Zukunftssicher

Der Weg zu quantensicherem Schutz vor Bedrohungen

Vanguard Report

April 2022

In Auftrag gegeben von

IBM

451 Research

S&P Global
Market Intelligence

Über den Autor

John Abbott

Leitender Forschungsanalyst, 4SIGHT

John Abbott befasst sich im Auftrag von 451 Research, ein Unternehmen von S&P Global Market Intelligence, mit Themen zur System-, Speicher- und Softwareinfrastruktur. In seiner mehr als 30-jährigen Laufbahn hat er Pionierarbeit in den Bereichen Unix, Supercomputing, Systemarchitektur, Softwareentwicklung und Speicherung geleistet.

Als einer der Mitbegründer von The 451 Group im Oktober 1999 leitete John Abbott den Analystenbetrieb in der Niederlassung San Francisco des Unternehmens. Er gehört zu den Hauptautoren zahlreicher Sonderberichte von 451 Research, u. a. der Berichte über Speichervirtualisierung und Blade-Server – die ersten umfassenden Studien zu diesen Themen, die veröffentlich wurden. Zuletzt standen Themen wie konvergente Infrastruktur, neue Systemarchitekturen, KI und die Beschleunigung von Deep-Learning in seinem Fokus. Darüber hinaus war er an der Gründung von 4SIGHT beteiligt, dem Framework von 451 Research für die vorausschauende, langfristige Berichterstattung über neue Technologien.

Bereits 1984 begann er damit, ausführlich über den Technologiesektor zu berichten und konnte dafür auf seine bereits gesammelten Erfahrungen als technischer Autor und seine direkte Mitarbeit an Mainframes, den frühen PCs und Unix-Workstations zurückgreifen. Als freiberuflicher Journalist schrieb er unter anderem für Publikationen wie Computing, Computer Weekly, The Financial Times und The Times. 1987 wurde er zum Redakteur des wöchentlichen Unix-Newsletters von ComputerWire, Unigram.X, ernannt und wurde später Redakteur des täglich erscheinenden Computergram International, zuerst in London und später in San Francisco. Außerdem gründete er die Zweigstelle von 451 Research in San Francisco, wo er mehr als zehn Jahre lebte.

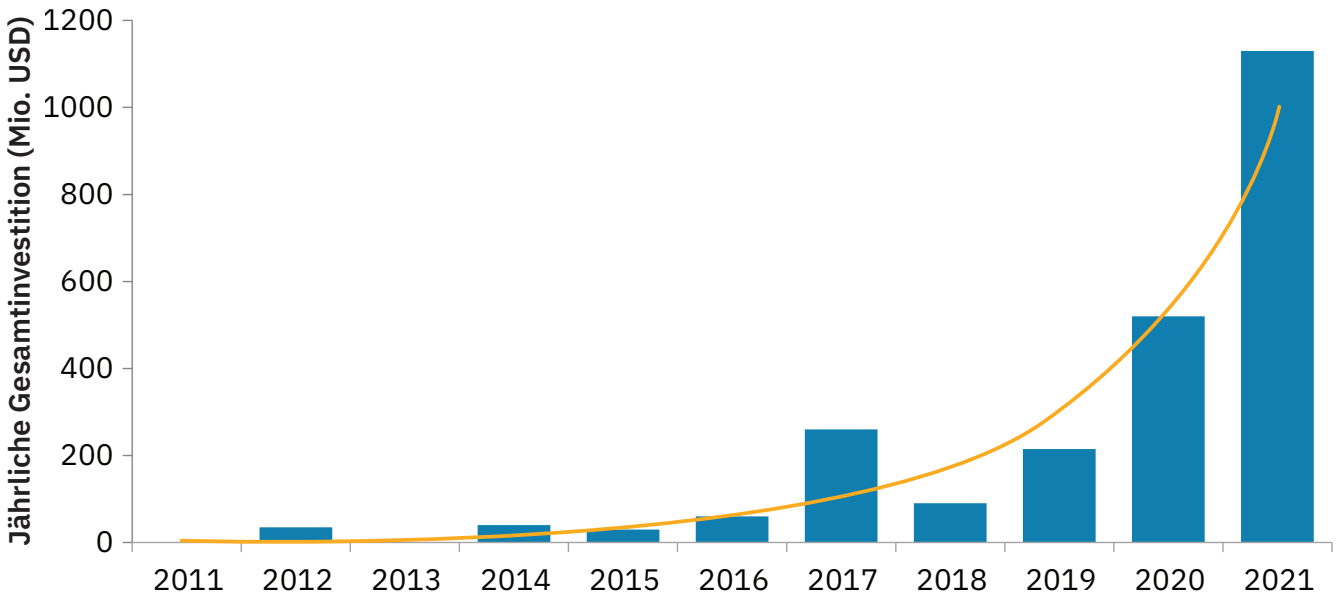
John Abbott studierte Musik an der Universität von Keele und hat einen MA in moderner englischer Literatur von der Universität London.

