Appendix 01
Abstract and Summary

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.

1 QKD

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.

2 RKD

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.

3 MKD

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.

4 The books aim

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."

5 Summary

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
Costs					
Robustness	★★☆☆☆	★★☆☆☆	★☆☆☆☆	★★★★☆	★★★★★
Manufacturer dependency	Yes	Yes	Yes	No	No
Authentication	Shared secret	Shared secret	Shared secret	Shared secret	Smart-card
Suitability for mobile devices	☆☆☆☆☆	★☆☆☆☆	☆☆☆☆☆	★★★★★	★★★★★
Disadvantages	Infra-structure	Infra-structure	Infra-structure	Transport	Transport

★★★★★ excellent
★★★★☆ good
★★★☆☆ moderate
★★☆☆☆ poor
★☆☆☆☆ very poor
☆☆☆☆☆ impossible

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