Chapter 9
Concluding Remarks and Summary

9.1 Achievability of Security Objectives

9.1.1 Confidentiality

As already explained at the beginning (in sect.2.6.1), mathematically provable confidentiality can only be achieved with the one-time pad method. All other encryption methods only achieve a certain degree of practically achievable confidentiality for which there is no rigorous proof, meaning that the possibility of a breach of confidentiality cannot be completely ruled out. The physical methods for generating and distributing cryptographic keys described in this book do not change this.

So, if you are not satisfied with practically achievable confidentiality for which there is no solid proof, you have to use the one-time pad, which in practice means that you need at least as much key material as you want to send or store in encrypted data.

QKD

The key rates currently achievable with QKD are sufficient for key material that can be used for AES encryption with frequently changing keys. (AES-256 is often used for this purpose.) The rate at which these AES keys can be changed depends on the key rate. If an average of 1000 bits/sec is generated, this is sufficient for approximately 4 key changes per second, which already achieves an extremely high level of practical confidentiality. But as mentioned, provable confidentiality can only be achieved with one-time pad encryption.

In QKD with entangled photons, the key rate for a one-time pad is also usually too low, especially in connection with satellites, where only a few bits per second can currently be achieved. For transmissions using optical fibers, the key rates for QKD are currently limited to a maximum of a few kilobits per second over longer distances (see Chap.3). For 1 TB of data, a key rate of 10 kbit/sec requires around

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_9

25 years of continuous key exchange. However, significant improvements in this area are expected for QKD over the next ten years. But as the past has shown, data volumes are also constantly increasing, which means that this race may only ever lead to limited success for QKD.

RKD

With RKD, a one-time pad cannot be used for data encryption because the key rate is very low. (Feasible values are a few bits per second, and this key rate can hardly be improved). However, AES encryption with frequently changing keys can still be implemented at very low cost if one is satisfied with changing the key every minute or less frequently.

MKD

Only MKD can currently exchange up to 16 TB of key material per transfer with a data carrier in a cost-effective and highly secure manner, thus guaranteeing the ideal use of the one-time pad. Today, very fast generators based on quantum mechanics require around 9 hours to generate non-deterministic random numbers for 1 TB of key material. MKD in conjunction with one-time pads therefore makes it possible to fully achieve the protection goal of mathematically provable confidentiality with today's state-of-the-art technology, at comparatively low cost, for large amounts of data, and without having to accept any losses due to the distance between the communication partners. And even if the amount of data to be encrypted should exceed the capacity of today's data carriers in the future, it can be assumed that the capacities of data carriers will grow at approximately the same rate.

9.1.2 Integrity and Authenticity

During Key Generation with QKD and RKD

In the case of QKD and RKD, integrity and authenticity during key generation must be ensured on the public channel by one of the methods already mentioned in sect.2.6.2., for example, by the Wegman-Carter method [1].[1] These methods derive their security from the mathematically strictly limited collision resistance of the hash function used, which in turn can be increased arbitrarily by enlarging the MAC tag [2].[2] However, MAC tags longer than a few hundred bits do not increase the actual overall security that can be achieved, because above a certain length of MAC tags, the probability of a hash collision is already so extremely low that other risks dominate (e.g., undetected implementation errors in the hardware or software of the communication devices). But the good news here is that although an attacker can use brute force methods to try to cause a hash collision in order to attach a MAC tag

[1] https://doi.org/10.1016/0022-0000(81)90033-7.

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

generated by the legitimate sender to a manipulated message without being noticed, it can be mathematically proven that it is impossible to develop an algorithm for this that is significantly more efficient than blind trial and error. (This assumes that the hash function used meets certain criteria, which are met in all common implementations.)

For the key exchange methods examined, this means that a certain portion of the key material must be branched off to ensure integrity. This portion represents a small percentage of the key set used for encryption and is therefore proportional to it. This in turn means that, from an integrity standpoint, nothing can be said about QKD, RKD, and MKD that does not already apply due to confidentiality.

During Key Transport with MKD

In the case of MKD, key generation and key transport are separate steps. Since key generation takes place before transport with the help of non-deterministic random number generators and excludes other partners, no special measures are necessary to secure this step. The same applies to the merging of the self-generated material with the partner's key material in the XOR link after transport.

With MKD, the transport itself is carried out physically and separately in two stages, with the storage medium containing the encrypted key being transported separately from the smart card. The smart card contains the key used to encrypt the key on the storage medium. Integrity can be achieved through cryptographic methods, but is also physically ensured by access protection to the storage media and smart cards. Authenticity is ensured by the smart card with a PIN and by the authentication of the start and destination addresses during transport (see Sect. 7.3 eCoC).

