bitkom

Quantensichere Kommunikation

Ein Leitfaden für Organisationen

Herausgeber
Bitkom e. V.
Albrechtstraße 10 | 10117 Berlin
Tel.: 030 27576-0 | bitkom@bitkom.org
www.bitkom.org

Ansprechpartner
Dr. Natalia Stolyarchuk | Bereichsleiterin Future Computing & Mikroelektronik
T 030 27576-187 | n.stolyarchuk@bitkom.org

Felix Kuhlenkamp | Referent Sicherheitspolitik
T 030 27576-279 | f.kuhlenkamp@bitkom.org

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

Autorinnen und Autoren
Leonie Bruckert (secunet Security Networks AG), Sven Bettendorf (TÜV Informationstechnik GmbH), Thomas Decker (JoS QUANTUM GmbH), Florian Fröwis (ID Quantique AG), Kevin Füchsel (Quantum Optics Jena GmbH), Swen Hildebrandt (Volkswagen AG), Efstathia Katsigianni (IBM Deutschland Research & Development GmbH), Felix Kuhlenkamp (Bitkom e. V.), Lukas Meinl (SVA System Vertrieb Alexander GmbH), Simon C. Müller (Telefónica Germany GmbH & Co. OHG), Oleg Nikiforov (Deutsche Telekom Technik GmbH), Natalia Stolyarchuk (Bitkom e. V.), Volker Reers (Qseidon GmbH), Manfred Rieck (Deutsche Bahn AG), Jasper Rödiger (Rohde & Schwarz GmbH & Co. KG), Johannes Schneemann (Arvato Systems GmbH), Martin Rehberg (DB Systel GmbH), Martin Winter (ISG - Information Services Group Germany GmbH).

Layout
Anna Stolz | Bitkom

Titelbild
© Tach – stock.adobe.com

Inhalt

1 Einleitung

Das Wichtigste in Kürze

In Deutschland fühlen sich 65 % der Unternehmen durch Cyberattacken in Ihrer Existenz bedroht.[1] Kryptografie stellt vor dieser Bedrohungslage und angesichts fortschreitender Digitalisierung einen unverzichtbaren Bestandteil der Informationssicherheit dar. Die schnelle Entwicklung des Quantencomputings wird in Zukunft eine fundamentale Bedrohung für kryptografische Verfahren darstellen. Mit dem Bedrohungsszenario »Harvest now, decrypt later« sind jedoch auch aktuelle Daten gefährdet, die heute gesammelt und in Zukunft mittels Quantencomputern entschlüsselt werden können.

Quantencomputer nutzen die Prinzipien der Quantenmechanik, um Berechnungen durchzuführen, die für klassische Computer nicht effizient möglich sind. Durch diese neuartigen Berechnungsmöglichkeiten ergeben sich durch die Verwendung von Quantencomputer Angriffsmöglichkeiten, die viele der heute als sicher geltenden kryptografischen Methoden in kurzer Zeit kompromittieren könnten. Dies bedroht damit die Sicherheit praktisch aller derzeit eingesetzten kryptografischer Verfahren wie Verschlüsselung bzw. Entschlüsselung und damit beinahe der gesamten kryptografischen Kommunikation weltweit.

Das BSI rechnet bereits ab dem Jahr 2030 mit einem sogenannten Q-Day, der die Einführung von leistungsfähigen Quantencomputern markiert, somit besteht ab 2030 ein Risiko gebrochener Verschlüsselungen, und damit der Verlust der Sicherheit von Daten. Angesichts dieser Entwicklungen gewinnt die quantensichere Kryptografie, die Methoden entwickelt, die auch den Fähigkeiten von Quantencomputern standhalten, zunehmend an Bedeutung. Deren Einführung wird bei vielen Organisationen jedoch viel Zeit benötigen. Um diesen Übergang sicher zu gewährleisten, ist ein frühzeitiges Planen und Handeln notwendig.

Organisationen müssen für die Risiken sensibilisiert werden, die mit der Weiterentwicklung des Quantencomputings einhergehen. Es ist wichtig, dass Organisationen frühzeitig die potenziellen Bedrohungen für ihre Systeme und Daten erkennen und die Dringlichkeit verstehen, zeitnah auf diese Entwicklungen zu reagieren. Hierzu gehört auch die Darstellung konkreter Zeithorizonte, um die Bedeutung eines rechtzeitigen Handelns zu verdeutlichen. Dadurch werden Organisationen in die Lage versetzt, ihre Sicherheitsstrategien entsprechend anzupassen, rechtzeitig quantensichere Maßnahmen zu implementieren und verschlüsselte Daten in ein neues Verfahren zu überführen.

1 Bitkom – Wirtschaftsschutzstudie 2024: ↗ https://www.bitkom.org/sites/main/files/2024-08/240828-bitkom-charts-wirtschaftsschutz-cybercrime.pdf

Darüber hinaus werden im Folgenden verschiedene technologische Ansätze für quantensichere Kryptografie vorgestellt und nach ihren Anwendungsgebieten geordnet. Ziel ist es, Unternehmen einen Überblick über die möglichen Lösungen und deren Relevanz für unterschiedliche Einsatzbereiche zu bieten. Dabei werden mögliche Transformationspfade aufgezeigt, die Unternehmen helfen sollen, die notwendigen Schritte zur Erreichung der Quantensicherheit zu identifizieren und umzusetzen.
Auch politische Akteure müssen für das Thema sensibilisiert werden. Es ist unerlässlich, politische Maßnahmen zu initiieren, um Technologien wie Quantum Key Distribution (QKD) und Post-Quantum Cryptography (PQC) zu fördern und auszubauen. Hierbei sollen politische Rahmenbedingungen geschaffen werden, die die notwendige Infrastruktur und die Implementierung quantensicherer Lösungen unterstützen.

Abschließend werden konkrete Zeitpläne für die Umsetzung der quantensicheren Transformationsmaßnahmen dargestellt, um den Organisationen klare Orientierungspunkte zu bieten. Die Zeit drängt: Quantencomputer mit entsprechenden Kapazitäten könnten in naher Zukunft verfügbar werden und werden die heutige (asymmetrische) kryptografischen Verfahren brechen können. Organisationen und politische Entscheidungsträger müssen daher bereits jetzt handeln, um die Informationssicherheit auch in einer Ära von fortgeschrittenem Quantencomputing zu gewährleisten.

Welche Sicherheitsauswirkungen birgt Quantencomputing?

Die moderne Kryptografie wird heutzutage für verschiedene Ziele eingesetzt, die durch spezifische Methoden unterstützt werden:

- **Vertraulichkeit:** Sicherstellung der Vertraulichkeit von Kommunikation (z. B. Instant-Messaging-Anwendungen) und personenbezogener Daten (Bankwesen, Gesundheitswesen) sowie auch andere sensible Informationen wie Unternehmens- und Regierungsdaten.
  - Methodenbeispiele: Symmetrische und asymmetrische Verschlüsselung.
- **Integrität:** Gewährleistung der Integrität von Dokumenten (z. B. Verträgen wie Lebensversicherungen oder Hypotheken) sowie von Software-Updates (z. B. für Fahrzeuge und Smartphones).
  - Methodenbeispiele: Digitale Signaturen, Hashfunktionen.
- **Authentifizierung:** Überprüfung der Identität von Benutzern oder Systemen, um unbefugten Zugriff zu verhindern.
  - Methodenbeispiele: Passwörter, Zwei-Faktor-Authentifizierung, digitale Zertifikate, biometrische Verfahren.

- **Non-Repudiation (»Nichtabstreitbarkeit«):** Non-Repudiation stellt sicher, dass keine Partei leugnen kann, eine Nachricht gesendet oder empfangen zu haben, oder eine Transaktion autorisiert zu haben. Das gilt z. B. für Kartenzahlungen, Online-Transaktionen, digitale Signaturen oder Dokumente.
  - Methodenbeispiele: Digitale Signaturen, Transaktionsprotokolle.

Die kryptografischen Verfahren lassen sich grob in zwei Klassen einteilen. Die symmetrischen Verfahren nutzen pro Kommunikationsbeziehung sowie für die Ver- und Entschlüsselung einen (den gleichen) geheimen Schlüssel. Die Sicherheit beruht dabei auf der Geheimhaltung dieses Schlüssels.

Die **asymmetrische** Kryptografie verwendet einen privaten bzw. geheimen und einen öffentlichen Schlüssel und basiert auf komplexen mathematischen Funktionen. Der private Schlüssel wird zum Signieren oder Entschlüsseln verwendet, während der öffentliche Schlüssel zur Verifizierung der Signatur oder zum Verschlüsseln eingesetzt wird. Die beiden Schlüssel sind durch mathematische Verfahren miteinander verknüpft. Die Sicherheit beruht dabei nicht nur auf der Geheimhaltung des privaten Schlüssels, wie bei symmetrischen Verfahren, sondern auch auf der Komplexität der mathematischen Probleme, auf denen die Verfahren basieren.