Einführung

Quantencomputing lässt sich heute am besten als Investition mit hohem Risiko und hohem Ertrag beschreiben. Es besteht keine Garantie dafür, dass noch zu unseren Lebzeiten ein universeller und praktikabler Quantencomputer zum Einsatz kommen wird. Forschungslabore – und zunehmend auch Privatunternehmen aus dem Technologiesektor – durchbrechen jedoch täglich Grenzen und sorgen für Innovationen an der Spitze der Wissenschaft. Und der Nutzen könnte gewaltig sein, denn es könnten Probleme gelöst werden, die derzeit von keinem (klassischen) Supercomputer bewältigt werden können. Dies erklärt, warum beide Seiten – sowohl Verkäufer als auch Benutzer – bereit sind, das Risiko mit dieser potenziell disruptiven Technologie einzugehen. Daten von S&P Capital IP Pro (Abbildung 1) belegen, dass sich Quanten-Startups in den vergangenen zehn Jahren 2,4 Milliarden US-Dollar an Investitionen sichern konnten. Das Jahr 2021 brachte mit Investitionen in Höhe von 1,1 Milliarden US-Dollar in Quantenunternehmen einen großen Interessenszuwachs mit sich. Und diese Daten beinhalten noch nicht einmal die massiven Investitionen etablierter IT-Unternehmen wie IBM, Amazon, Google und Honeywell.

Die Chance bringt aber auch einige große Bedenken mit sich. Am dringlichsten ist vielleicht die Bedrohung im Hinblick auf heutige Sicherheitspraktiken. Mithilfe von Quantencomputern wären böswillige Akteure in der Lage, digitale Signaturen zu fälschen und die derzeitigen Kryptographie- und Verschlüsselungssysteme zu knacken, einschließlich der Public-Key-Infrastructure, die heute auf der ganzen Welt tief in die IT-Systeme eingebettet ist. Schlimmer noch: Selbst verschlüsselte Daten, die derzeit geschützt sind, könnten für eine spätere Entschlüsselung gespeichert werden, sobald praktische Quantencomputer verfügbar sind. Das ist ein Problem, das nicht aufgeschoben werden kann. Je länger wir warten, desto mehr Daten erzeugen wir, die Gefahren ausgesetzt sind.

