Vergleich von physikalischen Verfahren zur quantencomputersicheren Erzeugung und Verteilung kryptografischer Schlüssel

Univ.-Doz. Dipl.-Ing. Dr. Ernst Piller
Dipl.-Ing. Hubert Schölnast
Hochschule für Angewandte Wissenschaften St. Pölten
St. Pölten, Dezember 2025

University of
Applied Sciences
St. Pölten

Die Studie wurde vom Bundesministerium für Finanzen (BMF) im Sicherheitsforschungs-Förderprogramm KIRAS/K-Pass der österreichischen Forschungsförderungsgesellschaft FFG finanziert.

1 Einführung

1.1 Allgemeines

Es existieren sehr viele Bücher und Studien über Kryptografie und einige davon behandeln auch physikalische Verfahren. Im Umfeld der physikalischen Kryptografie gibt es einige Bücher über QKD (Quantum Key Distribution). RKD (Radio-signal Key Distribution) und MKD (Memory Key Distribution) wurden bisher in Büchern nicht behandelt und es existiert auch kein Leistungsvergleich dieser Technologien und Verfahren.

Die vorliegende Studie behandelt erstmals allgemein verständlich QKD, RKD und MKD und vergleicht diese Technologien objektiv und technologieneutral nach Leistungskriterien der Praxis. Sie behandelt auch die praktische Umsetzung, einschließlich praktischer Erfahrungen. Die Studie wurde in erster Linie verfasst für Leser, die eine sehr hohe Datensicherheit und daher eine hochsichere Datenverschlüsselung benötigen, und für alle, die sich für IT-Sicherheit und Kryptografie interessieren, wie z.B. Informatiker, Manager, Beschaffer und Gutachter.

Bei der Kryptografie zählt die Sicherheit und nicht die Komplexität des Verfahrens. Das zeigt sich auch bei der Datenverschlüsselung, wo nur das einfachste Verfahren, das One-Time-Pad, beweisbar 100%ig sicher ist.

Die heutige Digitalisierung, Globalisierung und weltweite Vernetzung benötigen eine sichere Telekommunikation und Datenspeicherung und diese wiederum erfordern eine sichere Kryptographie. Die Entwicklung sicherer Datensicherungsverfahren für die Kommunikation und Datenspeicherung stellt eine zentrale Herausforderung dar. Die Sicherheitsbeurteilung der aktuellen Kryptographie baut auf der Vermutung auf, dass es mathematische Probleme gibt, die für einen Angreifer sehr schwer zu lösen sind. Wer deshalb mathematische Verfahren ablehnt, vor allem wenn es sich um sensible Forschungsdaten, medizinische Daten, vertrauliche Daten von Staaten und Unternehmen etc. handelt, muss physikalische Verfahren verwenden. Das Thema physikalische Verfahren der Kryptografie ist erst durch die Forderung nach Quantencomputer-sicher richtig populär geworden, es ist aber ein Thema, das schon seit Jahrzehnten die gleiche Berechtigung hatte und heute noch immer hat, weil es auch die heutige Datenverschlüsselung betrifft (Speicherung heute, Angriff in Zukunft). Wer dagegen mit der heutigen asymmetrischen Kryptografie zufrieden ist, wird es auch in Zukunft mit der Post-Quanten Kryptografie sein und benötigt keine physikalischen Verfahren. Und das gilt ebenso für symmetrische Verfahren wie dem AES (Advanced Encryption Standard).

In der vorliegenden Studie werden allgemein verständlich, technologieneutral und nachvollziehbar fünf verschiedene Technologien bzw. Verfahren der physikalischen Kryptografie vorgestellt und nach Leistungskriterien der Praxis verglichen. Der Vergleich erfolgt aus der Sicht der IT-Sicherheit, Marktreife, Schlüsselrate (bei QKD abhängig von der Entfernung), Distanz (Abstand zwischen den Kommunikationspartnern), Kosten, Robustheit / Störungsanfälligkeit, Eignung für bewegte Endgeräte etc. Sie enthält auch eine technologieneutrale Analyse der Vor- und Nachteile und der generellen Eignung

der Verfahren bzw. Technologien in Bezug auf verschiedene Anwendungsszenarien und eine aktuelle Marktanalyse der schon angebotenen europäischen Produkte / Lösungen.

IT-Sicherheit ist immer so gut wie das schwächste Glied in der Kette. Das gilt auch für die Datenverschlüsselung. Grundsätzlich gilt daher, dass wenn mathematische Verfahren abgelehnt werden, weil ihre Sicherheitsbeurteilung auf Vermutungen aufbaut, reicht es nicht aus, wenn nur die Erzeugung und Verteilung der kryptografischen Schlüssel mit physikalischen Verfahren erfolgt. Es muss auch die Verschlüsselung ohne mathematisches Verfahren auskommen und das erfordert ein One-Time-Pad (Bitweise Verschlüsselung durch XOR-Funktion) mit einem nichtdeterministischen Schlüssel (absolut zufällige Bitfolge). Weil der nichtdeterministische Schlüssel ebenfalls durch physikalische Verfahren entsteht, wird das One-Time-Pad trotz XOR-Funktion beweisbar absolut sicher. Und das Ganze gilt auch schon heute für die aktuelle Datenverschlüsslung und ist unabhängig von der Leistungsfähigkeit zukünftiger Quantencomputern oder „optischen Computern“. Wie bei der Datenverschlüsselung zur Sicherung der Vertraulichkeit lässt sich dies auch für die Integrität und Authentizität umsetzen, d.h. eine durchgehende Kryptografie ohne mathematische Verfahren (außer XOR-Operation).

Es geht daher bei der Studie um den gänzlichen Verzicht auf mathematische Verfahren der Kryptografie, insbesondere bei der Datenverschlüsselung und dem Schlüsselmanagement, weil diese keine beweisbaren Sicherheitsbeurteilungen zulassen. Mit den physikalischen Verfahren wird ein neues Paradigma der Kryptographie eingeführt, das sich von der heutigen komplexitätsbasierten Kryptographie abhebt. **Die Verfahren sind sicher gegen rechnerisch sehr starke Gegner und heute noch nicht veröffentlichte und daher der Kryptocommunity unbekannte mathematische Angriffsmethoden.** Und das gilt nicht nur für die Datenverschlüsselung (Sicherheitsziel Vertraulichkeit) und dem Schlüsselmanagement, sondern auch für die Sicherheitsziele Integrität und Authentizität. Die Sicherheit gegen rechnerisch sehr starke Gegner meint dabei leistungsstarke Quantencomputer und optische Computer (die nochmals um ein Vielfaches schneller sind). Bei der Sicherheit vor heute noch unbekannten mathematischen Angriffsmethoden geht es um unveröffentlichte mathematische Verfahren, die heutige mathematische kryptografische Verfahren und/oder die Post-Quanten Kryptografie brechen können. Wie die Vergangenheit gezeigt hat, hat es schon öfters unveröffentlichte Verfahren mit großen Auswirkungen auf die Kryptografie gegeben. Z.B. haben die Herren Williamson und Cox schon Jahre früher das Diffie-Hellman und das RSA-Verfahren in ähnlicher Form entwickelt und nicht veröffentlicht, was erst 1997 bekannt wurde. Auch haben sich schon öfters bis zu einem Zeitpunkt als ausreichend sicher eingestufte Verfahren später als unsicher herausgestellt, wie z.B. die „Supersingulare isogene Kurven Kryptografie“ (SIKE) beim NIST-Wettbewerb https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization).

