Netze quantensicher machen

Die Quantenbedrohung

Die Wahrung der Privatsphäre ist für unsere Gesellschaft von grundlegender Bedeutung und der Schutz sensibler Daten ist eine entscheidende Anforderung für eine sichere Geschäftstätigkeit. Mit kryptografischen Verfahren wird der Zugriff auf Informationen zuverlässig auf berechtigte Nutzer beschränkt. Dafür werden bewährte Hashing- und Verschlüsselungs-Algorithmen eingesetzt.

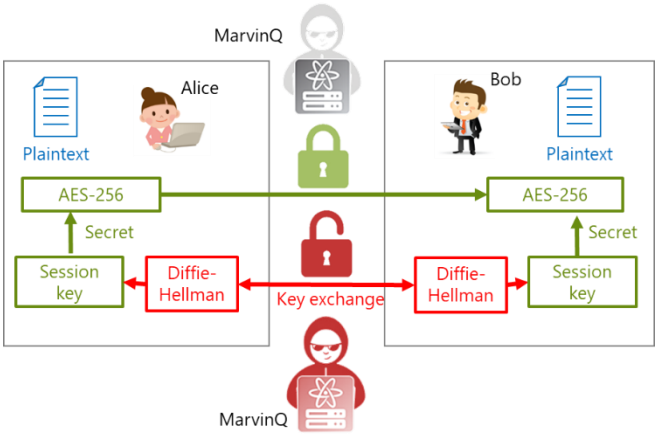
Protokolle für den Austausch geheimer Schlüssel nutzen asymmetrische Krypto-Algorithmen wie beispielsweise RSA oder Diffie-Hellman. Kommunikationspartner werden damit sicher authentifiziert. Die gemeinsam erzeugten Sitzungsschlüssel werden zum Verschlüsseln großer Datenmengen mit leistungsstarken symmetrischen Chiffren wie AES-256 verwendet. Die heutige eingesetzten Verschlüsselungs- und Hashing-Algorithmen bieten ein hohes Maß an Sicherheit, das auf einer tiefgehenden mathematischen Analyse und einem breiten Einsatz beruht. Bis heute konnte kein Angreifer diese Algorithmen brechen. Alice und Bob müssen sich keine Sorgen machen, dass Marvin ihre Kommunikation kompromittieren könnte, selbst wenn er die Unterstützung der leistungsstärksten Supercomputer hätte.

Diese Situation wird sich jedoch mit dem Aufkommen von Quantencomputern ändern. Die meisten Experten gehen davon aus, dass es in spätestens 15 Jahren Quantencomputer geben wird, die so leistungsfähig sind, dass RSA2048-Verschlüsselung innerhalb von 24 Stunden erfolgreich angegriffen werden kann und dass dann die bestehenden Krypto-Systeme nicht mehr als sicher angesehen werden können. Das Quanten-Computing stellt somit eine Bedrohung für die etablierten Methoden zur Sicherung von Kommunikationsnetzen dar.

Quantencomputer - ein Stolperstein für die Netzsicherheit

Quantenbits - sogenannte Qubits - werden durch Quantenzustände dargestellt. Das Verhalten eines Quantenzustands folgt nicht den Regeln der mechanischen Physik. Es kann den logischen Wert "0" oder "1" darstellen, aber auch eine Überlagerung dieser beiden Zustände. Daher kann ein Quantenbit viel mehr Informationen enthalten als ein klassisches Bit. Bestimmte komplexe Probleme können von Quantencomputern schnell und effizient gelöst werden.

Asymmetrische Verschlüsselungsalgorithmen gehören zu den mathematischen Problemen, die von einem Quantencomputer innerhalb von Stunden oder Tagen



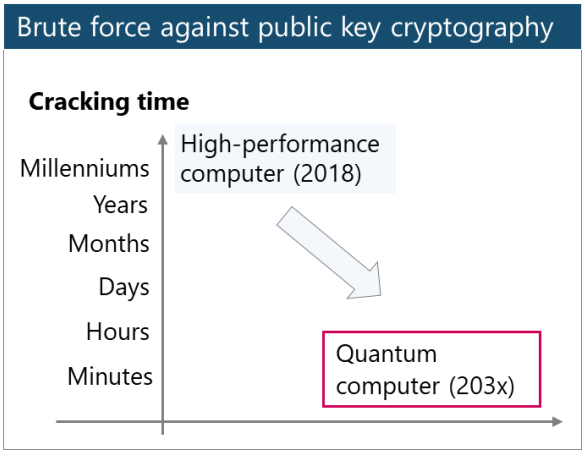
gelöst werden können – etwas, das klassische Supercomputer in keinem sinnvollen Zeitraum erreichen könnten. Ein von Peter Shor entwickelter Algorithmus für Quantencomputer ist in der Lage, asymmetrische Schlüsselaustauschverfahren (englisch: Public Key Cryptography) zu kompromittieren.

