Whitepaper

Post-Quanten-Kryptografie: Sichere Verschlüsselung für das Quanten-Zeitalter

Auf Quantencomputern basierte Technologie hat das Potential, unterschiedlichste IT-Bereiche und Branchen zu revolutionieren – sowohl im positiven als auch im negativen Sinne. Eine signifikante Steigerung der Rechenleistung bedeutet auf der einen Seite mehr Analyse- und Verarbeitungskapazität für große Datenmengen – und damit neue Erkenntnisse, neue Anwendungsfelder und Geschäftsmodelle. Auf der anderen Seite steht so aber auch mehr Rechenleistung zur Verfügung, um heutige Sicherheitsmechanismen auszuhebeln. Der Bereich IT-Sicherheit und insbesondere Verschlüsselungsmechanismen werden von der Einführung von Quantenrechnern betroffen sein. Einige der heute meistgenutzten Verschlüsselungsalgorithmen werden dadurch ungültig. Denn ihre Sicherheit baut im Wesentlichen darauf auf, dass aktuell verfügbare Computer mit ihrer Rechenkapazität zu lange brauchen, um sie entschlüsseln zu können.

Mit Quantenrechnern ist dies nicht mehr der Fall. Die Migration von aktuell sicheren kryptografischen Algorithmen hin zu quantensicheren Algorithmen kann in der Praxis sehr langwierig sein. Vor allem dann, wenn sie in Branchen und Anwendungsbereichen eingesetzt werden, in denen Produkte wie z. B. intelligente Stromzähler und Fahrzeuge heute schon entwickelt werden, um 10 oder 15 Jahren im Markt zu bleiben. Daher ist es vor allem bei Produkten mit langen Lebenszyklen für die Anwender von kryptografischen Algorithmen wichtig, heute schon auf Crypto-Agilität zu setzen. „Crypto Agility“ meint hier die Fähigkeit, die heute verwendeten Algorithmen gegen quantensichere Algorithmen auszutauschen – auch bei Produkten, die schon im Markt sind. Utimaco Hardware-Sicherheitsmodule und das flexible Software Development Kit sind für diese Aufgabe besonders geeignet – und werden daher auch von führenden Experten im Bereich Post-Quanten-Kryptografie eingesetzt.

Einleitung: Was Post-Quanten-Kryptografie ist

Mit Quantensystemen hat eine neue Generation von Rechnern die Bühne betreten. Diese arbeiten nicht mit Bits; das heißt, sie kennen nicht nur die Zustände 0 und 1 wie herkömmliche Computer. Stattdessen nutzen Quantenrechner so genannte Quantenbits – Qbits – mit drei Zuständen: 0, 1 sowie einem dazwischen, der Superposition. Im Gegensatz zu Bits kann ein Quantenbit beliebige Zustände gleichzeitig einnehmen. Dadurch ist ein solcher Rechner in der Lage, viel mehr Rechenoperationen parallel durchzuführen. Forscher schätzen, dass ein Quantensystem etwa 1.000 Mal so schnell[1] arbeitet wie ein heutiger Supercomputer.

Diese Rechenleistung lässt sich – leider – auch dazu nutzen, um vorhandene Verschlüsselungsverfahren zu kompromittieren. Daher müssen diese Technologien so modifiziert werden, dass sie Angriffen mit Quantenrechnern standhalten. Erforderlich ist dazu Post-Quanten-Kryptografie (PQC, Post-Quantum Cryptography). PQC-Verfahren sind Verschlüsselungssysteme (Krypto-Systeme), die auf herkömmlichen Rechnern, beispielsweise PCs und mobilen Endgeräten, eingesetzt werden können und Angriffen mit Quantencomputern standhalten können.

Chancen der Quanten-Technologie: Aktuelle Einsatzszenarien

Quantenrechner wurden natürlich nicht per se als „Cyber-Waffen" konzipiert. Solche Systeme eröffnen Unternehmen, Forschern und öffentlichen Einrichtungen neue Optionen. So lassen sich dank der hohen Rechenleistung solcher Computer komplexe Berechnungen mehrere Tausend Mal schneller durchführen, als mit konventionellen Systemen. Das gilt jedoch nicht für alle Arten von Rechenaufgaben.

