thus prove that a car key is not further than a certain distance away from the car it wants to open. Additionally, the prover node can use distance bounding to determine its correct position even under spoofing/wireless interference by an attacker. Furthermore, distance bounding can also enable secure position verification where a verifier verifies the position claim of an (untrusted) prover node [4].

The TESLA protocol and its derivatives/further developments enable the cryptographic authentication of broadcast communication such as those used in GNSS. It uses symmetric cryptography in connection with time as its asymmetric property to enable the receiver of the GNSS messages to verify the authenticity of the navigation content.

Finally, these methods compete with and complement many non-cryptographic methods using physical properties (think classical radar) to verify location claims and positions. An overview is given in [4].

31.2.2 Trends

The general expectation is that known secure solutions for navigation, positioning, and localization systems will mature and be deployed more widely. This will affect many important sectors in the industry, the government, and the military. For example, the GNSS market alone is growing steadily over the next decade, reaching cumulative revenues of €3860 bn [5]. Furthermore, with autonomous vehicles becoming increasingly essential and utilized in all domains (land, water, air), secure and robust positioning and navigation capabilities will be crucial. Nevertheless, many other growth segments will rely on secure navigation systems besides traditional navigation-dependent sectors such as shipping, aviation, cars, and rail. These include, but are not limited to, industrial automation, agriculture, climate services, infrastructure, insurance and finance, space, and urban development.

Actors developing and integrating such solutions range from startups and university spinouts such as 3db [6] to the major defense contractors and suppliers in the GNSS market (e.g., Garmin, car manufacturers, and tech companies such as Alphabet). We also expect disruption through the new Low Earth Orbit (LEO) mega-constellations such as Starlink and OneWeb, which could be used for navigation [7]. Last but not least, the major global powers behind the GNSS systems will be pushing for secure and robust solutions, exemplified by the recent addition of TESLA to Galileo, the European GNSS. [8].

31.3 Consequences for Switzerland

In terms of knowledge and research, Switzerland is well-placed with some of the significant academic research on secure positioning coming from Swiss universities

and/or conducted by Swiss academics. However, without its space missions and satellite constellation, Switzerland depends on the major global powers and their GNSS constellations, particularly GPS (US) and Galileo (Europe).

For smaller products such as keyless entry systems, the current startup ecosystem can provide the expertise for secure positioning solutions and their integration into consumer products and other dependent systems.

31.3.1 Implementation Possibilities: Make or Buy

This section presents the pros and cons of buying or making secure localization products (Table 31.1).

Table 31.1 Implementation possibilities for different sectors

	Make		**Buy**	
	Pros	Cons	Pros	Cons
Military	Strategic and operational independence	Cost (in particular GNSS) and Interoperability	Only practical approach for large-scale GNSS projects	Dependence on foreign actors and Additional redundant, independent technologies needed
Civil Society	Cheap for consumer tech (e.g. car keys) and Expertise can be utilized in many areas	Cost (in particular GNSS)	Only practical approach for large-scale GNSS projects and Cheaper, faster in the short term, increasing security quickly	Dependence on foreign actors and Additional redundant, independent technologies needed
Economy	Cheap for consumer tech (e.g. car keys) and Expertise can be utilized in many areas, business opportunities	Cost (in particular GNSS) and Interoperability	Only practical approach for large-scale GNSS projects and Cheaper, faster in the short term, increasing security quickly	Dependence on foreign actors and Additional redundant, independent technologies needed

31.3.2 Variations and Recommendation

We discuss three different options for secure localization. The differences between actors are relatively minor, particularly since control of crucial space-based global positioning and navigation technologies remains viable only for a handful of major state and supranational actors. The first option is the Timed Efficient Stream Loss-tolerant Authentication (TESLA) broadcast authentication protocol [3]. It has the advantage of being a practical option that can be fitted retroactively to GNSS. Nevertheless, on the other hand, it is costly and needs systemic changes. The second option is Distance Bounding [1, 2]. It has two main advantages for the military: flexible technology and proven applications. For civil society and the economy, it is available in consumer technology. On the other hand, it has the disadvantage of being primarily applicable for short distances. The last option is non-cryptographic solutions. The military they have the advantage (Table 31.2).

Table 31.2 Different options for secure localization

	Military		**Civil Society**		**Economy**	
	Pros	Cons	Pros	Cons	Pros	Cons
TESLA [3]	Practical option that can be fitted retroactively to GNSS	Costly systemic changes required	Practical option that can be fitted retroactively to GNSS	Costly systemic changes required	Practical option that can be fitted retroactively to GNSS	Costly systemic changes required
Distance Bounding [1, 2]	Flexible technology, proven applications	Technology primarily for short distances	Available in consumer technology	Technology primarily for short distances	Available in consumer technology	Technology primarily for short distances
Non-cryptographic solutions	Security can be scaled with additional expenditure	No cryptographic guarantees	Can be implemented flexibly and individually without systemic change	Potentially high cost to utility ratio	Can be implemented flexibly and individually without systemic changes	Potentially high cost to utility ratio

31.4 Conclusion

Secure positioning and localization is a comparatively small but essential part of the world of cryptographic applications. The integration of positioning in many embedded systems and using such methods in critical infrastructure and navigation systems make their security paramount. As of today, certainly in the civilian world, barely any secure localization methods are being employed. This is already changing in higher-end assets, where we see distance bounding used e.g. for keyless entry systems for expensive cars. We expect this will trickle down with falling costs and increased adoption.

Cryptographically-secure GNSS is available for the owners/operators of the different satellite constellations (e.g. the military version of GPS) and is trickling towards some of the civilian versions, as seen with Galileo. While technical developments in space can be slow and happen only over the long term, new consumer-oriented LEO constellations may change the pace significantly over the next few years.

Out of the scope of this analysis on cryptographic developments is the progress in non-cryptographic secure localization methods. Here, a quicker but more fragmented rollout can be expected in some critical areas as they can often be deployed independently and transparently. This is already the case in many military applications and may be seen in other vital assets.

References

1. Stefan Brands and David Chaum. Distance-Bounding Protocols. In Tor Helleseth, editor, *Advances in Cryptology — EUROCRYPT '93*, Lecture Notes in Computer Science, pages 344–359, Berlin, Heidelberg, 1994. Springer.
2. Kasper Bonne Rasmussen and Srdjan Čapkun. Realization of RF Distance Bounding. page 13.
3. Adrian Perrig and J. D. Tygar. TESLA Broadcast Authentication. In Adrian Perrig and J. D. Tygar, editors, *Secure Broadcast Communication: In Wired and Wireless Networks*, pages 29–53. Springer US, Boston, MA, 2003.
4. Srdjan Čapkun. The Cyber Security Body of Knowledge v1.0, 2019. University of Bristol, 2019. Section: Physical Layer & Telecommunications Security.
5. The European Commission and The European Union Agency for the Space Programme. EUSPA EO and GNSS Market Report. Technical report, Luxembourg, 2022.
6. 3db Access. https://www.3db-access.com/, August 2022.
7. SpaceX's Starlink broadband satellites could be used for GPS navigation | Space. https://www.space.com/spacex-starlink-gps-navigation, August 2022.
8. Galileo Open Service Navigation Message Authentication - Navipedia. https://gssc.esa.int/navipedia/index.php/Galileo_Open_Service_Navigation_Message_Authentication, August 2022.

Chapter 32
Secure Payment

Sophia Ding

32.1 Introduction

The shift towards a digital economy has led to an increase in electronic payment methods, from credit cards to online and mobile contactless payments. Secure payment is crucial in verifying and protecting transactions and customers. Despite implementing security measures such as data encryption and strong customer authentication, online fraud continues to be a concern in the industry. Standards such as the EMV Integrated Circuit Card Specification, Payment Card Industry Data Security Standard, and Revised Payment Services Directive regulate the payment services and providers, mandating various security measures to be in place.

32.2 Analysis

Secure payment is an essential element of digital commerce in a world where cash is becoming redundant, credit cards are becoming less and less important, and mobile devices are becoming means of payment. Secure payment relies on the verification of transactions and customers that make payments. However, this process has become increasingly challenging. It has been reported that false declines of transactions are increasing as a result of suspected fraudulent activities [1].

S. Ding (✉)
Eraneos Switzerland AG, Zurich, Switzerland
e-mail: Sophia.Ding@eraneos.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_32

32.2.1 Definition

Secure payment refers to a variety of payment methods - typically in relation to electronic payments. Therefore, it must be considered through the lens of a variety of payment methods: Credit cards have been around since the 1950s, but the introduction of chip technology and contactless payment raises new challenges for the security of payments [2]. Online payments were reported to have been conducted for the first time in the 1990s [3]. There has been an increase in the crime of online fraud since then [4]. Since the advent of smartphones in the 2000s, mobile (contactless) payment systems have become increasingly popular [5, 6]. Additionally, voice payments using voice assistants are becoming increasingly popular [7].

As a means of combating online fraud, banks and fintech companies have implemented techniques such as fraud monitoring (e.g., through the use of emerging technologies such as artificial intelligence [8]), employee training, and active management of compliance with standards and regulations [9]. The following are among them [10]:

- EMV Integrated Circuit Card Specification for Payment Systems: Payment card standard based on chip technology [11]
- Payment Card Industry Data Security Standard (PCI DSS): All major credit card companies support a set of rules relating to the processing of credit card transactions [12]
- Revised Payment Services Directive (PSD 2, Directive (EU) 2015/2366): This directive regulates the payment services and providers in the European Union (EU) and the European Economic Area (EEA) [13]

These standards require various security measures which include:

- Data encryption: The Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are cryptographic protocols that enable the establishment of a secure channel between systems and preserve the confidentiality and integrity of data. As of June 30, 2018, PCI requires migration from early versions of TLS and SSL to the later versions of TLS [12].
- Strong customer authentication (SCA): PSD 2 requires multi-factor authentication, which is the combination of multiple independent security factors (see Sect. 29.2). There are several exceptions to this requirement, such as for payments of very small amounts [13]. EMV 3-D Secure [14] is one method for implementing SCA for credit and debit cards. This protocol is designed to prevent unauthorized use of credit cards. It is offered, for example, under the name Verified by Visa or Mastercard Identity Check, and requires additional authentication with the card issuer for "card-not-present" transactions (i.e., neither the card nor the cardholder are present). Those merchants who use 3-D Secure can be assured that their payments will be received [15].
- Account verification, address verification service (AVS), and card verification value (CVV2) are all methods of validating payment accounts offered by credit

card companies. With the exception of U.S. and U.K. card issuers, AVS and CVV2 participation is optional [16, 17].

32.2.2 Trends

It is estimated that the total value of digital payments will reach $8.49 trillion in 2022. By 2026, it is forecast that the market will reach $13.75 trillion with an annual growth rate of 12.82% [18]. Table 32.1 provides a summary of key trends in secure payments in the coming years. As a prerequisite to the use case trends listed in the table, secure payment is necessary, emphasizing the importance of secure payment for the development of new applications in retail.

32.3 Consequences for Switzerland

PSD 2 is only applicable to EU member states; therefore, implementation in Switzerland is voluntary, and there is no corresponding regulation. SEPA membership, however, requires equivalence in a number of areas [31].

According to a study conducted in 2021 on the Swiss payment market, the number of cash payments is decreasing drastically as a result of the COVID-19 pandemic. Online shopping and the use of credit cards are both on the rise, with the latter being the most popular method of payment [32]. The popularity of mobile payment options is also increasing [33].

In the secure payment market, several Swiss startups are active. NetGuardians SA (Yverdon-les-Bains, JU) develops artificial intelligence-based fraud detection solutions for the banking industry. A payment ecosystem offered by Datatrans AG (Zürich, ZH) allows its customers to access secure payment methods that are most advantageous to them.

The recent outages of digital payment services have raised public awareness of their vulnerability to disturbances caused by service providers or infrastructure providers [34, 35]. In an incident involving Twint, Switzerland's number one mobile payment provider, a payment was wired to a previous owner of the intended recipient's mobile number, illustrating the challenges associated with ensuring secure payments with modern methods of payment [36].

32.3.1 Implementation Possibilities: Make or Buy

Typically, secure payment is implemented by commercial payment service providers, such as credit card issuers or infrastructure operators, such as SIX. A number of open-source solutions are currently available for automated clearing

Table 32.1 Key trends in secure payments

Trend Category	Trend	Description	
Use Cases	Voice shopping	A voice assistant is a personal assistant that provides assistance with daily tasks. Voice shopping, or the use of voice assistants for online purchases, is described as a major trend in retail, but it also poses new security challenges. While supermarket chains such as Walmart and Target offer voice shopping to their customers in the United States, the trend is less prevalent in Europe and Switzerland.	[19, 20]
	Intelligent shopping cart	In recent years, intelligent shopping carts have been tested. In these shopping carts, the items shopped as well as the shopper are automatically recognized. It is possible to avoid long lines at the check-out and payment with intelligent shopping carts. A secure payment can be made using either a universal payment interface or a one-time password.	[21]
Technical Development	Credit card Innovation	A number of credit card innovations are currently being introduced, including biometric cards and dynamic cryptograms, such as those introduced by BNP Paribas. A biometric card stores a client's fingerprint and allows an increase in credit limit if the client authenticates with a fingerprint. A dynamic cryptogram is a three-digit code that adjusts regularly and reduces the possibility of fraud.	[22]
	3-D Secure 2	The 3-D Secure 2 security protocol is a further development of the 3-D Secure security protocol which complies with PSD 2. This is regarded as the most significant change to consumer payment since Chip and PIN was introduced more than 16 years ago. 1) frictionless flow, i.e., the option of not requiring additional input from card holders, 2) non-payment authentication, i.e., the card holder is authenticated without making a payment, and 3) native mobile integration, which means that the merchant can integrate 3-D Secure into their mobile application.	[23, 15]
	Variants of Machine Learning for Fraud Detection	For fraud detection, machine learning (ML) will continue to play an increasingly important role. As an alternative to traditional rule-based systems or standard machine learning systems, ML variants that combine different ML techniques with other approaches, such as scoring models, are being used.	[24, 25]
	Payment apps	The Fintech industry provides a variety of services like Apple pay, Samsung pay and Google pay. The Swiss sector is however dominated by one player, Twint, which has more than 4 million active users.	[26, 27]
	Cryptocurrencies	Cryptocurrencies are now a seen as a mean or future mean of payment by a sgnificant proportion of the population living in the western world.	[28]
Risks	Outages of secure payment systems and underlying infrastructure	It is important to note that digital secure payment methods heavily rely on digital payment systems. Due to the lack of resilience of service providers (such as card terminals or networks), the secure payment ecosystem is more susceptible to disruptions than the cash payment ecosystem. As power shortages become more likely, business continuity measures need to be taken.	[29, 30]

house (ACH) payment (e.g., OpenACH), which is used to transfer money from one bank account to another [37]. Additionally, there are open-source payment gateways (e.g., Open-Source Payment Gateway), which facilitate the transfer of payment information. The providers of these open-source solutions claim that their products facilitate integration with existing systems on the client side and provide better customization due to their modularity and adaptability. It is important to note that while the source code is available, open source does not necessarily mean that the solution is free. In addition to PCI compliance, it still requires an underlying infrastructure and computing power.

32.3.2 Variation and Recommendation

Secure payment ecosystems can be established using distributed ledger technologies such as blockchain [38]. Due to technological advancements, current disadvantages such as inefficiency and elevated power consumption are expected to be mitigated in the future, making it a viable alternative to existing secure payment methods [39].

32.4 Conclusion

Regulations require the implementation of technical solutions such as 3-D Secure 2.0, which are becoming increasingly user-friendly as time goes on. Secure payment systems are the foundation of innovation in industries such as retail.