9.2 Comparison According to Criteria Relevant to Practice

9.2.1 Technological Maturity and Availability

The physical methods considered for generating and distributing cryptographic keys vary considerably in terms of their technological maturity. These differences stem less from the fundamental functionality of the underlying physical principles than from the degree of their technical maturity, system integration, and long-term operational experience. For this reason, experimental concepts, pilot applications, and systems with limited usability are considered separately.

Some of the quantum-based methods/technologies, in particular selected QKD approaches, have clearly moved beyond the stage of pure laboratory research. Integrated systems exist for these methods that can be operated under controlled conditions in test networks or in clearly defined application scenarios. However, these forms of application are often limited by specific infrastructural requirements, limited ranges, or increased operational requirements. Other QKD variants, on the other hand, are still in the experimental testing or conceptual development stage, where essential

properties have been demonstrated in principle, but it is not yet possible to make a reliable statement about their suitability for everyday use.

The state of research for RKD is also very advanced, but only one manufacturer is currently known to have a marketable product, which has not yet been certified for security.

For MKD, all the necessary components are available on the market in a wide range. They are security-certified (up to classified information) and available worldwide at low cost.

When assessing the degree of maturity, it is crucial to determine whether a process/technology is available as a closed, reproducible system or is primarily implemented as a combination of specialized individual components. Processes/technologies based on complex, sensitive, or only partially standardized components require considerable integration and operational effort in practice that goes beyond a mere demonstration of functionality. In contrast, physical approaches based on simple, well-understood, and independently verifiable components are easier to understand, implement, and manage organizationally, even if they are less formalized.

The state of standardization is another indicator of maturity, but it is not synonymous with broad applicability. While standardized interfaces and protocols can facilitate integration, they say little about long-term maintainability, operating costs, or dependencies on specific implementations. For a reliable assessment of technological maturity, it is therefore always necessary to consider the interplay between system availability, operational stability, integration effort, and organizational viability.

9.2.2 Key Rates, Range, and Scaling

Key rates and ranges are difficult to compare not only technologically but also conceptually in the methods/technologies under consideration: In the literature, "raw key," "sifted key," and "secret key rate (SKR)" are not always used consistently, and it is not always clear whether post-processing (error correction, privacy amplification) has already been fully taken into account. Where possible, the following information therefore explicitly uses values that are identified as secret key rates. Otherwise, they are classified as practical orders of magnitude or boundary conditions.

Technology class	Typical distance or attenuation	Practical key rate (order of magnitude)	Comments
DV-QKD	approx. 10–20 km (2–5 dB)	several kbit/s to several tens of kbit/s	advantageous conditions, short distances
	approx. 50–80 km (10–26 dB)	usually 100–1000 bit/s	typical for field tests and continuous operation

(continued)

(continued)

Technology class	Typical distance or attenuation	Practical key rate (order of magnitude)	Comments
	approx. 120–200 km (24–40 dB)	usually 10–100 bit/s	border range, only usable to a limited extent
CV-QKD	up to approx. 40 km (up to 8 dB)	usually 1–10 kbit/s	short distances, sensitive to noise
	approx. 50–100 km (10–20 dB)	usually 10–100 bit/s	practical working range
QKD with entanglement	approx. 10–50 km (2–10 dB)	usually 10–100 bits/s	highly dependent on source and detection
	over 70 km	less than 100 bits/s	experimental limit range
RKD	local radio connection, usually under 15 km	usually 1–10 bit/s	systemically limited, hardly scalable
MKD	physical transport of a data carrier	up to 16 TB per transfer; up to 240 Mbit/s (also 7 Gbit/s) during creation	not limited by transport, but by generation

For QKD over fiber optics, field tests and cross-manufacturer evaluations consistently show that the actual usable secret key rate (final key rate) drops sharply as channel attenuation increases. In the range of approximately 10–20 dB, practical values are often in the upper double-digit to lower four-digit bit/s range; at 25–30 dB, only a few hundred bit/s or less are often achieved. These orders of magnitude are found independently of the specific product and reflect the physically induced losses.

RKD is classified in this book as fundamentally very cost-effective and suitable for mobility (RKD requires movement), but at the same time as severely limited in terms of key rate and distance.

MKD follows a different metric: the "key rate" is effectively derived from the combination of

1. The amount of non-deterministic key bits that can be generated (e.g., 1 TB in approx. 9 hours with very fast random number generators) and.
2. Logistical transferability. The capacity per transfer is stated as up to 16 TB of key bytes, although there is no reason why several data carriers cannot be transported at the same time.

