

Quantensichere Kommunikation

Sammlung praxisnaher Anwendungsfälle

bitkom

Ausgangslage

Der rasante Fortschritt im Quantencomputing stellt eine wachsende Herausforderung für heutige kryptografische Verfahren dar. Leistungsfähige Quantencomputer könnten in naher Zukunft in der Lage sein, gängige Verschlüsselungen zu brechen und dadurch sensible Daten offenzulegen. Das BSI prognostiziert ab 2030 einen sogenannten Q-Day, an dem solche Quantencomputer einsatzbereit sein könnten. Ab diesem Zeitpunkt steigt das Risiko gebrochener Verschlüsselungen erheblich, was die Sicherheit vertraulicher Daten massiv gefährden würde. Bereits heute droht das Szenario »Harvest now, decrypt later«: Daten, die aktuell abgefangen werden, könnten in Zukunft von Quantencomputern entschlüsselt werden. Vor diesem Hintergrund ist es für Unternehmen und Organisationen entscheidend, frühzeitig auf quantensichere Verfahren umzusteigen, um die Integrität, Vertraulichkeit und langfristige Sicherheit ihrer Daten zu gewährleisten.

Die Wirtschaftsschutzstudie 2026 verdeutlicht, wie real und dringlich diese Bedrohung bereits ist: Cyberangriffe verursachten einen wirtschaftlichen Schaden von 160,4 bis 205,8 Milliarden Euro in der deutschen Wirtschaft. Zwei Drittel der deutschen Unternehmen rechnen damit, dass die Anzahl der Cyberattacken in den nächsten 12 Monaten stark oder eher zunehmen wird. Diese Zahlen machen deutlich, dass Cyberbedrohungen sowohl in der Gegenwart als auch mit Blick auf die zukünftigen Risiken durch Quantencomputing ernst genommen werden müssen.

58%

der Unternehmen haben in den vergangenen zwölf Monaten einen Schaden durch Cyberangriffe erlitten (Bitkom, 2026).

Um Unternehmen und Organisationen bei diesem Transformationsprozess zu unterstützen, wurde als Ergänzung zum Bitkom-Leitfaden »Quantensichere Kommunikation – ein Leitfaden für Organisationen« eine Sammlung praxisnaher Anwendungsbeispiele zusammengestellt. Sie zeigt exemplarisch einige der Lösungsansätze und Erfahrungen von Unternehmen aus dem Bereich ITK, sodass andere Unternehmen und Behörden nachvollziehen können, wie der Umstieg auf quantensichere Verfahren in der Praxis gelingen kann. Die Sammlung dient damit sowohl als Orientierungshilfe als auch als Impulsgeber, um den Einstieg in quantensichere Kommunikation systematisch, realistisch und zeitgerecht zu planen und so die eigene Cyberresilienz nachhaltig zu stärken. Die hier vorgestellten Lösungsansätze und Technologien stellen jedoch lediglich eine Auswahl ohne Anspruch auf Vollständigkeit der Möglichkeiten dar, sind also insbesondere nicht abschließend und auch nicht dahingehend ausgewählt, dass ein nicht genannter Lösungsansatz nicht erfolgsversprechend ist. Insofern sich Unternehmen oder eine Forschungseinrichtung mit Erfahrungsberichten an der Weiterentwicklung dieses Leitfadens und der quantensicheren Kommunikation beteiligen wollen, wird dieser Input gerne anonymisiert innerhalb dieses Leitfadens veröffentlicht.

Inhalt

1 Hybride QKD-PQC-Kommunikation für kritische Infrastrukturen 5

Ausgangslage 5

Technische Lösung 5

Ergebnis 6

2 Hybrides Quanten-Schlüsselnetzwerk 8

Hintergrund und Motivation 8

Technische Lösung 8

Ergebnis 9

3 Live-Quantenverschlüsselung in einem Glasfasernetz 10

Hintergrund und Motivation 10

Technische Lösung 10

Ergebnis 10

4 Nationales quantensicheres Netzwerk in Südostasien 12

Ausgangslage 12

Technische Lösung 12

Ergebnis 12

5 PQC-erweiterte Hochsicherheitskomponenten 14

Hintergrund und Motivation 14

Technische Lösung 14

Ergebnis 15

6 PQC in der Rechenzentrums-kommunikation 16

Hintergrund und Motivation 16

Technische Lösung 16

Ergebnis 17

7 QKD im Einsatz als Live-Netzwerk 18

Hintergrund und Motivation 18

Technische Lösung 18

Ergebnis 18

8 QKD in einem Telekommunikationsnetz 20

Hintergrund und Motivation 20

Technische Lösung 20

Ergebnis 20

9 Quantensicherer optischer Transport 22

Hintergrund und Motivation 22

Technische Lösung 22

Ergebnis 22

10 Migration auf quantensichere Authentifizierung in TLS 24

Hintergrund und Motivation 24

Technische Lösung 24

Ergebnis 25

1 Hybride QKD-PQC-Kommunikation für kritische Infrastrukturen

Ein regionaler Verteilnetzbetreiber setzt mit QKD auf Out-of-Band-Schlüsselverteilung, um zukunftssichere Kommunikation zu ermöglichen, ohne dabei die hohe Verfügbarkeit der Datenkommunikation zu gefährden.