Abbildung 1: Investitionen in Startups im Bereich Quanteninformatik



Quelle: S&P Capital IQ Pro

Einschätzung von 451 Research

Es ist nicht möglich, genau vorherzusagen, wann ein Quantencomputer, der den Shor-Algorithmus effektiv ausführen kann, so weit verbreitet sein wird, dass ein böswilliger Akteur Zugang zu ihm haben könnte. Bislang ist noch kein IT-Anbieter in der Lage, einen genauen Zeitplan zu benennen, bis wann Quantencomputing klassische Computer deutlich übertreffen wird. Doch die rasanten technologischen Fortschritte der letzten fünf Jahre und die erheblichen Investitionen, die heute getätigt werden, lassen vermuten, dass dieser Tag vielleicht schon zum Ende des Jahrzehnts kommen wird. Dann sind alle Informationen, die derzeit durch Public-Key-Algorithmen geschützt sind, von der Aufdeckung bedroht. Für staatliche Verteidigungs- und Nachrichtendienste sowie für Anbieter von Cloud-Diensten und Systemlieferanten, deren Kunden zu den regulierten Branchen gehören, ist das Risiko bereits zu hoch, um es zu ignorieren. Trotz der Fehlalarme der Vergangenheit (man denke nur an das Jahr 2000, als eine weit verbreitete Abkürzung in der Computerprogrammierung beim Jahreswechsel von 1999 auf 2000 verheerenden Schaden anzurichten drohte) und der Unwägbarkeiten der Zukunft ist eines klar: Die Gefahr, die heute von Cyberangriffen ausgeht, stellt ein immenses, nicht zu unterschätzendes Problem dar, denn immer wieder werden neue Arten von Bedrohungen und Schwachstellen auftauchen. Sicherheitsrichtlinien müssen ständig überprüft und aktualisiert werden. Hierbei spielen quantensichere Verschlüsselungstechnologien neben der Implementierung von Krypto-Agilität und einem Bestand an kryptografischen Ressourcen eine wichtige Rolle.

Quantenresistente und quantensichere Szenarien

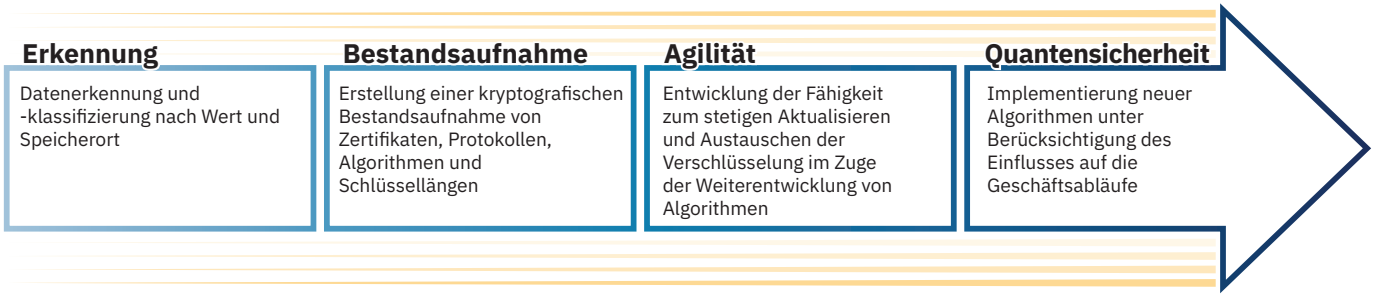
Das Problem: Die derzeitige Generation gängiger Sicherheitsalgorithmen basiert auf komplexen mathematischen Problemen, die für klassische Computer zu schwer zu knacken sind. Diese Probleme könnten jedoch leicht von einem Quantencomputer mit ausreichender Rechenleistung gelöst werden – eine Annahme, die seit 1994 weithin akzeptiert wird, als der amerikanische Mathematiker Peter Shor den Polynomialzeit-Algorithmus entdeckte, der heute als Shor-Algorithmus bekannt ist. Doch schon drei Jahre später wurde der erste Quantencomputer gebaut. Die Weiterentwicklung quantensicherer Algorithmen ist in den letzten zehn Jahren enorm vorangeschritten. Aber die Umstellung von in Behörden und der Industrie weit verbreiteten Public-Key-Verschlüsselungssystemen auf neue Algorithmen könnte Jahrzehnte dauern.

Aus diesem Grund haben Organisationen wie das National Institute of Standards and Technology (NIST) und das Department of Homeland Security in den USA sowohl an der Standardisierung der Algorithmen selbst als auch an Empfehlungen gearbeitet, die Unternehmen bei der Vorbereitung auf den Übergang zur Post-Quantum-Kryptografie helfen sollen. Diese Arbeit führte im Januar zu einem Memorandum des Weißen Hauses, das die Verteidigungs- und Nachrichtendienste der Regierung aufforderte, mit der Umstellung zu beginnen.