In the case of MKD, this shifts the performance limit from transmission losses, etc. to generation and logistics parameters. In order to classify MKD in terms of key rates, it must be taken into account that transporting a single, handy, and comparatively inexpensive 16-TB data carrier involves exchanging as much key material as QKD (at 1000 bit/s) does in more than 4000 years. Even if fast QKD solutions reaching speeds of 1 Mbit/s were to become available in a few years, they would have to be operated for four years to keep up with the physical transport of a single data carrier.

Therefore, the key rates for MKD are also sufficient for the use of a one-time pad and thus for provably 100% secure data encryption.

9.2.3 Operating Conditions and Robustness

The operating conditions of the methods/technologies under consideration differ significantly and have a direct impact on stability, availability, and organizational controllability. Optical QKD methods/technologies, regardless of whether they work with discrete variables, continuous variables, or entangled photons, are sensitive to environmental and system influences. In optical fibers, temperature changes, mechanical stress, or aging effects lead to polarization and phase drift, which must be continuously compensated for. In free-space and satellite-based connections, atmospheric effects (aerosols, fog, clouds, etc.), alignment errors, and background light also occur, which can lead to significant temporal fluctuations in the key rate or to interruptions. These influences are physically determined and can only be reduced to a limited extent by technical measures.

The ongoing operation of optical QKD systems therefore requires precise calibration, exact time and phase synchronization, and regular readjustment. These requirements tie up human and technical resources, especially over longer distances or in changing environmental conditions. Different QKD variants differ in detail, but share the need for continuously monitored and actively controlled operation. Deviations outside defined tolerances typically do not lead to gradual quality losses, but to a sharp drop in the key rate or complete termination of key exchange.

In comparison, RKD has very low requirements for precision calibration and synchronization, but is highly dependent on the characteristics of the radio channel. Interference from multipath propagation, shadowing, or foreign radio signals can further reduce the already low key rates or make them temporarily impossible. Robustness here results less from technical stability than from the ability to flexibly adapt procedures to changing conditions.

MKD is a special case in this respect. Although the generation of key bits is subject to the operating conditions of the random number generators used (which are optimized for security through the separate use of multiple generators), the actual transport is independent of sensitive transmission channels. Robustness is primarily determined by organizational and logistical factors, such as the secure handling, and transport of data carriers. In operation, this results in a very high fault tolerance, i.e., robustness against environmental and system influences, but is combined with a discrete rather than continuous provisioning model for the key material.

9.2.4 Security Assumptions and System Risks

The methods/technologies under consideration are based on different security models, each with its own assumptions and limitations. Quantum-based methods/technologies aim to trace the security of key generation and distribution back to the laws of quantum mechanics. In idealized form, they allow statements to be made about information-theoretical security against certain attacker models. However, these statements only apply under clearly defined conditions and are abstracted from practical implementation details. In contrast, RKD and MKD do not pursue quantum physical security models, but are based on classical physical properties of radio channels, hardware-based random number generators, storage media, smart cards, and processes, as well as organizational measures.

A key difference between the approaches lies in the number and type of additional assumptions. Optical QKD methods/technologies require that the devices used operate as specified, that detectors and sources are not tampered with, and that certain side channels are adequately controlled. In network-like structures, additional assumptions are often made, such as trust in intermediate stations or key management systems. In addition, all QKD variants require initial authentication, which in turn is based on pre-shared secrets or classical cryptographic methods. These additional assumptions relativize the formal security gain without necessarily negating it.

Post-processing (error correction, privacy amplification), which is based purely on mathematical methods, also plays an important role in QKD and RKD.

RKD also requires assumptions about the properties of the radio channel and about an attacker's ability to completely control or eavesdrop on it. Security here does not result from strict theoretical proofs, but from the practical difficulty of certain attacks.

MKD largely shifts the security assumptions to the organizational realm: the confidentiality of the key depends primarily on the secure generation, storage, and physical transport of the data carriers. In practice, attack surfaces do not arise from mathematical or physical weaknesses that determine non-deterministic random number generators and MKD-capable storage media, but from processes, personnel, and logistics.

Systemic risks arise in all processes/technologies from implementation, operation, and integration into existing infrastructures. Complex systems with many components and interfaces generally offer more points of attack than simple, clearly defined processes/technologies. With QKD in particular, side-channel attacks (see Chap. 3.8), misconfigurations, and post-processing (error correction and privacy amplification; see Chap.8) can result in practical security falling significantly short of theoretical expectations. Conversely, with MKD, the risks shift to organizational weaknesses, which, unlike with QKD, are easy to manage and control even without special expertise.