Kryptografie und damit auch die Datenverschlüsselung muss immer end-to-end erfolgen. Da ein Großteil der sensiblen Daten auf einem Endgerät (Desktop-PC, Laptop, Tablett, Smartphone, IoT-Gerät, Sensor, medizinischen Gerät etc.) entsteht, müssen sie auch schon dort ausreichend sicher verschlüsselt werden. Dabei erfolgt die eigentliche Verschlüsselung oft aus Sicherheitsgründen in einem HSM (Hardware Security Module), die

kostengünstig am Markt verfügbar sind. Die Daten dürfen aber auch direkt im Endgerät verschlüsselt werden, wenn sie mit einem One-Time-Pad erfolgt und für den Schlüsseltransport MKD+fähige Speichermedien verwendet werden. Weil die Mobilität eine zunehmende Bedeutung bekommt, wird auch die hochsichere Verschlüsselung auf Laptops, Tabletts, Smartphones und IoT-Geräte immer wichtiger.

Die wirtschaftlich sinnvollen Kosten, um das erforderliche Sicherheitsniveau der Verschlüsselung zu garantieren, orientieren sich dabei unter anderem aber nicht am Preis des Endgerätes und am HSM (Hardware Security Module), sondern am Wert der Daten. Das heißt, auch bei einem billigen Endgerät, wie z.B. Laptop, und HSM darf die gesamte Verschlüsslungslösung pro Endgerät wesentlich teurer sein, wenn der Wert der Daten, z.B. bei sehr wertvollen Forschungsdaten oder hochsensiblen staatlichen Daten, entsprechend hoch ist. Dabei müssen aber immer die Gesamtkosten betrachtet werden, d.h. auch die Verbindungskosten (Lichtleiter, Satellit, Transport der Speichermedien etc.) und die Betriebskosten inklusive Wartungskosten und diese Kosten können durch die erforderlichen end-to-end Verbindungen aller Endgeräte zueinander quadratisch ansteigen (wenn keine Verbindung doppelt genützt werden kann, beträgt die Anzahl an erforderlichen Verbindungen bei n-Teilnehmern (n2-n)/2 Verbindungen, d.h. bei z.B. n=100 sind schon 4.950 Verbindungen erforderlich).

In der Studie werden fünf Basistechnologien zur Erzeugung und Verteilung kryptografischer Schlüssel auf Basis physikalischer Verfahren untersucht und verglichen:

1. **QKD (Quantum-Key-Distribution) mit Verschränkung**, wo die gesamte Zufälligkeit des Schlüssels (Schlüsselentropie) auf quantentheoretischen Effekten basiert. Dies trifft bei den Verfahren mit Hilfe von verschränkten Photonen zu. Beide Seiten der Kommunikation (Alice und Bob) sind dabei gleichwertig und verwenden die gleichen Geräte zur Erzeugung und Verteilung der kryptografischen Schlüssel.
2. **QKD (Quantum-Key-Distribution) mit Polarisierung einzelner Photonen** (basiert auf der Teilchen-Natur des Lichts), wo die Zufälligkeit des Schlüssels von außen eingebracht wird und wo einzelne Photonen auf der Senderseite (Alice) eine Information erhalten und so per Glasfaser, Freistrahlkanal oder Satellit auf die Empfängerseite (Bob) übertragen werden. Eine Seite verwendet dabei ein Sendegerät, die andere ein Empfangsgerät. Beide Seiten (Alice und Bob) sind bei der Erzeugung und Verteilung der Schlüssel nicht gleichwertig.
3. **QKD (Quantum-Key-Distribution) mit einem kontinuierlichen Photonen-Strom** (basiert auf der Wellen-Natur des Lichts), wo die Zufälligkeit des Schlüssels von außen eingebracht wird und wo der Sender (Alice) die Phase und Amplitude moduliert. Der Empfänger (Bob) erhält per Glasfaser, Freistrahlkanal oder Satellit den Photonenstrom und misst die kontinuierlichen Werte. Eine Seite verwendet dabei ein Sendegerät, die andere ein Empfangsgerät. Beide Seiten (Alice und Bob) sind bei der Erzeugung und Verteilung der Schlüssel nicht gleichwertig.
4. **RKD (Radio-signal Key Distribution):** RKD verwendet Funksignale über 30MHz zur Berechnung und Verteilung kryptografischer Schlüssel und ist in der Literatur unter verschiedenen Bezeichnungen bekannt, z.B. „Physical layer key generation in wireless networks“ oder “Wireless Physical Layer Key Agreement”. RKD sind

physikalische Verfahren, die auf der Reziprozität der Funkübertragung und Messung von Funkkanaleigenschaften basieren. Beide Seiten der Kommunikation (Alice und Bob) sind dabei gleichwertig und verwenden die gleichen Geräte zur Erzeugung und Verteilung der kryptografischen Schlüssel.

5. **MKD (Memory Key Distribution) mit One-Time-Pad:** Erzeugung der Schlüssel durch einen nichtdeterministischen Zufallszahlengenerator und physische Verteilung durch MKD-fähige SSD (Solid-State-Speicher, aktuell bis 16 TByte) bzw. Memory Stick und Umsetzung der erforderlichen Prozesse. Diese Speichermedien enthalten mindestens eine eigene PIN-Tastatur, PIN-basierte Zugriffskontrolle, integrierte AES-256 HW-Verschlüsselung (im besten Fall ohne eigener Schlüsselspeicherung) und hochsichere Chipkarte (ISO/IEC 7816, im besten Fall zum Schlüsseltransport für die in der SSD integrierte AES-HW-Verschlüsselung und PIN-Prüfung). Beide Seiten der Kommunikation (Alice und Bob) sind dabei gleichwertig und verwenden die gleichen Geräte zur Erzeugung und Verteilung der kryptografischen Schlüssel. MKD kann auch mit Chipkarten als Datenträger verwendet werden, wenn statt dem One-Time-Pad ein mathematisches Verfahren wie der AES-256 verwendet wird.