Ausgangslage

Für Betreiber kritischer Infrastruktur ist Resilienz und langfristige Verfügbarkeit von essenzieller Bedeutung. Die Realisierung einer notwendigen quantensicheren Kommunikation mit einer Vielzahl an Unbekannten steht in einem Gegensatz zu einer auf lange Sicht angelegten Planungssicherheit. Vertraulichkeit wird zudem ein immer wichtiger Faktor für die kritische Infrastruktur, um z. B. schleichende und von langer Hand geplante Hackerangriffe zu verhindern. Ein Netzbetreiber in Europa hat sich daher zum Ziel gesetzt, die essenziellen Kommunikationsstrecken zwischen den Kontrollräumen unter Einsatz von Quantenschlüsselverteilung (QKD) auf zukunftsfähige Weise abzusichern.

Technische Lösung

QKD wird auf der Strecke zwischen den beiden Kontrollräumen eingesetzt, die mehrere Dutzend Kilometer voneinander entfernt sind. Die Schlüsselverteilung erfolgt über eine dedizierte Glasfaser des internen Glasfasernetzes. Die QKD-Terminals der Punkt-zu-Punkt-Verbindung befinden sich in den Serverräumen der Kontrollräume.

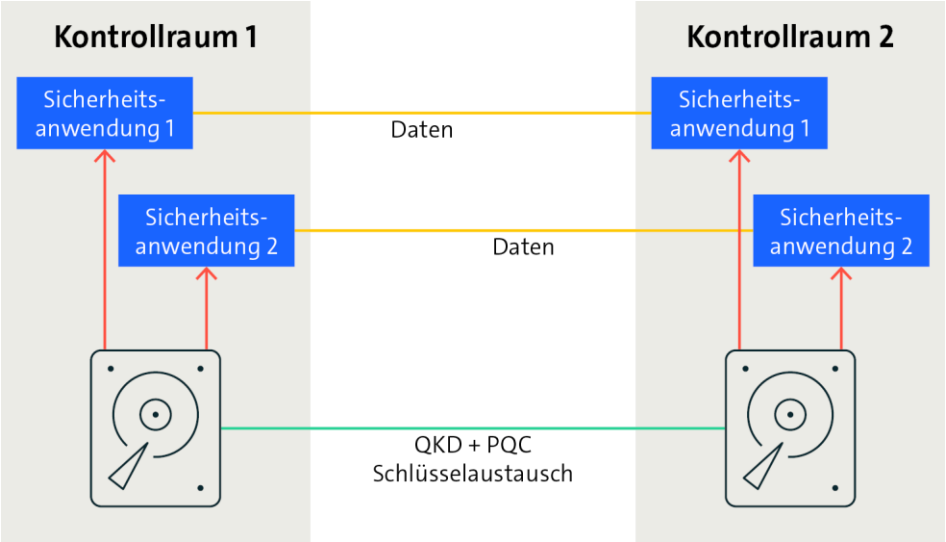


Abbildung 1: Quantensichere Schlüssel werden mittels hybriden Verfahrens (QKD und PQC) out-of-band zwischen den Kontrollräumen ausgetauscht und zwei Sicherheitsanwendungen auf lokale API-Aufrufe (rote Pfeile) zur Verfügung gestellt. Die ausgetauschten Daten können so zukunftssicher verschlüsselt werden.

Die gesamte Out-of-Band-Lösung besteht aus dem QKD-Link und einer zusätzlichen Verschlüsselung mittels Post-Quantum Kryptographie (PQC: ML-KEM). Die an die Anwendungen ausgegeben Schlüssel sind das Produkt eines sogenannten hybriden Verfahrens, dass zwei Schlüsselaustausch-Mechanismen (QKD + PQC) vereint. Die QKD-Terminals liefern diese quantensicheren Schlüssel lokal als Antwort auf authentifizierte API-Aufrufe an die Verschlüsselungsgeräte und andere Anwendungen (). Der QKD-Link versorgt mehrere Anwendungen parallel, z. B. eine Layer-1-Verschlüsselung und das SCADA-System.

Ergebnis

Der Netzbetreiber hat für die verwendeten Netzwerkverschlüsseler und andere Sicherheitsanwendungen zusätzlich zur bestehenden In-Band-Schlüsselverteilung der vorhandenen Sicherheitsanwendungen eine QKD-basierte quantensichere Kommunikation auf der Hauptstrecke seines Netzes eingerichtet. Der QKD-Link generiert und verteilt Schlüssel mit hoher Rate, die weit über den Anforderungen von Sicherheitsanwendungen liegt.

Die Out-of-Band-Schlüsselverteilung ermöglicht ein hohes Maß an Defense in Depth und »Crypto-Agility« durch die hybride Verwendung von QKD und PQC. Die Entkopplung von Datenkommunikation und Schlüsselverteilung erhöht die Ausfallsicherheit und Verfügbarkeit der Datenschicht.

Diese Punkt-zu-Punkt-Verbindung ist skalierbar und kann zu einem flächendeckenden QKD-Netz ausgebaut werden. Dank standardisierter Schnittstellen ist die Kombination unterschiedlicher QKD- und Schlüsselverteilungslösungen verschiedener Hersteller grundsätzlich möglich.