The comparison thus shows a clear difference between theoretical security and practical vulnerability. High formal security guarantees at the procedural/technological level are no substitute for robust implementation and controllable operating models. For a realistic assessment, it is therefore crucial to consider not only

the underlying security model, but also the entirety of assumptions and risks that come into play in concrete use.

9.2.5 Cost and Infrastructure Dependencies

The cost and infrastructure profiles of the procedures/technologies under consideration differ significantly and have a major impact on their practical applicability. Optical QKD procedures (DV-QKD, CV-QKD, and entanglement-based approaches) require highly specialized hardware on both sides of a connection. The investment costs are typically in the high five- to six-figure dollar range per link, plus installation, integration, and ongoing operating costs. Highly sensitive detectors, precision optical components, and (in certain cases) cryogenic cooling are particularly cost-relevant. In addition to energy and maintenance, operating costs also include qualified personnel for monitoring and troubleshooting.

These processes/technologies also require suitable physical infrastructure. Fiber-optic QKD requires access to dedicated or at least controllable fiber-optic lines; coexistence with data traffic is possible, but technically challenging. Free-space and satellite applications require clear lines of sight (i.e., no clouds, fog, etc.), precise alignment, and suitable locations. The resulting dependencies on network infrastructure, site conditions, and permits have a direct impact on costs, flexibility, and rollout.

In contrast, RKD has very low investment costs because it can rely on comparatively simple radio hardware and existing communications infrastructure. Operating costs remain manageable, but are offset by the very low key rates and distances, which limit its use to specific scenarios— mostly with moving devices. Additional infrastructure requirements arise primarily from the need for controlled radio environments.

MKD follows a fundamentally different cost model. The technical costs for generating large quantities of key material are very low and scale with the performance of the random number generators and storage systems used. The dominant cost factor lies in the organizational and logistical area: secure data carriers, transport, storage, and access control. In return, there are no requirements for continuous transmission infrastructure and highly specialized technology during operation. The economic evaluation here depends heavily on existing logistics structures and organizational integration.

Overall, it is evident that increasing technical complexity is accompanied by significantly higher investment and operating costs as well as greater infrastructure dependencies, while simpler physical approaches shift costs and risks more strongly into the organizational sphere.

9.3 Consolidated View

The preceding sections show that the methods/technologies considered cannot be classified along a linear scale of "better" or "worse," but rather represent different security, operational, and organizational paradigms. DV-QKD, CV-QKD, and entanglement-based QKD share the fundamental goal of securing the generation and distribution of keys via a physical transmission channel, but differ in their technical design, achievable performance, and operational complexity. RKD and MKD, on the other hand, pursue approaches in which security primarily results from the physical properties of devices, radio channels, or processes, as well as from organizational measures.

Quantum-based methods/technologies are characterized by a high degree of formal security at the method/technology level, which allows far-reaching security-theoretical statements under idealized assumptions. However, this strength is accompanied by structural limitations. The achievable key rates are limited and highly dependent on distance, attenuation, and operating conditions. In addition, the design and operation require complex systems with sensitive components, continuous calibration, and close monitoring. Practical applicability is therefore often limited to clearly defined scenarios in which the infrastructure, environment, and operation are controllable.

RKD occupies an intermediate position. The approach uses the physical properties of radio channels to extract keys, but does not provide the formal security guarantees of quantum-based methods/technologies. The strength of RKD lies in its comparatively low technical complexity and the possibility of using existing communication infrastructure. On the other hand, it has very low key rates and distances, a dependence on the respective radio environment, and dynamic requirements (movement of at least one device), which limits its use to niche applications.

MKD differs most significantly from the other approaches in terms of structure. Here, the generation and distribution of keys are decoupled from the actual use in terms of time and space. Very large quantities of key material can be generated independently of transmission channels and then physically distributed. This results in very high, effectively available key quantities with comparatively very low technical complexity during operation. At the same time, the security-related effort shifts to the organizational area: secure generation, storage, transport, and management of data carriers become the central control variables, which can be easily monitored and controlled without special expertise.

The characteristic strengths and weaknesses of the approaches cannot, therefore, be considered in isolation, but only in combination. Quantum-based methods/technologies offer conceptually elegant solutions for continuous key exchange over distance, but are very cost-intensive and operationally demanding. RKD is a technically simple but performance-limited alternative, but scores points in terms of mobile devices and costs. MKD offers exceptionally high key capacities, which also enable one-time pad encryption, and robust operating conditions at very low cost, but requires established logistical processes and clear organizational responsibilities.