In der Studie werden diese fünf Technologien inklusive einer ausführlichen Berücksichtigung der Unterschiede zwischen einer Realisierung über Glasfasernetze, Freistrahlkanäle und Satellitenverbindungen bei QKD und RKD behandelt. Bei MKD erfolgt ein persönlicher Transport oder mit Hilfe eines persönlichen Kuriers oder öffentlichen Paketdienstleisters. MKD wird in dieser Studie immer im Zusammenhang mit einem One-Time-Pad zur Datenverschlüsselung betrachtet, damit die gesamte Erzeugung und Verteilung der kryptografischen Schlüssel und Datenverschlüsselung völlig ohne Mathematik auskommt (rein physikalische Verfahren). MKD kann aber auch mit hochsicheren Chipkarten in Verbindung mit einem mathematischen Verschlüsselungsverfahren verwendet werden. Die Bezeichnungen RKD und MKD stammen vom Erstautor dieser Studie und sie wurden aus QKD abgeleitet.

Von der IT-Sicherheit betrachtet unterscheiden sich die oben angegebenen Verfahren / Technologien vor allem in den Bereichen Man-in-the-middle Angriffe, Seitenkanalangriffe, erforderlicher Einsatz von mathematischen Verfahren in physikalischen Verfahren der Kryptografie, Entstehung und Qualität der Schlüsselzufälligkeit inklusive der Gleichwertigkeit der beiden Kommunikationspartner und der Verwendbarkeit eines One-Time-Pads zur Datenverschlüsselung und damit einer durchgehenden physikalischen Kryptografie.

Die vorliegende Studie ist international die erste, die diese völlig verschiedenen Technologien und Verfahren technologieneutral vergleicht und allgemein verständlich macht.

1.2 Zusammenfassung der Studie

1.2.1 Gegenstand und Zielsetzung

In dieser Studie wird ein systematischer Vergleich zwischen physikalischen Verfahren zur Erzeugung und Verteilung kryptografischer Schlüssel durchgeführt. Untersucht werden jene Technologien, die nicht primär auf mathematischen Härteannahmen beruhen, sondern ihre sicherheitsrelevanten Eigenschaften aus physikalischen Gesetzmäßigkeiten ableiten. Dabei handelt es sich um drei Klassen von Quantenschlüsselverteilung (Quantum Key Distribution, QKD) in ihren praxisrelevanten Ausprägungen sowie um die Erzeugung und Verteilung von kryptografischen Schlüsseln mit Hilfe von Radiosignalen und Speichermedien:

- Prepare-and-Measure-QKD mit diskreten Variablen (DV-QKD)
- Prepare-and-Measure-QKD mit kontinuierlichen Variablen (CV-QKD)
- QKD mit verschränkten Photonen
- Radio-signal Key Distribution (RKD)
- Memory Key Distribution (MKD)

Die Gemeinsamkeit aller betrachteten Verfahren ist, dass sie sich ausschließlich mit der Erzeugung und Verteilung symmetrischer Schlüssel befassen. Die eigentliche Datenverschlüsselung sowie Mechanismen zur Sicherstellung von Integrität und Authentizität werden davon konzeptionell getrennt betrachtet, da sie jeweils zusätzliche Annahmen, Verfahren und Systemkomponenten erfordern. Die Studie verfolgt ausdrücklich keinen produkt- oder herstellerspezifischen Ansatz, sondern analysiert die Technologien auf Ebene ihrer physikalischen Prinzipien, ihrer systemischen Eigenschaften sowie ihrer praktischen Umsetzbarkeit.

Ziel des Vergleichs ist es, eine nachvollziehbare und technologieneutrale Grundlage für die Bewertung dieser Verfahren bereitzustellen. Die Studie richtet sich insbesondere an Beschaffer, Gutachter und Entscheidungsträger, die mit der Frage konfrontiert sind, ob und in welchem Umfang physikalische Verfahren der Kryptografie als Ergänzung oder Alternative zu etablierten mathematischen Verfahren in Betracht gezogen werden sollen. Dabei geht es nicht um eine abstrakte sicherheitstheoretische Bewertung, sondern um eine Einordnung entlang praxisrelevanter Kriterien wie Marktreife, Leistungsfähigkeit, Betriebsanforderungen, IT-Sicherheit, Kosten, Verwendbarkeit und infrastrukturelle Abhängigkeiten.

Der Vergleich verfolgt nicht das Ziel, eine Rangliste der untersuchten Technologien zu erstellen oder eine einzelne Lösung als allgemein überlegen darzustellen. Vielmehr sollen die strukturellen Unterschiede, Stärken und Schwächen der Ansätze transparent gemacht werden, um fundierte Entscheidungen im jeweiligen Anwendungskontext zu ermöglichen. Unterschiedliche Einsatzszenarien, wie etwa Telekommunikation, Datenspeicherung, hochsichere Punkt-zu-Punkt-Verbindungen und Einsatz in beweglichen Geräten, stellen unterschiedliche Anforderungen an Schlüsselrate, Reichweite, Robustheit, Infrastruktur und organisatorische Einbettung, denen die betrachteten Verfahren in unterschiedlichem Maß gerecht werden.

Nicht Gegenstand dieser Studie sind detaillierte sicherheitstechnische Bewertungen einzelner Implementierungen, der bei den Technologien bzw. Produkten verwendeten

mathematischen Verfahren, Quellcodeanalysen oder Zertifizierungsfragen konkreter Produkte. Ebenso wird die mathematische Kryptografie, einschließlich der Post-Quanten-Kryptografie, nicht grundsätzlich bewertet oder in Konkurrenz zu den physikalischen Verfahren gesetzt. Sie wird vielmehr als etablierter Referenzrahmen betrachtet, zu dem physikalische Verfahren je nach Sicherheitsannahme, Risikoprofil und Anwendungsfall in Beziehung gesetzt werden können. Die Studie versteht sich damit als Entscheidungs- und Orientierungsgrundlage, nicht als normative Vorgabe für den Einsatz bestimmter Technologien.

1.2.2 Grundlagen der Vergleichbarkeit

Die in dieser Studie vorgenommenen Vergleiche beruhen auf einer systematischen Zusammenführung unterschiedlicher Informationsquellen und Betrachtungsebenen. Grundlage bilden erstens der dokumentierte Stand der Technik aus wissenschaftlicher Literatur und öffentlich zugänglichen Forschungsberichten, zweitens Angaben von Herstellern zu ihren Produkten und Systemen sowie drittens Erfahrungsberichte von Anwendern, die entsprechende Technologien in realen bzw. praxisnahen Umgebungen eingesetzt haben.

Die Aussagekraft der herangezogenen Quellen ist dabei unterschiedlich zu bewerten.

- Wissenschaftliche Publikationen liefern in der Regel gut nachvollziehbare, aber oft unter idealisierten Bedingungen erhobene Ergebnisse.
- Herstellerangaben sind insbesondere für technische Eckdaten relevant, unterliegen jedoch naturgemäß marketinggetriebenen Verzerrungen und beziehen sich nicht immer auf den dauerhaften Praxisbetrieb.
- Anwenderberichte bieten wertvolle Einblicke in reale Einsatzbedingungen, sind jedoch häufig auf spezifische Konfigurationen und Einzelfälle beschränkt.