Tabellarischer Kurzsteckbrief

Marktstatus	Kommerziell verfügbar
Branchenanwendung	Kritische Infrastruktur
Technologie	Kombination aus Punkt-zu-Punkt QKD-Verbindungen und Ende-zu-Ende PQC-Verschlüsselung und -Authentifizierung.

2 Hybrides Quanten-Schlüsselnetzwerk

Ein Forschungsnetzwerk zur Verteilung quantensicherer Schlüssel in Metro-Netzen.

Hintergrund und Motivation

Das Netzwerk zur Verteilung quantensicherer kryptographischer Schlüssel in Metro-Netzen ist ein Ergebnis der Kollaboration zwischen einer deutschen Universität und einem Telekommunikationsanbieter. Es ist in erster Linie ein Forschungsnetz, das möglichst praxisnah an realer Infrastruktur implementiert werden soll. Perspektivisch ist geplant, dieses Netzwerk als Proof-of-Concept für interessierte Unternehmen in einem regionalen Umfeld weiter zu erproben.

Technische Lösung

Das Netzwerk ist ein Modell für ein hybrides Access-Netzwerk, welches mehrere Methoden zur Verteilung quantensicherer Schlüssel kombiniert: QKD, PQC und traditionelle Algorithmen. Diese Methoden werden unabhängig voneinander verwaltet und verwendet, können jedoch anschließend krypto-agil miteinander kombiniert werden.

Die Hardware für das QKD-Netzwerk ist eine Eigenentwicklung der Universität. Das verwendete QKD-Protokoll ist ein verschränkungsbasiertes QKD-Protokoll mit sternförmiger Topologie, das eine sternförmige Topologie mit einer Qubit-Quelle in der Mitte und einer großen Zahl von Empfängern in der Umgebung erlaubt. Die Phasen- und Zeitkodierung macht das Protokoll robust gegenüber Umwelteinflüssen, und ein Wavelength-Selective Switch (WSS) erlaubt eine dynamische Schaltung der Kanäle zwischen verschiedenen Nutzern, um einen zeitlich variierenden Schlüsselbedarf flexibel abzubilden.

Der Key-Management-Layer und Netzwerk-Controller werden im Projektumfeld entwickelt. Das Schlüsselmanagementsystem beinhaltet Softwarekomponenten für das Aushandeln traditioneller und PQC-Schlüssel sowie deren Hybridisierung, z. B. mit einer Schlüsselableitungsfunktion. Dabei werden Open-Source PQC Bibliotheken verwendet.

Ergebnis

Die Ergebnisse der Forschungskollaboration, insbesondere auf der Quantenebene, wurden bereits in mehreren wissenschaftlichen Publikationen vorgestellt. Weitere Publikationen, u. a. zur Schlüsselhybridisierung, sind derzeit in Vorbereitung.

Tabellarischer Kurzsteckbrief

Marktstatus	Forschungsphase
Branchenanwendung	Das System ist applikationsagnostisch und kann daher flexibel eingesetzt werden.
Technologie	Hybrider Schlüsselaustausch kombiniert QKD, PQC und traditionelle Algorithmen.

3 Live-Quantenverschlüsselung in einem Glasfasernetz

Live-Quantenverschlüsselung in einer realen Telekommunikationsinfrastruktur im Datacenterumfeld.

Hintergrund und Motivation

Herkömmliche Verschlüsselungsverfahren stoßen angesichts fortschreitender Rechenkapazitäten und Quantencomputern an ihre Grenzen. Kritische Infrastrukturen und sensible Datenkommunikation benötigen abhörsichere Übertragungswege, die auch gegen zukünftige Angriffsmethoden geschützt sind. Bislang war Quantenkryptografie hauptsächlich auf Laborumgebungen beschränkt und noch nicht für den praktischen Einsatz in bestehenden Netzinfrastrukturen erprobt. Ein QKD-Anbieter demonstrierte gemeinsam mit einem Telekommunikationsdienstleister und Netzbetreiber erstmals in Deutschland die praktische Anwendung von Quantenverschlüsselung in einer realen Telekommunikationsinfrastruktur.

Technische Lösung

Die implementierte Lösung basiert auf der Verteilung von verschränkten Lichtteilchen (Photonen) über das bestehende Glasfasernetz eines Telekommunikationsanbieters. Dabei werden Quantenzustände über eine 60 Kilometer lange Glasfaserverbindung zwischen zwei Standorten übertragen. Das System erzeugt digitale Schlüssel durch die quantenmechanische Messung der einzelne Lichtteilchen (Quanten) in Echtzeit und rekonfiguriert damit minütlich eine VPN-Verbindung mit neuen Quantenschlüsseln. Zur sicheren Speicherung und Verwaltung des Quantenschlüsselmaterials wird ein High Security Module (HSM) integriert, das insbesondere für kritische Infrastrukturen geeignet ist. Die Technologie nutzt verschränkte Lichtteilchen mit automatischer Angriffserkennung, da jeder Versuch, die Quantenschlüssel abzuhören, deren Quanteneigenschaften verändert und Angriffe dadurch sofort erkennbar macht.

Ergebnis

Eine Vorführung der Technologie zeigte, dass Quantenverschlüsselung über bestehende Glasfaserinfrastrukturen in einer realen Telekommunikationsumgebung erprobt und integriert werden kann. Die komplette Prozesskette von der Erzeugung verschränkter Lichtteilchen bis zur sicheren Schlüsselverwendung in VPN-Netzwerken konnte demonstriert werden.

