Chapter 1
Introduction

This book is aimed at anyone interested in high data security in telecommunications and data storage, especially procurers, experts, and decision-makers. Anyone involved in procurement in this field makes decisions about algorithms, technologies, and providers, and thus also about infrastructure and security. The generation and distribution of keys for data encryption play a central role in this. Because security assessments for mathematical methods are based on assumptions, physical methods are becoming interesting in the high-security sector. They promise to link security more closely to the laws of nature. This raises the key question: Which technology is suitable for which application scenario, and what assumptions, costs, and operational risks are involved?

This book provides answers and, for the first time, compares QKD (quantum key distribution), RKD (radio signal key distribution), and MKD (memory key distribution) in a common, comprehensible criteria grid: technology-neutral and practical. Secret key rates, ranges/attenuation, robustness, costs/infrastructure, standardization, and risks (implementation, integration, post-processing, side channels) are deliberately evaluated not as a ranking, but as a decision-making aid.

QKD derives its security from the laws of quantum physics, but secret key rates decrease with increasing attenuation. Key management systems connect short QKD distances over longer distances, but only at the cost of additional attack surfaces ("trusted nodes"). Its use for mobile applications fails due to a lack of technical maturity. Very high financial costs and high maintenance requirements for QKD solutions make them not very suitable.

RKD utilizes the reciprocal physical properties of a radio link and scores points for its low technical complexity, excellent suitability for mobile applications (e.g., vehicles or drones), and very low costs. However, RKD falls far short of the key rates achieved by QKD solutions and is still limited to shorter distances. In addition, there is no established infrastructure for distributing key material to more than two partners.

E. Piller and H. Schölnast, *Data Encryption at the Intersection of Mathematics and Physics*, SpringerBriefs in Information Security and Cryptography,
https://doi.org/10.1007/978-3-032-24764-3_1

MKD takes a completely different approach: each party produces key material, stores it on a data carrier, and transports it physically to the other party. Because MKD can securely transfer 16 TB of key material in a single transport, only MKD has the potential to continuously provide a one-time pad (OTP) and thus provably 100% secure data encryption. The price is organizational responsibility: secure generation, storage, transport, and documented chain of custody.

The book examines data security in telecommunications and data storage, discusses three new encryption methods specifically designed for QKD and RKD, and addresses the question of when "OTP-like" security is more practical than theoretical purity. The result of approximately one year of source-critical research and the comparison of literature, manufacturer specifications, and practical observations with systematic cross-checking and our own R&D activities, this book helps to justify architecture and procurement decisions, locate risks (side channels, misconfigurations, logistical vulnerabilities), and separate "security gains" from "new attack surfaces."

1.1 General

Data plays a very important role today, and so does data security. Digitalization, globalization, and global networking require secure telecommunications and data storage, which in turn require secure cryptography. The development of secure data protection procedures for communication and data storage is a key challenge.

The security assessment of current cryptography is based on the assumption that there are mathematical problems that are very difficult for an attacker to solve. In other words, it depends on the computing power of the attackers and their current knowledge of mathematical attack methods. Protection against mathematical attack methods that are still unknown today involves unpublished mathematical methods that can break today's symmetric and asymmetric cryptography and/or post-quantum cryptography. As the past has shown, there have often been unpublished methods with a major impact on cryptography. For example, Mr. Williamson and Mr. Cox developed the Diffie-Hellman and RSA methods in a similar form years earlier and did not publish them, which only became known in 1997 [WP–DH,[1] WP–MJW,[2] Cocks73[3]]. In addition, mathematical methods that were considered sufficiently secure for a long time have repeatedly been found to be insecure at a later date, such as "Supersingular Isogenic Curve Cryptography" (SIKE) in the NIST competition [NIST25].[4]

Anyone who rejects mathematical methods for this reason, especially when it comes to sensitive research data, medical data, confidential data from governments

[1] https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange.

[2] https://en.wikipedia.org/wiki/Malcolm_J_Williamson.

[3] https://web.archive.org/web/20080227001905/http://www.cesg.gov.uk/site/publications/media/notense.pdf.