Die bekannten klassischen Angriffsvektoren zielen darauf ab, den privaten Schlüssel entweder durch eine Brute-Force-Attacke zu erraten oder durch das Lösen mathematischer Probleme, die die beiden Schlüssel miteinander verbinden. Gegen diese Angriffsvektoren haben sich die heutigen kryptografischen Verfahren als hinreichend zuverlässig erwiesen. Weit verbreitete asymmetrische Kryptoverfahren wie RSA verlassen sich darauf, dass auf klassischen Rechnersystemen keine effizienten Verfahren zur Berechnung der verwendeten Schlüssel zum Beispiel mittels Primfaktorzerlegung zur Verfügung stehen.

Die rasanten Weiterentwicklungen des Quantencomputings stellen allerdings ein neues Bedrohungsszenario dar. Im Gegensatz zu klassischen Computern nutzen Quantencomputer quantenmechanische Phänomene für ihre Berechnungen und könnten damit hochkomplexe Probleme in verschiedenen Wirtschaftszweigen angehen, die bisher nicht zugänglich waren. Das bedeutet, dass Angriffe, die auf klassischen Computern nicht effizient oder in akzeptabler Zeit durchgeführt werden können, mit der Verfügbarkeit von Quantencomputern mit ausreichender Leistung erfolgreich umgesetzt werden könnten. Damit ist die praktische Sicherheit asymmetrischer Verfahren nicht mehr gegeben. Effiziente Entschlüsselungen durch Quantencomputer werden in erster Linie durch Algorithmen ermöglicht, die die besonderen Eigenschaften von Quantenbits ausnutzen. Die Eintrittswahrscheinlichkeit dieser Bedrohungsszenarien hängt von der erfolgreichen Entwicklung von Quantencomputern ab, welche die notwendige Rechenleistung realisieren können.

Quantenalgorithmen die Cybersicherheit bedrohen

- **Shor's Algorithmus für Primzahlfaktorisierung und diskrete Logarithmus (DLOG) Berechnungen**
  Shor greift die algorithmische Sicherheit von RSA, Diffie-Hellmann, DSA, und die ECC an. Mit der Veröffentlichung von Shor's Algorithmus ist klar geworden, dass dieses klassische asymmetrische kryptografische Verfahren durch kryptoanalytische Angriffe mit Quantencomputern bedroht sind.

- **Grover's Search für Datenbanksuchen oder Brute Force Angriffe**
  Grover's Search reduziert den Aufwand eines Brute Force Angriffs auf die Quadratwurzel des Aufwands mit klassischen Technologien. In anderen Worten wird mit Grover's Search das Sicherheitsniveau einer Verschlüsselung halbiert. Sie kann für Brute Force Angriffe auf jedes Kryptosystem genutzt werden und profitiert somit auch von Schlüsselräumen, die durch schwache Zufallsgeneratoren gebildet werden.

- **Die Quantum Algebraic Attack (QAA) für die Lösung von Booleschen Gleichungssystemen**
  Die QAA ist anwendbar auf Kryptosysteme, die auf Boolesche Gleichungssysteme reduziert werden können. Dazu zählen AES, Keccak, Trivium und MPQC. Dieser kryptoanalytische Angriff wird bei 256 Bit Schlüsseln mit gleich vielen Nullen und Einsen als nicht praktikabel eingeschätzt. Schlüssel mit dieser Eigenschaft entsprechen dem ersten Zufälligkeits-Kriterium für kryptografisch valide Zufallswerte nach NIST Standard.

Ab wann werden Quantencomputer kryptografische Verfahren brechen können?

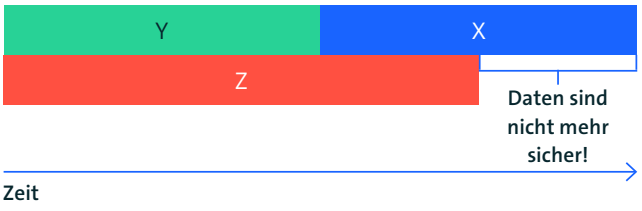
Derzeit befindet sich Quantencomputing noch in einem frühen technischen Entwicklungsstadium, was die Programmierung und anwendbare Algorithmen stark einschränkt. Trotzdem geht man davon aus, dass sich ein Vorteil von auf Quantencomputern basierenden Ansätzen in ausgewählten Einsatzszenarien in den nächsten Jahren zeigen wird. Aus diesem Grund wird die Forschung und Entwicklung im Quantencomputing seit einigen Jahren weltweit massiv vorangetrieben, um die Entwicklungsrichtung zu beeinflussen. Sobald sich praktisch relevante Quantenvorteile zeigen, werden Hersteller, Zulieferer und Anwender für Quantencomputer-Systeme ihre F&E-Aktivitäten nochmals verstärken.

Der Zeitpunkt, zu dem es skalierbare Quantencomputer geben wird, die in der Lage sind, heutige asymmetrische Kryptoverfahren zu brechen, ist noch schwer einzugrenzen. Dennoch verschärft sich das Risiko noch zusätzlich dadurch, dass verschlüsselte Kommunikationsdaten bereits jetzt auf Vorrat gespeichert werden können. Sobald die zur Entschlüsselung notwendigen Quantencomputer leistungsfähig genug sind, können diese Daten entschlüsselt werden– ein Konzept, das als »Harvest now, decrypt later« bekannt ist.

Die quantensichere Datenverarbeitung in Organisationen sollte daher bereits lange vor der Verfügbarkeit hochleistungsfähiger Quantencomputer erreicht werden. Um die Kritikalität der Risiken von Quantencomputern für die eigenen Systeme, Produkte oder Anwendungen zu beurteilen, kann man sich am Theorem von Michele Mosca (siehe Abbildung 1) orientieren und folgende Fragen stellen:

- Wie sensibel sind meine Daten und wie lange müssen sie deshalb mindestens sicher bleiben (x)?
- Wie lange dauert es, bis quantensichere Lösungen in die Infrastruktur meines Unternehmens umgesetzt sind (y)?
- Wann werden kryptografisch relevante Quantencomputer verfügbar sein (z)?

Mosca-Theorem



Wenn x + y > z, ist die Informationssicherheit durch nachträgliche Entschlüsselung bedroht.

Um den entsprechenden Schutz zu gewährleisten, sollte x + y kleiner als z sein. Da z nicht eindeutig bestimmt werden kann, wird empfohlen, eine Arbeitshypothese zu wählen. McKinsey schätzt den möglichen Zeitraum, in dem eine Angreifbarkeit beispielsweise von RSA-2048 gegeben sein könnte, auf Ende 2026 bis 2036[2]. Eine zuletzt 2023 aktualisierte Studie für das BSI geht für die Verfügbarkeit von kryptografisch relevanten Quantencomputern sogar von einem Zeitraum von mindestens 10–20 Jahren aus, falls es keine größeren Entwicklungssprünge gibt, hält aber gleichzeitig auch ein Szenario von 10 Jahren für zunehmend möglich, sollten sich in letzter Zeit veröffentlichte Erkenntnisse bestätigen[3]. Für Hochsicherheitsbereiche schlägt das BSI z. B. die Annahme vor, dass kryptografisch relevante Quantencomputer Anfang der

2 ↗ Steady progress in approaching quantum advantage | McKinsey
3 ↗ BSI – Zusammenfassung Entwicklungsstand Quantencomputer V2.0 (bund.de)

2030er Jahre zur Verfügung stehen.[4] Da die Einführung neuer quantensicherer resistenter Sicherheitsmaßnahmen mit langwierigen Prozessen in den Organisationen verbunden ist, besteht daher für die mittel- und langfristige Informationssicherheit bereits heute unmittelbarer Handlungsbedarf. Nicht die Frage, »ob« oder »wann« es Quantencomputer geben wird, sondern die Migration zur Post-Quanten-Kryptografie steht im Fokus.[5]

4 Migration to Post Quantum Cryptography (bund.de): https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Migration_to_Post_Quantum_Cryptography.pdf?__blob=publicationFile&v=2

5 ↗ BSI – Quantentechnologien und quantensichere Kryptografie (bund.de)

2 Technologische Ansätze für quantensichere Kommunikation

Um sich gegen die von Quantencomputern ausgehenden Bedrohungen zu schützen, werden derzeit zwei grundlegende Ansätze erforscht und teilweise bereits umgesetzt. Zum einen geht es um neue asymmetrische kryptografische Algorithmen, die unter dem Begriff Post-Quantum Cryptography (PQC) zusammengefasst werden. Beim zweiten Ansatz werden quantenphysikalische Prinzipien zur Erzeugung und Übertragung von symmetrischem Schlüsselmaterial genutzt – genannt Quantenschlüsselaustausch (engl.: Quantum Key Distribution, QKD).