References

1. Visa. 3-D Secure 2.0: Improving security and increasing authorizations for digital transactions. https://usa.visa.com/visa-everywhere/security/future-of-digital-payment-security.html, July 2022.
2. T. Editors of Encyclopaedia Britannica. Credit Card. https://www.britannica.com/topic/credit-card, March 2021.
3. Huffington Post. Pizza Hut Tells Twitter It Made The First Online Sale In 1994. *Huffington Post*, December 2014.
4. Europol. Payment Fraud. https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/forgery-of-money-and-means-of-payment/payment-fraud, July 2022.
5. Marc Pasquet, Joan Reynaud, and Christophe Rosenberger. Secure payment with NFC mobile phone in the SmartTouch project. In *2008 International Symposium on Collaborative Technologies and Systems*, pages 121–126, Irvine, CA, USA, May 2008. IEEE.
6. Hui et al. MOBILE PAYMENTSYSTEM. https://patentimages.storage.googleapis.com/97/a7/1a/16e48f1cd942e9/US20020073027A1.pdf, June 2002.
7. Anna Oleksyuk. The Rise of Voice Payment Technology in Banking. https://medium.com/@annoleksyuk/the-rise-of-voice-payment-technology-in-banking-96f94cb2211f, February 2019.

8. Yang Bao, Gilles Hilary, and Bin Ke. Artificial Intelligence and Fraud Detection. In Volodymyr Babich, John R. Birge, and Gilles Hilary, editors, *Innovative Technology at the Interface of Finance and Operations*, volume 11, pages 223–247. Springer International Publishing, Cham, 2022. Series Title: Springer Series in Supply Chain Management.
9. Michael H. Meissner. Accountability of senior compliance management for compliance failures in a credit institution. *Journal of Financial Crime*, 25(1):131–139, January 2018.
10. Wordline. Sichere Zahlungen leicht gemacht - Eine kurze Einführung in die neuen Anforderungen Europas für eine starke Kundenauthentifizierung. https://www.six-payment-services.com/dam/download/flyers/e-commerce/Worldline-SCA-position-paper-de.pdf, July 2022.
11. Michael Ward and Anita Ochieano. EMV. In Henk C. A. van Tilborg and Sushil Jajodia, editors, *Encyclopedia of Cryptography and Security*, pages 412–416. Springer US, Boston, MA, 2011.
12. Laura K. Gray. Webinar: SSL and Early TLS Migration: Preparing for 30 June Deadline. https://blog.pcisecuritystandards.org/webinar-ssl-and-early-tls-migration-preparing-for-30-june-deadline, March 2018.
13. European Union. Directive (EU) 2015/2366 of the European parliament and of the council of 25 November 2015 on payment services in the internal market, amending directives 2002/65/ec, 2009/110/ec and 2013/36/eu and regulation (EU) no 1093/2010, and repealing directive 2007/64/ec. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L2366, July 2022.
14. EMVCo. EMV®3-D Secure. https://www.emvco.com/emv-technologies/3d-secure/, August 2022.
15. Worldline. 3-D Secure 2.0. https://www.six-payment-services.com/de/shared/newsletter/01-2019/3-d-secure-2-0.html, July 2022.
16. Visa. Getting Started with Payment Account Validation. https://developer.visa.com/capabilities/pav/docs, July 2022.
17. SIX Payment Services. Increased security with the CVV2/CVC2/CID card verification value for distance payments with Visa, MasterCard, Diners Club, Discover and Maestro1. https://www.six-payment-services.com/dam/download/datasheets/110003502_DS_ErhoehteSicherheit_CHE_EN_opt.pdf.
18. Digital Payments. https://www.statista.com/outlook/dmo/fintech/digital-payments/worldwide, month = Jul, year = 2022, urldate = 2022-07-27, note = Statista,.
19. Ransome Epie Bawack, Samuel Fosso Wamba, and Kevin Daniel André Carillo. Exploring the role of personality, trust, and privacy in customer experience performance during voice shopping: Evidence from SEM and fuzzy set qualitative comparative analysis. *International Journal of Information Management*, 58:102309, June 2021.
20. Monitor Deloitte. Beyond Touch – Voice Commerce 2030: Wie Voice-assisted Interfaces den Handel in Europa revolutionieren werden. https://www.thinkwithgoogle.com/_qs/documents/8031/Beyond_Touch__Voice_Commerce_2030.pdf.
21. Sudipta Ranjan Subudhi and R. N. Ponnalagu. An Intelligent Shopping Cart with Automatic Product Detection and Secure Payment System. In *2019 IEEE 16th India Council International Conference (INDICON)*, pages 1–4, Rajkot, India, December 2019. IEEE.
22. BNP Paribas. Means of payment. https://group.bnpparibas/en/group/at-the-service-of-our-clients-and-society/innovative-solutions/means-of-payment, July 2022.
23. Barclaycard. Shopping online becomes even safer from today: The big change to how we pay that all Brits need to know about. https://home.barclaycard/press-releases/2022/03/shopping-online-becomes-even-safer/#:~:text=Rob%20Cameron%2C%20CEO%20of%20Barclaycard,all%20the%20safer%20for%20it., July 2022.
24. Payment Fraud: Why banks need a smarter approach to AI. https://netguardians.ch/enterprise-payment-fraud/, July 2022. NetGuardians.
25. John O. Awoyemi, Adebayo O. Adetunmbi, and Samuel A. Oluwadare. Credit card fraud detection using machine learning techniques: A comparative analysis. In *2017 International Conference on Computing Networking and Informatics (ICCNI)*, pages 1–9, Lagos, October 2017. IEEE.

26. Switzerland is using TWINT TWINT. https://www.twint.ch/en/press/switzerland-is-using-twint-four-million-active-users/, November 2022. TWINT.
27. Jungho Kang. Mobile payment in Fintech environment: trends, security challenges, and services. *Human-centric Computing and Information Sciences*, 8(1):32, October 2018.
28. Zlatko Bezovski, Ljupco Davcev, and Mila Mitreva. Current adoption state of cryptocurrencies as an electronic payment method. *Management Research and Practice*, 13(1):44–50, 2021. Number: 1.
29. Elektronischer Zahlungsverkehr für mehrere Stunden schweizweit gestört. November 2019. Aargauer Zeitung.
30. Digital payment systems briefly disrupted in Switzerland. June 2022. swissinfo.ch.
31. Andreas Imthurn. *Auswirkungen der PSD2-Regulierung auf die europäische Finanzindustrie unter besonderer Berücksichtigung der sogenannten Open Banking APIs*. PhD thesis, 2021.
32. Sandro Graf, Nina Heim, Marcel Stadelmann, and Tobias Trütsch. Swiss Payment Monitor 2021 - How does Switzerland pay? Short Report Issue 1/2021. https://www.alexandria.unisg.ch/263157/2/Short%20Report%20Swiss%20Payment%20Monitor%202021-1%20ENG.pdf, July 2022.
33. Statista. Volumen der Zahlungen via Mobile Payment im Schweizer Detailhandel mit Lebensmitteln, Getränken und Tabak von Februar 2021 bis Februar 2022. https://de.statista.com/statistik/daten/studie/1199896/umfrage/mobile-payment-transaktionsvolumen-im-schweizer-lebensmittel-detailhandel/, July 2022.
34. Netzwerkstörungen bei Six. June 2016. Swiss IT Magazine.
35. Erich Aschwanden. Wer ohne Bargeld an der Kasse steht, hat allenfalls Pech gehabt – Finanzdienstleister kämpfen mit Störungen. June 2022. Neue Z.
36. SRF News. Eine fatale Überweisung mit Twint. https://www.facebook.com/srfnews/videos/eine-fatale-%C3%BCberweisung-mit-twint/275016353860855/, June 2020.
37. Jochen Metzger. Automated Clearing House (ACH). https://wirtschaftslexikon.gabler.de/definition/automated-clearing-house-ach-30813/version-254389, August 2022. Gabler Wirtschaftslexikon.
38. Qi Xia, Emmanuel Boateng Sifah, Ke Huang, Ruidong Chen, Xiaojiang Du, and Jianbin Gao. Secure Payment Routing Protocol for Economic Systems Based on Blockchain. In *2018 International Conference on Computing, Networking and Communications (ICNC)*, pages 177–181, Maui, HI, March 2018. IEEE.
39. Lin Zhong, Qianhong Wu, Jan Xie, Jin Li, and Bo Qin. A secure versatile light payment system based on blockchain. *Future Generation Computer Systems*, 93:327–337, April 2019.

Chapter 33
Disk, File and Database Encryption

Linus Gasser and Imad Aad

33.1 Introduction

Disk, file, and database encryption are technologies used to protect data confidentiality when stored. Full disk encryption (FDE) encrypts all data on a disk except the part containing the code to unlock the rest of the disk, which is usually not encrypted. File-based encryption (FBE) operates at the file level and can be done by the operating system or an application. Manual file encryption requires user intervention and is not transparent. Database encryption (DBE) can be done using transparent DBE, column-level encryption, or field-level encryption. The goal of DBE is to encrypt the whole database or specific columns or fields to ensure that the data on physical storage cannot be read if stolen.

33.2 Analysis

To make use of the data, for example, to make computations with it, the data must be decrypted to be processed, unless one makes use of technologies like homomorphic Encryption (see Chap. 8). Whether or not the user of a turned-on and unlocked device must provide an additional secret to working on an encrypted file, disk, or database, the key material needed to do so must already be available on the system. When no additional secret needs to be provided, decryption and Encryption are transparent to the user, and the key material is usually entered or made available

L. Gasser (✉) · I. Aad
EPFL, Lausanne, Switzerland
e-mail: linus.gasser@epfl.ch; imad.aad@epfl.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_33

during a device's startup or unlocking phase. Consequently, the data is only secure when the device is turned off or locked.

33.3 Definition

33.3.1 Full Disk Encryption (FDE)

As the name suggests, FDE [1] encrypts all data on a disk unless it is the disk from which the system boots. In this case, the part containing the code to unlock/get the critical material needed to access the rest of the disk is not encrypted. This code usually does something like (1) reading encrypted key material from the unencrypted part of the disk, (2) having a user enter the password needed to decrypt it, and (3) starting booting the operating system as the data on the disk containing it can now be decrypted. Once the operating system has been booted, access to the disk is through the encryption driver and transparent to the user and any other person/attacker that gets her hands on such a system. This is mainly a problem when using FDE in a server environment, as it is difficult to guarantee that nobody else has access to the system while it is running. In addition, when using FDE in a server environment, care must be taken about how the password/secret key is input into the server's system [2]. Another problem is that if the unencrypted part of the disk is not protected against manipulation, for example, with secure boot technologies, an attacker could efficiently execute attacks like the evil maid attack [3]. A particular case of FDE is external harddisks that include the encryption algorithm and a PIN pad directly in the enclosure. This allows for easy usage with different systems since they do not need any support for FDE. FDE is fully transparent to them in this case.

33.3.2 File-Based Encryption (FBE)

A system using file-based Encryption is similar to a FDE system. However, it operates at the level of individual files instead of at the level of so-called blocks.[1] This means that an FBE system encrypts each file individually. Decryption and Encryption can be done by the operating system whenever a file is read and written or by an application, if it is limited to files read and written by that application. Today's FBE systems include modern smartphones running Android or iOS, Windows's built-in Encrypting File System (EFS), Linux systems with fscrypt, or cloud storage solutions like Proton Drive and others. To encrypt the content of files, FBE can use the same encryption key for all files or different keys for different files. This allows, for example, to introduce different protection levels for files, like

[1] A disk is usually partitioned into a large number of blocks of the same size.

on Apple devices running iOS. There, files accessible in a locked state are encrypted with different key material than files accessible only in an unlocked state. When the device is locked, the latter protection level's key material is no longer available. It can only be restored by unlocking the phone again. On the negative side, however, is that most of the FBE systems today leave one or more of the following metadata for an attacker to explore:

- Access times and size of the file—revealing if a file has been used recently and what type of file it might be
- Entry type (file or directory)—revealing applications used
- For password-protected zip files, even the filenames are in cleartext

33.3.3 Manual File Encryption

In contrast to FDE and FBE, manual file encryption requires intervention by the user and is not transparent. The most well-known system is to provide a password to create a .zip file. This password will encrypt most, but not all, of the data in the zip file. More elaborate tools like PGP exist, but they pose a fundamental management problem, as the sender needs access to the receiver's public key.

33.3.4 Database Encryption (DBE)

DBE is usually done with one of the following approaches: Transparent DBE, column-level Encryption, or field-level Encryption. The whole database is encrypted with the same symmetric key with transparent DBE. This ensures that data on the physical storage cannot be read if stolen. The other two approaches exploit how relational databases are structured. They consist of tables, tables consist of columns, and a column entry is called a field. With column-Level Encryption, one can use different encryption keys for different columns. This adds, for example, the ability to encrypt only parts of the data and/or bind key material to specific roles preventing users with a different role that manage to query such a column can read the data. However, encrypting columns individually can come at the cost of reduced speed, depending on whether just one or many columns are encrypted. Field-level Encryption is also possible. It allows users to search the DB without decrypting each field since one can encrypt the field content (only exact matches) and then search for this value. However, when Encryption is randomized, for example, by prepending a fixed-size random value to the content before encrypting it, a different result is generated for equal fields. This provides more security at the cost of jeopardizing encrypted searches.

33.4 Security Considerations

33.4.1 Encryption Algorithms

Some high-performance encryption devices exist in hardware, but most systems are based on software. The advantage of using software is that the system can be updated more easily. Also, a failing hardware component can make it impossible to continue using the system if a replacement for the component is unavailable.

Most systems use standard encryption algorithms like AES or ChaCha20, see Chap. 2. Only a few systems create their algorithms [4]. See also [5, 6] for an overview.

AES works as a block cipher, meaning it can only encrypt one data block. In the case of AES, this is 256 bits. To encrypt an entire disk, AES is combined with a *Block cipher mode* that allows it to encrypt larger blocks.

33.4.2 Key Management

The symmetric key used for Encryption is derived, in the simplest case, from a password given by the user. It is essential that the password is long enough and has enough entropy to be secure. This simple system cannot recover a lost password and cannot allow more than one user access to the same data.

More elaborate systems use asymmetric Encryption to protect the symmetric key. This additional, asymmetric key can be stored in a hardware element like a smartcard, a TPM, or another. These systems can also include two-factor authentication.

In all systems, there needs to be a way to recover the data in an emergency. For example, if the user needs to remember her password or private key. Nevertheless, this needs to be done so that the emergency procedure cannot be abused. Indeed, if this emergency option can be used to access unauthorized data, it can become more of a problem than a solution. Therefore there is a proper balance to find between confidentiality and availability.

33.4.3 Coercion

To access encrypted data, be it data protected by FDE, FBE, or DBE, some user-provided secret/key material is needed. An attacker might force the user to enter the password through coercion to get it. This might be violence, the threat of jail, or any other type of coercion [7]. To defeat this attack, some systems allow users to provide different passwords. Depending on the password, the system will open one of two containers. One password opens the standard system, file, or database, while another

opens a different one that does not contain sensitive data. For an external observer, it is nearly impossible to know which of the two systems they are currently looking at. One example of a solution that does this at the level of disks is VeraCrypt [8].

33.5 OS Examples

See Table 33.1.

33.6 Trends

The essential features of FDE and FBE are now readily available in popular operating systems like Windows, MacOSX, and Linux. However, it is still rare to see Encryption on the server side, except for servers from big players. For example, Google uses several layers of encryption. This also has to do with the fact that the users need to influence whether the data behind the cloud services is encrypted.

Two features of Encryption that can increase the user experience might get more traction until 2025. Both involve managing the secret key: delegated (custodial) key management and threshold encryption.