Das Knacken einer zusammengesetzten 2.048-Bit-Ganzzahl (durch Auffinden der Primfaktoren) würde auf den leistungsfähigsten Computern, die heute verfügbar sind, Millionen von Jahre dauern. Mithilfe eines Quantencomputers könnte diese Arbeit theoretisch in nur wenigen Stunden erledigt werden. Zu den aktuellen Public-Key-Schemata, die mit dem Shor-Algorithmus geknackt wurden, gehören der ehrwürdige RSA-Algorithmus – der bereits 45 Jahre alt ist, jedoch noch bis heute in nahezu allen internetbasierten Transaktionen verwendet wird – sowie der Data Security Standard, das Paillier-Kryptosystem, der Elliptic Curve Digital Signature Algorithm, der Elliptic Curve Diffie-Hellman und das ElGamal-Verschlüsselungsverfahren. Eine lange Liste an Standards, die von NIST, ISO/IEC, ETSI und IETF erstellt wurden, sind davon betroffen, was darauf hindeutet, dass es sich hierbei um ein weltweites Problem handelt: Der chinesische SM2-Algorithmus für digitale Signaturen und der nationale Verschlüsselungsstandard SM9 wurden ebenfalls geknackt.

Der 2016 mit einer Aufforderung zur Einreichung von Vorschlägen gestartete Standardprozess des NIST hat eine neue Reihe von quantenresistenten Kandidaten ermittelt. Zu den verschiedenen Ansätzen – wie gitter-, multivariate, hash- oder codebasierte Kryptographie – gehören der gitterbasierte CRYSTALS-Kyber-Schlüsselkapselungsmechanismus (KEM), McEliece (codebasierter KEM) und die Post-Quantum-Signaturverfahren Falcon (gitterbasiert) und Rainbow (multivariat). Diese sowie andere Finalisten werden nach der jetzt dritten abgeschlossenen Wettbewerbsrunde in einen Normentwurf aufgenommen. Runde vier, die auch alternative Algorithmen und die Aufforderung zur Einreichung zusätzlicher Signaturverfahren beinhaltet, wird noch dieses Jahr gestartet und bis Ende 2024 abgeschlossen sein.

Abbildung 2: Meilensteine auf dem Weg zur Quantensicherheit



Quelle: 451 Research

Der Weg zu quantensicherer Kryptografie

Welche Maßnahmen sollten Unternehmen jetzt ergreifen, um für die Integration quantensicherer Verschlüsselung in ihre Informationssicherheitsarchitektur über die nächsten zehn Jahre vorbereitet zu sein? Der erste bereits angelaufene Schritt beinhaltet die Teilnahme am Standardisierungsprozess. Jede Organisation, die ein Interesse daran hat, betrügerische Authentifizierung zu verhindern, die Integrität der Verschlüsselung zu schützen und die Kompromittierung der digitalen Signatur zu vermeiden, muss sich aktiv dafür einsetzen, dass ihre Anforderungen von der genehmigten Liste der endgültigen Algorithmen, Prozessoren und Tools erfüllt werden. Trotz guter Fortschritte seitens der Standardisierungsgremien handelt es sich hierbei um eine andauernde Herausforderung: Es werden mehr Algorithmen benötigt. Darüber hinaus führen die folgenden Meilensteine zur Quantensicherheit.