Tabellarischer Kurzsteckbrief

Marktstatus	Pilot-/Erprobungsphase.
Branchenanwendung	RZ-Kopplung, KRITIS
Technologie	Verschränkungsbasierte Quantenschlüsselverteilung

4 Nationales quantensicheres Netzwerk in Südostasien

In Südostasien wurde die erste landesweite quantensichere Infrastruktur geschaffen, um Unternehmen vor künftigen Bedrohungen durch Quantencomputer zu schützen.

Ausgangslage

Die Initiative entstand im Rahmen eines nationalen Auftrags durch eine staatliche Digitalbehörde, mit dem Ziel, die digitale Infrastruktur des Landes gegen die wachsenden Risiken durch Quantencomputer zu wappnen. Diese Computer könnten in naher Zukunft bestehende Verschlüsselungsstandards brechen und damit sensible Daten gefährden. Ein Telekommunikationsanbieter wurde beauftragt, ein nationales quantensicheres Netzwerk zu entwickeln, um insbesondere kritische Sektoren wie Finanzwesen, Gesundheitswesen und Regierung zu schützen. Ein konkretes Beispiel ist die Zusammenarbeit mit einem Finanzinstitut zur Absicherung von sensiblen Daten mittels quantensicherer Kommunikation.

Technische Lösung

Die technische Grundlage des Netzwerks bildet die Integration von Quantum Key Distribution (QKD) und einer Netzwerk-Software, die QKD mit PQC ergänzt und so Ende-zu-Ende quantensichere Schlüssel verteilt. Das darauf aufbauende Quantum-Safe Key as-a-Service (QSK-aaS) ermöglicht den Unternehmen die Kontrolle über ihre Verschlüsselungsschlüssel, inklusive Monitoring, Incident- und Change-Management.

Ein weiteres Angebot stellt quantensichere Bandbreite zwischen Unternehmensstandorten bereit. Die Lösung lässt sich vollständig in bestehende Glasfasernetzwerke integrieren und unterstützt Verschlüsselung auf den OSI-Schichten 1 bis 3 sowie MPLS.

Ergebnis

Unternehmen aus dem Bankwesennutzen die Infrastruktur bereits aktiv zur Absicherung ihrer Kommunikation. Die quantensicheren Dienste sind landesweit über das Glasfasernetz verfügbar und lassen sich nahtlos in bestehende IT-Architekturen integrieren. Die Lösung bietet nicht nur Schutz vor zukünftigen Bedrohungen, sondern reduziert auch den operativen Aufwand für Unternehmen erheblich. Die beteiligten Unternehmen haben dazu beigetragen, die digitale Resilienz durch die Einführung eines robusten, quantensicheren Ökosystems zu stärken.

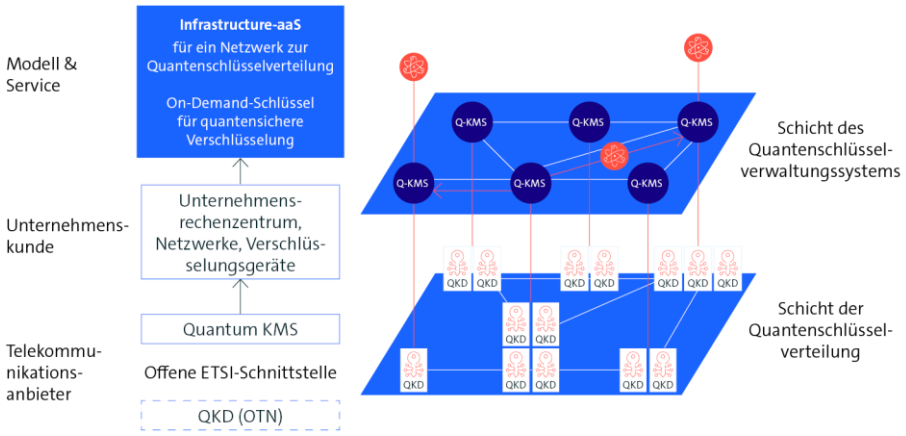


Abbildung 2: Einer der beiden QKD-basierten Dienste, die für Unternehmen angeboten werden. Mit QSK-aaS werden den Kunden quantensichere Schlüssel über eine standardisierte oder proprietäre API End-to-End zur Verfügung gestellt. Die Sicherheit wird durch QKD und PQC gewährleistet. QKD benötigt ein Optical Transport Network (Optische Faser). In diesem Modell haben die Kunden die Kontrolle über die Verwendung der Schlüssel, ohne sich um die zugrunde liegende QKD-Infrastruktur kümmern zu müssen.

Tabellarischer Kurzsteckbrief

Marktstatus	Im operativen Einsatz
Branchenanwendung	Unternehmen
Technologie	Faserbasierte Rechenzentrumskopplung mit QKD und PQC gesichert

5 PQC-erweiterte Hochsicherheitskomponenten

Ausstattung von Hochsicherheitskomponenten mit PQC, um Behörden und Bundeswehr einen quantenresistenten Schutz bis zur Geheimhaltungsstufe GEHEIM zu ermöglichen.