Glücklicherweise ist die Situation bei symmetrischen Verschlüsselungsalgorithmen wie beispielsweise dem Advanced Encryption Standard (AES) viel besser. Zwar haben Quantencomputer einen gewissen Vorteil beim Angriff auf diese Algorithmen, doch gilt die weit verbreitete Schlüssellänge von 256 als ausreichend lang, um AES-256 quantensicher zu machen.

Das Netzwerkdiagramm zeigt, dass Alice und Bob AES-256 zur Verschlüsselung ihrer Kommunikation und Diffie-Hellmann als Schlüsselaustauschprotokoll verwenden. Mit der Leistung eines Quantencomputers kann MarvinQ nun die Sitzungsschlüssel entschlüsseln. Mit diesen Schlüsseln kann er die Kommunikation von Alice und Bob lesen. Er ist jedoch nicht in der Lage, die mit einer symmetrischen Chiffre gesicherte Kommunikation direkt anzugreifen.

Quantencomputer gibt es noch gar nicht – müssen wir uns dennoch Sorgen machen?

Bis heute gibt es noch keinen Quantencomputer, der leistungsfähig genug wäre, um den Shor-Algorithmus anzuwenden und die heute eingesetzten Schlüsselaustausch-Algorithmen zu kompromittieren. Es wird jedoch viel Geld in die Entwicklung von Quantencomputern gesteckt, und man kann davon ausgehen, dass sie in den nächsten 10 bis 15 Jahren die notwendige Leistungsfähigkeit erreichen werden.



Das heißt aber nicht, dass wir tatenlos zusehen und abwarten sollten, bis dies passiert. Aus mehreren Gründen muss jetzt gehandelt werden:

- Nach dem Prinzip "jetzt speichern, später entschlüsseln" könnten Angreifer eine sichere Kommunikationsverbindung abhören und den verschlüsselten Datenverkehr einschließlich der Kommunikation zum Schlüsselaustausch speichern. Sobald ein hinreichend leistungsfähiger Quantencomputer verfügbar ist, könnten die Sitzungsschlüssel dechiffriert werden und damit wird auch ein Zugang zu den verschlüsselten Informationen ermöglicht.

- Sicherheitsprotokolle werden in Netzelemente implementiert, die für viele Jahre in den Netzen verbleiben. Es ist nicht ungewöhnlich, dass Gerätetechnik in Kabelnetzen oder auch kritischen Infrastrukturen für 10 Jahre und sogar noch länger betrieben wird. Daher sollte die heute installierte Hardware schon quantensicher sein, um einen teuren Hardwaretausch beim Aufkommen von leistungsfähigen Quantencomputern zu vermeiden.

- Asymmetrische Schlüsselaustauschverfahren (englisch: Public Key Algorithm) werden in vielen Anwendungen für die sichere Authentifizierung eingesetzt. Als solche werden sie auch bei der Blockchain-Technologie und bei Kryptowährungen verwendet. Hier müssen Datensätze für lange Zeit sicher gespeichert werden. Eine quantenresistente Lösung ist für den Schutz entsprechender Vermögenswerte unerlässlich und sollte zu einem möglichst frühen Zeitpunkt eingeführt werden.

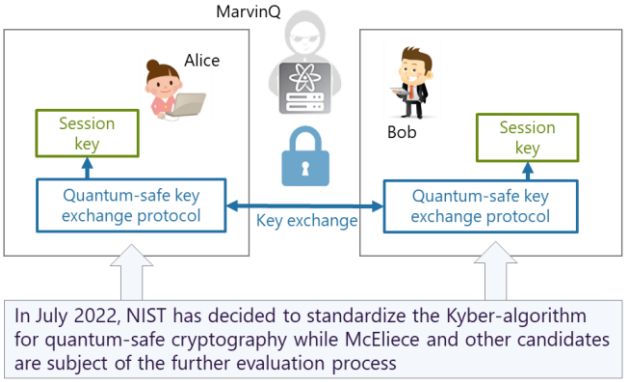
Obwohl heute keine unmittelbare Gefahr durch Quantenangriffe besteht, sollten Systeme auf die Gefährdungslage von morgen vorbereitet sein. Alle heute installierten Systeme sollten auf einfache Weise mit einem quantensicheren Verschlüsselungs-Algorithmus erweitert werden können.

Nationale Sicherheitsbehörden – wie die NSA in den USA und das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Deutschland – haben Aktivitäten gestartet, um quantensichere Kryptographie verfügbar zu machen, und Projekte initiiert, um Sicherheitslösungen für die Post-Quanten-Ära zu identifizieren, zu bewerten und schließlich zu standardisieren.