Derzeit werden zwei quantensichere Methoden entwickelt: Post-Quantum Cryptography (PQC) und Quantenschlüsselaustausch (engl.: quantum key distribution (QKD)).

Post-Quantum Cryptography (PQC)

Konzept

Die Post-Quantum Cryptography (PQC) ist eine Klasse von asymmetrischen kryptografischen Algorithmen, die zusätzlich zu den klassischen Angriffsvektoren auch gegen effiziente Angriffe durch Quantencomputer, wie z. B. mit Algorithmen von Shor und Grover, resistent sein sollen. Die PQC-Algorithmen können auf klassischen Computern ausgeführt werden.

Die PQC lässt sich in verschiedene mathematische Gebiete unterteilen, aus denen quantensichere Verfahren hervorgehen. Die wichtigsten Bereiche sind die gitterbasierte, die codebasierte und die hashbasierte Kryptografie[6]. Alle Klassen haben eines gemeinsam: Um ein asymmetrisches Kryptosystem zu konstruieren, werden mathematische Probleme verwendet, für die weder für klassische noch für Quantencomputer-Algorithmen bekannt sind, die diese effizient lösen können.

Jede dieser drei Kryptografie-Klassen hat ihre eigenen Stärken und Schwächen. Verfahren aus der gitterbasierten Kryptografie gelten als besonders effizient in der Praxis. Die codebasierte Kryptografie kann mit sehr guten theoretischen Sicherheitsanalysen punkten. Hashbasierte Kryptografie bringt Signaturverfahren hervor, deren Sicherheit direkt von der verwendeten Hashfunktion abhängt. Außerdem sind sowohl hashbasierte als auch codebasierte Verfahren schon lange bekannt und gut erforscht.

6 Die drei Kryptografie-Klassen unterscheiden sich, indem sie auf verschiedenen mathematischen Prinzipien basieren. Gitterbasierte Kryptografie nutzt mathematische Probleme in einem unendlichen Raster aus Punkten, z.B. bei dem man den kürzesten Vektor im Gitter finden muss. Hashbasierte Kryptografie erzeugt aus beliebigen Daten einen eindeutigen digitalen Fingerabdruck, der sicherstellt, dass die Daten nicht manipuliert wurden, und wird häufig für digitale Signaturen verwendet. Codebasierte Kryptografie basiert auf Fehlerkorrekturcodes, die ursprünglich zur Erkennung und Korrektur von Übertragungsfehlern entwickelt wurden, und bietet Schutz für sichere Kommunikation.

Einsatzbereiche

Die asymmetrischen Verfahren[7], die durch die Nutzung von Quantencomputern in der Zukunft gebrochen werden könnten, werden heutzutage in jedem Aspekt des digitalen Lebens verwendet. Sie werden unter anderem bei der Erstellung von digitalen Signaturen (z. B. auf Verträgen), bei Authentisierung sowie bei Public-Key-Verschlüsselung und Schlüsselaustausch (z. B. in TLS und VPN-Kommunikation sowie im E-Commerce), eingesetzt.

Bei Existenz eines kryptografisch relevanten Quantencomputers wäre es theoretisch möglich, durch gefälschte Authentifizierung auf Infrastruktur zuzugreifen oder digital signierte Dokumente zu manipulieren. Dadurch wären beispielsweise verschiedene Szenarien möglich:

- Erpressungsangriffe durch die Androhung, die erbeuteten Daten zu veröffentlichen
- Erstellung gefälschter Softwaresignaturen zum Einschleusen von Malware
- Erstellung ununterscheidbarer gefälschter Dokumente
- Erstellung von betrügerischen Transaktionen auf Blockchains
- Manipulation von Banktransaktionen
- Manipulation im Verkehrswesen (z. B. Automobile, Bahnbetrieb und Luftfahrzeuge). Insbesondere Produkte mit einer langen Betriebszeit werden neuen Angriffsrisiken ausgesetzt sein.
- Fernsteuerung kritischer Infrastrukturen

Die Post-Quantum-Kryptografie (PQC) kann in IT- und OT-Infrastrukturen eingesetzt werden, um die kryptografischen Ziele Vertraulichkeit, Authentifizierung, Integrität und Nichtabstreitbarkeit im Angesicht von Quantencomputer-Bedrohungen zu gewährleisten.

Nach dem Prinzip »Harvest now, decrypt later« könnte allerdings ein Angreifer schon heute diese wichtigen Kommunikationskanäle überwachen und verschlüsselte Daten speichern, um diese später mit einem Quantencomputer zu entschlüsseln.

Jede Kommunikation und Infrastruktur sind daher potenziell betroffen, insbesondere solche mit einer langen Lebensdauer (siehe Mosca-Theorem). Dazu gehören kritische Infrastrukturen, Verkehrsmittel, Bezahlanwendungen sowie die Kommunikation mit Banken und medizinischen Einrichtungen. Auch Personalausweise nutzen derzeit Algorithmen, die in Zukunft möglicherweise gebrochen werden könnten. Sie müssen also alle auf die Nutzung von quantensicherer Kryptografie migrieren.

7 Dazu gehören z. B. RSA, elliptische Kurve Kryptografie (Elliptic Curve Cryptography), DSA, Diffie Hellman-Schlüsselaustausch usw.

Herausforderungen

- Obwohl erste Standards für PQC-Signaturen bereits 2018 veröffentlicht wurden[8] und erste NIST-Standards seit 2024 verfügbar sind, gibt es Faktoren die die Migration zu quantensicherer Kryptografie beeinflussen bzw. verlangsamen, z. B.: In einigen Produkten können die Algorithmen nicht sofort 1:1 ausgetauscht werden, sondern erfordern Anpassungen in den Systemen. Diese Produkte sind daher noch nicht in der Lage, umgehend quantensichere Kryptografie anzubieten.
- Die notwendigen Anpassungen von Protokollen für die Netzwerksicherheit (geführt durch IETF) stehen noch aus.
- Industrien, die auf zertifizierte Hardware angewiesen sind, müssen noch warten, bis angepasste Zertifizierungen verfügbar sind.
- Nationale Migrationsempfehlungen sind manchmal noch unterschiedlich.
- Die Anforderungen der quantensicheren Algorithmen stellt eine Herausforderung für manche Systeme, zum Beispiel eingebettete Systeme (IoT, Automotive, Telco), dar.
- Einen Mangel an Budget sowie Expertinnen und Experten für die Transformation und quantensichere Kryptografie in den Organisationen.
- Obwohl die PQC-Algorithmen gut erforscht sind, besteht für sie ebenso wie für klassische Algorithmen aufgrund ihrer Abhängigkeit von mathematischen Verfahren das Risiko einer potenziellen Verwundbarkeit durch neue und unbekannte Angriffsklassen, z. B. durch fortgeschrittene KI-Forschung.

Dennoch kann bereits mit den Vorbereitungen zur Einführung von Post-Quantum Kryptografie begonnen werden, indem das Verständnis für die Auswirkung der Quantenbedrohung für das eigene Unternehmen geschaffen (*Kryptoagilität – eine Voraussetzung für langfristige Sicherheit*).

8 Universität Darmstadt – A recipe against the power of the quantum computers: ↗ https://www.tu-darmstadt.de/universitaet/aktuelles_meldungen/archiv_2/2018/2018quartal2/neuesausdertueinzelansichtbreitespalte_206400.en.jsp

NIST Standardisierung von PQC-Algorithmen

- NIST hat 2017 einen Standardisierungsprozess für PQC-Verfahren gestartet. Aus insgesamt 69 eingereichten Kandidaten in den Bereichen Schlüsselaustausch und Signaturen wurden die ersten vier Verfahren für eine Standardisierung im Jahr 2022 ausgewählt: CRYSTALS-Kyber für Schlüsselaustausch, CRYSTALS-Dilithium, Falcon und SPHINCS+ für Signaturen. Im August 2024 hat das NIST einen finalen Satz von PQC-Algorithmen veröffentlicht, die dem Angriff eines Quantencomputers standhalten sollen und für den sofortigen Einsatz bereit sind.
- Im Auswahlverfahren wurde neben der Sicherheit gegen quantenalgorithmische Angriffe auch die Sicherheit gegen klassische Angriffsmethoden berücksichtigt. Auch die Abwägung zwischen Laufzeit, Schlüsselgröße, Signaturgröße und Sicherheit war für die Auswahl entscheidend.
- Die vier ausgewählten Verfahren basieren zudem auf unterschiedlichen mathematischen Gebieten: der gitterbasierten und der hashbasierten Kryptografie. Um die Auswahl an Algorithmen auch aus anderen mathematischen Gebieten zu erweitern, wird der Standardisierungsprozess fortgesetzt. Zum einen werden weitere Schlüsselaustauschverfahren aus dem Bereich der codebasierten Kryptographie zur Standardisierung ausgewählt. Diese bieten eine sehr gute Sicherheit im Verhältnis zu Laufzeit und Schlüsselgröße. Zum anderen sollen weitere Signaturverfahren, auch aus anderen Bereichen, standardisiert werden.