Besonders effektiv sind Quantensysteme, wenn eine Aufgabe eine große Zahl von Kombinationsmöglichkeiten enthält. Das ist beispielsweise bei der Berechnung von Verkehrsströmen der Fall. Automobilkonzerne und Stadtplaner setzen bereits erste Versionen von Quantensystemen ein, um den Autoverkehr in Großstädten zu analysieren und eine optimale Verkehrsführung zu finden. Im Finanzbereich können Quantenrechner dabei helfen, für einen Kunden das optimale Aktienportfolio zusammenzustellen. Hersteller und Logistikunternehmen wiederum haben die Möglichkeit, mithilfe von Quantensystemen Lieferwege zu optimieren. Weitere Einsatzfelder sind unter anderem die Suche nach neuen Medikamenten, die Überprüfung von Software und das Trainieren von neuronalen Netzen, die im Bereich maschinelles Lernen eingesetzt werden.[2]

Die dunklen Seiten der Quanten-Technologie

Doch mit der Verfügbarkeit von Quantenrechnern sind auch Risiken verbunden. Dies gilt umso mehr, als solche Systeme künftig über die Cloud bereitgestellt werden. IBM bietet bereits jetzt Forschern und Wissenschaftlern einen Zugang zu einem Quantenrechner in der Cloud an. Unternehmen wie Google, IBM und Amazon Web Services werden folgen. Damit werden Quantenrechner für einen breiten Nutzerkreis verfügbar, auch solchen Anwendern, die diese Systeme für das „Knacken" von Verschlüsselungsverfahren verwenden. Forscher rechnen damit, dass in etwa zehn bis 15 Jahren Quantencomputer in größerem Maßstab verfügbar sein werden.

Hinzu kommt ein weiterer Faktor: Speziell Unternehmen aus Hightech-Ländern wie Deutschland müssen davon ausgehen, dass staatliche Stellen in anderen Nationen Quantenrechner dazu nutzen werden, um Geschäftsgeheimnisse und Forschungsergebnisse zu entwenden. Nach Angaben des Digital-

1 http://www.datasciencecentral.com/profiles/blogs/understanding-the-quantum-computing-landscape-today-buy-rent-or-w

2 https://www.dwavesys.com/sites/default/files/D-Wave%202000Q%20Tech%20Collateral_0117F.pdf
https://www.accenture.com/t00010101T000000__w__/br-pt/_acnmedia/PDF-45/Accenture-Innovating-Quantum-Computing-Novo.pdf

verbandes Bitkom wurden 2016 und 2017 mehr als 53 Prozent der deutschen Unternehmen Opfer von Wirtschaftsspionage und Datendiebstahl. Entwendet wurden vorzugsweise E-Mails, Finanzdaten sowie Informationen aus der Forschungsabteilung und dem Personalwesen.[3]

Wollen deutsche Unternehmen durch den Abfluss und Diebstahl von Know-how nicht wirtschaftlich ins Hintertreffen geraten, müssen sie sensible Informationen so verschlüsseln, dass sie auch mithilfe von Quantensystemen nicht kompromittiert werden können.

Quanten-Systeme und IT-Sicherheit

Das Kernproblem von Quantenrechnern im Zusammenhang mit Verschlüsselung ist, dass sich mit solchen Systemen herkömmliche Verschlüsselungstechniken aushebeln lassen. Dazu zählen Verfahren auf Basis elliptischer Kurven (Elliptic Curve Digital Signature Algorithm, ECDSA), mit denen beispielsweise die Schlüssel von Blockchain geschützt werden.

Gefährdet sind zudem asymmetrische Verschlüsselungstechniken, die mit einem öffentlichen und privaten Schlüssel arbeiten (Public-Key-Infrastruktur-Systeme, PKI). Dazu gehört das weit verbreitete RSA-Verfahren. Dessen Sicherheit basierte bislang darauf, dass es für einen konventionellen Rechner schwer ist, Produkte großer Primzahlen in ihre einzelnen Bestandteile zu zerlegen.

Ein Beispiel: Jeder PC kann zwar innerhalb kürzester Zeit 2.803 mit 4.219 multiplizieren. Das Ergebnis 11.825.857 in die beiden Ausgangszahlen zu zerlegen, erfordert jedoch eine immense Rechenleistung.