Quantensichere Kryptographie

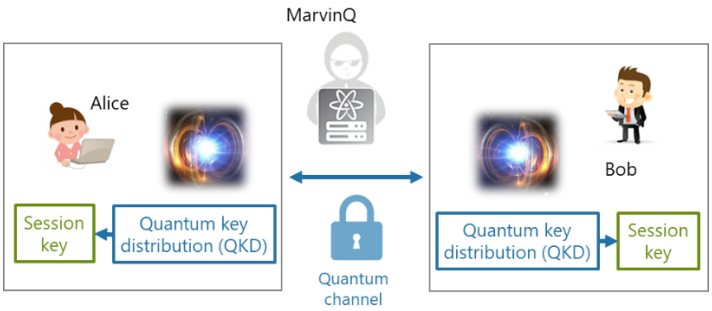
Es gibt verschiedene Möglichkeiten, um die Schwachstellen von asymmetrischen Schlüsselaustauchverfahren zu beseitigen und Netze gegen Quantencomputer-Angriffe zu sichern. Es können zwei sehr unterschiedliche Schutzmaßnahmen angewandt werden:

Asymmetrischen Schlüsselaustauchverfahren quantensicher machen: Die derzeit angewandten kryptografischen Verfahren beruhen auf der hohen Komplexität eines mathematischen Problems. Die Faktorisierung großer Primzahlprodukte oder das diskrete Logarithmusproblem stellt für klassische Computer eine ziemliche große Herausforderung dar und benötig sehr lange Rechenzeiten. Quantencomputer können mit speziellen Algorithmen diese schwierigen Aufgaben sehr schnell lösen. Allerdings gibt es noch andere mathematische Probleme, die selbst für die leistungsfähigsten Quantencomputer äußerst schwierig sind. Algorithmen auf Basis des McEliece-Kryptosystems gelten als resistent gegen Angriffe durch Quantencomputer.



Diese quantensichere Verschlüsselung wird als Post-Quanten-Kryptographie (PQC) bezeichnet, und eine Reihe vielversprechender Protokolle wird derzeit von der weltweiten Gemeinschaft der Sicherheitsexperten einer umfassenden Sicherheitsbewertung unterzogen. Im Juli 2022 hat NIST beschlossen, den Kyber-Algorithmus für quantensichere Kryptografie zu standardisieren, während McEliece und andere Kandidaten Gegenstand des weiteren Bewertungsprozesses sind. Bis dieser Prozess abgeschlossen ist, kann die Sicherheit durch die Verwendung von Pre-Shared Keys optimiert werden, vorzugsweise in Kombination mit krypto-agilen Implementierungen, die mit zukünftigen, standardisierten Post-Quanten-Algorithmen erweiterbar sind.

Post-Quanten-Algorithmen können relativ einfach mit klassischen Computern implementiert werden. Es ist allerdings nicht auszuschließen, dass neue Angriffsvektoren auch heute als sicher geltende PQC-algorithmen brechen können. Auch aus diesem Grund ist eine krypto-agile Implementierung vorteilhaft.



Verteilung von Schlüsseln auf quantensichere Weise: Ein ganz anderer Ansatz für eine quantensichere Kryptografie setzt auf physikalische Mechanismen zum Schutz gegen Angriffe durch Quantencomputer. Quantenzufallszahlengeneratoren (Quantum Random Number Generator, QRNG) und Quantenschlüsselverteilung (Quantum Key Distribution, QKD) nutzen die Quantenphysik, um die Integrität der Schlüsselerzeugung und des Schlüsselaustauschs zu schützen.

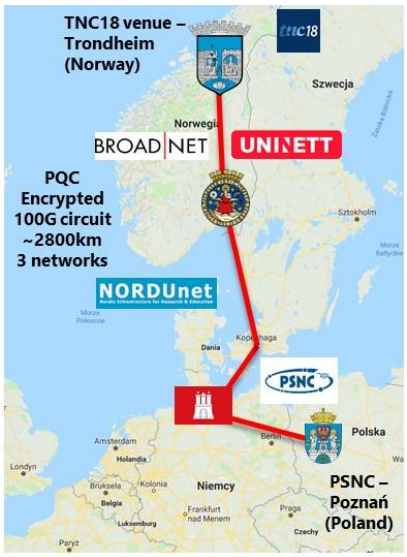
Da QKD auf Quantenphysik basiert, ist diese Methode zukunftssicher. Es besteht kein Risiko, dass neue Algorithmen oder leistungsfähigere Computer diese Methode brechen könnten, da die Sicherheit auf grundlegenden physikalischen Prinzipien beruht. Die Umsetzung erfordert einen sorgfältigen Entwurf des optischen Quantenkanals. Optische Verstärker können nicht verwendet werden, da beim Kopieren eines Quants der Zustand und damit die Information verändert wird. Um große Entfernungen zu überbrücken, können mehrere QKD-Verbindungen mit Hilfe von vertrauenswürdigen Knoten verkettet werden. In Zukunft könnten Quanten-Repeater die Implementierung von QKD-Systemen über große Entfernungen vereinfachen. Diese Technologie befindet sich in einer frühen konzeptionellen Phase.