The Delegated (Custodial) Key Management means that the key resides on a third-party server. This allows recovery of the key if the primary owner loses the key. Microsoft and Apple offer this service when installing FDE. While this system guarantees that the key will still be available even in the case of password loss, you

Table 33.1 Softwares used in different operating systems to add FDE or FBE

OS	Name	Type	Description
Windows	Bitlocker	Full Disk	Encrypts one or more drives using AES-256, allows fine control for access and encryption
	Device Encryption	Full Disk	Encrypts all available drives using AES-256
MacOSX	FileVault	Full Disk	Encrypts using AES-128
Linux	CryFS	File Based	Encrypts using AES-256 and stores the files as blocks to hide metadata
	DM-Crypt	Full Disk	Encrypts using AES-256 and is used by other tools
iOS	iPhone encryption	Full Disk and File Based	Encrypts all data using AES-256
Android	Direct Boot	File Based	Encrypts using AES-256

now have to trust the keeper of the key, in this case, Microsoft and Apple, not to give it away.

A more secure method is Threshold Encryption which shares the key with several parties. It requires a minimum of those parties to participate in recovering the key. In such a way, a single participant cannot leak the key. Several systems are working on this scheme. One is [9], developed at the EPFL by prof. Bryan Ford.

33.7 Consequences for Switzerland

From a user perspective, FDE and FBE are great tools to keep data privacy on the computer. No unauthorized person can access the data, even in the case of theft or loss of the device. On the other hand, from a law enforcement perspective, these tools make it more challenging to get the data necessary to convict a felon.

The department of computer science at ETH Zurich has two laboratories, the Applied Cryptography Group and the Information Security and Cryptography group, working on different cryptography applications. Their publications cover FDE, FBE, and DBE.

33.8 Conclusion

Both FDE and FBE allow good protection against data leakage in the case of device theft or loss. However, due to their nature, they cannot protect against an attacker who gets her hands on a device turned on (and unlocked) or any other intruders who can run programs on the computer. This might be somebody using phishing to access the computer or malware getting access to your computer through a bug in the operating system.

References

1. Wikipedia, Filesystem-level encryption. https://en.wikipedia.org/w/index.php?title=Filesystem-level_encryption&oldid=1093429694, June 2022.
2. Wikipedia, Disk encryption. https://en.wikipedia.org/w/index.php?title=Disk_encryption&oldid=1099993218, July 2022.
3. Wikipedia, Evil maid attack. https://en.wikipedia.org/wiki/Evil_maid_attack, February 2023.
4. Wikipedia, ZIP (file format). https://en.wikipedia.org/w/index.php?title=ZIP_(file_format)&oldid=1099335582, July 2022.
5. Dansimp. Overview of BitLocker Device Encryption in Windows - Windows security. https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-device-encryption-overview-windows-10, August 2022.
6. Wikipedia, FileVault. https://en.wikipedia.org/w/index.php?title=FileVault&oldid=1093491405, June 2022.

7. Security. https://xkcd.com/538/, August 2022.
8. Wikipedia, VeraCrypt. https://en.wikipedia.org/w/index.php?title=VeraCrypt&oldid=1100840194, July 2022.
9. Calypso-enabled Filesharing. https://github.com/calypso-demo/filesharing, July 2022.

Chapter 34
WEB3

Linus Gasser

34.1 Introduction

Web3 is the next generation of the internet, often referred to as the decentralized or blockchain web. It aims to address the shortcomings of the current centralized web, such as privacy concerns and lack of control over personal data, by leveraging decentralized technologies like blockchain and peer-to-peer networks. The vision of Web3 is to create a more open, secure, and democratic internet where users have full control over their data and interactions. The goal of Web3 is to build a new internet infrastructure that is more secure, user-centric, and decentralized than the current web, making it easier for individuals to own and control their data.

34.2 Analysis

Since its invention by Tim Berners Lee in 1989, the Web has undergone a major transformation, and depending on whom you talk to, another one, Web3, is on the horizon. The original internet, Web 1.0, allowed for static web pages with links to other web pages. Anything beyond that, for example, programming user interactions with these pages to implement web applications, was complicated. With the first transformation of Web 1.0 to Web 2.0, the Web became much more dynamic. Technologies like javascript and cascading style sheets offer myriad ways to interact with users and implement complex web applications. The possibilities of the Web 2.0 sparked services like Facebook and TikTok whose primary business is to engage

L. Gasser (✉)
EPFL, Lausanne, Switzerland
e-mail: linus.gasser@epfl.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_34

users to interact with content and to exploit these interactions for marketing and advertisement purposes. The user, or more precisely, the data collected about a user, became the new currency; in exchange for their data, users can use most services for "free". With Web 2.0 dominated by a few companies only, the "Big Tech" companies like Meta or Alphabet, some people wished for a less centralized Web. Web3 might become a more decentralized Web as it incorporates concepts such as decentralization, blockchain technologies, and token-based economics.

34.2.1 Definition

When discussing the next generation of the internet, two terms are often heard and sometimes also confused: Web3 and Web 3.0. Even though they both designate the future of the internet and decentralization, they are not the same [1]:

Web 3.0 has been coined by Tim Berners Lee as the Semantic Web, where the pages are machine-readable. In his implementation, Solid, people store their data securely in decentralized data stores called Pods. In Web3, decentralization is not achieved by the concept of Pods owned by the users, and can be hosted anywhere and moved around quickly but by using blockchain technology. With the blockchain as a basis, Web3 wants to be a platform that goes far beyond being a platform for Web content only. It leaves the Semantic Web focus aside and strives to become the future technical, legal, and payment infrastructure for the world. Web3 also wants to "cut out the middlemen" by directly contacting producers and consumers. This allows the producers to receive more money for their work while the consumer needs to pay less.

It is, therefore, confusing that Time Berners Lee stated that: *Web3 has been coined by Gavin Wood and is the name of his company that develops Web 3.0: Users own their data, not corporations; Global digital transactions are secure; Online exchanges of information and value are decentralized.*

34.2.2 Technologies

The technology for Tim Berner Lee's Web 3.0 revolves around the possibility of each internet user managing their Pods. Pods are like secure personal web servers for one's data. The Solid projects write the following about Pods:

> (Pods) can be hosted by the same Pod Provider or by different Providers or be self-hosted or any combination thereof. The number of Pods you have, as well as which Solid Server or Servers you use, is effectively transparent to your applications and services. This is because, in the Solid ecosystem, data is linked through your identity and not through the specifics of your Pod. This is true for your data and those that others have shared with you.

The user has complete control over who sees which part of her Pod. This allows the implementation of self-sovereign identities, which can free internet users from the need to depend on big companies like Google, Facebook, or TikTok for their identity [2].

Web3 goes much further in its decentralization and wants to promote a self-sovereign internet. This self-sovereign internet is based on a decentralized (peer-to-peer) infrastructure, currently embodied using blockchains. The goal is to replace a big part of the current infrastructure provided by the government through services based on blockchains and smart contracts [3].

In Web3, Cryptocurrencies and other financial assets like Non-Fungible Tokens (NFTs) replace the government's fiat money. In addition, smart contracts enable the creation of Digital Autonomous Organizations (DAOs), which reflect real-world structures in the Web3 world. Using DAOs, decisions can be made with less friction than with real-world organizations. Another component, Decentralized Finance (DeFi) allows the exchange of the different crypto-tokens directly on the blockchain without going through a centralized exchange [3].

Some also include the approaching Metaverse in Web3 and propose that exchanges between different Metaverse platforms can be done using NFTs. This allows things bought in one Metaverse to be used in another Metaverse [3].

34.2.3 Risks

As has been shown in 2021 and 2022, significant parts of the blockchain infrastructure for Web3 are not ready for prime time yet: systems are slow, they break, and the smart contracts contain many bugs which hackers exploit to steal the funds stored in these smart contracts [4].

Another risk needs to be considered concerning the societal effects of removing parts of the government: how can Web3 make sure that the social aspects of today's governments are kept so that people are not excluded? One unsolved question regarding decentralized finance is how to recover stolen or lost funds when blockchains are decentralized and immutable.

Finally, another hidden risk of WEB3 is that it is less decentralized and open than its advocates might say. Indeed, blockchain-based activity depends on services that are only possible with the cooperation of a handful of private, centralized companies [5].

34.2.4 Trends

Over the next few years, Web3 will mature, and its components will merge with current technologies. This might include upcoming Central Bank Digital

Currencies [6], which could remove some of the problems linked to the high volatility of cryptocurrencies.

There is an attempt to work on the privacy problem of blockchains through the use of Zero-Knowledge proofs, which can hide the actions of a user. While this technology currently is very limited due to its low speed, it might very well mature to the point of being usable in a broader context [7].

As there is very little research on how to implement theft and fraud protection in Web3, it is expected that these problems will persist for many years to come. One of the problems is that this protection can be solved quite easily in a centralized setup, but a decentralized setup makes it very hard to make the right decisions.

34.3 Consequences for Switzerland

Switzerland was one of the first countries to have a legal framework for blockchain applications [8]. This made it attractive and attracted many companies to Zug and other places [9]. There is also an ongoing effort for digital identity that should be self-sovereign [10]. This puts Switzerland in a good place to profit from the positive effects of Web3.

34.3.1 Adoption and Efficacy

The current adoption of Web3 is low, mainly because the technology needs to be more mature and widely used. In addition, the underlying blockchains are too slow and too difficult to use [4]. Also, they are currently incompatible with the "free through ads" internet, as they all need financial implications to participate.

From an efficacy point of view, some of the underlying services start to evolve into a usable form: [11] has a decentralized cloud management system, and [12] is running a fast and decentralized generic blockchain.

34.4 Conclusion

Web3 promises more power to the users and the removal of intermediaries between the users and the services. This can bring more privacy and better remuneration for the service providers on the internet. Furthermore, most Web3 propositions are based on blockchains, which allow increasing trust by removing power from some controllers, like Google or Facebook. Switzerland is in an excellent position to participate in the upcoming Web3, as it already has legal regulations that allow innovation and growth. However, this dream might not come true as a new big player could control this new infrastructure.

So far, current Web3 systems still need to scale to the many billions of users on the internet. Once Web3 scales, it may deliver on its promise of a more user-driven experience.

References

1. Web3 vs. Web 3.0: Key Differentiators and Why It's Important. https://www.reworked.co/information-management/why-web3-and-web-30-are-not-the-same/. reworked.co.
2. Tim Berners-Lee: Screw Web3 — my decentralized web has no blockchain.
3. San Gilbert. Crypto, web3, and the Metaverse, March 2022.
4. Molly White. Web3 Is Going Just Great. https://web3isgoinggreat.com/, August 2022.
5. Web3 is not the decentralized utopia you've been promised, January 2022. Quartz.
6. Central Bank Digital Currency (CBDC). https://www.investopedia.com/terms/c/central-bank-digital-currency-cbdc.asp, August 2022. Investopedia.
7. Overview Of Zero-Knowledge Blockchain Projects | Chainlink. https://blog.chain.link/zero-knowledge-projects/, July 2022.
8. Blockchain / dlt State Secretariat for International Finance Swiss. https://www.sif.admin.ch/sif/en/home/finanzmarktpolitik/digitalisation-financial-sector/blockchain.html, January 2022. SIF.
9. Bank Julius Raphael Nikola Züger Baer, Legal Counsel. Swiss regulations give greater certainty to digital tokens. https://www.juliusbaer.com/en/business-navigator/regulation/swiss-regulations-give-greater-certainty-to-digital-tokens/, August 2022.
10. Building a Swiss Digital Trust Ecosystem – Perspectives around an e-ID ecosystem in Switzerland. https://digitalswitzerland.com/building-a-swiss-digital-trust-ecosystem/, April 2022. digitalswitzerland.
11. Dominic Williams. The Decentralized Cloud Vision of the DFINITY Blockchain. https://medium.com/dfinity/the-decentralized-cloud-vision-of-the-dfinity-blockchain-f68449c49be2, June 2021.
12. Emin Gun Sirer, Founder Of The Avalanche Blockchain, Is Not Sweating A 76% Drop In Token Price.

Chapter 35
5G

Weyde Lin

35.1 Introduction

5G is the 5th generation technology standard for broadband cellular networks designed to address the increasing need for higher capacity and throughput in mobile devices, driven by new applications, use cases, and lower latency requirements. The first air interface standard for 5G (5G NR) was defined in 2018 by the 3rd Generation Partnership Project. It used two frequency ranges, including the millimeter wave spectrum, which offers high data speeds but has limited range. 5G is based on existing security controls with added features, such as an asymmetric key, network slicing, and improved local-to-home network authentication. 5G rollout started in 2019, with the European Commission endorsing the EU 5G toolbox in 2020 to address the security risks related to 5G networks. The trend toward virtualization of network elements is also growing, which increases operator flexibility and reduces costs. 6G is currently in the research stage and is expected to roll out in the 2030s.

35.2 Analysis

The number of mobile devices connected to a cellular network is constantly increasing [1], simultaneously they require higher capacity and throughput, partly driven by new devices or applications (e.g., IoT devices [2], machine-to-machine communications [3]), new use cases with increased download speed requirements (*e.g.*, video streaming, video meetings [4]) and lower latency requirements (*e.g.*,

W. Lin (✉)
Eraneos Switzerland AG, Zurich, Switzerland
e-mail: Weyde.Lin@eraneos.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_35

Industry 4.0 and mobile gaming [5]). The 5th generation technology standard for broadband cellular networks (5G) [6] is meant to address these challenges [7].

35.2.1 Definition

In 2018 the first air interface standard for 5G was defined by the 3rd Generation Partnership Project (3GPP) as the radio access technology 5G NR (New Radio) [8]. 5G NR can use the frequency ranges 410 MHz–7125 MHz (Frequency Range 1 [9]) and 24.25 GHz–71.0 GHz (Frequency Range 2 [10]). Frequency Range 2 (FR2), also known as the millimeter wave spectrum, is new in 5G and has not been used in previous cellular network standards (i.e., 1G–4G). As a result, FR2 offers very high data speeds. However, the range is limited as the signal cannot travel far and is easily blocked by buildings or trees [11]. Therefore, the millimeter wave spectrum is primarily used in an urban environment to provide high network capacity in crowded environments [12].

From a security point of view, 5G is based on the previously existing security controls. Nevertheless, it adds some new security features. Indeed, this new generation now contains an asymmetric key. Some other improvements are the authentication of the local to-home network, even if using an untrusted serving network, and the network slicing to provide differentiated handling of service requirements for different applications [13].

35.2.2 Trends

Global 5G rollout by mobile operators started in 2019 [7]. In 2021, the global population 5G coverage already reached 25%, which is significantly faster than the 4G rollout that took 18 months longer to reach the same global population coverage [14]. This is partly driven by the fact that the mobile data traffic roughly doubles every 2 years [15]. GSMA predicts that in 2025, 44% of all mobile connections in Europe will be with 5G [16].

Securing 5G networks is crucial for the success of its adoption, especially for its business users. The European Commission, therefore, endorsed the EU 5G toolbox in 2020 [17], the toolbox outlines mitigation measures to address the security risk related to the 5G networks.

In network evolution and the 5G rollout especially, the increased virtualization of network elements is a growing trend [18]. This allows hardware and software network resources to be maintained and configured by a single software-based administrative entity called virtual network [19]. This increases the operator's flexibility and reduces costs as no physical changes to the network are required in case of network reconfiguration (See also *Network Slicing* and *Multi-access edge*

computing below). However, this solution is only available if the 5G antenna is linked to a 5G core [20].

The following cellular network generation is already being worked on (6G). However, the technology is currently only in the research stage and is expected to roll out in the 2030s [21].