Quantenschlüsselaustausch (QKD)

Konzept

Unter dem Schlagwort Quantenschlüsselaustausch werden kryptografische Protokolle zusammengefasst, die physikalische Eigenschaften von einzelnen Lichtteilchen (Photonen) für die sichere Erzeugung und/oder Übertragung eines geheimen symmetrischen Schlüssels zweier Kommunikationspartner nutzen. Die Informationssicherheit ergibt sich in diesen Fällen nicht mehr ausschließlich durch die mathematischen Algorithmen, sondern vielmehr durch die Prinzipien der Quantenmechanik wie der Quantenverschränkung, dem No-Cloning-Theorem. Das resultiert in einem entscheidenden Vorteil von QKD, die sogenannte »Forward Security« (Vorwärtssicherheit). Dies bedeutet, dass Schlüssel, die zum Zeitpunkt der Erzeugung sicher waren, auch in Zukunft nicht rekonstruiert werden können. Es ist anzumerken, dass sich diese Annahme auf die theoretische Langzeitsicherheit bezieht, während die praktische Implementierung von Systemen heutzu-

tage noch zahlreiche Herausforderungen mit sich bringt und anfällig für Angriffe sein kann.[9] Mögliche Angriffe beschränken sich allerdings nur den Zeitpunkt der Schlüsselübertragung und sind nach der erfolgreichen Schlüsselübertragung nicht möglich.

In den 40 Jahren der Existenz dieser Methode entstanden zahlreiche Protokolle, die unterschiedliche Quanteneffekte und verschiedene physikalische Messgrößen, wie z. B. die Polarisation von Photonen oder Phasenmodulationen, ausnutzen. Diese Protokolle können in mehrere Klassen aufgeteilt werden: Prepare-and-Measure, Verschränkungsbasiert, Measurement-Device-Independent (MDI) und Continious Variable (CV). Der Unterschied zwischen den Klassen liegt in der Art und Weise, wie Quantenzustände erzeugt und gemessen werden sowie in den Sicherheitsmechanismen, die sie bieten.

Sie haben gemeinsam, dass ein potenzieller Angreifer aufgrund der Quantenphysik bei jeglichem Versuch den Schlüssel abzuhören stets selbst verrät, indem er Spuren in den Messdaten der Kommunikationspartner hinterlässt. Mithilfe der Prinzipien der Informationstheorie kann in der Nachbearbeitung außerdem verhindert werden, dass der Angreifer von seinem Abhörversuch auf den ausgetauschten Schlüssel schließen kann.

Derzeit werden in der Community verschiedene Ansätze zur Realisierung des Schlüsselaustauschs vorangetrieben. Von verschiedenen deutschen, europäischen und weltweiten Herstellern können bereits einsatzbereite QKD-Module erworben werden.

Im Folgenden wird die Funktionsweise eines Quantenschlüsselaustauschprotokolls anhand eines generischen Prepare-and-Measure-Protokolls beschrieben. Es erfordert:

- Dedizierte Hardware,
- eine authentifizierte und klassische Verbindung (IP oder Ethernet),
- einen optischen Quantenkanal zwischen zwei Kommunikationspartnern (Alice und Bob).

Der anschließende Prozess besteht aus mehreren Schritten:

- Über den Quantenkanal schickt der Sender (Alice) eine Zufallsfolge an Quantenzuständen (Qubits) kodiert in Photonen (Lichtteilchen) an den Empfänger Bob. Dies geschieht optisch entweder über Glasfaser oder über das Medium Luft (Freistrahl- und Satelliten-QKD). Bob führt Quantenmessungen an den empfangenen Qubits gemäß dem verwendeten QKD-Protokoll durch. Er wählt zufällig verschiedene Einstellungen des Messgerätes, um die Qubits auszulesen.

- Alice und Bob vergleichen über den klassischen Kanal die Geräteeinstellungen, die sie jeweils verwendet haben, um die Qubits zu senden und zu messen, um zu einem gemeinsamen geheimen Schlüssel zu gelangen (das sogenannte »Sifting«) und verwenden im Weiteren nur diejenigen Qubits, bei denen ihre Geräteeinstellungen zueinander gepasst haben.

9 ↗ BSI – A Study on Implementation Attacks against QKD Systems (bund.de): https://www.bsi.bund.de/EN/Service-Navi/Publikationen/Studien/QKD-Systems/Implementation_Attacks_QKD_Systems_node.html

- Im nächsten Schritt überprüfen Alice und Bob mögliche Fehler in den Daten durch Ermittlung bestimmter Parameter beim Senden und Empfangen der Qubits. Bei Beobachtung durch einen Angreifer werden die quantenmechanischen Zustände gestört, was zu messbaren Fehlern bzw. Änderung der Parameter in den QKD-Protokollen führt. So werden Lauschangriffe vom System direkt erkannt.
- Mithilfe eines Korrekturalgorithmus werden die aufgetretenen Fehler behoben, sodass Alice und Bob nun den gleichen Schlüssel besitzen, der allerdings noch nicht vollständig geheim ist.
- Im letzten Schritt führen Alice und Bob mithilfe der Informationstheorie und der gemessenen Parameter die sogenannte »Privacy Amplification« durch, die dafür sorgt, dass der so generierte finale Schlüssel dem Angreifer nachweislich nicht bekannt sein kann.
- Am Ende dieses Prozesses haben Alice und Bob einen sicheren gemeinsamen Schlüssel, den nur sie kennen. Dieser Schlüssel kann nun verwendet werden, um beispielsweise Nachrichten sicher zu verschlüsseln und zu entschlüsseln.

Einsatzbereiche

QKD ermöglicht die sichere Generierung und den Austausch von symmetrischen Schlüsseln zwischen zwei Parteien. Diese Schlüssel können dann für die Verschlüsselung und Entschlüsselung von Daten mit symmetrischen Algorithmen verwendet werden.

Damit kann QKD die asymmetrische Kryptografie als Schlüsselaustauschverfahren ergänzen, wobei typischerweise QKD und asymmetrische Algorithmen in hybriden Lösungen parallel verwendet werden können. Im Vergleich zu PQC-Methoden kann die QKD daher hauptsächlich in Anwendungsszenarien eingesetzt, die das Ziel der Vertraulichkeit verfolgen.

Mit steigendem Reifegrad kann Technologie in Zukunft insbesondere für die Hochsicherheitsbereiche wie Militär oder Finanzsektor in bestimmten Fällen als zusätzlicher Sicherheits-Layer relevant werden. Bereits heute gibt es dafür die ersten Anwendungen in der Praxis.[10] QKD bietet dann einen zusätzlichen Schutz gegen Abhörversuche und Angriffe durch Quantencomputer.

Für die Übertragung werden optische links, wie Glasfaser-, terrestrische Freistrahl- und Satelliten-Links mit verschiedenen Vor- und Nachteilen verwendet.

- Glasfaser-QKD ist durch Verluste in der Faser auf einige 100 km Reichweite beschränkt (siehe Herausforderungen).
- Bei Freistrahl-QKD können kurze Strecken von wenigen Kilometern ohne Bedarf an Glasfaserinfrastruktur überwunden werden.

10 JP Morgan – JPMorgan Chase establishes quantum-secured crypto-agile network: ↗ https://www.jpmorgan.com/technology/news/firm-establishes-quantum-secured-crypto-agile-network

- Satelliten-QKD ermöglicht eine weltweite sichere Verbindung zwischen Orten.

Bei den beiden letzteren Technologien stellt die Wetterabhängigkeit und Sonnenlicht eine technische Herausforderung dar.

Zusammengefasst bietet QKD eine vielversprechende Methode, um symmetrische Schlüssel sicher auszutauschen und so die Vertraulichkeit von Kommunikation zu erhöhen. Die versprochene Vorwärtssicherheit kommt jedoch zum Preis höherer Kosten und Anforderungen an die Infrastruktur im Vergleich zu asymmetrischen Verfahren.