[4] https://csrc.nist.gov/pqc-standardization.

and companies, etc., must use physical methods of cryptography. Physical methods introduce a new paradigm of cryptography that differs from today's complexity-based cryptography. The methods are secure against computationally powerful adversaries, such as powerful quantum computers or optical computers (which, according to many predictions, will be many times faster), and against mathematical attack methods that are still unknown to experts today, i.e., secure against as-yet-unpublished mathematical methods that can break today's mathematical methods, including post-quantum cryptography. And this applies not only to data encryption (security goal: confidentiality) and key management, but also to the security goals of integrity and authenticity. In symmetric and asymmetric cryptography today, there are, on the one hand, many mathematical methods that use short keys—usually under 5,000 bits—and their security assessment is based on assumptions. On the other hand, for data encryption, there is one-time pad (OTP) with a very long key, which can reach into the GByte and TByte range, and its security can be proven to be 100% secure. Asymmetric cryptography for key management can be replaced by physical methods such as QKD (Quantum Key Distribution), RKD (Radio-signal Key Distribution), or MKD (Memory Key Distribution) to ensure the highest possible level of security. The physical methods, particularly QKD and RKD, currently provide key sizes that are much too large for mathematical data encryption methods, but are usually too small for the one-time pad. And it is precisely this gap that is covered by two new encryption methods (called OTPH and OTPS) and two new encryption modes of operation (called XTSO and OTPM) described in Chap. 6 of the book and at https://cryptography.study/phys/modes. The key sets achievable with QKD and RKD are perfectly suited to the new encryption methods/modes, and while the security assessment cannot be proven to be 100% secure, it is based on the security of HKDF / hash functions and the XOR operation, which are used in QKD and RKD themselves.

The topic of physical cryptography methods has only become really popular due to the demand for security against quantum computers, but it is a topic that has been just as relevant for decades and still is today because it also affects today's data encryption (storage today, attack in the future). On the other hand, those who are satisfied with today's asymmetric cryptography will also be satisfied with post-quantum cryptography [WP–PQC][5] in the future and will not need physical methods. This also applies to symmetric methods such as AES (Advanced Encryption Standard) [WP–AES].[6]

1.1.1 The Compared Methods/Technologies

This book provides a systematic comparison of physical methods/technologies for generating and distributing cryptographic keys. It examines methods/technologies that are not primarily based on mathematical hardness assumptions, but derive

[5] https://en.wikipedia.org/wiki/Post-quantum_cryptography.

[6] https://en.wikipedia.org/wiki/Advanced_Encryption_Standard.

their security-relevant properties from physical laws. These include three classes of quantum key distribution (QKD) in their practical forms, as well as the generation and distribution of cryptographic keys using radio signals (RKD) and storage media (MKD). The QKD, RKD, and MKD methods/technologies presented each consist of a variety of different individual technologies and methods, which are collectively referred to in this book as methods/technology.

Specifically, the following five methods/technologies of physical cryptography are presented and compared according to practical performance criteria:

1. **DV-QKD (Discrete Variable Quantum Key Distribution)**

   This method exploits the quantum physical properties (specifically: the polarization directions) of indivisible units (specifically, individual photons, i.e., light particles) to generate identical random bit sequences at a transmitter and a receiver. However, the randomness of the key material does not arise "by itself," but must be introduced externally on the sender's side. This random quantum information is transmitted to the receiver via fiber optic cable, free-space channel, or satellite and measured there. Due to the quantum nature of the transmission, any eavesdropping attempt will be detected.
2. **CV-QKD (Continuous Variable Quantum Key Distribution)**

   This works largely like DV-QKD, with the following difference: the carriers of the quantum information are not indivisible units (i.e., not individual photons), but weak light pulses consisting of several photons. As with DV-QKD, randomness is introduced externally at the transmitter and imposed on the individual light pulses as modulation of amplitude (corresponding to the number of photons in the pulse) and phase. This modulation is performed in the same way as in conventional telecommunications. Due to the low intensity of the pulses and a quantum physical relationship between amplitude and phase, eavesdropping attacks can also be reliably detected with this method/technology.
3. **QKD (quantum key distribution) with entanglement**

   In methods of this class, the sender of the quantum information is not one of the two key exchange partners, but a third party that does not need to be trusted. This source generates entangled photon pairs and sends one photon from each pair to the two key exchange partners, who measure these photons. The two partners therefore have equal roles. Another very important difference from the previously mentioned QKD variants is the randomness that arises "by itself" here, i.e., directly from the quantum nature of entanglement. The randomness does not have to be generated by a separate generator. Because an eavesdropping attacker inevitably destroys the entanglement of the two photons, such attacks are reliably detected here as well.
4. **RKD (Radio Signal Key Distribution)**

   RKD uses radio signals above 30 MHz to calculate and distribute cryptographic keys and is known in the literature under various names, e.g., "Physical layer key generation in wireless networks" or "Wireless Physical Layer Key Agreement."