35.3 Consequences for Switzerland

Since the start of the 5G rollout in 2019, the installation of 5G capable equipment in Switzerland has been fast-paced. As a result, the largest Swiss mobile operator (Swisscom) already had a population coverage (i.e., "the percentage of inhabitants living within range of a mobile-cellular signal" [22]) of 90% by the end of 2019 [23]. At the end of 2021, Swisscom had a population coverage of 98% while Sunrise reached 96% of the population [15].

There is a small but vocal minority of the Swiss population that is very critical of the 5G technologies and tries to block the construction of new 5G antennas [24] or even destroys them [25]. On the other hand, the Swiss mobile operators warn that with the blockage of new 5G antennas, the network capability will not be able to keep up with the yearly increase in mobile data usage [26].

35.3.1 Implementation possibilities: Make or Buy

The largest vendors for 5G equipment are Ericsson, Nokia, Huawei and ZTE [27]. Multiple countries (US, Canada, UK) have banned the Chinese 5G vendors Huawei and ZTE from supplying equipment for their countries' 5G mobile network infrastructure [28]. They cite security concerns for the ban. The Chinese government dismisses these claims and argues that the ban is politically motivated.

35.3.2 Variation and Recommendation

Private Networks

These are 5G networks that are nonpublic and isolated from the public network. Compared to Wi-Fi, they offer extended coverage and speed. Private 5G networks are especially interesting for industrial applications [29] due to their low latency (e.g., for IoT devices in a factory) [30]. Private networks offer privacy and greater control since network operation can assign different priority levels for different devices [31].

Network Slicing
This method allows multiple virtual networks to be defined on top of the physical network. This allows mobile operators to tailor them to the needs of individual customers. The GSMA (Global System for Mobile Communications, an industry organization representing the worldwide mobile communications industry) estimates that network slicing will generate a revenue of $300 billion by 2025 [32]. Network slicing is part of the 5G standard set by 3GPP [33].

Multi-Access Edge Computing (MEC)
MEC (sometimes known as mobile edge computing or mobile edge cloud) brings cloud computing capacity close to the edge of the cellular network, i.e., closer to the mobile device user. This results in lower latency and higher bandwidth uninhibited by network congestion. This allows for novel real-time applications (e.g., augmented reality headsets in construction sites). A standardization effort by ETSI is in progress (European Telecommunications Standards Institute) [34].

Fixed Wireless
Mobile operators offer 5G router-based "fixed" access for stationary internet access as an alternative to fixed line broadband [35]. This is needed mainly in rural areas where the fixed broadband coverage might not be complete.

35.4 Conclusion

5G is a further development of the cellular network standard that allows for higher bandwidth, throughput, and lower latency. The improved performance in 5G and the addition to the network standard enable novel uses cases such as private networking or MEC. Due to the increased reliance on mobile connectivity for business and industrial customers, securing the mobile cellular network is indispensable. The 5G network standard was designed to address security shortcomings of the previous network standard (i.e., 2G/3G/4G) directly [36]. The only drawback is that most of the new security features will not be available until the 5G network is fully deployed (5G standalone (SA)), i.e., 5G end-to-end with 5G core and 5G antennas.

References

1. Number of mobile devices worldwide 2020-2025. https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/, September 2022. Statista.
2. ALEXANDER HELLEMANS. Why IoT Needs 5G. https://spectrum.ieee.org/5g-taking-stock, May 2015. IEEE Spectrum.
3. Carsten Bockelmann, Nuno Pratas, Hosein Nikopour, Kelvin Au, Tommy Svensson, Cedomir Stefanovic, Petar Popovski, and Armin Dekorsy. Massive machine-type communications in 5g: physical and MAC-layer solutions. *IEEE Communications Magazine*, 54(9):59–65, September 2016. Conference Name: IEEE Communications Magazine.

4. Caroline Frost. How 5G will banish awkward video conference calls when you're out of the office, and cut your commute time. https://www.businessinsider.com/how-5g-banish-awkward-conference-calls-and-cut-commute-2019-8. Business Insider.
5. Ericsson. 5G for gaming. https://www.ericsson.com/en/5g/5g-for-gaming, July 2021.
6. CSRC Content Editor. 5G - Glossary | CSRC. https://csrc.nist.gov/glossary/term/5g.
7. Qualcomm. What is 5G | Everything You Need to Know About 5G. https://www.qualcomm.com/5g/what-is-5g, September 2022.
8. 3GPP. 3GPP specification series: 38series. https://www.3gpp.org/DynaReport/38-series.htm, August 2022.
9. 3GPP. Specification # 38.101-1. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3283, September 2022.
10. 3GPP. Specification # 38.101-2. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3284, September 2022.
11. Nokia. 5G spectrum bands explained — low, mid and high band. https://www.nokia.com/networks/insights/spectrum-bands-5g-world/, September 2022.
12. Ericsson. Leveraging the potential of 5G millimeter wave. https://www.ericsson.com/en/reports-and-papers/further-insights/leveraging-the-potential-of-5g-millimeter-wave, February 2021.
13. Gerrit Holtrup, William Lacube, Dimitri Percia David, Alain Mermoud, Gérôme Bovet, and Vincent Lenders. 5G System Security Analysis, August 2021. arXiv:2108.08700 [cs].
14. Ericsson. Network coverage forecast – Mobility Report. https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/network-coverage, November 2020.
15. Federal Communications Commission ComCom. Mobile coverage. https://www.comcom.admin.ch/comcom/en/home/dokumentation/zahlen-und-fakten/mobilfunkmarkt/mobilfunkabdeckung.html, August 2022.
16. GSMA. The Mobile Economy 2022. page 48, 2022.
17. European Commission. Commission endorses EU toolbox to secure 5G networks. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_123, September 2022. European Commission - European Commission.
18. Qualcomm. 5G network virtualization and interoperability: Why the time is now. https://www.qualcomm.com/news/onq/2020/10/5g-network-virtualization-and-interoperability-why-time-now, September 2022.
19. Red Hat. What is network virtualization? https://www.redhat.com/en/topics/virtualization/what-is-network-virtualization, September 2022.
20. Vuilleumier Philippe. 5G and Beyond: Security of future Mobile Infrastructures, October 2022.
21. Shuping Dang, Osama Amin, Basem Shihada, and Mohamed-Slim Alouini. What should 6G be? *Nature Electronics*, 3(1):20–29, January 2020. Number: 1 Publisher: Nature Publishing Group.
22. Proportion of population covered by at least 4G mobile network - Sustainable Development Goals - United Nations Economic Commission for Europe. https://w3.unece.org/SDG/en/Indicator?id=133, September 2022.
23. Interview with Urs Schaeppi on the 5g rollout. https://www.swisscom.ch/en/about/news/2019/12/19-interview-urs-schaeppi.html, September 2022.
24. 5G-Netz - Swisscom beklagt: 3000 Einsprachen gefährden Netzausbau. https://www.srf.ch/news/wirtschaft/5g-netz-swisscom-beklagt-3000-einsprachen-gefaehrden-netzausbau, October 2021. Schweizer Radio und Fernsehen (SRF).
25. Anschlagsserie im Kanton Bern - Militanter Kampf gegen 5G: Die Attacken nehmen zu.
26. Sunrise-Chef im Interview – "Frau Sommaruga hätte sich mehr gegen Fake News engagieren können".
27. Claudia Eckert, Thomas Magedanz, Manfred Hauswirth, Martin Schell, Albert Heuberger, Bernhard Niemann, Haya Shulman, and Michael Waidner. 5G-Netze und Sicherheit. page 11.
28. Annabelle Liang. Canada to ban China's Huawei and ZTE from its 5G networks. May 2022. BBC News.

29. Adnan Aijaz. Private 5G: The Future of Industrial Wireless. *IEEE Industrial Electronics Magazine*, 14(4):136–145, December 2020. Conference Name: IEEE Industrial Electronics Magazine.
30. Toby McClean. Council Post: Private 5G Networks Are On The Rise, Fueling The Industry 4.0 Drive. https://www.forbes.com/sites/forbestechcouncil/2021/08/09/private-5g-networks-are-on-the-rise-fueling-the-industry-40-drive/, September 2022. Forbes.
31. RedHat. What is private 5G? https://www.redhat.com/en/topics/5g-networks/what-is-private-5g, September 2022.
32. GSMA. Network Slicing Use Case Requirements. Technical report, September 2022.
33. Nokia. Network Slicing explained. https://www.nokia.com/about-us/newsroom/articles/network-slicing-explained/, September 2022.
34. Sabine Dahmen-Lhuissier. ETSI - Multi-access Edge Computing - Standards for MEC. https://www.etsi.org/technologies/multi-access-edge-computing, August 2022. ETSI.
35. Jürg Müller. Mobilfunkstandard 5G droht ein lukratives Geschäft zu untergraben. June 2018. Neue Zürcher Zeitung.
36. GSMA. Securing the 5G Era. https://www.gsma.com/security/securing-the-5g-era/, September 2022. Security.

Chapter 36
Email Security

Emilia Nunes

36.1 Introduction

In 2020, approximately 306 billion emails were sent and received daily, and this number is expected to rise to over 376 billion by 2025. A standard attack vector is phishing, a type of social engineering where a fraudulent message is sent to trick a person. Emails were not designed with cyber-attack protection in mind, making them an attractive target for cybercriminals. 83% of companies have been attacked by phishing, according to a study conducted in 2021. End-to-end encryption (E2EE) or transport layer security (TLS) can be used to secure emails. E2EE standards include Pretty Good Privacy (PGP) and Secure/Multipurpose Internet Mail Exchange (S/MIME). The use of E2EE in email is still rare; many emails are sent an as plain, unencrypted text. Nevertheless, the market for encrypted email revenue has tripled from $0.5 billion to $1.5 billion from 2015 to 2020. Technical developments in email security include cloud-based email services, artificial intelligence, blockchain, multi-factor authentication, and security extensions.

36.2 Analysis

Ray Tomlinson sent the first email in 1971 [1]. Since then, the number of email users has steadily increased. In 2020, approximately 306 billion emails were sent and received worldwide every day, and this number is expected to increase to over 376 billion by 2025 [2]. A primary attack vector is phishing, a type of social

E. Nunes (✉)
Eraneos Switzerland AG, Zurich, Switzerland
e-mail: Nunes.Emilia@eraneos.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_36

engineering in which a fraudulent message is sent to trick a person. In addition, emails were not designed with the protection against cyber-attacks in mind [3], making them an attractive target for cybercriminals. According to a study conducted in 2021, 83% of companies have been attacked by phishing [4], a widely used technique to steal personal information from users, such as via email [5]. Based on surveys of companies in the United States, the United Kingdom, France, Germany, and Australia [6], this represents a 46% increase from 2020. Phishing is not the only form of cybercrime, but it is the most widespread and is expected to remain a significant problem in the future. As a result, it is even more critical to ensure information security, especially its authenticity, in emails [7].

36.2.1 Definition

Email is usually used to refer to one of the following: (1) a means or system for transmitting messages between computers on a network or (2) a message sent and received electronically through an email system. Here, we focus on securing the messages rather than the email system. Email messages can be secured using cryptography. For example, end-to-end encryption (E2EE) could be used to protect them in transit and at rest. In addition, transport Layer Security (TLS) [8] is used to protect emails in transit between email servers and clients. TLS uses a combination of asymmetric (see Chap. 3) and symmetric cryptography (see Chap. 2). Common standards used for E2EE email encryption are:

- Pretty Good Privacy (PGP): One of the most widely used standards [9] is OpenPGP, which provides message encryption and digital signatures as security services (see Chap. 15). OpenPGP encryption software is an open standard that employs a combination of asymmetric (see Chap. 3) and symmetric encryption (see Chap. 2) [10].
- Secure/Multipurpose Internet Mail Exchange (S/MIME): Another widely used standard is S/MIME, which is also based on asymmetric and symmetric encryption. The system provides authentication, message integrity (i.e., the message was not modified during transmission), non-repudiation of origin (using digital signatures), and data confidentiality (using encryption). The certification process to verify the signatures is carried out by certified authorities [11].

36.2.2 Trends

End-to-end email encryption today is a rare, partial, and often perceived impractical solution. So most emails are sent as plain, easy-to-read, unencrypted text [3, 12]. Nevertheless, over 2015–2020, encrypted email revenue tripled from $0.5 billion to $1.5 billion [13]. Several factors drive growth, including an increase in fraud

(particularly phishing), an increase in email users, a high demand for cloud-based encryption services, and regulations requiring privacy compliance.

Technical Development There are a variety of technical developments that apply to email security. Cloud-based email services, including cost-effectiveness and scalability. In addition, security is included as part of the cloud service and does not require in-house development, implementation, and maintenance [14, 15]. Artificial Intelligence can detect various types of attacks. Furthermore, a blockchain eliminates the need for trusted intermediaries and keeps track of all previous transactions (see Chap. 25). Multi-factor authentication adds additional layers of security, making it harder for attackers to steal a person's identity (see Chap. 29). Finally, extensions such as Pleask Email Security or Virtru can help users against attacks.

Risks Risks are in a continuous development phase. Phishing via email is a standard method of phishing, which is becoming dangerous as phishing as a service (PhaaS) is becoming increasingly prevalent. Using PhaaS, cybercriminals assist others in conducting phishing attacks for a fee. This provides cybercriminals with a new source of revenue and permits anyone, regardless of their level of expertise, to conduct more professional attacks. PhaaS increases the number of phishing attempts while also increasing the likelihood that attacks will be effective [16]. With the rise of offensive artificial intelligence, organizations must adopt new defenses that circumvent conventional rule-based detection software [17].

36.3 Consequences for Switzerland

In 2021, Switzerland reported twice as many cyber incidents as the previous year. The most frequent reports [18] came from emails sent by perpetrators masquerading as law enforcement agencies. In recent years, more and more Swiss providers have entered the market with solutions that enable automated email encryption and signing, as email remains the most common means of communication in the public and private sectors. For example, IncaMail (Swiss Post) [19], HIN Mail (Health Info Net AG) [20], and SEPPmail (SEPPmail AG) [21] offer an integrated, comprehensive solution for their clients. The Federal Department of Justice and Police (FDJP) has recognized these solutions as secure delivery platforms in the context of proceedings. Therefore, these solutions can be utilized following the "ordinance concerning electronic communication in civil and criminal proceedings, as well as school proceedings and competitions" [22, 23]. Lawyers, for example, may receive court submissions or send court decisions in compliance with the law (see Chap. 37).

In Switzerland, email security is also actively researched, although more as part of fundamental research in cyber security (see Chap. 37). Protonmail is also a remarkable Swiss success story in email security. Indeed this company brings a service like no other to the table [24].

36.3.1 Implementation possibilities: Make or Buy

A secure email security solution should include strong encryption and address network vulnerabilities when purchased or built. Various solutions have now been established on the market, including SEPPmail [21], IncaMail [19], and HIN [20], which meet the legal requirements of the federal government and can be considered to be easy to use [25]. These solutions may also be used to exchange messages securely with communication partners that are not themselves subscribers to those solutions.

36.4 Conclusion

According to trends, email security is moving towards scalable, faster, safer, and more convenient solutions. As a result, system offerings that provide end-to-end encryption and are more user-friendly are taking up an increasing amount of the market. Since the email system was originally not designed to be secure, considerable effort had to be made to ensure the security of emails. Nevertheless, emails may never be as secure as newly designed solutions with solid end-to-end encryption and robust architecture (see Chap. 37).