Die Vergleichbarkeit der untersuchten Technologien ist zudem durch strukturelle Unterschiede begrenzt. Die Verfahren unterscheiden sich grundlegend hinsichtlich physikalischer Prinzipien, Systemarchitekturen, Reifegrad und Einsatzkontext. Einheitliche Kennzahlen, die eine direkte quantitative Vergleichbarkeit erlauben würden, existieren nur eingeschränkt. Aussagen zu Schlüsselraten, Reichweiten, Kosten oder Robustheit sind daher stets im jeweiligen Kontext zu interpretieren.

Der vorliegende Vergleich versteht sich vor diesem Hintergrund nicht als exakte Gegenüberstellung einzelner Messwerte, sondern als qualitativ fundierte Einordnung technologischer Eigenschaften und Rahmenbedingungen. Ziel ist es, Entscheidungsgrundlagen zu liefern, die Stärken, Schwächen und Abhängigkeiten der Verfahren transparent machen, ohne eine Genauigkeit vorzutäuschen, die angesichts der heterogenen Quellenlage und der dynamischen technologischen Entwicklung nicht erreichbar ist.

1.2.3 Vergleich nach praxisrelevanten Kriterien

Technologischer Reifegrad und Verfügbarkeit

Die betrachteten physikalischen Verfahren zur Erzeugung und Verteilung kryptografischer Schlüssel weisen erhebliche Unterschiede im technologischen Reifegrad auf. Diese

Unterschiede ergeben sich weniger aus der grundsätzlichen Funktionsfähigkeit der zugrunde liegenden physikalischen Prinzipien, als aus dem Grad ihrer technischen Ausreifung, Systemintegration und längerfristigen Betriebserfahrung. Daher werden experimentelle Konzepte, Pilotanwendungen und begrenzt einsatzfähige Systeme voneinander abgegrenzt betrachtet.

Ein Teil der quantenbasierten Verfahren, insbesondere ausgewählte QKD-Ansätze, hat den Status reiner Laborforschung klar hinter sich gelassen. Für diese Verfahren existieren integrierte Systeme, die unter kontrollierten Bedingungen in Testnetzen oder in klar abgegrenzten Anwendungsszenarien betrieben werden können. Diese Einsatzformen sind jedoch häufig durch spezifische infrastrukturelle Voraussetzungen, begrenzte Reichweiten oder erhöhte betriebliche Anforderungen eingeschränkt. Weitere QKD-Varianten befinden sich demgegenüber weiterhin im Stadium experimenteller Erprobung oder konzeptioneller Entwicklung, bei denen wesentliche Eigenschaften zwar prinzipiell gezeigt wurden, eine belastbare Aussage zur Alltagstauglichkeit jedoch noch nicht möglich ist.

Für RKD ist der Forschungsstand auch sehr weit gediehen, ein marktfähiges Produkt ist aber aktuell nur von einem Hersteller bekannt, das aber noch nicht sicherheitszertifiziert ist.

Für MKD sind alle erforderlichen Komponenten am Markt in einer großen Auswahl vorhanden. Sie sind sicherheitszertifiziert (bis zu Verschlusssache) und kostengünstig weltweit verfügbar. MKD+fähige Speichermedien, wo in Verbindung mit einem One-Time-Pad zur Datenverschlüsselung kein HSM (Hardware Security Module) erforderlich ist, sind noch nicht verfügbar, erfordern aber nur eine Softwareanpassung bei vorhandenen Speichermedien inklusive neuer Zertifizierung.

Für die Bewertung des Reifegrads ist entscheidend, ob ein Verfahren als geschlossenes, reproduzierbares System vorliegt oder primär als Kombination spezialisierter Einzelkomponenten umgesetzt wird. Verfahren, die auf komplexen, empfindlichen oder nur begrenzt standardisierten Komponenten beruhen, erfordern in der Praxis einen erheblichen Integrations- und Betriebsaufwand, der über die reine Funktionsdemonstration hinausgeht. Demgegenüber sind physikalische Ansätze, die auf einfachen, gut verstandenen und unabhängig überprüfbaren Komponenten beruhen, leichter nachzuvollziehen, umzusetzen und organisatorisch zu handhaben, auch wenn sie weniger stark formalisiert sind.

Der Stand der Standardisierung bildet einen weiteren Indikator für den Reifegrad, ist jedoch nicht mit breiter Einsatzfähigkeit gleichzusetzen. Während standardisierte Schnittstellen und Protokolle die Integration erleichtern können, sagen sie nur begrenzt etwas über langfristige Wartbarkeit, Betriebskosten oder Abhängigkeiten von spezifischen Implementierungen aus. Für eine belastbare Einordnung des technologischen Reifegrads ist daher stets das Zusammenspiel aus Systemverfügbarkeit, betrieblicher Stabilität, Integrationsaufwand und organisatorischer Tragfähigkeit zu betrachten.

Schlüsselraten, Reichweite und Skalierung

Schlüsselraten und Reichweite sind bei den betrachteten Verfahren nicht nur technologisch, sondern auch begrifflich schwer vergleichbar: In der Literatur werden „Rohschlüssel“, „sifted key“ und „Secret Key Rate (SKR)“ nicht durchgängig trennscharf verwendet, und es ist nicht

immer ersichtlich, ob Post-Processing (Fehlerkorrektur, Privacy Amplification) bereits vollständig berücksichtigt ist. Die nachfolgenden Angaben verwenden daher, sofern das möglich ist, explizit als Secret Key Rate ausgewiesene Werte. Ansonsten werden sie als praxisnahe Größenordnungen bzw. als Randbedingungen eingeordnet.