RKD is a physical process based on the reciprocity of radio transmission and measurement of radio channel properties. Both sides of the communication are equal and use the same devices to generate and distribute the cryptographic keys. Randomness arises "by itself" through the process, and protection against eavesdropping is based on the fact that the radio properties of these two locations cannot be reconstructed at locations other than directly at the transmitter or receiver.

5. **MKD (Memory Key Distribution)**

   With MKD, physical distribution is carried out using a storage medium such as high-security smart cards or SSDs (solid-state storage, currently up to 16 TB), which contain at least one integrated AES-256 HW encryption unit and a high-security smart card for key transport for the AES HW encryption integrated in the SSD. Both sides of the communication (Alice and Bob) are equal and use the same devices to generate and distribute the cryptographic keys. Randomness must be introduced from outside. To carry out an eavesdropping attack, an attacker would have to gain physical access to the storage medium and be in possession of the smart card containing the key.

In addition, the QKD variants and RKD also examine the different transmission paths: fiber optic networks (only for QKD), free-space channels, and satellite connections. With MKD, transport is carried out in person or with the help of a personal courier or public parcel service. The terms RKD and MKD were coined by the first author of this book and were chosen in analogy to QKD.

What all the methods considered have in common is that they deal exclusively with the generation and distribution of symmetric keys and are physical methods. The actual data encryption and mechanisms for ensuring integrity and authenticity are considered separately from this conceptually, as they each require additional assumptions, procedures, and system components. The book explicitly does not pursue a product- or manufacturer-specific approach, but analyzes the methods/technologies in terms of their physical principles, systemic properties, and practical feasibility.

1.1.2 Comparison Criteria

The five physical cryptography procedures mentioned above are presented in this book in a generally understandable and technology-neutral manner and compared in a comprehensible way using the following practice-relevant performance criteria:

- IT security
- Market readiness
- Key rate (dependent on distance in the case of QKD)
- Distance (distance between communication partners)
- Cost
- Robustness/susceptibility to interference

- Suitability for mobile devices
- Infrastructural dependencies

The book also contains a technology-neutral analysis of the advantages and disadvantages and, in conjunction with the webpage https://cryptography.study/phys, a current market analysis of the European products/solutions already on offer. Furthermore, the applications *of telecommunications and data storage with physical processes* and the *XOR function* are discussed. In the case of the XOR function, the relationship to physics and the implementation of the security objectives of confidentiality with the one-time pad and integrity and authenticity with the MAC are described.

1.1.3 Fundamentals of Comparability

The comparisons made in this book are based on a systematic compilation of various sources of information and levels of analysis. They are based firstly on the documented state of the art from scientific literature and publicly available research reports, secondly on information provided by manufacturers about their products and systems, and thirdly on experience reports from users who have employed the relevant processes/technologies in real or practical environments.

The significance of the sources used must be evaluated differently.

- Scientific publications generally provide easily verifiable results, but these are often obtained under idealized conditions.
- Manufacturer information is particularly relevant for key technical data, but is naturally subject to marketing-driven distortions and does not always refer to long-term practical operation.
- User reports offer valuable insights into real-world operating conditions, but are often limited to specific configurations and individual cases.

The comparability of the processes/technologies examined is also limited by structural differences. The processes differ fundamentally in terms of physical principles, system architectures, maturity, and context of use. Uniform key figures that would allow direct quantitative comparability exist only to a limited extent. Statements on key rates, ranges, costs, or robustness must therefore always be interpreted in the respective context.

Against this background, the present comparison is not intended as an exact comparison of individual measured values, but rather as a qualitatively sound classification of technological characteristics and framework conditions. The aim is to provide a basis for decision-making and to make the strengths, weaknesses, and dependencies of the processes transparent. In doing so, no attempt is made to feign a level of accuracy that is unattainable given the heterogeneous sources and dynamic technological developments.