References

1. Die E-Mail ein Auslaufmodell? March 2016. SRF News.
2. S Dixon. Number of e-mail users worldwide 2017-2025. Technical report, August 2022. Statista.
3. Scott Ruoti and Kent Seamons. Johnny's Journey Toward Usable Secure Email. *IEEE Security & Privacy*, 17(6):72–76, November 2019.
4. proofpoint. 2022 State of the Phish. Technical report, 2022.
5. NIST Computer Security Resource Center. phishing. https://csrc.nist.gov/glossary/term/phishing, August 2022. Information Technology Laboratory.
6. Gretel Egan. 2022 State of the Phish Report Explores Increasingly Active Threat Landscape, Importance of People-Centric Security. https://www.proofpoint.com/us/blog/security-awareness-training/2022-state-phish-explores-increasingly-active-threat-landscape, August 2022.
7. Adam Pilkey. Phishing is here to stay. https://blog.f-secure.com/phishing-is-here-to-stay/, August 2022. F-Secure.
8. NIST. Transport Layer Security (TLS). https://csrc.nist.gov/glossary/term/transport_layer_security, August 2022. Computer Security Resource Center (CSRC).
9. OpenPGP.
10. International Electrotechnical Commission. Pretty Good Privacy (PGP). https://std.iec.ch/terms/terms.nsf/3385f156e728849bc1256e8c00278ad2/39b4bbf83979035ac12574ab003677a1?OpenDocument, August 2022.

11. Internet Engineering Task Force and (IETF). Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification. https://datatracker.ietf.org/doc/html/rfc5751, January 2010.
12. Geoff Duncan. Here's why your email is insecure and likely to stay that way. https://www.digitaltrends.com/computing/can-email-ever-be-secure/, August 2013. digitaltrends.
13. Global e-mail encryption market 2015-2020. https://www.statista.com/statistics/535009/worldwide-email-encryption-market-revenue/. Statista.
14. Raktim Dey, Sandip Roy, Rajesh Bose, and Debabrata Sarddar. ASSESSING COMMERCIAL VIABILITY OF MIGRATING ON-PREMISE MAILING INFRASTRUCTURE TO CLOUD. *International Journal of Grid and Distributed Computing*, 14:1–10, March 2021.
15. Justina Alexandra Sava. Cloud-based email security market size worldwide in 2020 and 2026. Technical report, July 2022. Statista.
16. Jonathan Weinberg. The rise of phishing as a service (PhaaS) and how to tackle it. https://www.itpro.co.uk/security/cyber-security/368284/what-is-phishing-as-a-service-phaas, June 2022.
17. MIT Technology Review. Preparing for AI-enabled cyberattacks. https://www.technologyreview.com/2021/04/08/1021696/preparing-for-ai-enabled-cyberattacks/.
18. Nationales Zentrum für Cybersicherheit NCSC. Halbjahresbericht 2021/II (Juli – Dezember). Technical report.
19. Die Schweizerische Post. IncaMail – sending sensitive information. https://www.post.ch/en/business-solutions/e-mail-encryption, August 2022. Swiss Post.
20. Health Info Net AG (HIN). HIN Mail: So versenden Sie sichere E-Mails. https://www.hin.ch/services/hin-mail/, April 2020.
21. SEPPmail AG. SEPPmail - Secure E-Mail Communication. https://www.seppmail.com/, August 2022.
22. Philipp Bachmann. Sichere E-Mail-Kommunikation im E-Government. October 2021.
23. Verordnung über die elektronische Übermittlung im Rahmen von Zivil- und Strafprozessen sowie von Schuldbetreibungs- und Konkursverfahren. https://www.fedlex.admin.ch/eli/cc/2010/413/de, January 2011.
24. Professor Kumkum Saxena, Dev Rajdev, Divesh Bhatia, and Manav Bahl. ProtonMail: Advance Encryption and Security. In *2021 International Conference on Communication information and Computing Technology (ICCICT)*, pages 1–6, June 2021.
25. Stefan Klein. SEPPmail – Nummer 1 für die sichere E-Mail-Kommunikation. September 2021. Computerworld.

Chapter 37
Secure Messaging

Emilia Nunes

37.1 Introduction

In today's digital world, instant messaging and social networking have become ubiquitous. The widespread use of these communication channels, especially in the workplace, has raised security concerns for individuals and organizations. Secure messaging refers to protecting and safeguarding communication infrastructure, such as emails, messaging apps, and instant messaging platforms, through various security mechanisms like end-to-end encryption (E2EE). E2EE uses encryption and decryption keys to ensure the privacy of messages and the authenticity of the sender and recipient. With the increasing number of mobile messaging users, the need for secure messaging systems is rising. Technological advancements, such as cloud-based and blockchain-based platforms, drive growth in the secure messaging market. However, risks like phishing and cyberattacks remain persistent and are projected to continue targeting messages in the future.

37.2 Analysis

37.2.1 Definition

A *message* is defined as any piece of information that a person communicates to another individual or group. On the other hand, a *secure messaging* system is a method of protecting and securing individuals' and organizations' communication

E. Nunes (✉)
Eraneos Switzerland AG, Zurich, Switzerland
e-mail: Nunes.Emilia@eraneos.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_37

infrastructure [1]. Among the communication channels are emails, messaging apps, and social networking platforms for instant messaging (e.g., WhatsApp). Access to these channels is possible from various systems, such as mobile phones and computer messaging applications. In addition to preventing cyberattacks, appropriate security mechanisms can also enhance confidentiality (i.e., only intended recipients can view messages) and authenticity (i.e., verifying the identity of senders and recipients) [2].

E2EE (end-to-end encryption) can be used to secure messages while transferring them from one system or device to another. E2EE is intended to secure communication in a way that prevents third parties from accessing information. A message in E2EE is encrypted on the system or device of the sender, and only the intended recipient is permitted to decrypt it. The encryption and decryption keys are stored on each endpoint of the communication system. To facilitate key management (see Chap. 4), most systems make use of Public Key Cryptography (see Chap. 3).

37.2.2 Trends

It is anticipated that the number of mobile messaging users will increase from 2.9 billion users in 2020 to 3.5 billion in 2025 [3]. The increasing need for organizations to secure their messaging infrastructure is a key driver for growth, especially as businesses increasingly use mobile messaging applications to communicate. A list of key trends in the coming years is presented in Table 37.1.

37.3 Consequences for Switzerland

Threema is a Swiss solution used by more than 7'000 corporate customers, including the Swiss government. This solution provides some significant advantages like zero-knowledge security, on-premise servers, and metadata restrains [12]. However, vulnerabilities were discovered in the messenger application by the Applied Cryptography Group at the ETH Zurich [13]. They were fixed after 3 months, the time, Threema asked the researchers to hold the information.

It is common for Switzerland to conduct research on topics related to security and privacy, which lay the foundation for secure messaging, for example the Zurich Information Security & Privacy Center at ETH Zurich [14], Identity and Access Management (IAM) at Bern University of Applied Sciences (BFH) [15], or Center for Intelligent Systems (CIS) at EPFL [16]. The IBM Research Zurich team conducts commercial research on system security and cryptography [17].

Table 37.1 Key trends of secure messaging

Trend Category	Trend	Description	
Technical Development	Cloud-based platforms	Secure messaging is becoming increasingly influenced by cloud-based platforms. This is especially true for communications platform as a service (cPaaS), which provides a cloud-based middleware on which communication software can be developed, run, and distributed.	[4]
	Blockchain-based platforms	In recent years, blockchain technology has been pushed as a means of decentralizing communications, as well as providing users with more privacy and anonymity than common end-to-end encryption techniques (e.g., pretty good privacy (PGP)). The messaging app *Session* uses blockchain technology to hide the IP addresses of its users and makes it possible for users to communicate without providing a phone number	[5, 6]
	Instant messaging applications	A number of applications available on smartphones, tables and computer have reached an intersting maturity point. Furthermore, these solutions are under continuous development, which makes them necessary to follow.	[7]
Risks	Phishing	Email is a common means used for phishing, which is now becoming even more dangerous as phishing as a service (PhaaS) is on the rise. With this service, cybercriminals help others carry out phishing attacks for a fee. This provides cybercriminals with a new source of revenue and allows anyone, even without expertise, to perform more professional attacks. PhaaS not only increases the phishing rate, but also makes each attack potentially more effective .	[8]
	Cyberattacks in general	Cyberattacks, such as malware and phishing, will continue to target messages in the future for three main reasons: financial gain, data theft, and business disruption.	[9, 10, 11]

37.3.1 Implementation possibilities: Make or Buy

In response to increased public attention, more and more solutions for secure messaging have emerged. However, many of these solutions do not provide strong and well-defined security features [7]. Many of the secure messaging solutions have no answer to the problem of protecting the metadata [7].

Secure messaging solutions should be purchased with a strong analysis based on the needs of each organization as end-to-end encrypted messages sent on unique channels could be easily attacked by spam, flooding, and denial-of-service [7].

37.4 Conclusion

The demand for secure messaging solutions is growing, and the solutions are becoming more convenient and secure. However, if solutions exist, choosing them and implementing them in a efficient way remains a big challenge.

References

1. Justin Engler and Cara Marie. Secure Messaging for Normal People. Technical report, NCC Group, August 2022.
2. Benjamin Dowling and Britta Hale. Secure Messaging Authentication against Active Man-in-the-Middle Attacks. In *2021 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 54–70, Vienna, Austria, September 2021. IEEE.
3. Mobile messaging users worldwide 2025. https://www.statista.com/statistics/483255/number-of-mobile-messaging-users-worldwide/, August 2022. Statista.
4. Council Post: The CPaaS Industry Is In Hyper Growth: A Blueprint Of CPaaS And Its Future.
5. Session | Send Messages, Not Metadata. | Private Messenger. https://getsession.org/, August 2022. Session.
6. Global Relay. Engineered Anonymity: How Blockchain is Disrupting Secure Messaging. https://www.globalrelay.com/how-blockchain-is-disrupting-secure-messaging/, May 2022.
7. Nik Unger, Sergej Dechand, Joseph Bonneau, Sascha Fahl, Henning Perl, Ian Goldberg, and Matthew Smith. SoK: Secure Messaging. In *2015 IEEE Symposium on Security and Privacy*, pages 232–249, May 2015. ISSN: 2375-1207.
8. NIST. Back to Basics: What's multi-factor authentication - and why should I care? https://www.nist.gov/blogs/cybersecurity-insights/back-basics-whats-multi-factor-authentication-and-why-should-i-care, August 2022.
9. MIT Technology Review Insights. Preparing for AI-enabled cyberattacks. Technical report, April 2021.
10. Expert Insights. What Does AI Mean For The Future Of Email Security? https://expertinsights.com/insights/ai-and-the-future-of-cyber-security-for-business/#:~:text=AI%20is%20helping%20businesses%20achieve,before%20it%20can%20take%20place, March 2022.
11. IBM. What is a cyberattack? https://www.ibm.com/topics/cyber-attack, August 2022.
12. Threema – Maximum Security Chat App. For Companies and Individuals.–Overview. https://threema.ch/en, December 2022.
13. Vulnerabilities in secure messenger Threema discovered. https://inf.ethz.ch/news-and-events/spotlights/infk-news-channel/2023/01/threema.html.
14. ZISC – Zurich Information Security and Privacy Center. https://zisc.ethz.ch/, August 2022.
15. Identity and Access Management (IAM). https://www.bfh.ch/en/research/research-areas/identity-access-management-iam/, August 2022.
16. Center for Intelligent Systems (CIS). https://www.epfl.ch/research/domains/cis/, August 2022. EPFL.
17. Security Research, IBM Research Europe Zurich. https://www.zurich.ibm.com/security/, August 2022.

Chapter 38
Secure Smartphone

Yann Donon, Fabien Künzler, Pawel Jasinski, Carl Piening, and Arnaud Savary

38.1 Introduction

Secure smartphones highlight the privacy and data safety issues in off-the-shelf smartphones and the need for secure smartphones to address these concerns. The article focuses on several key features of secure smartphones, including trusted hardware, secure boot, encryption, and mobile network. These features play a critical role in ensuring the security of a smartphone and protecting users and organizations against data leaks and cyberattacks. The section also briefly discusses the challenges in implementing these features and the importance of using trusted sources, dedicated encryption engines, and high-quality entropy sources to design secure smartphones.

38.2 Analysis

Off-the-shelf (OTS) smartphones are known to present data safety and privacy issues [1]. These devices often change location with their user and are notably vulnerable to theft, malicious access points, or malware [2, 3]. To face these risks, secure smartphones are being developed. They are designed to have increased resistance against cyberattacks and to protect users and organizations against data leaks while aiming to maintain the practicality of smartphones.

Y. Donon (✉) · F. Künzler · P. Jasinski · C. Piening · A. Savary
RUAG, Emmen, Switzerland
e-mail: yann.donon@ruag.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_38

38.3 Definition

Smartphones are devices combining the features of a computer and a mobile phone. As such, typical vulnerabilities of both systems exist in smartphones. The hardening of smartphones, a process intended to eliminate means of attack by patching vulnerabilities and turning off nonessential services [4], is, therefore, key to making it more secure. Given the extensive range of features that address known vulnerabilities and the democratization of smartphones, research focusing on such features is numerous. This article focuses on a set of features that seems most relevant when evaluating the need for a secure smartphone.

38.3.1 Trusted Hardware

The hardware includes all physical parts of a smartphone. It is required to run the software. As such, hardware security is critical to support software security. However, as the design complexity of hardware (system-on-chip, SoC) increased, foundries capable of producing these SoCs became increasingly complex and expensive. This phenomenon resulted in the global scarcening of foundries, making it extremely difficult to acquire components from trusted sources. This represents a challenge close to unverifiable for any manufacturer aiming to provide secure hardware [5]. While approaches exist or are being researched to review hardware or execute secure operations on untrusted hardware [6], capabilities in that direction remain limited [7, 8].

38.3.2 Secure boot

Secure boot is key to bringing a device into a certain operational state. It aims at securing the consistency and integrity of the firmware and operating system (OS). Would the device be compromised at this level, it would leave the whole system vulnerable [9]. Implementation of secure boot takes advantage of a hardware root of trust—the public key of a vendor. The public key is immutable—stored in ROM. The boot process verifies the signature of loaded images against the vendor key. Some vendors allow the use of user-supplied public keys during the later stages of the boot process. The location of the storage of these keys is critical. In the ideal case, the keys are stored in a dedicated module to prevent alteration. During the secure boot, the device performs an additional security function called downgrade check. In order to effectively preventing the downgrading of the operating system to a version with known security exploits [10].

38.3.3 Encryption

Encryption is a process of encoding information so that only an entity with access to a secret can decode it can access the original information. Modern smartphones do not only use full disc encryption (FDE) but also rely on file-based encryption (FBE) to effectively increase protection granularity by using different sets of keys for different sets of files (see Chap. 33). This allows, for example, for a file encryption key on a per-application basis to prevent applications from accessing files from other applications [11]. The keys used for encryption are usually derived from a unique device identifier and, for some of the keys, also from some user-provided secret. Use of trusted execution environments, which can perform computations in isolation from the operating system or the central application processor (see Chap. 18), minimize or even entirely prevent exposure of the encryption keys to the rest of the system. Ideally, encryption is performed using a dedicated, hardware-based encryption engine designed to withstand side-channel attacks such as static or dynamic power analysis or timing analysis [12]. Finally, suppose a device comes with device keys generated in the factory. In that case, it is crucial that they are stored in a tamper-resistant way and that all cryptographic operations with them are performed so that the keys are not exposed to the user or operating system. Moreover, to generate keys on the device itself, it is essential to have a high-quality entropy source on the device, which is usually a true random number generator implemented in hardware [13].