Herausforderungen

Quantenschlüsselaustausch verspricht bei idealer Umsetzung eine informationstheoretisch sichere Methode für den symmetrischen Schlüsselaustausch. Eine zertifizierte Sicherheitsprüfung der verfügbaren praktischen Produkte durch unabhängige Labore wurde bisher allerdings nur eingeschränkt durchgeführt. IT-Sicherheitsbehörden vieler Länder (wie auch BSI[11] und NSA[12]) fordern daher weitere Maßnahmen zur Sicherstellung eines sehr hohen Schutzniveaus. Dabei gilt es folgende ingenieurs- und sicherheitstechnische Aufgaben zu bewältigen:

- **Seitenkanal-Angriffe:** Es sollten weitere Erfahrungswerte im Umgang mit potenziellen Seitenkanälen gesammelt werden.[13]
- **Standardisierung:** Obwohl verschiedene Projekte vorangetrieben werden und es außereuropäische Zertifizierungsverfahren gibt, fehlen bisher die Standards, um die Protokolle und deren Sicherheitsbeweise beschreiben.
- **Evaluierung:** Es wird eine geeignete Infrastruktur zur Evaluierung dieser Produkte benötigt.
- **Zertifizierung:** Es mangelt an einer umfassenden Zertifizierung der QKD-Systeme
- **Reichweitenbegrenzung:** Aktuell werden für den Einsatz von QKD auf die Distanzen über 100 km Trusted Nodes[14] benötigt. Dies stellt eine potenzielle Schwachstelle dar, die entsprechend geschützt werden muss. Perspektivisch kann der Einsatz von Quantenrepeater, die es ermöglichen, Quantenzustände über größere Distanzen ohne Trusted Nodes zu übertragen, eine Lösung bieten. Allerdings befindet sich diese Technologie noch im Forschungsstadium und ist noch nicht praxisreif.

11 BSI – Quantentechnologien und quantensichere Kryptografie – Position Paper on Quantum Key Distribution: ↗ https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.pdf

12 NSA – Quantum Key Distribution (QKD) and Quantum Cryptography (QC): ↗ https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

13 Aktuelle QKD-Systeme sind theoretisch zwar anfällig für Seitenkanalangriffe, in der Praxis wurden sie jedoch noch nicht durch solche Angriffe gebrochen. Die meisten bekannten Angriffe auf QKD sind nur theoretisch beschrieben worden. Einige wenige sind rudimentär und unvollständig demonstriert worden, ohne jedoch den Schlüssel selbst zu »stehlen«. Siehe auch A Study on Implementation Attacks against QKD Systems (BSI): ↗ https://www.bsi.bund.de/EN/Service-Navi/Publikationen/Studien/QKD-Systems/Implementation_Attacks_QKD_Systems_node.html

14 Trusted Nodes sind Punkte im Netzwerk, an denen die Quantenschlüssel in klassische Schlüssel umgewandelt und ausgetauscht werden müssen. Bei Satelliten- QKD fungieren die Bodenstationen als Trusted Nodes.

Insgesamt bietet die Quantenschlüsselverteilung (QKD) vielversprechende Ansätze für sichere Kommunikation. Allerdings müssen noch einige Herausforderungen gelöst werden, bevor eine breitere Anwendung empfohlen werden kann. Es gibt bereits QKD-Systeme und -Produkte, die sich auf einem guten technischen Niveau befinden, allerdings fehlt noch das Vertrauen in Form von geeigneten Zertifizierungsverfahren. Außerdem können das Potenzial und die Sicherheit von QKD trotz bestehender Sicherheitsbeweise derzeit nicht mit den gleichen Verfahren bewertet werden wie bei traditionellen Methoden.

Es ist jedoch zu erwarten, dass mit der Weiterentwicklung der Technologie die ersten Produkte in etablierten Evaluierungsprozessen getestet werden. Dies könnte zu einer Neubewertung durch die zuständigen Behörden führen. Derzeit nimmt QKD eine Nischenrolle ein und bietet vor allem in speziellen Anwendungsfällen Vorteile gegenüber komplexitätsbasierten Verfahren.

> Quantenschlüsselverteilung verspricht höchste Sicherheit bei Schlüsselaustausch, hat allerdings eine geringere Einsatzbreite als PQC.

Kryptoagilität – eine Voraussetzung für langfristige Sicherheit

Die Einführung von Quantencomputern stellt eine erhebliche Bedrohung für die heutige Kryptografie dar. Methoden, die gegen einen möglichen Angriff durch Quantencomputer resistent sind, befinden sich zum Teil noch in der Entwicklungsphase bzw. werden standardisiert und optimiert. Es ist daher auch möglich, dass mit der Entwicklung des Quantencomputings oder mit anderen algorithmischen oder technischen Methoden neue Algorithmen gefunden werden, die die Sicherheit der neu entwickelten, quantensicheren Methoden gefährden. Um dieser Herausforderung zu begegnen, ist es entscheidend, dass Organisationen die Fähigkeit entwickeln, ihre benutzten kryptografischen Komponenten und ihre Infrastruktur als Reaktion auf sich entwickelnde Bedrohungen, neue Technologien und sich ändernde Standards möglichst schnell anzupassen. Dieses Konzept der Anpassungsfähigkeit wird als Kryptoagilität bezeichnet.

Kryptoagilität soll Nutzer von Infrastrukturen auf allen Ebenen ermöglichen, schnell von einer kryptografischen Technologie auf eine andere zu wechseln. Zum anderen ermöglicht Kryptoagilität einer Organisation aber auch, auf Implementierungsfehler oder bekannt gewordene Schwachstellen in Kryptoalgorithmen zu reagieren. Die Voraussetzungen dazu müssen sowohl auf technischer als auch organisatorischer Ebene geschaffen werden. Nationale Empfehlungen sehen den hybriden Einsatz von klassischen und quantensicheren Algorithmen vor (BSI, ANSSI). So kann zum einen der schnelle Austausch klassischer Algorithmen gegen neue PQC-Verfahren gewährleistet werden. Auch aus Perspektive des Bitkom ist auf technischer Ebene der Kryptoagilität eine möglichst große Auswahl an praktisch einsetzbaren und zertifizierten kryptografischen Verfahren erforderlich.

Zukünftig sollen verschiedene Ansätze und Methoden für die Sicherung von Netzwerken und Infrastrukturen auf allen Schichten verfügbar sein. PQC und QKD bilden in diesem Kontext das Potenzial für synergetische quantensichere Lösungen in Bereichen mit höheren Sicherheitsanfor-

derungen.[15] Die sinnvolle Kombination verschiedener Ansätze, auch unter andauernder Verwendung von klassischen Technologien, kann Angriffsvektoren weiter reduzieren und die IT-Sicherheit in komplexeren Architekturen erweitern.

Die folgende Tabelle fasst die zentralen Merkmale von klassischer asymmetrischer Kryptografie, PQC und QKD in Bezug auf ihre Anwendungsgebiete, Sicherheit und Implementierung zusammen. Sie spiegelt die Sichtweise der Autoren dieses Papiers wider. Es ist zu beachten, dass die Bewertungen den aktuellen Entwicklungs- und Wissensstand von 2024 darstellen.

		Klassische asymmetrische Kryptoverfahren	PQC	QKD
Anwendung	Kryptografische Zwecke	Vertraulichkeit, Authentifizierung, Integrität und Nichtabstreitbarkeit	Vertraulichkeit, Authentifizierung, Integrität und Nichtabstreitbarkeit	Vertraulichkeit
	Technische Voraussetzungen	Bekannt und erfüllt	Ggf. zusätzliche Speicher- & Rechenkapazitäten	Zugang zu dedizierter Hardware und optischer Übertragung (z. B. Glasfaser oder Satelliten)
	Reichweite des effizienten Schlüsselaustauschs	Unbegrenzt	Unbegrenzt	ca. 100 km bzw. unbegrenzt mit Trusted Nodes
Sicherheit	Quantensicher (bekannte Angriffe)	Nein	Ja	Ja
	Theoretische Langzeitsicherheit	Potenzielle Verwundbarkeit durch neue und unbekannte Angriffsklassen	Potenzielle Verwundbarkeit durch neue und unbekannte Angriffsklassen	Vorhanden
	Standardisierung	Ausgearbeitet und verfügbar	NIST-Standards verfügbar	In Arbeit (z. B. ETSI, ISO)
	Zertifizierte Geräte & Lösungen	Verfügbar	Erste Lösungen in Arbeit	Noch nicht verfügbar
Implementierung	Kosten und Aufwand	n. a.	Höherer Aufwand/ Kosten durch Migrationsprozess	Vergleichsweise höchster Aufwand / Kosten, insb. für den Aufbau der Infrastruktur und Hardware

> Branchen oder Bereiche, die ein Höchstmaß an Sicherheitsanforderungen erfüllen müssen, können dies in Zukunft nur durch einen kombinierten Ansatz aus verschiedenen klassischen, PQC- und QKD-Verfahren gewährleisten.