Finally, for a comprehensive classification, it is crucial that the procedures/technologies differ not only in performance parameters but also in their fundamental understanding of the system. While QKD approaches and RKD primarily understand security as a property of an ongoing physical transmission process, MKD treats security as the result of controlled physical and organizational processes. These structural differences shape all other aspects, from costs and scalability to attack surfaces, and form the framework for the subsequent consolidation of key findings.

9.4 Condensed Key Statements

A comparison of the methods/technologies under consideration shows that physical methods of key provision do not form a uniform solution field, but represent different security and organizational concepts. A key finding is that the performance, operational requirements, and security assumptions of the methods vary greatly and cannot be compared without context. Statements about the "superiority" or "inferiority" of individual approaches are therefore only meaningful in relation to specific conditions of use.

Quantum-based methods/technologies achieve only limited key rates under realistic operating conditions and are sensitive to distance, attenuation, and environmental conditions. These limitations are physical in nature and independent of individual implementations. At the same time, their setup and operation are technically demanding and involve considerable investment and operating costs. It can be considered certain that QKD solutions are currently only practicable in clearly defined scenarios with controllable infrastructure.

RKD represents an approach with low technical complexity, but its performance is limited by very low key rates and distances. It is certain that RKD is not suitable for applications with high key requirements or longer distances, but is well suited for moving devices (vehicles, drones, moving IoT devices, etc.). However, it remains unclear to what extent RKD can provide additional benefits in specialized niches when combined with other methods.

MKD differs fundamentally from all transmission-based approaches. It is certain that the physical distribution of large quantities of key material can effectively achieve very high key capacities that far exceed the orders of magnitude of optical methods/technologies. It is also certain that the central security assumptions and risks here shift to the organizational and logistical areas and that the costs are low. It remains to be seen to what extent existing organizations can reliably integrate these processes.

Overall, it is clear that theoretical security models alone do not provide a sufficient basis for procurement decisions. Rather, the decisive factors are practical assumptions, systemic risks, and organizational controllability in real-world operations. Open questions relate in particular to future technological developments, possible advances in standardization, and the question of how different methods/technologies can be combined in a meaningful way. The present results thus provide a reliable

basis for informed decisions, but do not replace a context-specific assessment of the respective application scenario.

Summary performance comparison of the five methods/technologies DV-QKD (quantum key distribution with polarization of individual photons), CV-QKD (quantum key distribution with a continuous photon stream), QKD (quantum key distribution) with entanglement, RKD (radio signal key distribution), and MKD (memory key distribution)

Criterion	DV-QKD	CV-QKD	QKD with entanglement	RKD	MKD
Distance	★★★★☆	★★☆☆☆	★★★★☆	★☆☆☆☆	★★★★★
Key rate for short distances	★★★☆☆	★★★☆☆	★★☆☆☆	★☆☆☆☆	★★★★★
Key rate at long distances	★☆☆☆☆	☆☆☆☆☆	★☆☆☆☆	☆☆☆☆☆	★★★★★
Market readiness	★★★★☆	★★★★☆	★★★☆☆	★★★★☆	★★★★★
IT security issues	M, S, T	M, S, T	M, S	M	T
Cost					
Robustness	★★☆☆☆	★★☆☆☆	★☆☆☆☆	★★★★☆	★★★★★
Manufacturer dependency	Yes	Yes	Yes	No	No
Authentication	Shared secret	Shared secret	Shared secret	Shared secret	Smart-card
Suitability for mobile devices	☆☆☆☆☆	★☆☆☆☆	☆☆☆☆☆	★★★★★	★★★★★
Disadvantages	Infrastructure	Infrastructure	Infrastructure	Transport	Transport

★★★★★ = excellent; ★★★☆☆ = moderate; ★☆☆☆☆ = very poor; ☆☆☆☆☆ = not

Explanation of IT security issues:

- M = Mathematical methods
- S = Side-channel attacks
- T = Risk via true random number generator (TRNG)

Explanation of disadvantages:

- Infrastructure: Complex communication infrastructure (fiber optics, free-space optics, satellites, ground stations, trusted nodes)
- Transport: Physical transport of storage media required

References

[Weg81] M.N. Wegman, L. Carter, New hash functions and their use in authentication and set equality. J. Comput. Syst. Sci. **22**, 265–279 (1981). https://doi.org/10.1016/0022-0000(81)90033-7

[WP-MAC] Wikipedia contributors, "Message authentication code," Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/wiki/Message_authentication_code