38.3.4 Mobile Network

The ability to control the connection to the carrier network may protect from connecting to unsafe, intrusive, or compromised service providers. However, most off-the-shelve devices maintain some degree of connectivity with network providers at all times and states as long as the battery lasts. Therefore, removing the phone's main antennas and replacing them with ones that can be physically connected or disconnected (e.g., with a switch) might offer some protection from unwanted connectivity. However, in general, this is insufficient to prevent all forms of wireless communication as the phone might have components capable of sensing and sending signals independently from this antenna (e.g., electromagnetic emissions from the devices' screen [14]). The difficulty of controlling connectivity is that support for standard IPv4 and IPv6 protocol stack is usually built-in and ready for use with all wireless and non-wireless network technologies like carrier networks, Wi-Fi, Bluetooth, USB, or even Ethernet with the help of USB-Ethernet adapter.

38.3.5 Open source

Open source designates disclosing source code and permitting modification and redistribution of source code [15]. Disclosing the source code is generally beneficial for security since it makes it possible for any interested party to review the source code for security problems. However, it is crucial that disclosure processes for vulnerabilities in open source are carefully designed to prevent leakage of information around reported vulnerabilities since exploiting them might be more straightforward than when the source code is not available [16]. It is important to note that providing access to source code to some entities only is different from a healthy open source-based security ecosystem. The complexity and cost of performing code reviews and vulnerability analysis by a few entities are prohibitive, especially considering that new software releases are provided and need to be reviewed frequently. A trend that might increase trust in open source-based systems further is the introduction of reproducible builds. With reproducible builds, independent third parties can reconstruct all OS components and compare them (e.g., using their hashes (see Chap. 5) with the images provided by a vendor. This can confirm that the code published is indeed the one running on a device without compromising secure boot integrity [17].

38.3.6 Mobile Applications

Mobile applications are software designed to run on mobile devices. They provide functionality but are also a potential threat since they may contain vulnerabilities and are usually provided by untrusted third parties. While some applications are created to deceive users and gain access to information available on the phone, others do this without trying to hide it. After all, many benign applications out there collect information about the user as part of their business model [18]. Because of this, special care has to be taken to limit access and capabilities of applications by following a need-to-know and principle of least privilege approach. In practice, the combination of the user and the operating system is often responsible for deciding what an application is allowed to do. The operating system uses sandboxing techniques and a permissions framework to restrict and control them [19]. However, the user (or risk owner in the case of managed devices) decides whether the requested access and capabilities are appropriate for a given application. Unsurprisingly, breaches or unintended use of features are numerous [20].

38.4 Trends

As the mobile smartphone ecosystem continues to grow, the number of security threats and data breaches has increased dramatically. There is the need of increased smartphone security for individuals, businesses, and governments [21]. Recently, there has been a lot of media coverage about malware campaigns, privacy policy changes, and data theft, which has led to growing public awareness. A prominent example in this coverage is the Pegasus spyware used by NSO Group. It revealed the extent of vulnerabilities in all operating systems [22]. Google Play Protect Service also made the news, struggling to provide a layer of efficient protection, leading to data theft from several popular applications, highlighting another kind of privacy and security weak point on smartphones [23]. Finally, the continuing concentration of consumer data in the hands of a few, with the acquisition of WhatsApp by Facebook in 2015 as a prominent example, has raised serious concerns regarding the use and commercialization of such data [18, 24, 25].

The multiplication of similar cases combined with the complexity and increasing use of smartphones has heightened public awareness of security issues and the growing need for secure smartphones. Valued at 3.3 billion dollars in 2020, the global mobile security market is projected to reach 22.1 billion dollars by 2030, growing at a compound annual growth rate (CAGR) of 21.1% from 2021 to 2030 [26]

38.5 Consequences for Switzerland

While convenient, bring your own device (BYOD) models put organizations at increased risk of privacy and data security breaches from smartphones [27]. Malicious apps may access sensitive and private information. This includes but is not limited to the phone number, calendar, contact list, usernames and passwords, messages, the camera, the microphone, or GPS information [28]. Smartphones are also regularly used in unsecured networks. As a result, users may inadvertently download malicious software [29] or apps, even through official stores [30, 31]. In addition, Advanced Persistent Threats have been able to breach security on multiple occasions [2]. Such attacks are more sophisticated and targeted, often against large corporations, governments, or the military. In this context, the secure smartphone may become a necessity as it is a valuable tool to address the security risks in our evolving workspace.

38.6 Implementation possibilities: Make or Buy

Making a secure smartphone is a multi-faceted problem and is generally not an option for companies where making smartphones and/or secure operating systems is their core business. When buying a secure smartphone, there is a multitude of critical factors that must be considered and taken into account. Among them are the threat model, the desired level of protection and privacy, and your trust in hardware manufacturers, operating systems- and software providers.

38.7 Conclusion

Smartphones are a use case that integrates numerous technologies described in this book. Technologies like hardware security modules (see Chap. 16) or full-disk- or file-based encryption (see Chap. 33) play an essential role in implementing or securing the key components outlined in this article. Since those technologies are not perfect, it is logical that smartphones also suffer from those imperfections. While it is unrealistic to proactively protect ourselves from all the threats they may imply, more secure smartphone options will become available. To what extent this privacy and security are to be leveraged by each individual or organization, taking into account operational needs, threat models, and the degree of convenience.

References

1. O. Ugus, D. Westhoff, and H. Rajasekaran. A leaky bucket called smartphone. pages 374–380, 2012.
2. Mahinderjit Singh M. Jabar T. Exploration of mobile device behavior for mitigating advanced persistent threats (apt): A systematic literature review and conceptual framework. 2022.
3. Sandeep B. Vanjale, P. B. Mane, and Sandip V. Patil. Wireless lan intrusion detection and prevention system for malicious access point. In *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, pages 487–490, 2015.
4. CSRC Content Editor. Hardening - Glossary | CSRC. https://csrc.nist.gov/glossary/term/hardening.
5. Yier Jin. Introduction to hardware security. *Electronics*, 4(4):763–784, 2015.
6. Moritz Schneider, Ramya Jayaram Masti, Shweta Shinde, Srdjan Capkun, and Ronald Perez. Sok: Hardware-supported trusted execution environments. *arXiv preprint arXiv:2205.12742*, 2022.
7. Nicolas Sklavos, Ricardo Chaves, Giorgio Di Natale, and Francesco Regazzoni. Hardware security and trust. *Cham, Switzerland: Springer*, 2017.
8. David Kohlbrenner, Shweta Shinde, Dayeol Lee, Krste Asanovic, and Dawn Song. Building open trusted execution environments. *IEEE Security & Privacy*, 18(5):47–56, 2020.

9. Richard Wilkins and Brian Richardson. Uefi secure boot in modern computer security solutions. In *UEFI forum*, pages 1–10, 2013.
10. Rashmi R.V. and Karthikeyan A. Secure boot of embedded applications - a review. In *2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, pages 291–298, 2018.
11. GrapheneOS. Faq : Security and privacy. https://grapheneos.org/faq#encryption, September 2022.
12. Apple Inc. Secure enclave. https://support.apple.com/guide/security/secure-enclave-sec59b0b31ff/1/web/1, September 2022.
13. Fatemeh Tehranipoor, Wei Yan, and John A. Chandy. Robust hardware true random number generators using dram remanence effects. In *2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 79–84, 2016.
14. Zhuoran Liu, Niels Samwel, Leo Weissbart, Zhengyu Zhao, Dirk Lauret, Lejla Batina, and Martha A. Larson. Screen gleaning: A screen reading TEMPEST attack on mobile devices exploiting an electromagnetic side channel. In *28th Annual Network and Distributed System Security Symposium, NDSS 2021, virtually, February 21-25, 2021*. The Internet Society, 2021.
15. Bruce Perens et al. The open source definition. *Open sources: voices from the open source revolution*, 1:171–188, 1999.
16. Jaap-Henk Hoepman and Bart Jacobs. Increased security through open source. *Communications of the ACM*, 50, 02 2008.
17. Manuel Pöll and Michael Roland. Analyzing the Reproducibility of System Image Builds from the Android Open Source Project. page 27.
18. Kim Doyle. Facebook, whatsapp and the commodification of affective labour. 2015.
19. Wenna Song, Jiang Ming, Lin Jiang, Yi Xiang, Xuanchen Pan, Jianming Fu, and Guojun Peng. Towards transparent and stealthy android os sandboxing via customizable container-based virtualization. New York, NY, USA, 2021. Association for Computing Machinery.
20. Wasiq Waqar, Yuanzhu Chen, Andrew Vardy, et al. Exploiting smartphone sensors for indoor positioning: A survey. In *Proceedings of the Newfoundland Conference on Electrical and Computer Engineering*, 2011.
21. Ali Balapour, Hamid Reza Nikkhah, and Rajiv Sabherwal. Mobile application security: Role of perceived privacy as the predictor of security perceptions. *International Journal of Information Management*, 52:102063, 2020.
22. JD Rudie, Zach Katz, Sam Kuhbander, and Suman Bhunia. Technical analysis of the nso group's pegasus spyware. In *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*, 2021.
23. Shinelle Hutchinson, Bing Zhou, and Umit Karabiyik. Are we really protected? an investigation into the play protect service. In *2019 IEEE International Conference on Big Data (Big Data)*, 2019.
24. Rizaldi Wahaz, Rakha Nadhifa Harmana, Amiruddin Amiruddin, and Ardya Suryadinata. Is whatsapp plus malicious? a review using static analysis. In *2021 6th International Workshop on Big Data and Information Security (IWBIS)*, 2021.
25. Carolina Lituma and Teresa Guarda. Whatsapp in the judicial processes. In *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, 2019.
26. Vineet Kumar Kanhaiya Ramesh Kathoke, Pradeep Ravi. Mobile security market research, 2030. https://www.alliedmarketresearch.com/mobile-security-market, September 2022.
27. Wang P. Sbeit R.O. Ratchford, M. Byod security risks and mitigations. volume 558. Springer, 2018.
28. et al. Wang, Yuanda. Ghosttalk: Interactive attack on smartphone voice system through power line. In *The Network and Distributed System Security (NDSS) Symposium 2022*, 2022.
29. Adrienne Porter Felt, Matthew Finifter, Erika Chin, Steve Hanna, and David Wagner. A survey of mobile malware in the wild. New York, NY, USA, 2011. Association for Computing Machinery.

30. Xuetao Wei, Lorenzo Gomez, Iulian Neamtiu, and Michalis Faloutsos. Malicious android applications in the enterprise: What do they do and how do we fix it? In *2012 IEEE 28th International Conference on Data Engineering Workshops*, pages 251–254, 2012.
31. Nisreen Ameen, Ali Tarhini, Mahmood Hussain Shah, and Nnamdi O. Madichie. Employees' behavioural intention to smartphone security: A gender-based, cross-national study. *Computers in Human Behavior*, 104:106184, 2020.

Part VI
Analysis and Conclusion

Chapter 39
Scientometric and Wikipedia Pageview Analysis

Alexander Glavackij, Sarah Ismail, and Percia David Dimitri

39.1 Introduction

This chapter explores trends in data protection and encryption technologies across different technologies. The technologies analyzed are taken from the previous chapters.

Any trend assessment concerning data protection and encryption technologies constitutes a challenging task for various reasons. The swift development of the security technologies brings a myriad of novel protocols, tools, and procedures, whose technological readiness levels (TRL) also evolve rapidly [1]. Also, while some technologies thrive, others stagnate or vanish in favour of more market-adapted technologies or enhanced operational implementation [2]. Moreover, in such a fast-paced and growing environment, opportunities and threats evolve quickly, making it difficult to evaluate the whole spectrum of technologies available on the market [3]. Consequently, evaluations of the security consequences of the arrival and evolution of such technologies on data protection are complex.

Following the previous individual analysis of the data protection and encryption technologies, we evaluate these technologies through time by benchmarking a development indicator—the *attention* paid by different communities [4].

A. Glavackij · S. Ismail
Cyber-Defence Campus, Thun, Switzerland
e-mail: alexander.glavackij@ar.admin.ch; sarah.ismail@ar.admin.ch

P. D. Dimitri (✉)
HES-SO Valais-Wallis, Sion, Switzerland
e-mail: dimitri.perciadavid@hevs.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_39

39.2 Analysis

39.2.1 Scientometric analysis

We conduct a scientometric analysis of the book's technologies to better understand how they evolved over the last 20 years. Most cryptographic technologies are the result of long-term research efforts. Therefore, we analyze the number of associated scientific works through time for each technology, which can be seen as an indicator of scientific interest in that technology [5]. Growing attention points toward promising or emerging technologies, as researchers tend to dedicate significant resources to potentially valuable technologies. Conversely, low interest in a given technology correlates with the lack of technological novelty and obsolescence.

To provide such a scientometric analysis, we use the OpenAlex dataset, which describes scholarly entities (works, authors, institutions, venues, and concepts) and their connectivity patterns using a graph structure.[1] Importantly, each scholarly work has concepts associated with it that are represented in the paper. OpenAlex organizes publications' concepts into a tree structure, where general concepts are parents of more fine-grained ones. OpenAlex has 65,026 concepts, ranging from Political Science to Physics. Scientific works are tagged automatically using a classification model trained on the Microsoft Academic Graph (MAG) [6]. Thus, OpenAlex provides a taxonomy of topics discussed in the scientific literature, used here to retrieve scientific works tagged with this book's 38 technologies. We scrape the scientific works tagged with those 38 technologies, taking for each a monthly count of the number of published papers. This yields a time series for each technology, which we use to analyze the technologies over time.

The technologies' time series display different development patterns; therefore, we cluster them according to the exhibited pattern into three classes: no growth, moderate growth, and strong growth. We calculate the clusters in the following manner: we divide the average number of publications during the first 3 months in 2022 by the average number of publications during the first 3 months in 2012. We refer to the resulting ratio as *growth ratio*. If growth ratio < 1.05, we deem the technology as not growing. The technology exhibits moderate growth if $1.05 <$ growth ratio < 2. The technology thrives if growth ratio > 2.

Additionally, we cluster the technologies into low, moderate, and high-interest technologies. A technology is a high-interest technology if the average monthly publication count is $c \geq 50$, a moderate-interest technology if $15 \leq c < 50$, and a low-interest technology if $c < 15$. The growth pattern and interest level form a two-dimensional matrix where we can arrange the technologies. Table 39.1 shows the resulting matrix for 24 selected technologies.

We emphasize interesting patterns. High-interest technologies which have been researched extensively, include Blockchain, Hash Function, and Asymmetric

[1] https://docs.openalex.org/.

Table 39.1 Selected technologies of this book assorted into a two-dimensional matrix, created by clustering the technologies by their past growth and interest in the research community

Growth Pattern \ Interest	Low Interest	Moderate Interest	High Interest
No Growth	Confidential Computing, Digital Rights Management, Disk Encryption	Authentication, Digital Signature, Identity Management, Key Management	Asymmetric Encryption
Moderate Growth	Electronic Voting, Functional Encryption	Quantum Cryptography, Random Number Generation, Symmetric Cryptography	Biometrics, Hash Function
Strong Growth	Hardware Acceleration, Hardware Security Module, Post-Quantum Cryptography, Zero-Knowledge Proof	Differential Privacy, Homomorphic Encryption, Quantum Key Distribution	Blockchain

Encryption in this cluster. Except for Blockchain, these technologies represent the backbone of today's cybersecurity landscape. However, Blockchain is the only one exhibiting strong growth. This might indicate that Blockchain technology has a large part of its development ahead of it. Moderate-interest technologies represent more specialized techniques and methodologies that have established themselves. Digital Signatures, Authentication, and Key Management are well-known and widely used technologies, but interest in them is not growing further, indicating technical convergence. Emerging technologies, especially Differential Privacy and Quantum-related technologies, exhibit growth and can be counted on to become more critical in the future. Low interest and not growing technologies are niche technologies, like Disk Encryption and Functional Encryption. However, some low-interest technologies exhibit strong growth, like Post-Quantum Cryptography, Zero-Knowledge Proof, and Hardware Security Modules. These technologies have been relatively recently established, and the research interest indicates that most discoveries in those technologies are yet to be made (Fig. 39.1).