- **Datenerkennung und -klassifizierung:** Es ist eine Bestandsaufnahme kritischer Daten durchzuführen. Welche besitzen den größten Wert? Wo befinden sich die Daten? Welche Anforderungen sind zu erfüllen? Dieses Verständnis ist von entscheidender Bedeutung, da viele Unternehmen weder über den genauen Umfang noch den Wert ihrer Daten informiert sind. Ohne dieses Wissen können sie ihre größten Sicherheitslücken jedoch nicht identifizieren. Sie müssen daher zunächst eine Datenbestandsaufnahme mit definierten Zuständigkeiten erstellen und verwalten.
- **Bestand an Verschlüsselungsressourcen:** Eine kryptografische Bestandsaufnahme gibt Auskunft darüber, wo und wie anfällige Public-Key-Verschlüsselung verwendet wird, und enthält Details wie Zertifikate, Verschlüsselungsprotokolle, Algorithmen und Schlüssellängen. Der Bestand muss so verwaltet werden, dass er den gesamten Lebenszyklus von Zertifikaten und Kodierungsschlüsseln abdeckt.
- **Agilität von Verschlüsselungsressourcen:** Bei ihren Plänen und Übergangsprozessen müssen Unternehmen die Agilität von Verschlüsselungsressourcen berücksichtigen, damit sie Anpassungen reibungslos vornehmen können, wenn sich die Technologie weiterentwickelt und sich die Umstände ändern. Sie sollten Prozesse entwickeln und einführen, mit denen sie die Kryptografie der aktuellen Generation innerhalb genau festgelegter Vorlaufzeiten leichter aktualisieren oder ersetzen – und anschließend testen – können.
- **Quantensicher:** Unternehmen müssen neue Algorithmen implementieren und sich der potenziellen Auswirkungen quantensicherer Kryptografie auf die Geschäftsleistung bewusst sein.

Jedes Unternehmen ist anders und nicht jedes wird alles ändern können (oder dazu bereit sein) – ob aus Kostengründen oder aufgrund von Problemen beim Lebenszyklusmanagement. Aber die Möglichkeit, Sicherheitsprotokolle zu aktualisieren oder zu ersetzen, ist sowohl kurz- als auch langfristig von entscheidender Bedeutung. Da sie eng mit der Systeminfrastruktur verknüpft ist, erfordert das Erreichen agiler Verschlüsselungsressourcen die Zusammenarbeit von Systemdesignern, Anwendungsentwicklern und Sicherheitsexperten. Derzeit fehlt es an Instrumenten zur Unterstützung dieses Prozesses.

Für Unternehmen werden bei der Priorisierung einer quantensicheren kryptografischen Ersatzlösung eine Vielzahl von Faktoren eine Rolle spielen: Wert der geschützten Vermögenswerte, Schwachstellen der geschützten Daten (z. B. Schlüsselspeicher und Kennwörter), vernetzte Systeme, die betroffen sein könnten (z. B. Informationsaustausch mit externen Stellen, einschließlich Bundesbehörden), und Dauer des Schutzes von Daten. Hybride Verfahren, die klassische und quantensichere Algorithmen kombinieren, werden während der langen Übergangszeit notwendig sein.

Umsetzung, Motivation und Antriebsfaktoren

Systemanbieter und die großen Cloud-Service-Anbieter, deren Anlagen und Infrastrukturen unternehmenskritische Workloads beherbergen, können es sich nicht leisten, auf die Fertigstellung der Standards für quantensichere Kryptografie zu warten. Sie arbeiten bereits seit mehreren Jahren an diesem Problem und haben zur Auswahl von Algorithmen und Protokollen beigetragen, die auf der Liste der endgültigen Normen im Jahr 2024 ganz oben stehen werden. Eine Reihe von cloudbasierten Schlüsselmanagementservices unterstützt bereits die Algorithmen der zweiten und dritten Runde. Auch Kunden beginnen, diese Services zu nutzen, um die potenziellen Auswirkungen auf die Anwendungsleistung messen zu können, die sich voraussichtlich aus der zusätzlichen Belastung der Bandbreitennutzung und der Latenz ergeben werden. Außerdem versuchen sie wahrscheinlich auftretende Verbindungsausfälle auf den Proxy-Ebenen der Transportebenensicherheit abzufedern. Alle sind sich jedoch darüber einig, dass es sich beim Übergang zur Quantensicherheit um einen langjährigen Prozess handeln wird, da sich Standards und Technologien ständig weiterentwickeln. Ebenso einig ist man sich darüber, dass dieser Prozess mit dem Schutz der Kerninfrastruktur beginnt.