Quantencomputer schaffen solche Aufgaben deutlich schneller als konventionelle Computer. Der Amerikaner Peter W. Shor hat bereits 1994 einen entsprechenden Algorithmus vorgestellt. Ab 2019, so Fachleute, ist damit zu rechnen, dass Quantenrechner verfügbar sind, welche die RSA-Verschlüs-

Name	function	pre-quantum security level	post-quantum security level
Symmetric cryptography			
AES-128 [1]	block cipher	128	64 (Grover)
AES-256 [1]	block cipher	256	128 (Grover)
Salsa20 [2]	stream cipher	256	128 (Grover)
GMAC [3]	MAC	128	128 (no impact)
Poly1305 [4]	MAC	128	128 (no impact)
SHA-256 [5]	hash function	256	128 (Grover)
SHA-3 [6]	hash function	256	128 (Grover)
Public-key cryptography			
RSA-3072 [7]	encryption	128	broken (Shor)
RSA-3072 [7]	signature	128	broken (Shor)
DH-3072 [8]	key exchange	128	broken (Shor)
DSA-3072 [9, 10]	signature	128	broken (Shor)
256-bit ECDH [11, 12, 13]	key exchange	128	broken (Shor)
256-bit ECDSA [14, 15]	signature	128	broken (Shor)

Das Sicherheitsniveau von Verschlüsselungsverfahren – mit und ohne Berücksichtigung von Quantencomputing (Quelle: Daniel J. Bernstein / Tanja Lange, 2016)

3 https://www.bitkom.org/Presse/Presseinformation/Spionage-Sabotage-Datendiebstahl-Deutscher-Wirtschaft-entsteht-jaehrlich-ein-Schaden-von-55-Milliarden-Euro.html

selung „knacken“ können. Gleiches gilt für Verfahren auf Basis von Diffie-Hellman (DH) und des Digital Signature Algorithm (DSA).

Auch symmetrische Verschlüsselungstechniken wie AES (Advanced Encryption Standard) und SHA (Secure Hash Algorithm) verlieren durch Quantenrechner einen Teil ihrer Schutzwirkung.

Forscher wie Daniel L. Bernstein und Tanja Lange haben ermittelt, dass beispielsweise AES mit 256-Bit-Schlüsseln zukünftig nur noch so sicher ist wie heute eine AES-Verschlüsselung mit 128 Bit langen Keys.

Bereits jetzt handeln

Selbst dann, wenn Quantensysteme erst in zehn oder 15 Jahren für jedermann verfügbar sein sollten, müssen IT-Verantwortliche und Geschäftsführer bereits heute das Thema „Post-Quantum-Kryptografie“ auf die Agenda setzen. Ein Grund ist, dass es Zeit kostet, vorhandene Verschlüsselungsverfahren auf eine neue Basis zu stellen. Die Cloud Security Alliance (CSA)[4] geht zum Beispiel von fünf bis zehn Jahren aus.

Ein weiterer Punkt ist, dass Daten, die mithilfe älterer Verfahren verschlüsselt wurden, anfällig für Quantenangriffe sind. Angreifer könnten sich dadurch Zugang zu solchen Daten verschaffen. Unternehmen und öffentliche Einrichtungen müssen somit dafür Sorge tragen, dass alle gefährdeten vertraulichen Daten mithilfe von PQC-Verfahren gegen solche Attacken geschützt werden. Das erfordert einen erheblichen Aufwand, von der Erfassung und Kategorisierung solcher Informationsbestände bis hin zur Neuverschlüsselung mithilfe von PQC-Lösungen.

Zu den wichtigsten Faktoren, die eine Post-Quantum-Kryptografie erfordern, zählt jedoch die Digitalisierung. Konzepte wie Industrie 4.0, der digitale Handel, Smart Metering, autonomes Fahren und das Internet der Dinge basieren auf einer sicheren Kommunikation. Gelingt es Hackern, Fabriken, Verkehrsleitsysteme oder Kraftwerke lahmzulegen, kann das katastrophale Folgen haben. Doch gerade solche Einrichtungen mit einer gehärteten IT-Sicherheits- und Ver schlüsselungstechnologie auszustatten, erfordert einen Vorlauf von mehreren Jahren.