Technologie-klasse	**typische Distanz bzw. Dämpfung**	**Praxisnahe Schlüsselrate (Größenordnung)**	**Anmerkungen**
DV-QKD	ca. 10 – 20 km (2 – 5 dB)	einige kbit/s bis mehrere 10 kbit/s	günstige Bedingungen, kurze Strecken
	ca. 50 – 80 km (10 – 26 dB)	meist 100 – 1000 bit/s	typisch für Feldtests und Dauerbetrieb
	ca. 120 – 200 km (24 – 40 dB)	meist 10 – 100 bit/s	Grenzbereich, nur eingeschränkt nutzbar
CV-QKD	bis ca. 40 km (bis 8 dB)	meist 1 – 10 kbit/s	kurze Distanzen, empfindlich gegenüber Rauschen
	ca. 50 – 100 km (10 – 20 dB)	meist 10 – 100 bit/s	praxisnaher Arbeitsbereich
QKD mit Verschränkung	ca. 10 – 50 km (2 – 10 dB)	meist 10 – 100 bit/s	stark abhängig von Quelle und Detektion
	über 70 km	unter 100 bit/s	experimenteller Grenzbereich
RKD	lokale Funkver-bindung, meist unter 15 km	meist 1 – 10 bit/s	systemisch begrenzt, kaum skalierbar
MKD	physischer Transport eines Datenträgers	bis 16 TByte pro Transfer. Bei Erzeugung bis zu 240 Mbit/s (auch 7 Gbit/s)	nicht durch Transport limitiert, sondern durch Erzeugung

Bei QKD über Glasfaser zeigen Feldtests und herstellerübergreifende Auswertungen konsistent, dass mit steigender Kanaldämpfung die tatsächlich nutzbare Secret-Key-Rate (endgültige Schlüsselrate) stark abfällt. Im Bereich von etwa 10–20 dB liegen praxisnahe Werte häufig im oberen zweistelligen bis unteren vierstelligen bit/s-Bereich; bei 25–30 dB werden vielfach nur noch einige 100 bit/s oder weniger erreicht. Diese Größenordnungen finden sich unabhängig vom konkreten Produkt und spiegeln die physikalisch bedingten Verluste wider.

RKD wird in der Studie als grundsätzlich sehr kostengünstig und mobilitätsgeeignet eingeordnet (RKD benötigt meist Bewegung), zugleich aber hinsichtlich der Schlüsselrate und Entfernung als stark begrenzt.

MKD folgt einer anderen Metrik: Die „Schlüsselrate“ ergibt sich effektiv aus der Kombination aus

1. erzeugbarer Menge nichtdeterministischer Schlüsselbits (z.B. 1 TByte in ca. 9 Stunden mit sehr schnellen Zufallszahlengeneratoren) und
2. logistischer Transferfähigkeit. Als Kapazität pro Transfer werden bis 16 TByte an Schlüsselbytes genannt, wobei aber nichts dagegen spricht, auch mehrere Datenträger zugleich zu transportieren.

Damit verschiebt sich die Leistungsgrenze von Übertragungsverlusten etc. hin zu Erzeugungs- und Logistikparametern.

Betriebsbedingungen und Robustheit

Die Betriebsbedingungen der betrachteten Technologien unterscheiden sich deutlich und wirken sich unmittelbar auf Stabilität, Verfügbarkeit und organisatorische Beherrschbarkeit aus. Optische QKD-Verfahren, unabhängig davon, ob sie mit diskreten Variablen, kontinuierlichen Variablen oder verschränkten Photonen arbeiten, reagieren empfindlich auf Umwelt- und Systemeinflüsse. In Glasfasern führen Temperaturänderungen, mechanische Belastungen oder Alterungseffekte zu Polarisations- und Phasendrift, die kontinuierlich kompensiert werden müssen. Bei Freiraum- und satellitengestützten Verbindungen treten zusätzlich atmosphärische Effekte (Aerosole, Nebel, Wolken etc.), Ausrichtungsfehler und Hintergrundlicht auf, die zu starken zeitlichen Schwankungen der Schlüsselrate oder zu Abbrüchen führen können. Diese Einflüsse sind physikalisch bedingt und lassen sich nur begrenzt durch technische Maßnahmen reduzieren.

Der laufende Betrieb optischer QKD-Systeme erfordert daher eine präzise Kalibrierung, exakte Zeit- und Phasensynchronisation sowie regelmäßige Nachregelung. Insbesondere bei längeren Distanzen oder wechselnden Umweltbedingungen binden diese Anforderungen personelle und technische Ressourcen. Verschiedene QKD-Varianten unterscheiden sich im Detail, teilen jedoch die Notwendigkeit eines kontinuierlich überwachten und aktiv geregelten Betriebs. Abweichungen außerhalb definierter Toleranzen führen typischerweise nicht zu graduellen Qualitätseinbußen, sondern zu einem starken Einbruch der Schlüsselrate oder zum vollständigen Abbruch des Schlüsselaustauschs.

RKD weist im Vergleich dazu sehr geringe Anforderungen an Präzisionskalibrierung und Synchronisation auf, ist jedoch stark von den Eigenschaften des Funkkanals abhängig. Störungen durch Mehrwegeausbreitung, Abschattung oder fremde Funksignale können die ohnehin niedrigen Schlüsselraten weiter reduzieren oder zeitweise unmöglich machen. Die Robustheit ergibt sich hier weniger aus technischer Stabilität als aus der Möglichkeit, Verfahren flexibel an wechselnde Rahmenbedingungen anzupassen.

MKD stellt in dieser Hinsicht einen Sonderfall dar. Die Erzeugung der Schlüsselbits unterliegt zwar den Betriebsbedingungen der eingesetzten Zufallszahlengeneratoren, der eigentliche Transport erfolgt jedoch unabhängig von empfindlichen Übertragungskanälen. Die Robustheit wird primär durch organisatorische und logistische Faktoren bestimmt, etwa den sicheren Umgang mit Datenträgern, deren Lagerung und Transport. Im Betrieb resultiert daraus eine sehr hohe Fehlertoleranz, d.h. Robustheit, gegenüber Umwelt- und

Systemeinflüssen, allerdings verbunden mit einem nicht kontinuierlichen, sondern diskreten Bereitstellungsmodell für das Schlüsselmaterial.

Sicherheitsannahmen und Systemrisiken

Die betrachteten Technologien beruhen auf unterschiedlichen Sicherheitsmodellen, die jeweils eigene Annahmen und Grenzen mit sich bringen. Quantenbasierte Verfahren zielen darauf ab, die Sicherheit der Erzeugung und Verteilung der Schlüssel auf die Gesetze der Quantenmechanik zurückzuführen. In idealisierter Form erlauben sie Aussagen über informationstheoretische Sicherheit gegenüber bestimmten Angreifermodellen. Diese Aussagen gelten jedoch nur unter klar definierten Voraussetzungen und abstrahieren von praktischen Implementierungsdetails. RKD und MKD verfolgen demgegenüber keine quantenphysikalischen Sicherheitsmodelle, sondern stützen sich auf klassische physikalische Eigenschaften von Funkkanälen, hardwarebasierten Zufallszahlengeneratoren, Speichermedien, Chipkarten und Prozessen sowie auf organisatorische Maßnahmen.

Ein zentraler Unterschied zwischen den Ansätzen liegt in der Anzahl und Art zusätzlicher Annahmen. Optische QKD-Verfahren setzen voraus, dass die eingesetzten Geräte wie spezifiziert arbeiten, dass Detektoren und Quellen nicht manipuliert sind und dass bestimmte Nebenkanäle ausreichend kontrolliert werden. In netzartigen Strukturen kommen häufig weitere Annahmen hinzu, etwa das Vertrauen in Zwischenstationen oder Schlüsselmanagementsysteme. Zudem ist in allen QKD-Varianten eine initiale Authentisierung erforderlich, die ihrerseits auf vorab geteilten Geheimnissen oder klassischen kryptographischen Verfahren beruht. Diese Zusatzannahmen relativieren den formalen Sicherheitsgewinn, ohne ihn notwendigerweise aufzuheben.