15 Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography | Shaping Europe's digital future (europa.eu): ↗ https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography

Mit der Auswahl an technischen Lösungen allein ist jedoch noch nicht die Voraussetzung für schnelle Reaktion im Falle einer eintretenden Bedrohung geschaffen. Vielmehr muss die Organisation »Quantum Ready« gemacht werden. Dies bedeutet, dass eine grundlegende Kryptoagilität auf organisatorischer Ebene erreicht werden muss, um die eigenen Verfahren schnell anpassen zu können. Dazu sind folgende Punkte notwendig:

- Ein umfassendes Management von Infrastruktur-Komponenten mit den notwendigen technischen und kryptografischen Informationen, Netzwerkkommunikationspartnern und den jeweiligen Verantwortlichen. Hierbei können die Standards von CycloneDX[16] und CSAF[17] als Orientierung dienen.
- Verbesserung der Kryptographie-Governance, einschließlich Prozesse für Schlüssel und Zertifikatsverwaltung sowie Segregation of Duties.
- Aufbau von Testbeds für Benchmarks von verschiedenen Lösungen: Bewertung der Kryptoagilität aller Anwendungen im Hinblick auf Lösungen unter Verwendung von Kryptoagilitätsprinzipien und optionalen kryptografischen Produkten.
- Klassifizierung aller Anwendungen in Bezug auf Langzeit-Vertraulichkeit der verarbeiteten Daten.
- Einbindung von Quantencomputing-Bedrohungsszenarien wie das Konzept »Harvest now, decrypt later« in das reguläre Informationsrisikomanagement.
- Aufbau von internen Crypto-Threat-Intelligence für plötzlich auftretende kryptografische Sicherheitsprobleme.
- Aufbau von Skills im Bereich Kryptografie, Prozessen und Technologie um Kryptografische Vulnerabilities zu verwalten.
- Entwicklung eines Plans bzw. Notfallplan für den Wechsel von einer Technologie zu einer anderen für jede Klasse von Anwendungen.
- Prozessdefinitionen für die jeweiligen Wechsel.

16 CycloneDX: ↗ https://cyclonedx.org/guides/OWASP_CycloneDX-Authoritative-Guide-to-SBOM-en.pdf
17 CSAF: ↗ https://oasis-open.github.io/csaf-documentation/

3 Politische Handlungsstränge im Vergleich

Deutschland

Die Bundesregierung hat im April 2023 ein »Handlungskonzept Quantentechnologien der Bundesregierung«[18] veröffentlicht, um die anwendungsorientierte Entwicklung von Quantentechnologien in Deutschland gezielt voranzutreiben. Konkrete Meilensteine in der Quantenkommunikation und der Post-Quanten-Kryptografie bis 2026 sind unter anderem der Aufbau von QKD-Teststrecken zwischen ausgewählten Behördenstandorten, die Realisierung eines bundesweiten Glasfaser-Backbones für die Quantenkommunikation, die Erstellung einer PQC-Migrationsstrategie sowie Weiterführung und Einleiten der PQC-Migration in sicherheitskritischen Bereichen.

In dem Leitfaden »Kryptografie quantensicher gestalten«[19] gibt das BSI umfangreiche Hintergrundinformationen zur Thematik, insbesondere aber auch konkrete Handlungsempfehlungen, um die Bedrohung durch Quantencomputer kurz- und mittelfristig abzuwenden. Insbesondere für den Hochsicherheitsbereich hat das BSI bereits frühzeitig eine Empfehlung für die Schlüsseleinigungsverfahren FrodoKEM (gitterbasiert) und Classic McEliece (codebasiert) ausgesprochen. Bei beiden Verfahren steht die Sicherheit im Vordergrund, was zulasten der Laufzeit und der Schlüsselgröße geht. Das BSI wird seine Empfehlungen erweitern, nachdem jetzt die NIST Standards finalisiert sind (siehe auch TR-02102[20]).

Im Bereich Quantenschlüsselaustausch hat das BSI im Januar 2024 mit Partnerbehörden aus Frankreich (ANSSI), den Niederlanden (NLNCSA) und Schweden (Schwedische NCSA) ein Positionspapier veröffentlicht, welches ein informiertes Urteil über den Einsatz von QKD ermöglichen soll.[21] Ein Schirmprojekt in diesem Bereich ist SQuaD[22]. Auf der Webseite ist unter anderem eine grobe Übersicht über die aktuellen QKD-Teststrecken in Deutschland zu finden. Zusätzlich sind weitere Teststrecken im Aufbau, wie z. B. DemoQuanDT[23]. Projekte wie QuNET[24] und QR.X[25] erforschen zudem die Vorbereitung von quantensicherer IT-Infrastruktur.

18 BMBF – Handlungskonzept Quantentechnologien: ↗ https://www.bmbf.de/SharedDocs/Downloads/de/2023/230426-handlungskonzept-quantentechnologien.html
19 BSI – Kryptografie quantensicher gestalten: ↗ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Kryptografie-quantensicher-gestalten.html
20 BSI – BSI TR-02102-2 »Kryptografische Verfahren: Verwendung von Transport Layer Security (TLS)« Version: 2024-1: ↗ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.html
21 BSI – Position Paper on Quantum Key Distribution: ↗ https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.html
22 Home | SQuaD – Quantenkommunikation in Deutschland: ↗ https://www.squad-germany.de/
23 DemoQuanDT — Vernetzung und Sicherheit digitaler Systeme: ↗ https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/demoquandt
24 QuNET: ↗ https://qunet-initiative.de/anwendungsszenarien/
25 QR.X: ↗ https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/qr.x

EU

Auf der EU-Ebene gibt es zahlreiche Akteure, die die Aktivitäten zu quantensicherer Kommunikation, initiiert durch die Europäische Kommission, vorantreiben. In ihrem Weißbuch »How to master Europe's digital infrastructure needs« sieht die Kommission die Langzeitsicherheit der digitalen Kommunikation durch eine hybride Verwendung von QKD- und PQC-Algorithmen gewährleistet. Dafür wurden im Rahmen des »Digital Europe Programme« sowie des »Horizon Europe Programme« Förderprojekte ausgeschrieben, mit dem Ziel, eine europäische Strategie und Roadmap für die PQC-Migration zu entwickeln und eine Europäische Quantenkommunikationsinfrastruktur (EuroQCI) zu entwickeln sowie zu betreiben.

Für die PQC-Migration hat die Kommission im April 2024 eine Empfehlung an die Mitgliedstaaten ausgesprochen. Diese hält die Mitgliedstaaten dazu an, eine Strategie zur baldigen Migration in öffentlichen Verwaltungen und kritischen Infrastrukturen aufzustellen. Daraus sollen sich klare Zielvorgaben, Meilensteine und Fristen für einen sogenannten »Fahrplan für die koordinierte Umsetzung des Übergangs zur Post-Quanten-Kryptografie« ergeben. Dieser soll eine zeitliche Abstimmung nationaler Bemühungen und grenzüberschreitende Interoperabilität ermöglichen. Relevante EU-Algorithmen sollen bewertet und ausgewählt werden, um anschließend als gemeinsame Normen angenommen zu werden.

Als nächste Schritte sollen die Mitgliedstaaten:

- bestehende Strukturen im Bereich der Cybersicherheit nutzen, um sich abzustimmen,
- eine Untergruppe der NIS-Kooperationsgruppe einsetzen,
- sich in diesen Untergruppen mit geeigneten Maßnahmen für den Fahrplan befassen,
- nach zwei Jahren einen vollständigen Plan vorlegen.

Die Kommission wird die Zusammenarbeit überwachen und die Auswirkungen der eigenen Empfehlung spätestens im April 2027 bewerten. Mitgliedstaaten müssen bis dahin zweckdienliche Informationen liefern, damit gegebenenfalls auch weitere Maßnahmen ergriffen werden können.

Der Plan für EuroQCI sieht bis 2027 den Aufbau und den initialen Betrieb eines paneuropäischen QKD-Netzwerks vor, der aus einer Satelliten-Domäne und einem Verbund nationaler terrestrischer Domänen besteht. Die Hauptziele dabei sind die Demonstration der Einsatztauglichkeit dieser Technologie mit Geräten, die in der EU entwickelt und gebaut worden sind. Dabei wird in mehreren Schritten vorgegangen. Die Entwicklung der marktreifen QKD-Produkte wird im Rahmen des Projekts DIGITAL-2021-QCI-01-INDUSTRIAL[26] unterstützt. Parallel dazu wurden die einzelnen Mitgliedstaaten der EU im Rahmen der Projekte DIGITAL-2021-QCI-01-DEPLOY-NATIONAL und DIGITAL-2022-QCI-02-DEPLOY-NATIONAL dazu aufgerufen, eine nationale QKD-Infrastruktur zu planen und aufzubauen.

26 EU Funding & Tenders Portal: ↗ https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-2021-qci-01-industrial

Eine der Herausforderungen der QKD-Technologie ist die fehlende Infrastruktur zur Beurteilung der Sicherheitsfunktionen und der Vertrauenswürdigkeitsstufe der Hardware. Um dieses Problem anzugehen, hat die Europäische Kommission im Rahmen des Digital Europe Programme 4 (Nostradamus)[27] die Entwicklung einer Infrastruktur zur Evaluierung von QKD-Geräten gestartet.