> Unternehmen und öffentliche Einrichtungen sollten sich bereits jetzt mit der Tatsache beschäftigen, dass herkömmliche Verschlüsselungsverfahren in wenigen Jahren durch Quantenrechner obsolet sind. Denn die Umstellung auf eine Post-Quantum-Kryptografie kostet Zeit und erfordert eine gute Vorbereitung.
>
> *Malte Pollmann, CEO von Utimaco*

4 https://downloads.cloudsecurityalliance.org/assets/research/quantum-safe-security/applied-quantum-safe-security.pdf

> Crypto Agility ist eine Anforderung an zukunftssichere Kryptografie-Lösungen, die auch im Zeitalter von Quantenrechnern Bestand haben sollen. Eine zentrale Rolle bei solchen Lösungen spielen Hardware-Sicherheitsmodule und flexible Software Development Kits.
>
> *Malte Pollmann, CEO von Utimaco*

Koexistenz von neuen und bestehenden Umgebungen

Bei der Umstellung auf eine quantenresistente Krypto-Systemumgebung in Unternehmen oder öffentlichen Einrichtungen gilt es einen wesentlichen Punkt zu bedenken: Es ist meist nicht möglich, alles auf einmal umzusetzen und quasi auf der „grünen Wiese" zu starten. Das wäre der Fall, wenn ausschließlich Lösungen, Algorithmen, Verfahren für den Austausch von Schlüsselmaterial und Zertifikate zum Einsatz kämen, die bereits für das PQC-Zeitalter ausgelegt sind.

Das Amerikanische „National Institute of Standards and Technology" (NIST) geht davon aus, dass sie im Jahr 2023 Algorithmen veröffentlichen werden, die gegen Angriffe mit Quantenrechnern resistent sind.[5] Doch ist es aufwändig, vorhandene Schlüssel und Krypto-Materialien gegen neue Versionen auszutauschen. In der Praxis werden somit Krypto-Systeme unterschiedlicher Art koexistieren – solche, die Post-Quanten-Kryptografie unterstützen und solche, die dies nicht tun.

Hinzu kommt ein weiterer Punkt: die unterschiedlichen Entwicklungs- und Nutzungszeiträume von Produkten. In dieser Beziehung gibt es erhebliche Unterschiede. In der Industrie, dem Energiesektor und dem Automobil-Bereich sind Entwicklungszyklen von zwei bis vier Jahren üblich. Die Nutzungsdauer von Maschinen und Fahrzeugen liegt meist bei sieben Jahren oder länger.

Das heißt, eine Kryptografie-Lösung muss sich an neue Anforderungen anpassen lassen, beispielsweise Post-Quanten-Verschlüsselungslösungen. Das ist nur dann mit akzeptablem Aufwand möglich, wenn eine Kryptografie-Umgebung agil ist, sprich „Crypto Agility" unterstützt.