Hintergrund und Motivation

Zukünftige Quantencomputer stellen eine erhebliche Bedrohung für kryptografisch geschützte Daten dar. Das betrifft nicht nur die alltägliche Kommunikation im Internet, in Gefahr sind insbesondere hochsensible Daten bis hin zu Staatsgeheimnissen. Abhilfe versprechen neuartige, quantenresistente Algorithmen (PQC), die in den letzten Jahren entwickelt wurden. Heute sind bereits mehrere Netzwerk-Komponenten, die von Behörden und Bundeswehr für den Umgang mit Verschlusssachen eingesetzt werden, mit PQC ausgestattet.

Technische Lösung

Mehrere zentrale Komponenten eines Hochsicherheitsportfolios eines Sicherheitsanbieters wurden bereits mit PQC-Elementen ausgestattet, darunter Lösungen für Sprachkommunikation, VPN-Gateways und gehärtete Arbeitsplatzrechner, die eine Kombination von performanter Kryptografie und hoher Rechenleistung liefern. Die Kernkomponenten dieses Ansatzes sind ein Client (Workstation, Terminal), eine Box (Netzwerkverschlüsseler) und ein Management-System. Mit diesen drei Komponenten mit PQC lässt sich ein Schlüsselaustausch quantenresistent umsetzen. Um die Vertraulichkeit von Daten bei der Übertragung gegenüber Quantencomputern zu gewährleisten, müssen sowohl der Verschlüsselungsalgorithmus als auch das Schlüsselaustauschverfahren, das zur Ableitung des Schlüssels verwendet wird, quantenresistent sein. In der Regel ist der Verschlüsselungsalgorithmus bereits quantenresistent, wenn er mit ausreichend großen Schlüsseln verwendet wird. Die konventionellen Schlüsselaustauschverfahren sind jedoch gegenüber Quantencomputern potentiell anfällig. Das BSI empfiehlt die Verwendung so genannter Hybridverfahren: Durch die Kombination von konventioneller Kryptografie und PQC müsste ein Angreifer jeden Algorithmus brechen, um die Hybridlösung zu knacken. Die beschriebenen Komponenten unterstützen einen hybriden quantenresistenten Schlüsselaustausch mit BSI-BSI empfohlenen PQC-Algorithmen. Perspektivisch werden weitere kritischen Funktionalitäten, insbesondere Secure Boot, Software-Updates, Authentifizierung und Public-Key-Infrastrukturen (PKI), sowohl für die Stufe GEHEIM als auch für niedrigere Geheimhaltungsstufen wie VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD), mit PQC realisiert werden.

Ergebnis

Die beschriebenen Komponenten wurden vom BSI als Verschlüsselungsprodukte mit PQC für die Geheimhaltungsstufe GEHEIM zugelassen. Im europäischen Vergleich ist Deutschland damit Vorreiter bei Kryptogeräten, die bereits heute mit PQC arbeiten. Damit steht eine Generation von gehärteten Laptops, die für den Einsatz unter extremen Bedingungen konzipiert sind, für den weiteren Ausbau quantenresistenter Funktionalitäten bereit.

Tabellarischer Kurzsteckbrief

Marktstatus	Kommerziell verfügbar
Branchenanwendung	Nationale und internationale Behörden und Organisationen wie z. B. die Bundeswehr mit besonderen Sicherheitsanforderungen, die eingestufte Daten bis zum Grad GEHEIM bearbeiten.
Technologie	Die beschriebenen Komponenten unterstützen einen hybriden quantenresistenten Schlüsselaustausch mit BSI-empfohlenen PQC-Algorithmen.

6 PQC in der Rechenzentrums-kommunikation

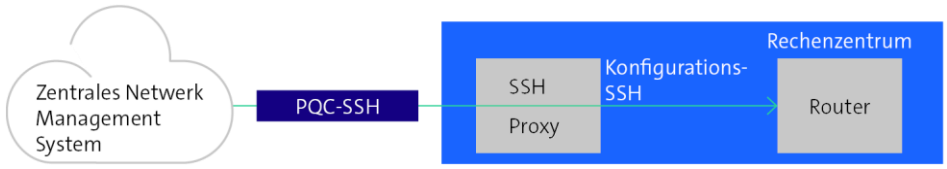
Absicherung der Verbindungen zwischen den globalen Rechenzentren einer Bank mit Post-Quantum-Kryptographie.

Hintergrund und Motivation

Quantum Key Distribution (QKD) wird häufig als nützliche Anwendung zur Absicherung der Verbindungen zwischen Rechenzentren angeführt. QKD ist allerdings in seiner Reichweite begrenzt und benötigt eine angepasste Infrastruktur. Anwender dieser Technologie aus dem Bereich des Bankwesens haben für die Vernetzung der global verteilten Rechenzentren einen Ansatz unter Verwendung von Post-Quantum-Kryptographie (PQC) gewählt, der die Verbindungen unter weitgehender Verwendung existierender Infrastruktur schützt.