USA

Die US-amerikanische Standardisierungsbehörde NIST hat 2017 einen internationalen Standardisierungsprozess für Post-Quanten-Kryptografie gestartet (siehe Kapitel 2). Die daraus hervorgehenden Standards für Schlüsseleinigung und digitale Signaturen werden voraussichtlich weltweit Anwendung finden. Im Juli 2022 hat das NIST aus den verbliebenen Kandidaten die ersten zukünftigen Standards ausgewählt, anschließend Entwürfe für die Standards geschrieben, die im August 2024 veröffentlicht wurden.[28]

Bereits im September 2022, also kurz nach Bekanntgabe der ersten zukünftigen PQC-Standards durch das NIST, hat die NSA mit der CNSA 2.0 eine Suite von Algorithmen, basierend auf den zukünftigen NIST PQC-Standards inklusive Zeitvorgaben für die Migration, veröffentlicht. Bis spätestens 2033[29] soll die Migration auf die CNSA 2.0 abgeschlossen sein. Dies ist im Einklang mit einem zuvor veröffentlichten National Security Memorandum, dem NSM10 sowie dem Quantum Computing Cybersecurity Preparedness Act H.R. 7535. Die Vorgaben der USA können Auswirkungen auf andere Länder haben, so müssen beispielsweise Zulieferer aus der EU diese einhalten.

In Bezug auf QKD nimmt die NSA eine kritische Haltung ein[30]: Aufgrund der technischen Beschränkungen wird der Einsatz von QKD in nationalen Sicherheitssystemen nicht akzeptiert. Allerdings beschäftigen sich private amerikanische Unternehmen mit QKD, wie z. B. die größte Bank JP Morgan, die eine hybride Strategie angekündigt hat.

China

Die chinesische Regierung hat Quantenkommunikation, also die sichere Übertragung von Information durch quantenphysische Mechanismen, zu einer Priorität gemacht und als erstes Land einen Quantensatelliten namens Micius gestartet, welcher eine verschränkungsbasierte Quantenschlüsselverteilung über mehr als 1.000 km demonstriert hat[31]. Das integrierte Quantenkommunikationsnetzwerk in China hat eine Gesamtlänge von mehr als 4.600 Kilometern, erstreckt sich über mehrere Provinzen und verbindet verschiedene Knotenpunkte.[32] Mehr als 20 Städte sind

27 Deutsche Telekom – EU launches Nostradamus – prepares Europe for a quantum world: ↗ https://www.telekom.com/en/media/media-information/archive/eu-launches-nostradamus-prepares-europe-for-a-quantum-world-1056746

28 Post-Quantum Cryptography | CSRC (nist.gov): ↗ https://csrc.nist.gov/projects/post-quantum-cryptography

29 Für einige Anwendungsfälle wie z. B. Firmware Signing soll dies bereits bis 2030 erfolgen.

30 National Security Agency/Central Security Service > Cybersecurity > Quantum Key Distribution (QKD) and Quantum Cryptography QC: ↗ https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

31 Micius Quantum Communication Satellite (QUESS): ↗ https://www.aerospace-technology.com/projects/micius-quantum-communication-satellite/

32 Chen, YA., Zhang, Q., Chen, TY. et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature 589, 214–219 (2021). ↗ https://doi.org/10.1038/s41586-020-03093-8

über das Metropolnetzwerk angeschlossen. Der Micius-Satellit und weitere Mikrosatelliten können Quantenschlüssel über sechs Bodenstationen verteilen. Von Anwendungsseite sind bereits Regierungs-, Banken-, Energieversorgernetzwerke sowie erste mobile Kommunikationssysteme integriert. Nach eigenen Angaben sind QKD-Systeme großflächig kommerziell im Einsatz.[33] [34] Ziel ist es, mit den weiteren Technologieentwicklungen eine Technologieführerschaft für ein sicheres quantenbasiertes Internet zu schaffen.

Im August 2018 kündigte die Chinese Association for Cryptologic Research (CACR) einen nationalen Wettbewerb zur Auswahl der vielversprechendsten quantensicheren kryptografischen Algorithmen (PQC) an. Die Gewinner wurden im Januar 2020 bekannt gegeben. Im Gegensatz zum NIST-Wettbewerb implementierten die am chinesischen Wettbewerb teilnehmenden Algorithmen kryptografische Mechanismen für digitale Signaturen, Public-Key-Verschlüsselung und Schlüsselvereinbarungsprotokolle zweier Sicherheitsstufen (128 und 256 Bit), die den NIST-Stufen I und V entsprechen. Die CACR-Expertinnen und -Experten bevorzugen gitterbasierte Algorithmen. Die Materialien sind derzeit nur in chinesischer Sprache verfügbar, doch es ist zu erwarten, dass China seine Post-Quantum-Entwicklungen international standardisieren wird, z. B. auf ISO-Ebene.

33 Chinas großer Sprung zum Quantencomputer – Goethe-Institut: ↗ https://www.goethe.de/prj/lqs/de/art/22927140.html

34 Monitoring-Bericht 1 – Quantenkommunikation (fraunhofer.de): ↗ https://publica.fraunhofer.de/entities/publication/dc597f63-802e-4206-be4f-78a49f16a5c1/details

4 Handlungsempfehlungen

Aktionsplan für Organisationen

Prinzipiell ist die komplette IT und OT aller Branchen und entlang der gesamten Wertschöpfungskette betroffen. Überall dort, wo heute und in Zukunft kryptografische Verfahren wie Verschlüsselung zum Einsatz kommen oder kommen sollten, besteht Handlungsbedarf, insbesondere für Hersteller von IT- und Telekommunikation, Hardware und Software, IT-Dienstleister sowie die Betreiber von kritischer Infrastruktur.

Die Migration zu quantensicherer Kryptografie ist eine komplexe Transformation für jeden Betroffenen. Sie ist mit zahlreichen Herausforderungen verbunden, wie zum Beispiel:

- Wie lässt sich die Migration wichtiger Elemente, wie einer PKI, ohne größere Unterbrechungen planen?
- Welche Sofortmaßnahmen sind erforderlich?
- Welche Algorithmen sollten verwendet werden (spezielle Anwendungsfälle)?
- Wie lassen sich bei der Umsetzung von Maßnahmen Prioritäten für die Faktoren »kritische Daten«, »wertvoll«, »zeitkritisch« setzen?

Mit diesen Herausforderungen sollten die Organisationen nicht alleine und jede für sich umgehen müssen. Obwohl es schwierig vorauszusagen ist, wann ein kryptografisch relevanter Quantencomputer entwickelt wird, empfehlen zahlreiche nationale Sicherheitsbehörden, dass Unternehmen einen Plan für diese Transformation erstellen, und sich das Ziel setzen, diese Transformation in den frühen 2030er Jahren durchgeführt zu haben.

Je nachdem, ob ein Unternehmen Anbieter oder Anwender von Architekturen und Produkten mit kryptografischen Komponenten ist, ändert sich die Komplexität dieser Transformation und die notwendigen Schritte. Auch Unternehmensgröße und die jeweilige Industrie können einen Einfluss haben. Daher müssen die folgenden Punkte beachtet werden:

- Industriespezifische Verordnungen
- Unterschiedliche Abhängigkeiten
- Unterschiedliche Produkt-Laufzeiten und Kontrolle der Infrastruktur

Nichtsdestotrotz empfehlen wir dringend die folgenden ersten Schritte, die für jede betroffene Organisation wichtig sind:

1. **Kryptoagilität einführen:** In jeder Organisation sollte eine Strategie zur Einführung der Kryptoagilität im eigenen Kontext und in Bezug auf die Anforderungen an Vendoren erarbeitet werden, um die Organisation Quantum Ready zu machen und sich hierdurch auf die breite Einführung von leistungsfähigen Quantencomputern vorzubereiten. Es ist wichtig, sich schnell an veränderte Bedrohungslagen und neue Standards anpassen zu können.

2. **Stakeholder identifizieren und einbinden:** Alle relevanten Stakeholder innerhalb der Organisation sollten für Quantencomputing-Bedrohungen ergänzend zur Informationssicherheit und dem Datenschutz sensibilisiert werden. Die Kommunikation mit Dienstleistern und Lieferanten über die jeweiligen Zeitpläne und Anforderungen an quantensichere Kryptografie und Kryptoagilität sollte sichergestellt werden.

3. **Bewusstsein aufbauen:** Unternehmen müssen sich schon jetzt mit dem Entwicklungsstand des Quantencomputings vertraut machen und Expertise in der Kryptografie aufbauen, um die verschiedenen Schutzkonzepte im Themenfeld Informationssicherheit bewerten zu können.

4. **Risiko bewerten:** Die mit dem Quantencomputing verbundenen Risiken sollten systematisch im Risikomanagement der Unternehmen verankert werden. Die GSMA (2023) erläutert zum Beispiel in ihrem an Telekommunikationsunternehmen gerichteten Leitfaden mögliche Frameworks für die Risikobewertung, die hier als Orientierung dienen können[35].