1.1.4 Comparison Methods and References

Three methods were used to compare the performance of the various processes/technologies:

1. Process/technology perspective: what is possible with the current state of the art, etc.?
2. Perspective of suppliers of real products on the market
3. Perspective of third parties who act as users of real products on the market

The performance criteria listed above can be compared using these three methods with varying degrees of accuracy and objectivity, i.e., without bias or prejudice. For example, distance and key rate can be compared using all three methods, but the best results come from method 3 (users). Method 3 is also the most suitable for costs, robustness, and market readiness. In contrast, method 1 is best suited for IT security and suitability for mobile end devices.

For method 1, we examined the state of the art in detail and carried out the comparison on that basis. For method 2, we surveyed suppliers of real products and conducted research on the Internet. The results of method 2 had to be treated with caution in some cases, as they often involved marketing statements or tests in laboratory environments. However, the results from methods 2 and 3 were always presented together in the book so that both sides of the argument were visible. For method 3, we surveyed users of real products. However, this was very difficult for some processes/technologies because either there are only a few users or the users have not carried out sufficiently scientifically sound analyses according to these performance criteria and, if they have, they do not release the results.

For QKD, we obtained the results for method 3 from the AIT (Austrian Institute of Technology) as stated in the book. The AIT procured seven different products from the market and tested them extensively and objectively as users in various practical environments. Due to the large number of different products and thus processes/technologies, the AIT was able to compare the various products relatively well according to some performance criteria in this book in a technology-neutral and objective manner in practical environments.

For RKD and MKD, we obtained the results specified in the book for method 3 from the Institute for IT Security Research at the USTP (University of Applied Sciences St. Pölten, Austria).

1.2 Physics and Security

Although physical cryptography methods are based on the laws of physics, as will be explained in detail in the main part of the book, other factors also contribute to security, particularly in QKD (quantum key distribution) and RKD (radio key distribution). The security of a method or technology is always determined by its

weakest link, and that is not the physical fundamentals. In QKD and RKD, the concrete implementations, primarily due to hardware design decisions, lead to many real possibilities for side-channel attacks (see Sect. 3.8). The necessary mathematical procedures, which are required for post-processing (error correction and privacy amplification, see Sect. 8), also offer potential points of attack.

In cryptography, what ultimately counts is the security of the procedure and not its complexity or the scientific discipline on which it is based. A good example of this is the simplest method of data encryption, namely the one-time pad [WP–OTP][7,8] (bitwise encryption using the XOR function, see Sect. 6.2), which is the only method that is mathematically provably 100% secure.

Data encryption must always be end-to-end. Since a great deal of sensitive data is generated on an end device (desktop PC, laptop, tablet, smartphone, IoT device, sensor, medical device, etc.), it must also be encrypted sufficiently securely there. For security reasons, the actual encryption often takes place in an HSM (hardware security module) or a cryptobox. Such devices are available on the market at low cost. However, the data may also be encrypted directly on the end device if this is done with a one-time pad and storage media suitable for key transport (see Sect. 5.2) are used. As mobility becomes increasingly important, high-security encryption on laptops, tablets, smartphones, and IoT devices is also becoming more important (e.g., laptops with multisession operation with several parallel virtual workstations with different security levels at the operating system level, from open to closed).

1.3 Economic Aspects of Security

However, the economically reasonable costs necessary to guarantee the required level of encryption security are not based on the price of the end device or the value of an HSM or cryptobox, but primarily on the value of the data. This means that even with a cheap end device, such as a laptop, the total encryption solution per end device may be significantly more expensive than the end device itself if the value of the data, e.g., in the case of very valuable research data or strictly confidential government data, is correspondingly high. However, the total costs must always be taken into account, i.e., the connection costs (fiber optics, satellite, transport of storage media, etc.) and the operating costs, including maintenance costs. These costs can increase quadratically due to the necessary end-to-end connections between all end devices (if no connection can be used twice, the number of connections required for n participants is $\frac{n^2-n}{2}$ connections, i.e., for example, $n = 100$ already requires 4.950 connections).

[7] https://en.wikipedia.org/wiki/One-time_pad.

[8] See Sect. 6.2.

1.4 Objective of the Book

The aim of the comparison is to provide a comprehensible and technology-neutral basis for evaluating these methods. The book is aimed at anyone interested in cryptography, especially procurers, experts, and decision-makers who are faced with the question of whether and to what extent physical cryptography methods should be considered as a supplement or alternative to established mathematical methods. The aim is not to provide an abstract security theory assessment, but rather a classification based on the above criteria.