39.2.2 Evolution of public attention

To explore more, we look at the evolution over time of public attention to technologies through Wikipedia's pageviews statistics. The motivation of the public to know more about a technology provides good information on the position and the popularity of the technologies [7]. Wikipedia's pageviews statistics show the number of pages visited over a given period at a given chosen frequency (either daily, monthly, or yearly data—in this work, we use the monthly frequency). Such statistics cover each page. The statistics do not consider the time Internet users spend on a page. Whatever its duration, it will be counted as a view. We collect data for 37 technologies over 82 months, from July 2015 to April 2022. Again, we group the technology time series into three classes: no growth, moderate growth, and high growth. Clusters are calculated as follows: we divide the average pageviews

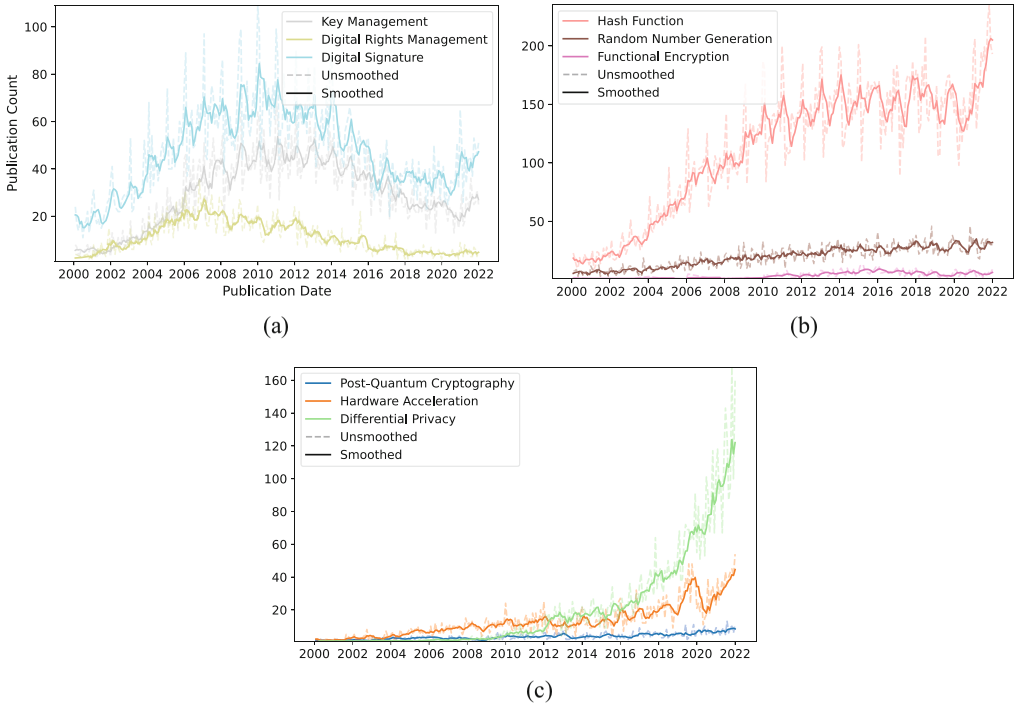

Fig. 39.1 Number of monthly scientific works established between 2000 and 2022, taken from OpenAlex, for three samples from each growth pattern cluster. The No Growth technologies in (a) have already achieved their peak of maximal interest, i.e., interest in those technologies is waning. For the Moderate Growth technologies (b), growth has been slowing recently. If researchers do not discover new research areas in those fields, interest will decrease further, and these technologies will shrink soon. The fast-growing technologies (c) are fairly recently established technologies and can be expected to be further developed. (**a**) No growth. (**b**) Moderate growth. (**c**) Strong growth

Table 39.2 Technologies of this book assorted to a two-dimensional matrix created by clustering the technologies by their past growth and public interest

Growth Pattern \ Interest	Low Interest	Moderate Interest	High Interest
No Growth	Authentication, Confidential Computing, Disk Encryption, Electronic Voting, Email Security, Hardware Security Module, Identity Management, Key Management, Quantum Cryptography, Secure Messaging, Secure Operating System, Symmetric Cryptography, Tunneling	Biometrics, Digital Rights Management, Digital Signature	Asymmetric Encryption, Hash Function
Moderate Growth	Differential Privacy, Functional Encryption, Hardware acceleration, Homomorphic Encryption, Quantum Key Distribution	Random Number Generation	
Strong Growth	Identity-based Cryptography, Multi-party Threshold Cryptography, Post-quantum Cryptography, Private Set Intersection, Searchable Symmetric Encryption, Secure Multi-Party Computation, Trusted Execution Environment, Zero-knowledge Proof		Blockchain

of the last 3 months by the average pageviews of the last 3 months from 6 years ago. We refer to the resulting ratio as *growth ratio*. If growth ratio < 1.05, we deem the technology as not growing. The technology exhibits moderate growth if $1.05 <$ growth ratio < 2. The technology thrives if $2 <$growth ratio. We also cluster the technologies into low, moderate, and high-interest technologies. A technology is a high-interest technology if the average number of pageviews per month is $c \geq 50{,}000$, a moderate-interest technology if $25{,}000 \leq c < 50{,}000$, and a low-interest technology if $c < 25{,}000$. We provide the two-dimensional matrix clustering the technologies according to their growth in Table 39.2 (Fig. 39.2).

Again, the technologies attracting significant public interest are Blockchain, Hash Function, and Asymmetric Encryption. Blockchain shows strong growth, unlike Hash Function and Asymmetric Encryption, which show no growth. Again, technologies with more specialized techniques and methodologies, such as Digital Signatures and Biometrics, are seeing moderate interest. Low-interest and no-growth technologies are niche technologies, such as Disk Encryption, or long-standing technologies, such as Email Security. However, some low-interest technologies, such as Post-quantum Cryptography, still show strong growth (Fig. 39.3).

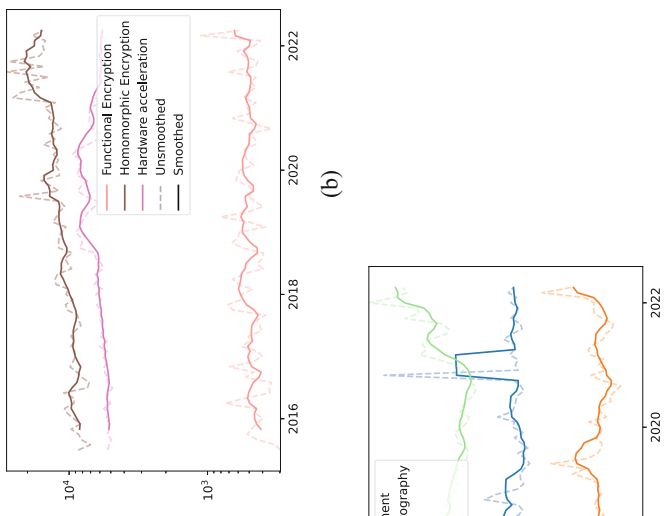

Fig. 39.2 Number of monthly pageviews of Wikipedia between 2015 and 2022 for three samples from each growth pattern cluster. The No Growth technologies in (a) are already at their peak of maximal interest, i.e., interest in those technologies is waning. For the Moderate Growth technologies (b), growth has been slowing recently. If researchers do not discover new research areas in those fields, interest will decrease further, and these technologies are expected to shrink soon. The fast-growing technologies (c) are fairly recently established technologies and can be expected to be further developed. (**a**) No growth. (**b**) Moderate growth. (**c**) Strong growth

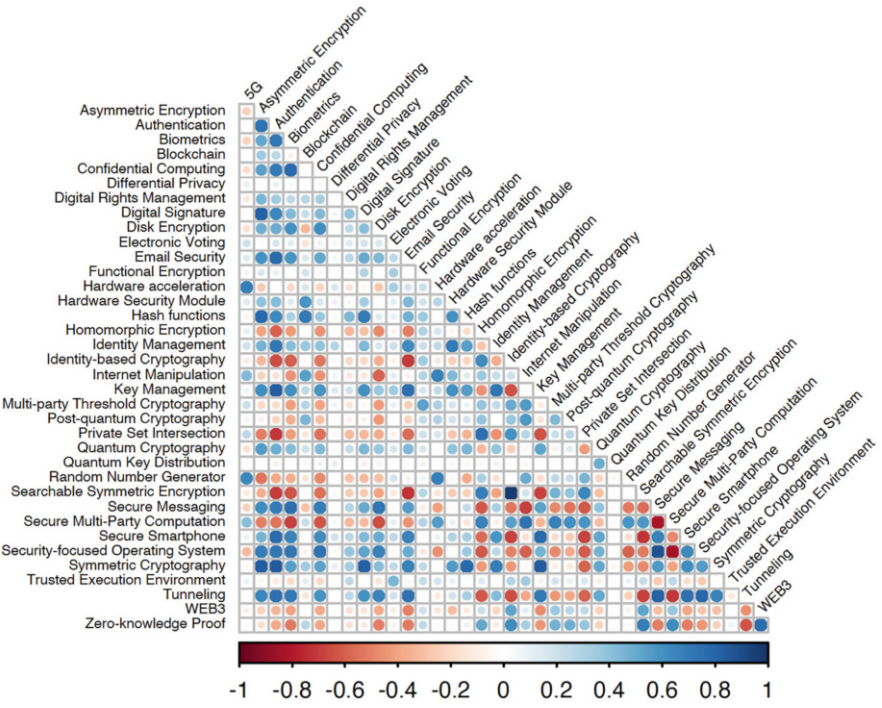

Fig. 39.3 Correlation between pageviews of technologies in Wikipedia from July 2015 to April 2022

39.2.3 Correlation Analysis

In order to proceed to an exploratory data analysis and get an idea of the potential existing relationships between these technologies, we display a correlation matrix of Wikipedia's monthly pageviews. However, these correlations can potentially contain confounding factors and spurious relationships (as time series are not stationary). Figure 39.4 shows positive or negative correlations between page views. For instance, we notice that "Identity-based encryption" and "Searchable symmetric encryption" highly correlate. On the other hand, "Quantum Key Distribution" has no or a very weak correlation with all the other technologies.

39.2.4 Comparison of public and expert attention

The relationship between these proxies for the two types of attention diverges over time. However, graphically, we observe that expert attention follows public attention by a few months. For instance, in the case of Random Number generation, public

Fig. 39.4 These plots compare public attention from Wikipedia page views (blue line) and expert attention from the number of publications on OpenAlex (red line). We discard outliers, and the study period is from July 2015 to April 2022. Data is provided on a monthly frequency. The method used on the data is the robust z-score with a scale from −5 to 5 to have a better view and eliminate large outliers

attention increased around 2019, while expert attention started to pick up 1 year later.

39.3 Conclusion

In conclusion, this chapter evaluates data protection and encryption technology trends through time. We used a benchmarking development indicator, the attention brought by different communities, to perform the analysis. This attention was measured through a scientometric analysis of the production of scientific works and the public attention was given to these technologies through Wikipedia pageviews. Our results showed that high-interest technologies like Blockchain, Hash Function, and Asymmetric Encryption are widely researched and used, but only Blockchain exhibited strong growth. Moderate-interest technologies like Digital Signatures, Authentication, and Key Management have established themselves but need to show growth, indicating technical convergence. Finally, emerging technologies like Differential Privacy and Quantum-related technologies showed growth, indicating their potential to become more critical in the future. This analysis provides valuable insights into the development of data protection and encryption technologies and their impact on the security landscape.

References

1. Yu-Wei Chang and Jiahe Chen. What motivates customers to shop in smart shops? the impacts of smart technology and technology readiness. *Journal of Retailing and Consumer Services*, 58:102325, 2021.
2. Bram Faber. A tale of three technologies: A survival analysis of municipal adoption of websites, twitter, and youtube. *Digital Government: Research and Practice*, 2022.
3. Alessandro Merendino, Sally Dibb, Maureen Meadows, Lee Quinn, David Wilson, Lyndon Simkin, and Ana Canhoto. Big data, big decisions: The impact of big data on board level decision-making. *Journal of Business Research*, 93:67–78, 2018.
4. JooYoung Lee, Siqi Wu, Ali Mert Ertugrul, Yu-Ru Lin, and Lexing Xie. Whose advantage? measuring attention dynamics across youtube and twitter on controversial topics. In *Proceedings of the International AAAI Conference on Web and Social Media*, volume 16, pages 573–583, 2022.
5. Tugrul U Daim. *Digital Transformation: Evaluating Emerging Technologies*, volume 6. World Scientific, 2020.
6. Zhihong Shen, Hao Ma, and Kuansan Wang. A web-scale system for scientific knowledge exploration.
7. Yujia Yang, Shi Lu, Huan Zhao, and Xiaoqian Ju. Predicting monthly pageview of wikipedia pages by neighbor pages. In *Proceedings of the 2020 3rd International Conference on Big Data Technologies*, pages 112–115, 2020.

Chapter 40
Trends in Open Source Software for Data Protection and Encryption Technologies

Lucía Gómez Teijeiro and Thomas Maillart

40.1 Introduction

Software editors and practitioners have increasingly developed and used open-source software tools to implement their cybersecurity strategies. By its unique intellectual property regime, open-source software fosters transparency and sharing values, which have been recognized as important to finding and fixing vulnerabilities and quickly avoiding threats. By selecting 41 technologies related to the one presented in the book, we show that open-source software for cybersecurity is a rapidly growing complex ecosystem of 3456 GitHub repositories with 5000+ users. While some repositories are prominent, many have evolved under the radar, serving niche or emergent needs. Here, we provide the first account of trends in open-source software for cybersecurity and develop a non-parametric forecasting approach to provide an outlook of its development towards 2025.

40.2 Open Source Software and Cybersecurity

Following Eric Raymond's adage, "Given enough eyeballs, all bugs are shallow" [1], key promises of open source software (OSS) have been transparency, task self-selection, and peer-review [2]. In times of increasing economic, social, and political challenges in cyberspace, securing full access to software code has become a critical aspect of digital sovereignty [3]. Organizations face numerous dangers using software they do not control, such as forced technology obsolescence, product

L. G. Teijeiro (✉) · T. Maillart
University of Geneva, Geneva, Switzerland
e-mail: lucia.gomez@unige.ch; thomas.maillart@unige.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_40

discontinuity, and cybersecurity risks. For organizations with short business cycles, such risks are limited compared to the opportunity to use somewhat highly efficient closed-source solutions. However, for critical infrastructures built over decades or more, the risk of not having control over software or hardware code is serious. For instance, the European Organization for Nuclear Research (CERN) has been at the forefront of open-source software and open hardware strategy developments precisely because their research infrastructures take more time to build and operate than the expected lifespan of most technology providers [4].

OSS development, as a community of collective action [5], carries numerous benefits associated with the power of collective intelligence [6, 7]. Those benefits are highly desirable in many cyber-security applications (e.g., hunting vulnerabilities through bug bounty programs) [8]. Moreover, given its short reaction overhead, collective action appears to be a rational response to increasingly time-critical cybersecurity challenges [9].

With an increasing need for transparency and the pressure to ensure continuously reliable systems, OSS for cybersecurity is expected to keep developing as a complement and an alternative to closed source.