5. **Inventar erstellen und Abhängigkeiten identifizieren:** Eine systematische Bestandsaufnahme der im Unternehmen eingesetzten Kryptografie sollte durchgeführt und laufend aktualisiert werden.

6. **Prioritäten setzen:** Es ist wichtig zu bewerten, welche Elemente in der Organisation am wichtigsten zu schützen und am schwierigsten zu migrieren sind. Dabei sind die Lebensdauer der Systeme und der Vertraulichkeitszeitraum zu berücksichtigen.

7. **Migrationsplan erstellen:** Ein Migrationsplan zu quantensicherer Kryptografie mit konkreten Zielen sollte mit hoher Dringlichkeit erstellt und laufend aktualisiert werden. Für die langfristige Strategie sollte ebenfalls geprüft werden, inwieweit auch eine zusätzliche Sicherheit durch die Integration von QKD-Ansätzen in Betracht kommt.

8. **Best Practices aufrechterhalten:** Wie bereits für klassische Kryptografie empfohlen, sollten kryptografische Schlüssel auch unter PQC und QKD in einer sicheren Umgebung aufbewahrt werden – zum Beispiel in einem Hardware-Sicherheitsmodul (HSM). Für Integrationstests mit den vorhandenen Applikationen wird empfohlen, einen HSM-Simulator zu verwenden.

35 Quantum Cryptanalysis Risk Framework for Telco: ↗ https://www.gsma.com/get-involved/working-groups/wp-content/uploads/2023/09/Guidelines-for-Quantum-Risk-Management-for-Telco-v1.0.pdf

Aktionsplan für die Politik

Nach Einschätzung des Bitkom sind die derzeitigen sicherheitspolitischen Handlungsaktivitäten in Deutschland und Europa nicht ausreichend, um den Schutz der IT öffentlicher Einrichtungen und Unternehmen vor Quantencomputing-Angriffen zu gewährleisten. Folgende Maßnahmen sollten daher dringend umgesetzt bzw. verstärkt werden.

1. **Quantensicherheit ressortübergreifend behandeln:** Die Empfehlungen zum Umgang mit Quantencomputing und den damit verbundenen Risiken sollten in allen relevanten Regierungsaktivitäten auch sektorübergreifend betrachtet werden (insbesondere mit Fokus auf KRITIS). Es bedarf einer klaren Federführung und Koordination durch das BMI mit Unterstützung des BSI, um die Quantensicherheit von Behörden und Unternehmen übergeordnet zu adressieren.

2. **Entwicklung und Umsetzung einer PQC-Migrationsstrategie für den öffentlichen Sektor:** Wir unterstützen die im Handlungskonzept hinterlegten Vorhaben der Bundesregierung zum Thema PQC. Diese gilt es nun mit konkreten Umsetzungsschritten zu unterlegen und zügig einen Migrationsplan zur Einführung von Kryptoagilität in den Behörden zu erarbeiten und nach einem konkreten Zeitplan umzusetzen. Auch hier ist es wichtig, die schützenswerten Daten zu identifizieren und entsprechend zu priorisieren.

3. **Standardisierungsprozess offen und international gestalten:** Ein offener Austausch von regulatorischen Institutionen, Marktteilnehmern und entsprechenden internationalen Standardisierungsgremien sollte gefördert und Best Practices mit anderen Ländern ausgetauscht werden (zum Beispiel im Rahmen der EU-US TTC). Außerdem fordern wir die Bundesregierung auf, sich auf europäischer Ebene für eine gemeinsame Herangehensweise einzusetzen.

4. **Eine Führungsposition in der QKD F&E in Deutschland anstreben:** Die aktuellen Herausforderungen sollten durch gezielte Förderprogramme in enger Zusammenarbeit mit der Industrie angegangen werden. Dazu zählen Standardisierung, Zertifizierung und Sicherheitsnachweise. Zudem sollte die Entwicklung von Testbeds zu Implementierungen in aktiven Leitungen übergehen, um die Robustheit der Technologie in realen Umgebungen zu testen. Die Integration dieser Technologie in bestehende Infrastrukturen ist entscheidend für den Aufbau eines quantensicheren Netzwerks. Das Problem der Reichweite von Punkt-zu-Punkt-Verbindungen soll vorübergehend durch die Zertifizierung und Akzeptanz von Trusted Nodes als vertrauliche Ansatz gelöst werden. Das BSI sollte sich mit den Fragen »Wo kann QKD verwendet werden?« und »Wie lässt sich PQC effektiv kombinieren?« befassen und entsprechende Empfehlungen an die Industrie ausgeben. Hier sollte aufgrund der sicherheitspolitischen Relevanz nicht nur Grundlagenforschung, sondern auch die produktnahe Entwicklung hin zu TRL-8 oder 9 (wie auf EU-Ebene z. B. in DIGITAL-2021-QCI-01-INDUSTRIAL) gefördert werden.

5. **Regelmäßige Überprüfung des Stands der Technik:** Der aktuelle Stand des Quantencomputings und der Quantensicherheitstechnologien sollte in einem jährlichen oder zweijährlichen Bericht des BMI/BSI überprüft werden, um sicherzustellen, dass die getroffenen Maßnahmen stets den neuesten Entwicklungen und Erkenntnissen entsprechen.

6. **Unterstützung bei der Umsetzung der quantensicheren Migration:** Aufgrund des Fachkräftemangels im IT-Sicherheitsbereich stellt die Migration auf quantensichere Verfahren eine weitere Herausforderung dar, insbesondere für kleine und mittlere Unternehmen. Die Politik sollte dazu entsprechende Fördermaßnahmen und finanzielle Anreize bereitstellen, wie etwa gezielte Förderprojekte oder steuerliche Abschreibungen für neu beschaffte quantensichere Produkte. Dem Fachkräftemangel muss durch Bürokratieabbau und die Förderung von Frauen in der IT-Sicherheitsbranche entgegengewirkt werden.

Weitere Publikationen

- AVID | The PQC Migration Handbook: ↗ https://english.aivd.nl/publications/publications/2023/04/04/the-pqc-migration-handbook
- BSI | Kryptografie – Marktumfrage Kryptografie und Quantencomputing: ↗ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Marktumfrage_Kryptografie_Quantencomputing.html
- BSI | Migration to Post Quantum Cryptography: ↗ https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Migration_to_Post_Quantum_Cryptography.pdf?__blob=publicationFile&v=2
- BSI | Position Paper on Quantum Key Distribution: ↗ https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.pdf?__blob=publicationFile&v=4
- BSI | Zusammenfassung Entwicklungsstand Quantencomputer V2.0: ↗ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/Entwicklungsstand_QC_Zusammenfassung_V_2_0.pdf?__blob=publicationFile&v=3
- ComputerWeekly | Die Auswirkungen von Quantum Computing auf Kryptografie: ↗ https://www.computerweekly.com/de/feature/Die-Auswirkungen-von-Quantum-Computing-auf-Kryptografie
- CSRC (nist.gov) | Migration to Post-Quantum Cryptography: ↗ https://csrc.nist.gov/pubs/pd/2021/08/04/migration-to-postquantum-cryptography/final
- ETH Zurich | The debate over QKD: A rebuttal to the NSA's objections: ↗ https://arxiv.org/abs/2307.15116
- European Policy Center | A quantum cybersecurity agenda for Europe (Discussion Paper): ↗ https://epc.eu/content/PDF/2023/Cybersecurity_DP.pdf
- Darmstadt University of Applied Sciences | Managing the Migration to Post-Quantum-Cryptography: ↗ https://arxiv.org/vc/arxiv/papers/2301/2301.04491v1.pdf
- GSMA | Guidelines for Quantum Risk Management for Telco: ↗ https://www.gsma.com/get-involved/working-groups/wp-content/uploads/2023/09/Guidelines-for-Quantum-Risk-Management-for-Telco-v1.0.pdf
- GSMA | Post Quantum Telco Network Impact Assessment Whitepaper: ↗ https://www.gsma.com/newsroom/wp-content/uploads/PQ.1-Post-Quantum-Telco-Network-Impact-Assessment-Whitepaper-Version1.0.pdf

- IBM | Advancements in Quantum Computing and AI May Impact PQC Migration Timelines: ↗ https://www.preprints.org/manuscript/202402.1299/v1
- Library of Congress | Text – H.R.7535 – 117th Congress (2021–2022): Quantum Computing Cybersecurity Preparedness Act: ↗ https://www.congress.gov/bill/117th-congress/house-bill/7535/text
- McKinsey | Steady progress in approaching quantum advantage: ↗ https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/steady-progress-in-approaching-the-quantum-advantage#/
- NSA | Announcing the Commercial National Security Algorithm Suite 2.0: ↗ https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

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.

Bitkom e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
bitkom@bitkom.org

bitkom.org

bitkom