The comparison does not aim to create a ranking of the methods/technologies examined or to present a single solution as generally superior. Rather, the structural differences, strengths, and weaknesses of the approaches are to be made transparent in order to enable informed decisions in the respective application context. Different application scenarios, such as telecommunications, data storage, highly secure point-to-point connections, and use in mobile devices, place different demands on key rates, range, robustness, infrastructure, and organizational integration, which the methods under consideration meet to varying degrees.

This book does not cover detailed security assessments of individual implementations, the mathematical methods used in the procedures/technologies or products, source code analyses, or certification issues relating to specific products. Similarly, mathematical cryptography, including post-quantum cryptography, is not fundamentally evaluated or placed in competition with physical methods. Rather, it is considered an established frame of reference to which physical methods can be related depending on security assumptions, risk profiles, and use cases. The book is thus intended as a basis for decision-making and orientation, not as a normative guideline for the use of specific methods/technologies.

1.5 Unique Selling Point of this Book

There are many books on cryptography, and some of them also deal with physical methods. In the field of physical cryptography, there are several books on QKD (quantum key distribution). However, RKD (radio signal key distribution) and MKD (memory key distribution) have not yet been covered in books, and there is no performance comparison of these methods/technologies and procedures.

This book is the first internationally to compare these completely different physical cryptography methods in a technology-neutral way and make them generally understandable.

1.6 Reference to the Book's Website

The performance comparisons also included many products from different manufacturers to ensure that the results are comprehensible and manufacturer-neutral. However, because this data is constantly changing—the market is evolving—and because individual results are not very meaningful, the individual results of the products and manufacturers were not included in the book. However, they are available from the St. Pölten University of Applied Sciences via the website https://cryptography.study/phys (the references can be found in the relevant sections of the book) and are considered to be external appendices to the book. This webpage also contains other interesting aspects of the book, including important necessary hardware components (photon sources, detectors, etc.), descriptions of QKD protocols, an overview of random number generators, and a practical RKD implementation, etc. These external appendices therefore represent important additions to the book. Furthermore, four encryption methods/modes developed specifically for QKD and RKD are presented, and a complete eCoC implementation for MKD is discussed.

All supplements and appendices related to this book as well as book proofreading and editing can be found at the following address: https://cryptography.study/phys.

1.7 Origin of the Book, Acknowledgments

The book was written at the St. Pölten University of Applied Sciences, Austria, at the Institute for IT Security Research. It is based on the study "Crypto comparison" and four other projects (KIF, LoRaBridge, RKD, LISA), all of which were funded by the Austrian Research Promotion Agency FFG. The study has been funded by the Austrian security research program KIRAS/K-Pass of the Austrian Ministry of Finance (BMF).

The authors of the book would like to express their gratitude to Simon Tjoa and Henri Ruotsalainen (St. Pölten University of Applied Sciences), Gerald Trost (Federal Chancellery of Austria), Ralf Hammer and Lukas Siebeneicher (Austrian Federal Ministry of Finance), Florian Kutschera (AIT), and the FFG for their support.

References

[WP-DH] Wikipedia contributors, Diffie–Hellman key exchange. Wikipedia, the Free Encyclopedia. https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

[WP-MJW] Wikipedia contributors, Malcolm J. Williamson. Wikipedia, the Free Encyclopedia. https://en.wikipedia.org/wiki/Malcolm_J._Williamson

[Cocks73] C.C., Cocks, A Note on 'Non-Secret Encryption. CESG Memo. 20 Nov 1973. https://web.archive.org/web/20080227001905/http://www.cesg.gov.uk/site/publications/media/notense.pdf

[NIST25] National Institute of Standards and Technology (NIST); Computer Security Resource Center (CSRC). PQC Standardization Process (Post-Quantum Cryptography). Created 03 Jan 2017; updated 11 Dec 2025. https://csrc.nist.gov/pqc-standardization

[WP-PQC] Wikipedia contributors, Post-quantum cryptography. Wikipedia, the Free Encyclopedia. https://en.wikipedia.org/wiki/Post-quantum_cryptography

[WP-AES] Wikipedia contributors, Advanced Encryption Standard. Wikipedia, the Free Encyclopedia. https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[WP-OTP] Wikipedia contributors, One-time pad. Wikipedia, the Free Encyclopedia. https://en.wikipedia.org/wiki/One-time_pad