40.3 GitHub: A Social Coding Paradigm in Software and Hardware Development

GitHub was established in 2008 [10] as a *social coding* platform based on *git* technology, a distributed software version control system initiated by Linus Torvalds to efficiently track changes in software source code in the decentralized setting compatible with Linux Kernel development [11]. Nowadays, GitHub has become the primary online platform for collaborative OSS development. Here, we studied GitHub repositories associated with data protection and encryption.[1] We found that the number of created repositories increases exponentially (c.f., Fig. 40.1).

The exponential growth of the repository creation rate is expected for data protection and encryption, given that it is a relatively new GitHub platform. In addition, as more OSS code accumulates, the marginal cost of repository creation decreases. Indeed, previous software artifacts can be reused as a complex adaptive network of package dependencies [12], git forks, or simply through code copy-paste.

[1] We investigated 9003 GitHub repositories created since 2008 relating to the 41 data protection and encryption technologies. We collected descriptive data for each repository (description, keywords, README.md) and creation date.

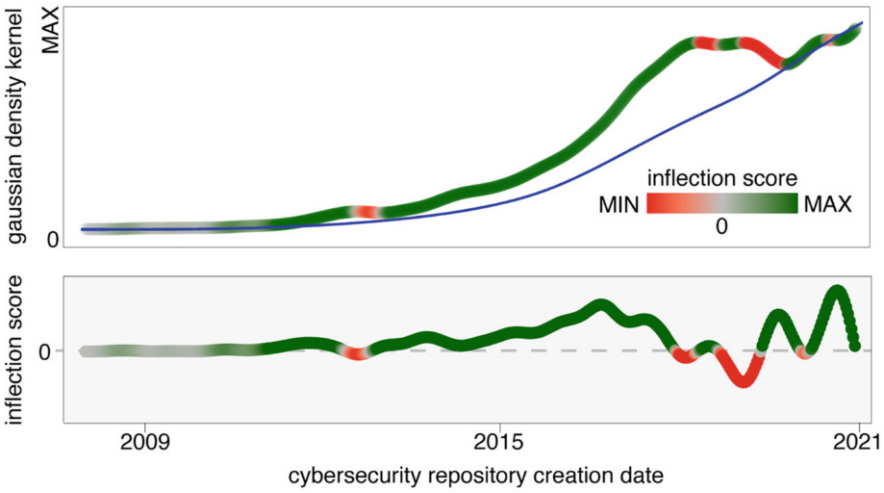

Fig. 40.1 (upper panel) Evolution of repository creations with a color-coded continuous measure of inflection. Repository creation is best fitted by an exponential model (blue curve) with rate $k = 1/\tau = 0.88$ ($p < 0.001$ and $R^2 = 0.88$). (lower panel) inflection score captures the velocity (i.e., the derivative) of repository creations

40.4 Clustering the Complexity of OSS Cybersecurity Ecosystems

When considering OSS ecosystems in data protection and encryption, a significant challenge is to make sense of a complex landscape of repositories covering overlapping topics. Indeed, frameworks used or developed in GitHub repositories are likely to cover several technologies, some more pervasive than others. Figure 40.2 shows how technologies, as queried on GitHub search engine, intersect with clusters of repositories build using non-supervised machine learning on (1) repository descriptions, (2) keywords, and (3) README files.[2] Some technology categories robustly match specific clusters (e.g., digital signatures, symmetric cryptography, blockchain, Web3), while others spread across several clusters (e.g., 0,1,2) thus being less specific.

[2] Text was processed for term frequency-inverse document frequency (tf-idf) word embedding and reduced into a 2D Uniform Manifold Approximation and Projection for Dimension Reduction (UMAP). Communities were detected using Louvain clustering.

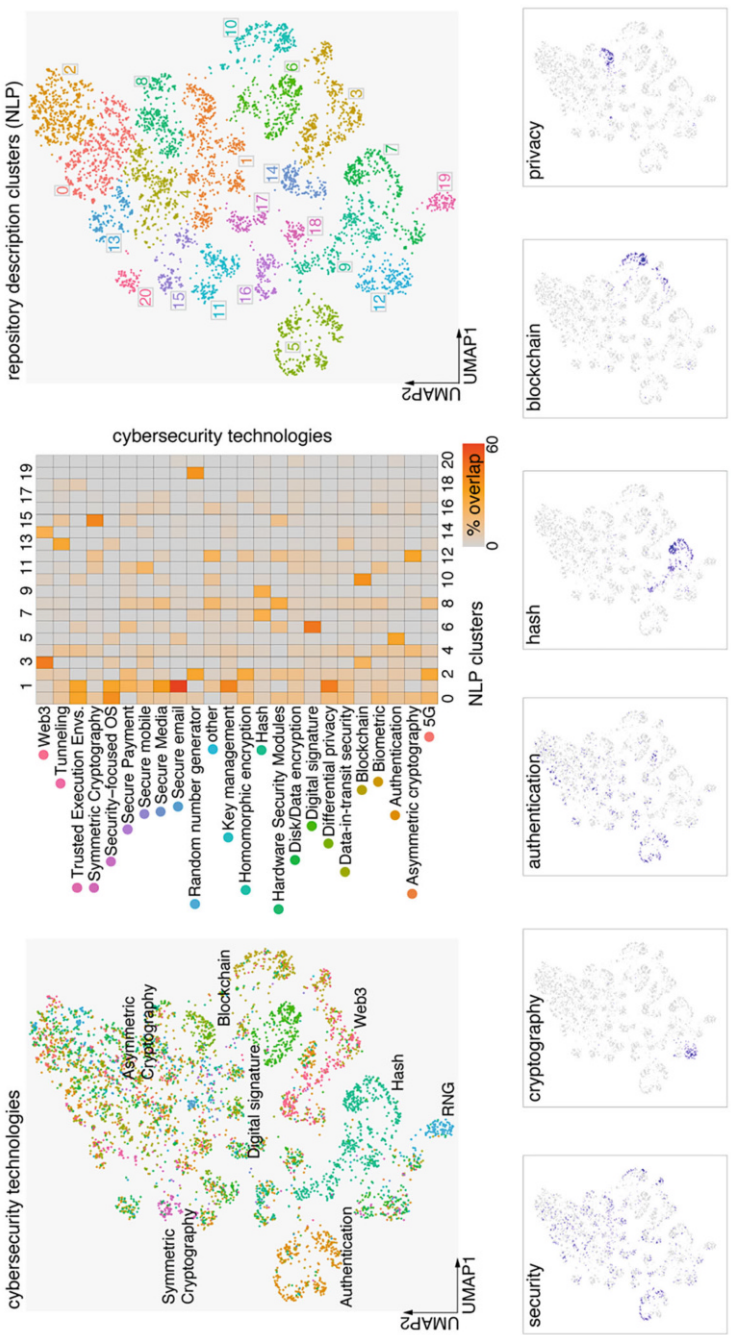

Fig. 40.2 Natural language processing (NLP) embedding and clustering on repository description feature across the data protection and encryption technologies covered in this book. As queried on the GitHub topic search, those categories differ significantly from description clusters generated using NLP. Some categories robustly match specific clusters (e.g., RNG and blockchain), while others spread across several clusters (e.g., 0,1,2), thus being less specific

40.5 Outlook Towards 2025

Monitoring OSS repositories for data protection and encryption technologies is like investigating a hidden giant finally emerging to the light of day: the number of repositories being created has been growing exponentially until now. Some became successful commercial products (e.g., Threema in Switzerland), others became central components of Web security architectures (e.g., OpenSSL), while many are still addressing niche needs. Notably, some of these niches will eventually turn mainstream. Therefore, detecting and monitoring current and future repositories that count, respectively will count, for cybersecurity is critical to identify and harness development opportunities for data protection and encryption technologies, digital sovereignty, and sound business.

Combining long-term exponential growth rates, inflection dynamics, and growth density for each data protection and encryption category, we forecasted their development until 2025. Figure 40.3 shows that forecast until 2025, combined with their historic growth dynamics.[3]

40.5.1 Consequences for Switzerland

Improving OSS monitoring for data protection and encryption is critical for Switzerland. As a small country with limited ability to see domestic tech giants emerge and yet a reputation of safety and reliability, Switzerland's researchers and entrepreneurs have an edge in leveraging OSS ecosystems. One example is Threema, which has built an authoritative secure messaging OSS app. In addition, having full access to software code is crucial for the accountability of solutions provided by the industry and hence, for the cybersecurity of critical infrastructures. Finally, understanding and forecasting future trends in OSS cybersecurity ecosystems is key to assessing and anticipating the evolution of critical data protection and encryption technologies.

[3] Specifically, we fitted and cross-penalized three TES models over creation date dynamics: density kernel, exponential cumulative distribution, and inflection score.

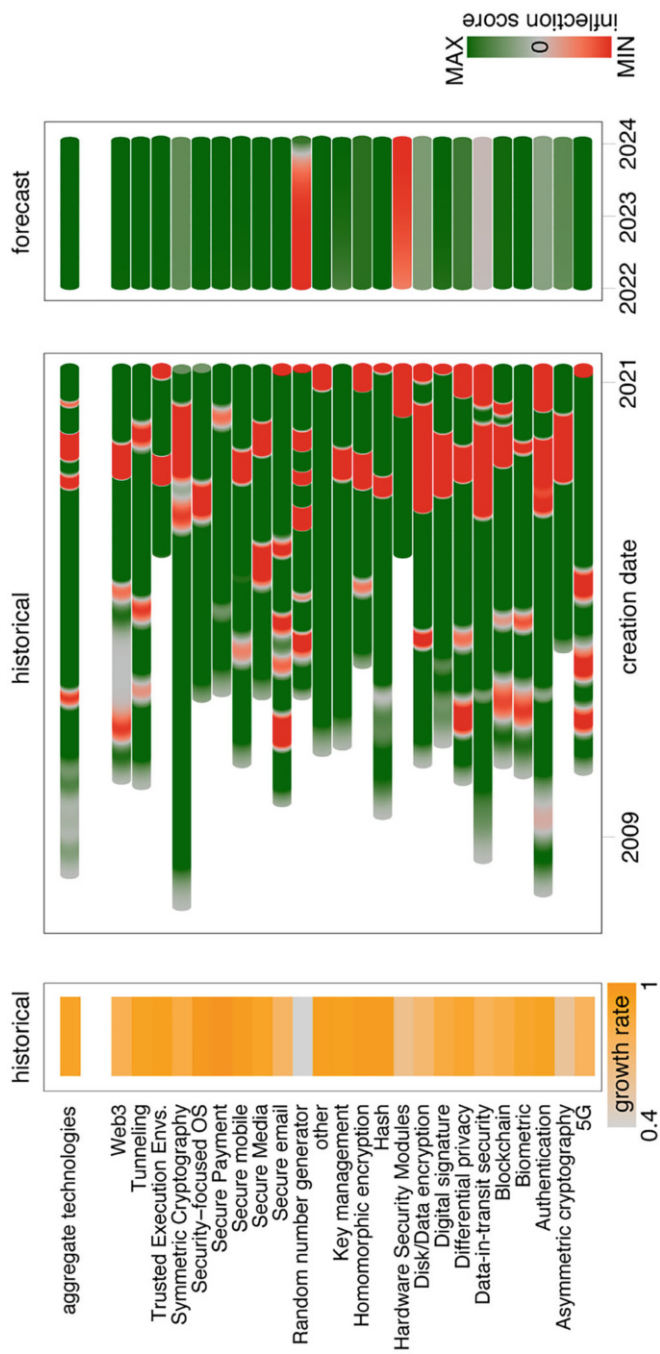

Fig. 40.3 (left panel) Exponential growth rate of repository creation per technology. (middle panel) Evolution of inflection velocity on repository creations over the history of categories. (right panel) Inflection velocity forecast until the end of 2024

References

1. Eric Raymond. The cathedral and the bazaar. *Knowledge, Technology & Policy*, 12(3):23–49, September 1999.
2. Yochai Benkler. Coase's Penguin, or, Linux and "The Nature of the Firm". *The Yale Law Journal*, 112(3):369+, December 2002.
3. Julia Pohle and Thorsten Thiel. Digital sovereignty. *Internet Policy Review*, 9(4), December 2020.
4. Pietari Matti Veikko Kauttu. Open hardware as an experimental commercialization strategy: challenges and potentialities | CERN IdeaSquare Journal of Experimental Innovation. July 2019.
5. Elinor Ostrom. *Governing the Commons: The Evolution of Institutions for Collective Action (Political Economy of Institutions and Decisions)*. Cambridge University Press, November 1990. Published: Paperback.
6. Didier Sornette, Thomas Maillart, and Giacomo Ghezzi. How Much Is the Whole Really More than the Sum of Its Parts? 1 1 = 2.5: Superlinear Productivity in Collective Group Actions. *PLoS ONE*, 9(8):e103023, August 2014.
7. Thomas Maillart and Didier Sornette. Aristotle vs. Ringelmann: On superlinear production in open source software. *Physica A: Statistical Mechanics and its Applications*, 523:964–972, June 2019.
8. Thomas Maillart, Mingyi Zhao, Jens Grossklags, and John Chuang. Given enough eyeballs, all bugs are shallow? Revisiting Eric Raymond with bug bounty programs. *Journal of Cybersecurity*, 3(2):81–90, June 2017.
9. Sébastien Gillard, Dimitri Percia David, Alain Mermoud, and Thomas Maillart. Efficient Collective Action for Tackling Time-Critical Cybersecurity Threats, October 2022. arXiv:2206.15055 [physics].
10. GitHub, October 2022. Page Version ID: 1115484009.
11. Git, October 2022. Page Version ID: 1116314204.
12. T. Maillart, D. Sornette, S. Spaeth, and G. von Krogh. Empirical Tests of Zipf's Law Mechanism in Open Source Linux Distribution. *Physical Review Letters*, 101(21):218701+, 2008.

Chapter 41
Conclusion

Valentin Mulder

41.1 Summary

The qualitative analysis performed in Chap. 39 has found that the technologies in the field are either ready for use or will be ready soon, with no signs of being outdated. The specialist also highlights the tremendous academic research opportunities in Switzerland and the attractive economic prospects in this sector. On the other hand, a quantitative analysis, which analyzed research through various metrics such as publications, public attention, Wikipedia page views, open source software, and GitHub repositories, supports the findings of the qualitative analysis, with only some minor differences observed.

41.2 Limitation

The limitations of this study include the static nature of the information presented, as the data and research used are limited to the time of conducting this research. Therefore the results may not accurately reflect any changes or developments in the field since it was completed. The challenges faced when defining and accurately categorizing the data protection and encryption technologies discussed were numerous. Finally, the field is constantly evolving, and new technologies may emerge that require to be adequately addressed in the study.

These limits should be considered when interpreting the results and conclusions investigated in this study. It is important to note that the projections and predictions

V. Mulder (✉)
Cyber-Defence Campus, Thun, Switzerland
e-mail: valentin.mulder@ar.admin.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_41

are based on the most relevant and available information. However, they may not necessarily reflect the actual outcomes. The analysis and conclusions presented are subject to change as the domain continues to evolve and new technologies are explored and developed. In summary, this book delivered a snapshot of the current state of data protection and encryption technologies in 2022, but it needs to be more exhaustive and definitive.

41.3 Outlook

Conducting research and gathering more data will enhance the accuracy and relevance of the findings.

It is also important to reevaluate the findings in 2025. The world of data protection and encryption technologies is constantly evolving, and new technologies and developments may need to be adequately addressed. In addition, this reevaluation will provide an opportunity to assess the accuracy of the predictions and projections. This better understanding of these technologies will make updating or correcting the final results necessary.

This study provides an expansive overview of data protection and encryption technologies. There is still a lot to be discovered and understood. Therefore, the following steps are future reevaluations of the results to provide a more complete and accurate panorama of the trends and developments in data protection and encryption technologies.