Eine wichtige Rolle spielt bei QKD und RKD auch das sogenannte Post-Processing (Fehlerkorrektur, Privacy Amplification), das rein auf mathematischen Verfahren basiert.

RKD benötigt ebenfalls Annahmen über die Eigenschaften des Funkkanals und über die Fähigkeit eines Angreifers, diesen vollständig zu kontrollieren oder abzuhören. Die Sicherheit ergibt sich hier nicht aus strikten theoretischen Beweisen, sondern aus der praktischen Schwierigkeit bestimmter Angriffe.

MKD verschiebt die Sicherheitsannahmen weitgehend in den organisatorischen Bereich: Die Vertraulichkeit des Schlüssels hängt primär von der sicheren Erzeugung, Lagerung und dem physischen Transport der Datenträger ab. Angriffsflächen entstehen in der Praxis nicht durch mathematische oder physikalische Schwächen, die die nichtdeterministischen Zufallszahlengeneratoren und MKD-fähigen Speichermedien bestimmen, sondern durch Prozesse, Personal und Logistik.

Systemische Risiken ergeben sich bei allen Technologien aus Implementierung, Betrieb und Integration in bestehende Infrastrukturen. Komplexe Systeme mit vielen Komponenten und Schnittstellen bieten grundsätzlich mehr Angriffspunkte als einfache, klar abgegrenzte Verfahren. Gerade bei QKD können Seitenkanalangriffe, Fehlkonfigurationen und das Post-Processing (Fehlerkorrektur und Privacy Amplification) dazu führen, dass die praktische Sicherheit deutlich unter den theoretischen Erwartungen liegt. Umgekehrt verlagern sich bei

MKD die Risiken auf organisatorische, die aber vergleichsweise zu QKD auch ohne speziellen Know-how einfach überschaubar und kontrollierbar sind.

Der Vergleich zeigt damit eine klare Differenz zwischen theoretischer Sicherheit und praktischer Angriffsfläche. Hohe formale Sicherheitsgarantien auf Protokollebene sind kein Ersatz für robuste Implementierung und beherrschbare Betriebsmodelle. Für eine realistische Bewertung ist daher entscheidend, nicht nur das zugrunde liegende Sicherheitsmodell zu betrachten, sondern auch die Gesamtheit der Annahmen und Risiken, die im konkreten Einsatz wirksam werden.

Kosten- und Infrastrukturabhängigkeiten

Die Kosten- und Infrastrukturprofile der betrachteten Technologien unterscheiden sich deutlich und prägen maßgeblich ihre praktische Einsetzbarkeit. Optische QKD-Verfahren (DV-QKD, CV-QKD sowie verschränkungsbasierte Ansätze) erfordern hochspezialisierte Hardware auf beiden Seiten einer Verbindung. Die Investitionskosten liegen typischerweise im hohen fünf- bis sechsstelligen Euro-Bereich pro Link, hinzu kommen Aufwände für Installation, Integration und laufenden Betrieb. Besonders kostenrelevant sind hochsensitive Detektoren, optische Präzisionskomponenten sowie (in bestimmten Ausprägungen) Kryokühlung. Die Betriebskosten umfassen neben Energie und Wartung auch qualifiziertes Personal für Überwachung und Fehlersuche.

Diese Verfahren setzen zudem geeignete physische Infrastruktur voraus. Für Glasfaser-QKD ist der Zugang zu dedizierten oder zumindest kontrollierbaren Glasfaserstrecken erforderlich; Koexistenz mit Datenverkehr ist zwar möglich, aber technisch anspruchsvoll. Freiraum- und Satellitenanwendungen benötigen freie Sichtlinien (d.h. auch keine Wolken, Nebel etc.), präzise Ausrichtung und geeignete Standorte. Die resultierenden Abhängigkeiten von Netzinfrastruktur, Standortbedingungen und Genehmigungen wirken sich unmittelbar auf Kosten, Flexibilität und Ausrollbarkeit aus.

RKD weist demgegenüber deutlich geringere Investitionskosten auf, da es auf vergleichsweise einfache Funkhardware und vorhandene Kommunikationsinfrastruktur zurückgreifen kann. Die Betriebskosten bleiben überschaubar, werden jedoch durch die sehr niedrigen Schlüsselraten und Entfernungen relativiert, die den Einsatz auf spezielle Szenarien – meist mit bewegten Geräten - beschränken. Zusätzliche Infrastrukturanforderungen entstehen vor allem durch die Notwendigkeit kontrollierter Funkumgebungen.

MKD folgt einem grundsätzlich anderen Kostenmodell. Die technischen Kosten für die Erzeugung großer Mengen von Schlüsselmaterial sind vergleichsweise sehr gering und skalieren mit der Leistungsfähigkeit der eingesetzten Zufallszahlengeneratoren und Speichersysteme. Der dominante Kostenfaktor liegt im organisatorischen und logistischen Bereich: sichere Datenträger, Transport, Lagerung und Zugriffskontrolle. Dafür entfallen komplett die Anforderungen an kontinuierliche Übertragungsinfrastruktur und hochspezialisierte Technik im laufenden Betrieb. Die wirtschaftliche Bewertung hängt hier stark von bestehenden Logistikstrukturen und organisatorischer Einbettung ab.

Insgesamt zeigt sich, dass steigende technische Komplexität mit deutlich höheren Investitions- und Betriebskosten sowie stärkeren Infrastrukturabhängigkeiten einhergeht,

während einfachere physikalische Ansätze Kosten und Risiken stärker in den organisatorischen Bereich verlagern.

1.2.4 Zusammenführende Betrachtung

Die vorangegangenen Abschnitte zeigen, dass sich die betrachteten Technologien weniger entlang einer linearen Skala von „besser“ oder „schlechter“ einordnen lassen, sondern vielmehr unterschiedliche sicherheitstechnische, betriebliche und organisatorische Paradigmen repräsentieren. DV-QKD, CV-QKD und verschränkungsbasierte QKD teilen das grundlegende Ziel, die Erzeugung und Verteilung der Schlüssel über einen physikalischen Übertragungskanal abzusichern, unterscheiden sich jedoch in technischer Ausgestaltung, erreichbarer Leistung und operativer Komplexität. RKD und MKD verfolgen demgegenüber Ansätze, bei denen Sicherheit primär aus physikalischen Eigenschaften von Geräten, Funkkanälen oder Prozessen sowie aus organisatorischen Maßnahmen resultiert.

Quantenbasierte Verfahren zeichnen sich durch einen hohen Grad formaler Absicherung auf Protokollebene aus, der unter idealisierten Annahmen weitreichende sicherheitstheoretische Aussagen erlaubt. Diese Stärke geht jedoch mit strukturellen Einschränkungen einher. Die erzielbaren Schlüsselraten sind begrenzt und stark abhängig von Distanz, Dämpfung und Betriebsbedingungen. Zudem erfordern Aufbau und Betrieb komplexe Systeme mit empfindlichen Komponenten, kontinuierlicher Kalibrierung und enger Überwachung. Die praktische Einsetzbarkeit ist daher häufig auf klar definierte Szenarien beschränkt, in denen Infrastruktur, Umgebung und Betrieb kontrollierbar sind.

RKD nimmt eine Zwischenstellung ein. Der Ansatz nutzt physikalische Eigenschaften von Funkkanälen, um Schlüssel zu extrahieren, verzichtet jedoch auf die formalen Sicherheitsgarantien quantenbasierter Protokolle. Die Stärke von RKD liegt in der vergleichsweise sehr geringen technischen Komplexität und der Möglichkeit, vorhandene Kommunikationsinfrastruktur zu nutzen. Dem stehen sehr niedrige Schlüsselraten und Entfernungen, eine Abhängigkeit von der jeweiligen Funkumgebung und Dynamikanforderungen (Bewegung zumindest eines Gerätes) gegenüber, was den Einsatz auf Nischenanwendungen beschränkt.

MKD unterscheidet sich strukturell am deutlichsten von den anderen Ansätzen. Hier wird die Erzeugung und Verteilung der Schlüssel zeitlich und räumlich vom eigentlichen Einsatz entkoppelt. Sehr große Mengen von Schlüsselmaterial können unabhängig von Übertragungskanälen erzeugt und anschließend physisch verteilt werden. Daraus ergeben sich sehr hohe effektiv verfügbare Schlüsselmengen bei vergleichsweise sehr geringer technischer Komplexität im laufenden Betrieb. Gleichzeitig verlagert sich der sicherheitsrelevante Aufwand in den organisatorischen Bereich: sichere Erzeugung, Lagerung, Transport und Verwaltung der Datenträger werden zu den zentralen Stellgrößen, die ohne speziellen Know-how einfach überwachbar und kontrollierbar sind.

Die charakteristischen Stärken und Schwächen der Ansätze lassen sich daher nicht isoliert, sondern nur im Zusammenspiel betrachten. Quantenbasierte Verfahren bieten konzeptionell elegante Lösungen für den kontinuierlichen Schlüsselaustausch über Distanz, sind jedoch sehr kostenintensiv und betrieblich anspruchsvoll. RKD stellt eine technisch einfache, aber leistungsmäßig stark eingeschränkte Alternative dar, kann aber bei bewegten Geräten und

den Kosten punkten. MKD bietet außergewöhnlich hohe Schlüsselkapazitäten, die zur Verschlüsselung auch ein One-Time-Pad ermöglichen, und robuste Betriebsbedingungen bei sehr geringen Kosten, erfordert dafür jedoch etablierte logistische Prozesse und klare organisatorische Verantwortlichkeiten.

Für eine übergreifende Einordnung ist schließlich entscheidend, dass sich die Technologien nicht nur in Leistungsparametern unterscheiden, sondern in ihrem grundlegenden Systemverständnis. Während QKD-Ansätze und RKD die Sicherheit primär als Eigenschaft eines laufenden physikalischen Übertragungsprozesses begreifen, behandelt MKD die Sicherheit als das Ergebnis kontrollierter physischer und organisatorischer Abläufe. Diese strukturellen Unterschiede prägen alle weiteren Aspekte, von den Kosten über die Skalierbarkeit bis hin zu den Angriffsflächen, und bilden den Rahmen für die nachfolgende Verdichtung der zentralen Erkenntnisse.

1.2.5 Verdichtete Kernaussagen

Der Vergleich der betrachteten Technologien zeigt, dass physikalische Verfahren zur Schlüsselbereitstellung kein einheitliches Lösungsfeld bilden, sondern unterschiedliche sicherheitstechnische und organisatorische Konzepte repräsentieren. Eine zentrale, gesicherte Erkenntnis, dass sich die Leistungsfähigkeit, die betrieblichen Anforderungen und die Sicherheitsannahmen der Verfahren stark unterscheiden und nicht ohne Kontext miteinander vergleichbar sind. Aussagen über „Überlegenheit“ oder „Unterlegenheit“ einzelner Ansätze sind daher nur bezogen auf konkrete Einsatzbedingungen sinnvoll.

Für quantenbasierte Verfahren gilt, dass sie unter realistischen Betriebsbedingungen nur begrenzte Schlüsselraten erzielen und empfindlich auf Distanz, Dämpfung und Umweltbedingungen reagieren. Diese Einschränkungen sind physikalisch bedingt und unabhängig von einzelnen Implementierungen. Gleichzeitig sind Aufbau und Betrieb technisch anspruchsvoll und mit erheblichen Investitions- und Betriebskosten verbunden. Als gesichert kann gelten, dass QKD-Lösungen derzeit nur in klar abgegrenzten Szenarien mit kontrollierbarer Infrastruktur praktikabel sind.

RKD stellt einen Ansatz mit geringer technischer Komplexität dar, dessen Leistungsfähigkeit jedoch durch sehr niedrige Schlüsselraten und Entfernungen begrenzt ist. Gesichert ist, dass RKD für Anwendungen mit hohem Schlüsselbedarf oder größere Entfernungen nicht geeignet ist und für bewegte Geräte (Fahrzeuge, Drohnen, bewegte IoT-Geräte etc.) gut geeignet ist. Offen bleibt hingegen, inwieweit RKD in spezialisierten Nischen durch Kombination mit anderen Verfahren einen ergänzenden Nutzen entfalten kann.

MKD unterscheidet sich grundlegend von allen übertragungsgestützten Ansätzen. Gesichert ist, dass durch die physische Verteilung großer Mengen von Schlüsselmaterial effektiv sehr hohe Schlüsselkapazitäten erreicht werden können, die die Größenordnungen optischer Verfahren weit übersteigen. Ebenso gesichert ist, dass sich die zentralen Sicherheitsannahmen und Risiken hierbei in den organisatorischen und logistischen Bereich verlagern und die Kosten gering sind. Offen bleibt, in welchem Maß bestehende Organisationen diese Prozesse zuverlässig integrieren können.

Übergreifend zeigt sich als gesicherte Erkenntnis, dass theoretische Sicherheitsmodelle allein keine hinreichende Grundlage für Beschaffungsentscheidungen darstellen.

Entscheidend sind vielmehr die praktisch wirksamen Annahmen, die systemischen Risiken und die organisatorische Beherrschbarkeit im realen Betrieb. Offene Punkte betreffen insbesondere die zukünftige technologische Entwicklung, mögliche Standardisierungsfortschritte sowie die Frage, wie unterschiedliche Verfahren sinnvoll kombiniert werden können. Die vorliegenden Ergebnisse bieten damit eine belastbare Grundlage für informierte Entscheidungen, ersetzen jedoch keine kontextbezogene Bewertung des jeweiligen Einsatzszenarios.

1.3 Vergleich nach Leistungskriterien der Praxis

Die zentralen Themen der Studie sind einerseits eine allgemein verständliche Beschreibung der Technologien und Verfahren der physikalischen Kryptografie inklusive Umsetzung in der Praxis und andererseits ein technologieneutraler, herstellerunabhängiger und objektiver Vergleich der verschiedenen Technologien und Verfahren nach Leistungskriterien der Praxis.

Bei den Leistungskriterien der Praxis handelt es sich um die Marktreife, Distanz (Abstand zwischen den Kommunikationspartnern), Schlüsselrate (bei QKD abhängig von verschiedenen Distanzen), Kosten, Robustheit / Störungsanfälligkeit, IT-Sicherheit (Man-in-the-middle Angriffe, Seitenkanalangriffe etc.), Eignung für bewegte Endgeräte und Standardisierung. Für den Leistungsvergleich der verschiedenen Technologien und Verfahren wurden drei Methoden verwendet:

1. Sicht der Technologie und Verfahren: was ist mit dem aktuellen Stand der Technik möglich etc.?
2. Sicht der Anbieter von realen Produkten des Marktes
3. Sicht von Dritten, die als Anwender von realen Produkten des Marktes fungieren

Die oben angegebenen Leistungskriterien lassen sich mit diesen drei Methoden verschieden gut und objektiv, d.h. wertfrei und unvoreingenommen, vergleichen. Z.B. lassen sich Distanz und Schlüsselrate durch alle drei Methoden vergleichen, die besten Ergebnisse kommen aber von Methode 3 (Anwender). Für die Kosten, Robustheit und Marktreife ist ebenfalls die Methode 3 am geeignetsten. Demgegenüber eignet sich für die IT-Sicherheit und Eignung für bewegte Endgeräte am besten die Methode 1.

Für die Methode 1 haben wir ausführlich den Stand der Technik untersucht und daraus den Vergleich durchgeführt. Für die Methode 2 haben wir Anbieter von realen Produkten befragt bzw. im Internet recherchiert. Die Ergebnisse von Methode 2 waren zum Teil mit Vorsicht zu verwenden, weil es sich dabei oftmals um Marketingaussagen bzw. Tests in Laborumgebungen gehandelt hat. In der Studie wurden aber die Ergebnisse aus Methode 2 und 3 immer gemeinsam angegeben, sodass beide Betrachtungsseiten sichtbar wurden. Für die Methode 3 haben wir Anwender von realen Produkten befragt. Dies war aber für einige Technologien und Verfahren sehr schwierig, weil entweder nur wenige Anwender existieren bzw. die Anwender keine ausreichend wissenschaftlich fundierten Analysen nach diesen Leistungskriterien durchgeführt haben und wenn doch die Ergebnisse nicht freigeben.

Für QKD haben wir bei der Methode 3 die in der Studie angegebenen Ergebnisse von der AIT (Austrian Institut of Technology) bekommen. Das AIT hat sieben verschiedene Produkte vom Markt beschafft und als Anwender in verschiedenen Praxisumgebungen ausführlich und

objektiv getestet. Durch die große Anzahl an verschiedenen Produkten und damit Technologien und Verfahren, konnte das AIT relativ gut die verschiedenen Produkte nach einigen Leistungskriterien dieser Studie technologieneutral und objektiv in Praxisumgebungen vergleichen.

Für RKD und MKD haben wir bei der Methode 3 die in der Studie angegebenen Ergebnisse vom Institut für IT-Sicherheitsforschung der USTP (University of Applied Sciences St. Pölten) erhalten.

1.4 Entstehung der Studie

Die Studie wurde an der Hochschule für angewandte Wissenschaften St. Pölten durchgeführt und vom österreichischen Bundesministerium für Finanzen (BMF) im Sicherheitsforschungs-Förderprogramm KIRAS/K-Pass der österreichischen Forschungsförderungsgesellschaft FFG finanziert. Bedarfsträger waren das österreichische Bundeskanzleramt und das Bundesministerium für Landesverteidigung (BMLV).

Die Studienautoren sind Univ.-Doz. Dipl.-Ing. Dr. Ernst Piller und Dipl.-Ing. Hubert Schölnast, beide vom Institut für IT-Sicherheitsforschung der Hochschule St. Pölten.

Die Studie wurde vom 1.10.2024 bis 23.12.2025 erstellt. Die schriftliche Ausfertigung der Studie in deutscher Sprache ist seit 23.12.2025 verfügbar, wegen der Buchveröffentlichung aber vertraulich. Eine englische Version ist als Buch mit dem Titel „Data Encryption at the Intersection of Mathematics and Physics – Comparing Physical Methods of Cryptography" im Springer Nature Verlag erschienen (siehe https://link.springer.com/book/9783032247636). Weitere Studienteile, die nicht im Buch veröffentlicht wurden, sind auf der website https://cryptography.study/phys veröffentlicht.

Die Autoren der Studie bedanken sich vor allem bei Dr. Simon Tjoa und Jakob Heigl-Auer, BSc (Hochschule St. Pölten), Dipl.-Ing. Gerald Trost, BSc (Bundeskanzleramt), Dr. Ralf Hammer und Mag. Lukas Siebeneicher (Bundesministerium für Finanzen), Florian Kutschera (AIT) und der FFG für die Unterstützung.

Die Studie basiert auf dem Stand der Technik, umfangreichen Recherchen insbesondere mit Anbietern und Anwendern von QKD-, RKD- und MKD-Produkten, mehreren Masterarbeiten und den Ergebnissen mehrerer Projekte, die von der FFG gefördert wurden und für die Kapitel RKD und MKD sehr wichtig waren. Dazu gehören die Projekte „Hochsichere, langzeitige Kryptografie für kabellose Kommunikation mit Integration von Funkmessdaten" (FFG KIRAS), „RKD - Lösung für die Erzeugung und Verteilung von kryptografischen Schlüsseln auf Basis von Funkkanaleigenschaften" (FFG KIRAS/K-Pass AKUT), Secret Key Generation for Low Power Wide Area Networks" (FFG Bridge 1) und „LISA" (FFG Basisförderung). Auch im Rahmen der Studie erfolgten eigene Tests von Technologien und Produkten des Marktes nach den angegebenen Leistungskriterien.

Die gesamten Inhalte der Studie befinden sich im Buch „Data Encryption at the Intersection of Mathematics and Physics – Comparing Physical Methods of Cryptography", siehe https://link.springer.com/book/9783032247636 und auf der website https://cryptography.study/phys.