In der Systemwelt sind Großrechner (Mainframes) als hochverfügbare und sichere Kerninfrastruktur für die größten Banken, Versicherungsgesellschaften sowie Telekommunikations-, Einzelhandels- und Transportunternehmen immer noch weit verbreitet – eine Position, die sie seit über einem halben Jahrhundert innehaben. Die neueste Generation von Mainframes wird mit quantensicheren Hardwaresicherheitsmodulen ausgestattet sein. Diese arbeiten in Verbindung mit aktuellen Betriebssystemkomponenten, Schlüsselmanagement-APIs und als Unterstützung für eine Reihe der neuen quantenresistenten Algorithmen. Quantensichere Secure-Boot-Technologie mit einer Root-of-Trust-Hardware wird zum Schutz der Integrität der Systemboot-Firmware eingesetzt. Außerdem werden quantensichere Mechanismen für den sicheren Austausch kryptografischer Schlüssel mit Geschäftspartnern über Anwendungsprogrammierschnittstellen bereitgestellt.

Cloud-Service-Provider und Lieferanten übernehmen eine wichtige Rolle dabei, ihre Kunden bei der Umstellung auf quantensichere Verschlüsselung zu unterstützen. Gesetzliche Verlautbarungen allein reichen nicht aus. Sie sind in der Regel nicht präskriptiv genug, um klare Richtlinien für Organisationen bereitzustellen, die über keine umfangreichen eigenen Fachkenntnisse verfügen. Anbieter, die bereits unternehmenskritische Infrastrukturen bereitstellen, können den Prozess vereinfachen, indem sie den Schutz des Kerngeschäftssystems ohne zusätzliche Änderungen auf Systemebene für die Aktivierung bereitstellen. Sie können auch dringend benötigte Erkennungstools für die Analyse von kryptografischen Anwendungen bereitstellen. Unternehmen, die für Daten verantwortlich sind, müssen sicherstellen, dass ihre Daten über den gesamten Lebenszyklus geschützt sind – sowohl heute als auch in Zukunft. Denn Daten, die heute noch mit klassischen Algorithmen verschlüsselt werden, könnten in der Zukunft mithilfe eines fortschrittlichen Quantencomputers entschlüsselt werden. Wenn diese Daten 20 Jahre lang gesichert werden müssen, reicht dies bis weit in die 2040er-Jahre hinein. Selbst Skeptiker, die glauben, dass der Einsatz von praktikablem Quantencomputing noch in weiter Zukunft liegt, müssen mittlerweile anerkennen, dass sich die Wahrscheinlichkeit in Anbetracht des derzeitigen Fortschritts bis dahin deutlich erhöht haben wird.

Schlussfolgerungen

Ein vollständig realisierter Quantencomputer würde Fortschritte in den Bereichen Chemie, maschinelles Lernen, Finanzen, Verkehr, Gesundheitswesen und darüber hinaus in vielen anderen Bereichen ermöglichen. Quantencomputer würden die Verarbeitung von Gleichungen, die mit den heute verwendeten klassischen, deterministischen Computern nicht durchführbar sind, exponentiell beschleunigen.

Die Kehrseite der Medaille sind die Auswirkungen, die das Quantencomputing auf die bereits wachsende Bedrohung des Datenschutzes und der Privatsphäre durch Cyberangriffe haben könnte. Mit steigendem geschäftlichen Nutzen von Daten steigen auch Umfang und Kosten der Datenschutzanforderungen. Und da die Daten über einen langjährigen Wert verfügen, muss mit zunehmender Wahrscheinlichkeit in Betracht gezogen werden, dass Quantencomputing in absehbarer Zeit Realität werden wird. Frühe Maßnahmen werden eine sichere und kontrollierte Entwicklung hin zu einer quantensicheren Kerninfrastruktur und der Implementierung von Tools begünstigen, die aktuelle Sicherheitslücken auf der Anwendungsebene aufdecken. Außerdem werden sie zum Schutz von Schlüsselaustauschsystemen, die unternehmensübergreifend eingesetzt werden können, und ebenso zum kontinuierlichen Schutz der in den Daten dauerhaft gespeicherten Geheimnisse beitragen.

KONTAKT

Nord- und Südamerika
+1 877 863 1306
market.intelligence@spglobal.com

Europa, Naher Osten & Afrika
+44 20 7176 1234
market.intelligence@spglobal.com

Asien/Pazifik
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence