Sichere Kommunikation durch Quantenschlüsselverteilung (QKD)

Abhörsichere Kommunikation ist in der aktuellen geopolitischen Lage wichtiger denn je. Längerfristig ist mit Entschlüsselungsversuchen durch Quantencomputer zu rechnen. Welche technischen Schutzvorkehrungen gibt es hierzu? Wie aufwendig ist der Einsatz entsprechender Maßnahmen für die einzelne Organisation und wer hilft bei der Umsetzung?

Keine Angst vor Quantentechnologien!

Die Informationstechnische Gesellschaft (ITG) im VDE hat bereits frühzeitig[1] auf die Möglichkeiten der Quantentechnologie hingewiesen, welche die Zukunft der Kommunikation und Verschlüsselung prägen werden. Auch in der Normung wird das Thema bereits diskutiert, bei ETSI, ITU-T, CEN/CLC/JTC 22 aber auch auf IEC- und ISO-Ebene.[2]

Quantenkommunikation ist eine Technologie auf Basis quantenphysikalischer Effekte, welche Kommunikations- und Informationsnetze sicher und effizient machen soll.[3] Ein wichtiges Verfahren ist hierbei die sog. *Quantenschlüsselverteilung* (*QKD - Quantum Key Distribution*). QKD-Protokolle sind – zumindest theoretisch – sowohl gegenüber zu erwartenden Quantencomputern als auch im Falle eines zukünftigen algorithmischen Durchbruches sicher. Sie behaupten insbesondere, sicher zu sein gegen das Szenario eines *store now – decrypt later* (*jetzt speichern - später entschlüsseln*).[4]

Die sog. *Post-Quanten-Kryptographie* (*Quantum Safe Cryptography*) dagegen basiert nicht(!) auf quantenphysikalischen Effekten und nutzt stattdessen spezielle Verschlüsselungsalgorithmen, die – so die Hoffnung – auch von leistungsfähigen Quantencomputern nicht entschlüsselt werden können.

Wo stehen wir technisch bei der Quantenkommunikation insb. bei QKD?[5]

Der Reifegrad der unterschiedlichen Ansätze ist dadurch zu bestimmen, inwiefern funktionierende Systeme bereits aufgebaut und demonstriert werden können. Die Überführung dieser in breite Anwendungen heutiger Kommunikationssysteme ist eine weitere Herausforderung.

Funktionierende QKD-Systeme sind bereits heute auf dem Markt verfügbar und können in bestehende Infrastrukturen integriert werden. Hierbei liefern die QKD-Systeme sichere Schlüssel, welche dann in klassische Verschlüsselungssysteme mit einer in der ETSI Standardisierungs-Gruppe standardisierten Schnittstelle eingespeist werden können.

Es ist allerdings wichtig zu verstehen, in welchen Punkten sich QKD-Systeme von bisherigen kryptographischen Ansätzen unterscheiden. Im Folgenden werden die wichtigsten Punkte diskutiert.

Die Schlüsselrate hängt von den optischen Verlusten ab und sinkt irgendwann auf Null: QKD-Systeme versenden Licht mit quantenmechanischen Eigenschaften von A nach B, entweder über Glasfaser oder über eine Sichtverbindung. Die übliche Menge an Licht ist dabei im Regelfall sehr gering, also in der Größenordnung weniger Photonen.

Durch Verluste in der Glasfaser oder durch Strahlaufweitung in der Atmosphäre, bleiben irgendwann so gut wie keine Photonen mehr übrig, was sich auf die Schlüsselrate auswirkt, welche dann allmählich auf Null sinkt.

Insofern sind QKD-Systeme, bestehend aus einem Sender und einem Empfänger, erstmal nur für Punkt-zu-Punkt-Verbindungen geeignet. Übliche Distanzen sind ca. 100 km Glasfaser, bzw. 20 dB Verlust. Im Bereich von satellitenbasierter QKD kann man mit speziellen Technologien die Reichweite bis ca. 50 dB erhöhen und damit den Low Earth Orbit erreichen.

QKD Punkt-zu-Punkt Verbindungen können durch „Trusted Nodes“ überbrückt werden:

Sollte es nun drei Knotenpunkte A, B und C geben, wobei A und C jeweils eine sichere Ende-zu-Ende Verbindung benötigen, ist ein sog. „Trusted Node“-Ansatz das Mittel der Wahl. Zur Illustration des Prinzips: A denkt sich eine Zufallszahl Z aus, schickt diese verschlüsselt nach B mit dem QKD-Schlüssel zwischen A und B. B kann diese dann mit demselben Prinzip an C schicken. So halten A und C am Ende die gleiche Zufallszahl Z, welche dann als sicherer Schlüssel verwendet werden kann. Die Prämisse ist, dass B ein gesicherter Knoten („Trusted Node“) ist, welcher die Zufallszahl ebenfalls kennt. Solche Ansätze sind dann praktisch, wenn es sich bei A, B und C jeweils z.B. um Firmenstandorte handelt, in denen ohnehin bereits unverschlüsselter Klartext vorliegt. In der Praxis übernehmen sog. „Key Management Systeme“ die Schlüsselweiterleitung und damit die Vernetzung zu beliebigen Topologien, wie z.B. einem vermaschten Netz. In der Grundlagenforschung wird noch an sog. *Quantenrepeatern* gearbeitet, welche heutige Trusted Nodes durch Untrusted Nodes ersetzen würden. Der Einsatz dieser Technologie ist allerdings noch mehrere Jahre entfernt.

QKD-Systeme benötigen üblicherweise eine dedizierte, dunkle Glasfaser:

Da optische Signale bereits vorhandener Telekommunikationsgeräte die Quantenzustände der QKD-Systeme stören, werden QKD-Systeme üblicherweise auf einer dunklen Glasfaser betrieben, auf der sonst keine weiteren Signale vorliegen. Dies wirkt sich auf die Gesamtnutzungskosten aus, da dunkle Glasfaser teuer ist. Verschiedene QKD-Hersteller arbeiten daran, einen Betrieb neben Telekommunikationssignalen im sog. *wavelength division multiplexing* zu ermöglichen. Die Schlüsselrate der QKD-Systeme hängt jedoch von der Kanalbelegung und den vorhandenen optischen Leistungen ab und muss im Einzelfall bestimmt werden.

Die Sicherheit der QKD-Systeme beruht auf wissenschaftlichen Publikationen und der Sicherheitsgarantie der Hersteller:

QKD-Systemhersteller bieten QKD-Systeme unter der Prämisse an, dass die QKD-Protokolle im Sinne des dahinterliegenden, meist aus der QKD-Forschung stammenden, Sicherheitsbeweises korrekt implementiert sind. Trotz der guten wissenschaftlichen Qualifikation entsprechender Firmen, ist eine solche Vorgehensweise auf Dauer nicht sinnvoll. In Europa wird deswegen an einer Sicherheitszertifizierung der QKD-Systeme gearbeitet, welche sich der Methodik des ISO-Standards „Common Criteria“ bedient. Externe Prüflabore sollen in Zukunft sicherstellen, dass der QKD-Sicherheitsbeweis mit der Implementierung im Einklang ist und in Zusammenarbeit mit nationalen Sicherheitsbehörden ein entsprechendes Sicherheitsniveau unterstützt.

QKD-Systeme sind noch nicht kostengünstig genug für einen großflächigen Einsatz:
Für einen Einsatz zur Netzintegration zum Zweck eines *proof of concepts* oder in kleinen Anwendungsszenarien sind QKD-Systeme erschwinglich genug. Für einen Netzausbau im großen Stil sind die Kosten potenziell noch zu hoch. Verschiedene QKD-Hersteller arbeiten an der Miniaturisierung, z.B. durch photonische Chipintegration und an skalierbaren Produktionsstätten um zukünftige Kosten zu reduzieren.

Zusammenfassung:
Es ist wichtig, sich frühzeitig mit dem Thema der quantensicheren Kryptographie zu befassen und ein Bewußtsein zu entwickeln, ob derzeit eingesetzte Lösungen sicher genug sind oder ob eine schnelle Umstellung auf algorithmische Lösungen (*Post-Quanten-Kryptographie*) notwendig ist. Der Einsatz von QKD muss im Zusammenspiel zwischen QKD-Herstellern und Anwendern weiter evaluiert werden und kann heute schon hybrid integriert werden.

Abhörsichere Kommunikation – der VDE unterstützt bei der Umsetzung

Expertinnen und Experten der ITG sind in den Bereichen Quantentechnologie und Quantenschlüsselverteilung auf dem neuesten Stand und speisen ihr Know-how in das CERT@VDE, die Normung und das VDE Prüfinstitut ein. Diese Entitäten des VDE unterstützen Unternehmen und Organisationen bei Sicherheitsanalysen und beim Umstieg auf quantensichere kryptographische Verfahren durch Schulung und Beratung.

Die ITG bündelt damit die Expertise aus universitärer und außeruniversitärer Forschung sowie der Industrie in den unterschiedlichen Fachbereichen, um den Erkenntnistransfer aus der Grundlagenforschung in die Anwendung zu überführen. So finden ausgewählte Ergebnisse aus Forschungsförderprojekten ihren Weg in Systeme und gesellschaftlichen Nutzen. So auch das Forschungsprojekt mit dem Titel *DemoQuanDT* bei dem über lange Strecken QKD Verbindung mit 18 Trusted Nodes zwischen Berlin und Bonn (ca. 900 km) experimentell in einer praktischen Umgebung untersucht werden. Hier geht die Expertise aus Akademia und Industrie Hand-in-Hand, da die Partner ADVA Network Security GmbH, Deutsche Telekom Technik GmbH, Rohde & Schwarz Cybersecurity GmbH, Technische Universität Darmstadt, Hochschule Darmstadt und KEEQuant GmbH an diesem praktischen Experiment zusammenarbeiten.[6]

Neben der Weiterentwicklung, Standardisierung und Zertifizierung der Technologie und ihrer Komponenten ist vor allem die Sensibilisierung für IT-Sicherheitsrisiken bei Anwendern aus Industrie, Behörden und Gesellschaft eine Herausforderung, die es jetzt gemeinsam anzugehen gilt.

---

[1] ITG NEWS 3/2021, S. 4-11 sowie TAE/ITG Kolloquium Quantentechnologie vom 7.-9. Okt. 2019 in Esslingen.

[2] via ISO/IEC JTC 1/ Subkomitee 27 (mit ISO/IEC 27000 zu Cybersecurity) und IEC TC57WG15 Data and Communication Security, IEC 62351.

[3] Bassoli, R. et al. (2023). Quantenkommunikationsnetze. SpringerVieweg Verlag.

[4] BSI et al. (2024). Position Paper on Quantum Key Distribution. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.pdf?__blob=publicationFile&v=4 (letzter Zugriff: 06.12.2024)

[5] Imran Khan (2024) – Managing Director und Co-Founder KEEQuant GmbH.

[6] DemoQuanDT, Quantenschlüsselaustausch im deutschen Telekommunikationsnetz für höhere IT-Sicherheit, https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/demoquandt (letzter Zugriff: 06.12.2024)

Dr. Damian Dudek & Dr. Matthias Wirth

VDE Verband der Elektrotechnik
Elektronik Informationstechnik e.V.
Merianstraße 28
63069 Offenbach am Main
Tel. +49 69 6308-360
damian.dudek@vde.com
matthias.wirth@vde.com