Technische Lösung

Die Bank verwendet hauptsächlich MACsec (IEEE802.1AE) zur Absicherung der Kommunikation zwischen Rechenzentren. Die Verschlüsselung dieser Kommunikation verwendet AES, welcher nach allgemeinem Konsens als quantensicher eingestuft wird. Sowohl QKD-Systeme als auch die neu standardisierten PQC-Algorithmen setzen daher dort an, wo Quantencomputer zukünftig zu Sicherheitsrisiken führen können: dem Schlüsselaustausch. Zur Erzeugung des Schlüsselmaterials werden unter anderem Pre-Shared Keys verwendet. Sofern diese Pre-Shared Keys quantensicher verteilt werden können, so kann daher nach Stand der Technik die Kommunikation zwischen den Rechenzentren als quantensicher betrachtet werden. Die Konfiguration der Router in den Rechenzentren erfolgt üblicherweise mithilfe des SSH-Protokolls. OpenSSH hat bereits mit der Integration von hybriden PQC-Verfahren begonnen, wie sie auch vom BSI empfohlen werden, unter anderem unter Verwendung des Schlüsselaustausch-Verfahren MLKEM768-X25519. Diese Lösung ist auch dort einsetzbar, wo die Router selbst dieses Verfahren noch nicht unterstützen unter Verwendung eines sogenannten SSH-Proxies. Diese Komponente kann lokal im Rechenzentrum installiert werden, um dort einen quantensicheren SSH-Tunnel zu terminieren. Der Router kann nun wie bisher konfiguriert werden über das sichere Netzwerk innerhalb des Rechenzentrums. Sobald der Router quantensicheren Schlüsselaustausch unterstützt, kann durch einfache Konfigurationsanpassung die quantensichere SSH-Verbindung auch bis in den Router hinein verlängert werden.



Ergebnis

Die globalen Rechenzentren der Bank sind mit der beschriebenen Lösung ausgestattet worden und erlauben eine quantensichere Konfiguration der Router weltweit ohne Reichweitenbegrenzung oder Installation zusätzlicher Hardware oder Leitungen. Als taktische Lösung war der Aufbau der SSH-Proxies notwendig.

Tabellarischer Kurzsteckbrief

Marktstatus	Im operativen Einsatz
Branchenanwendung	Finanzsektor
Technologie	Aktuelle OpenSSH-Implementierungen mit hybriden PQC-Verfahren

7 QKD im Einsatz als Live-Netzwerk

Aufbau und Betrieb einer wirknetznahen Quantum Backbone-Verbindung

Hintergrund und Motivation

Quantenkommunikation wurde in vielen Initiativen wissenschaftlich untersucht. Es fehlte bisher jedoch die anwendungsnahe Demonstration eines Quantenkommunikationsnetzes über alle für den praktischen Betrieb notwendigen Komponenten, Systeme und Prozesse hinweg. Durch Innovationspartner aus dem Bereich Telekommunikation, Cybersicherheit und angewandter Forschung wurde in einem Pilotprojekt[1] eine vollständige QKD-Strecke mit einer Länge von 900 km aufgebaut mit dem Ziel, einen wirknetznahen Testbetrieb zu ermöglichen, der alle operationalen Aspekte eines zukünftigen Wirkeinsatzes abdeckt. Das Projekt bietet ein Modell für ein Backbone QKD Netzwerk, welches die Quantenschlüssel über mehrere Trusted Nodes vermittelt.

Technische Lösung

Die verwendete Netzarchitektur ist konform zu ITU-T Y.3802 und die verwendeten Komponenten, wie z. B. die QKD-Netzelemente und Schlüsselmanagement-Systeme, sind kommerziell verfügbare Lösungen. Für das Projekt wurden insbesondere ein Konzept für den Aufbau und Überwachung von Trusted Nodes und ein DevOps Konzept zum ferngesteuerten quantensicheren Ausrollen der Software für die Netzkomponenten entwickelt und umgesetzt.

Ergebnis

Das Hauptergebnis dieses Pilotprojekts ist die erfolgreiche Demonstration, dass die QKD-**Technologie unter praxisnahen Bedingungen in Live-Netzwerken eingesetzt werden kann**. Zusätzlich wurde die Sicherheit einzelner Komponenten und des gesamten Systems im Hinblick auf zukünftige Produkte untersucht und beurteilt.

[1] Verbundprojekt zur Erprobung von QKD in einem realen Telekommunikationsnetz

Tabellarischer Kurzsteckbrief

Marktstatus	Pilot-/Erprobungsphase
Branchenanwendung	Telekomunikation
Technologie	QKD-Geräte, Key Management Systeme, L2 und L3 Verschlüsselungssysteme, Netzmanagementsysteme und OSS (Operational Support Systems)

8 QKD in einem Telekommunikationsnetz

Verschränkungsbasierte Schlüsselübertragung in Telekommunikationsnetzen

Hintergrund und Motivation

Quantencomputer haben das Potential, künftig herkömmliche Verschlüsselungsmethoden zu knacken, insbesondere asymmetrische Verschlüsselungsverfahren, die auf mathematischen Verfahren basieren. Weiterentwickelte Quantencomputer könnten durch komplexe Berechnungen in kürzester Zeit diese etablierten Sicherheitsmechanismen überwinden. Während symmetrische Verschlüsselungsverfahren auch gegenüber Quantencomputern als sicher gelten, liegt die Herausforderung im sicheren Austausch der Schlüssel zwischen den kommunizierenden Parteien. Um die Sicherheit der Datenübertragung auch in Zukunft zu gewährleisten, werden neue quantensichere Verfahren unter dem Begriff Post Quantum Security entwickelt. Ein Telekommunikationsanbieter testete gemeinsam mit einem QKD-Anbieter eine kommerzielle verschränkungsbasierte Schlüsselübertragung für quantensichere Kommunikation in einem realen Telekommunikationsnetz. Der Proof of Concept demonstrierte die praktische Anwendbarkeit von Quantum Key Distribution (QKD) innerhalb eines lokalen Glasfasernetzes