Auf dem Weg zu sicheren Post-Quanten-Übertragungsnetzen

Schon im Jahr 2014 begann ADVA mit Arbeiten zu quantensicheren Technologien und entwickelte Demonstratoren für QKD-fähige WDM-Verschlüsselung sowie einen Post-Quanten-Schlüsselaustausch. Im Jahr 2018 wurde mit der Erprobung dieser Technologien in Betriebsnetzen ein wesentlicher Meilenstein erreicht. Seither hat sich der Schwerpunkt auf die Kommerzialisierung von quantensicherer Verschlüsselungstechnik verschoben.

Gemeinsam mit den Technologiepartnern ID Quantique und Toshiba wurden QKD-Lösungen für den Einsatz in operativen Netzen weiter optimiert. Da sich Quanten nicht mittels stimulierter Emission mit den gleichen Zuständen vervielfachen lassen, können auf einer QKD-Verbindung keine optischen Verstärker eingesetzt werden. Für die praktischen Versuche musste die Entfernung zwischen den Standorten, an denen die Schlüssel generiert wurden, in Abhängigkeit von den Dämpfungseigenschaften der Glasfaser auf 40km bis 80km beschränkt werden. Es ist allerdings davon auszugehen, dass durch technologische Neuerungen in Zukunft auch längere Strecken überbrückt werden können.

Mit unserer umfangreichen Erfahrung bei der Implementierung und Zertifizierung von Sicherheitsfunktionen konnten unsere Kunden schon seit dem Jahr 2021 von robusten quantensicheren DWDM-Lösungen profitieren. Sie können sich zwischen QKD oder PQC für den geschützten Austausch von Sitzungsschlüsseln entscheiden. Beide Lösungen nutzen unsere zertifizierte und zugelassene quantenresistente AES-GCM-256-Verschlüsselung, um den breitbandigen Nutzverkehr in Echtzeit und mit geringster Latenzzeit zu schützen. Für den Anschluss von QKD-Geräten wurde in unserer FSP 3000 Plattform ein standardisiertes Schlüsselaustauschprotokoll implementiert. Damit lässt sich die quantenbasierte Schlüsselgenerierung von Drittanbietern wie ID Quantique oder Toshiba problemlos mit unserem optischen Übertragungssystem für höchste Bandbreiten kombinieren.



Schon im Jahr 2018 hatten wir eine PQC-Lösung mit einem McEliece-Algorithmus in unserem optischen Hochgeschwindigkeits-Transportsystem implementiert und konnten damit eine quantensichere 100-Gbit/s-Übertragung über 2800 km in einem Glasfasernetz mit Live-Verkehr demonstrieren. Unsere PQC-Lösung kombiniert klassische Verschlüsselung mit quantensicheren Algorithmen und kann mit QKD noch sicherer gemacht werden. Solche Hybridmodelle nutzen unsere umfassende Erfahrung bei der Implementierung bewährter Protokolle mit dem zusätzlichen Schutzniveau, das zur Abwehr von Quantenangriffen erforderlich ist.

ADVA hat Pionierarbeit bei der Entwicklung von Übertragungssystemen mit hoher Bitrate und niedrigster Latenz geleistet und macht nun einen großen Schritt in Richtung quantensicheren Schutz. Unsere jüngsten Produkte nutzen unsere Erfahrungen aus der frühen Entwicklung von Demonstratoren und den Tests in operativen Netzen. ADVA ist das erste Unternehmen, das eine quantensichere optische FSP 3000 Transportlösung sowie eine krypto-agile FSP 150 Lösung für Datennetze auf den Markt gebracht hat. Beide Lösungen können mit Post-Quanten-Kryptographie betrieben und auf aktuelle PQC-Algorithmen – wie beispielsweise die von NIST standardisierten Verfahren – aufgerüstet werden. Unser bahnbrechendes Engagement im Bereich der quantensicheren Übertragung sehr hoher Bandbreiten bietet unseren Kunden die einzigartige Möglichkeit, sich schon heute gegen zukünftige Angriffe durch Quantencomputer zu schützen. Durch die Integration aller Sicherheitsfunktionen in einem kompakten, manipulationsgeschützten Krypto-Modul schaffen wir eine wirklich zukunftssichere Lösung. Unsere Kunden können ihre Netze mit unseren optischen Übertragungssystemen und Lösungen für den Netzzugang sicher ausbauen, ohne sich Sorgen über eine Quantenbedrohung machen zu müssen.