Technische Lösung

Das getestete System nutzt Quantum Key Distribution mit verschränkten Photonenpaaren zur sicheren Schlüsselübertragung. Die Lösung basiert auf dem quantenphysikalischen Prinzip, dass jede Beobachtung eines Quantenobjekts dieses verändert. Die spezifischen Eigenschaften des Photons sind den kommunizierenden Parteien auch über große Distanzen bekannt. Versucht ein Angreifer einen Schlüssel während der Übertragung abzufangen oder eine Kopie des Photons zu erstellen, können Sender und Empfänger dies erkennen und die Kommunikation umgehend abbrechen, um ihre Daten zu schützen. Während der gesamten Testdauer wurden Photonenpaare generiert und quantensichere Schlüssel zuverlässig zwischen den beiden Empfangseinheiten über das lokale Glasfasernetz ausgetauscht.

Ergebnis

Der Test erbrachte den erfolgreichen Nachweis der Anwendbarkeit einer der ersten kommerziell verfügbaren verschränkungsbasierten QKD-Lösungen im realen

Telekommunikationsnetz. Dadurch konnte die praktische Implementierung und zuverlässige Funktion dieser Methodik in einem bestehenden Glasfasernetz demonstriert werden. Der erfolgreiche Test bildet für Telekommunikationsanbieter eine Basis zur weiteren Evaluation von Post Quantum Security Lösungen und demonstriert das Potential für eine mögliche Netzwerkintegration. Forschungsprojekte und die erfolgreiche praktische Umsetzung bestehender oder neu entwickelter Lösungsansätze sowie das Mitwirken an solchen Vorhaben ermöglichen es den beteiligten Unternehmen, die Entwicklung von Sicherheitstechnologien an vorderster Front mitzuprägen und sich auf die Herausforderungen der Post-Quantum-Ära vorzubereiten.

Tabellarischer Kurzsteckbrief

Marktstatus	Pilot-/Erprobungsphase
Branchenanwendung	Telekommunikationsnetzwerk
Technologie	Verschränkungsbasierte Quantenschlüsselverteilung

9 Quantensicherer optischer Transport

Quantensicheres optisches Transportnetz mit BSI-Zulassung für nationalen IT-Dienstleister des Bundes

Hintergrund und Motivation

Das Ziel war der Schutz eines bundesweiten Glasfasernetzes zur Anbindung von zahlreichen Standorten vor der Bedrohung durch zukünftige Quantencomputer. Aufgrund der hohen Sicherheitsanforderungen muss eine Lösung über eine BSI-Zulassung für VS-NfD verfügen. Zudem sollten möglichst alle Dienste auf dem Netz zeitnah geschützt werden – schließlich könnte selbst durch aktuell gängige Verschlüsselungsmethoden gesicherte Kommunikation, welche heute aufgezeichnet und gespeichert werden kann, bereits in wenigen Jahren mit Quantencomputern entschlüsselt werden (»Harvest now, decrypt later« attack).

Technische Lösung

Eine quantensichere Verschlüsselung auf der untersten Transportschicht (OSI-Schicht 1) per AES mit einer langen Schlüssellänge schützt alle übertragenen Daten, auch die Header von Ethernet oder IP-Paketen werden verschlüsselt. Als Schlüsselaustausch wird eine hybride Kombination von PQC und klassischem Schlüsselaustausch eingesetzt. In diesem Bereich existieren bereits passgenaue und skalierbare Lösungen eines Sicherheitsanbieters zur Verschlüsselung mit BSI-Zulassung für verschiedene Anforderungen. Die Verschlüsselung auf Schicht 1 kann durch eine zusätzliche quantensichere Verschlüsselung für einzelne Services auf höheren Schichten ergänzt werden, z. B. um Standorte ohne dedizierten Faserzugang anzubinden.

Ergebnis

Das Resultat ist eine Lösung, die hohen Datendurchsatz mit geringer Latenz und BSI-konformer Verschlüsselung kombiniert und sich damit auch für die sichere und performante Anbindung von Rechenzentren eignet. Sie ist auch kryptoagil, da alle Knoten des optischen Transportnetzes ohne Kompatibilitätsprobleme mit neuen Schlüsselaustauschalgorithmen aktualisiert werden können. Deshalb konnte im vorliegenden Anwendungsfall die Installation der Netzelemente durchgeführt werden noch bevor der finale Standard für den quantensicheren Schlüsselaustausch vorlag. Die Erweiterung mit PQC erfolgte danach einfach in einem Software-Update für die existierende Hardware.

Tabellarischer Kurzsteckbrief

Marktstatus	Kommerziell verfügbar
Branchenanwendung	Nationale Behörden, Organisationen und Dienstleister mit besonderen Sicherheitsanforderungen.
Technologie	Verschlüsselung auf der optischen Übertragungsschicht (L1), hybrider Schlüsselaustausch (PQC und klassisch)

10 Migration auf quantensichere Authentifizierung in TLS

Erprobtes Migrationsmuster für TLS 1.3 -Verbindungen in verschiedenen Praxisprojekten

Hintergrund und Motivation

TLS-Verbindungen sind zentral für die Migration zu quantensicherer Kryptografie, da sie sensible Daten mit Kunden und Partnern schützen. Die Vertraulichkeit wird in TLS über symmetrische Verschlüsselung sichergestellt, deren Schlüssel jedoch asymmetrisch ausgetauscht werden. Asymmetrische Kryptographie wird in TLS auch für andere Zwecke genutzt, etwa zur Authentifizierung des Servers (und in mutual TLS auch des Clients) über Zertifikate. Die Umstellung auf QS-Schlüsselaustauschverfahren in TLS ist dringend da der Algorithmus zwischen den Kommunikationspartnern ausgehandelt wird. Die Signaturalgorithmen werden allerdings während eines TLS-Handshakes nicht ausgehandelt. Der Server hat im Normalfall ein TLS-Zertifikat. Versteht der Client den verwendeten Signaturalgorithmus eines quantensicheren Server-Zertifikats nicht, kann er das Zertifikat nicht verifizieren und die Verbindung bricht ab. Das bedeutet, dass Clients, die keine quantensicheren Algorithmen verstehen, keine TLS-Verbindungen zu einem Server mit quantensicherem Zertifikat aufbauen können.

Technische Lösung

Die technische Lösung setzt daher an zwei Stellen des TLS-Handshakes an: beim flexibel aushandelbaren Schlüsselaustausch und bei der gezielten Auswahl geeigneter Zertifikate für Clients mit unterschiedlichem Unterstützungsstand. Da der Schlüsselaustausch im TLS-Handshake ausgehandelt wird, kann der Server nach einem Update der entsprechenden Libraries und Konfiguration quantensichere Algorithmen und hybride Kombinationen wie ML-KEM-768 oder X25519MLKEM768 während des TLS-Handshakes als Optionen anbieten und sogar bevorzugen. Unterstützt der Client diese noch nicht, bleibt mit klassischen Verfahren wie ECDH weiterhin eine Fallback-Möglichkeit bestehen, solange deren Sicherheitsniveau noch als ausreichend gilt, sodass sich das Harvest-now-decrypt-later-Risiko schrittweise reduzieren lässt. Bei Signaturen ist dies nicht automatisch möglich. Organisationen müssen entscheiden, ab wann ihre Server und TLS-Termination-Punkte (z. B. Web Application Firewalls) quantensichere Zertifikate nutzen – ab diesem Zeitpunkt sind Verbindungen mit Legacy-Clients nicht mehr möglich. Um eine schrittweise Migration zu ermöglichen, kann der Server aber so konfiguriert werden, dass er sowohl ein Legacy- als auch ein quantensicheres Zertifikat besitzt. Während des TLS-Aufbaus wird im »Client-Hello« auch die »signature_algorithms« Erweiterung geschickt. Diese beschreibt

Signaturalgorithmen, die der Client unterstützt. Auf dieser Basis kann der Server dynamisch das passende Zertifikat auswählen. So können TLS-Verbindungen quantensichere Authentifizierung nutzen, sobald der Client sie unterstützt, ohne die Abwärtskompatibilität zu verlieren.

Ergebnis

Durch die beschriebene Logik können Server und Web Application Firewalls mit quantensicheren Zertifikaten ausgestattet und gleichzeitig abwärtskompatibel Schritt für Schritt auf quantensichere Signaturen umgestellt werden. Alternativ lässt sich auch ein Proxy mit QS-Schlüsselaustausch und entsprechender Logik einsetzen, um mehrere Verbindungen abzusichern, ohne Änderungen direkt auf den Servern vorzunehmen. In Umgebungen, in denen diese Logik implementiert ist, können quantensichere und produktionsreife Zertifikate eingeführt werden, sobald sie verfügbar sind.

Tabellarischer Kurzsteckbrief

Marktstatus	Pilot-/Erprobungsphase
Branchenanwendung	Finanzindustrie
Technologie	Konzept für TLS-Migration

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner/in
Felix Kuhlenkamp | Leiter Sicherheit
T +49 30 27576-279 | f.kuhlenkamp@bitkom.org

Natalia Stolyarchuk | Bereichsleiterin Future Computing & Mikroelektronik
T +49 30 27576-187 | n.stolyarchuk@bitkom.org

Greta Lubinski | Trainee

Verantwortliches Bitkom-Gremium
AK Informationssicherheit
AK High Performance Computing & Quantum Computing

Copyright
Bitkom 2026

Diese Publikation stellt eine allgemeine unverbindliche Information dar. Die Inhalte spiegeln die Auffassung im Bitkom zum Zeitpunkt der Veröffentlichung wider. Obwohl die Informationen mit größtmöglicher Sorgfalt erstellt wurden, besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität, insbesondere kann diese Publikation nicht den besonderen Umständen des Einzelfalles Rechnung tragen. Eine Verwendung liegt daher in der eigenen Verantwortung des Lesers. Jegliche Haftung wird ausgeschlossen. Alle Rechte, auch der auszugsweisen Vervielfältigung, liegen beim Bitkom oder den jeweiligen Rechteinhabern.