Warum Crypto Agility wichtig ist

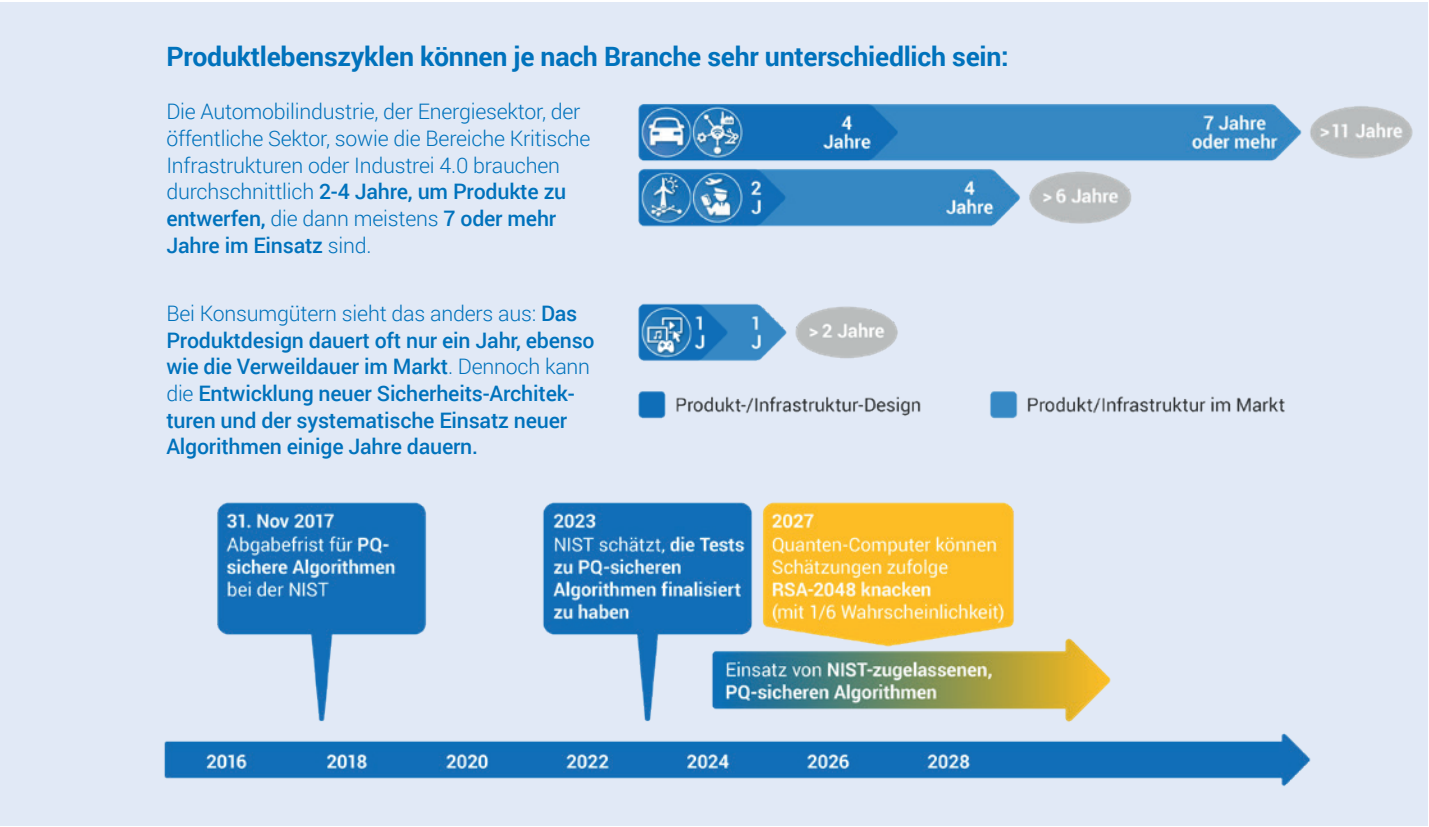
Krypto-Agilität bedeutet, dass Applikationen, Endgeräte und Hardware-Sicherheitsmodule im Bereich Verschlüsselung flexible und „agile" Protokolle und Update-Verfahren verwenden sollten, die zum Beispiel eine Umstellung auf Post-Quantum-Kryptografie-Primitive ermöglichen. Das muss auf einfache und schnelle Weise erfolgen, um die Angriffsfläche zu verringern und den Aufwand für den Nutzer in Grenzen zu halten.[6]

Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) rät dazu, bei der Neu- und Weiterentwicklung darauf zu achten, dass neue Standards und Algorithmen im Bereich Verschlüsselung umgehend implementiert werden können.[7] Der Hintergrund: Das BSI hat angesichts der schnellen Entwicklung

5 https://csrc.nist.gov/CSRC/media/Presentations/Update-on-the-NIST-Post-Quantum-Cryptography-Proje/images-media/2_post-quantum_dmoody.pdf

6 https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Practical.PostQuantum.Cryptography_WP_FraunhoferSIT.pdf?_=1503992279

7 https://www.bsi.bund.de/DE/Publikationen/BSIForumkes/forumkes_node.html;jsessionid=84FC91445F5B5E029EC976F5CF4A882C.2_cid341



Ein Höchstmaß an Crypto Agility ist alleine wegen der höchst unterschiedlichen Produktzyklen notwendig (Bildquelle: Utimaco)

im Bereich Quantenrechner seine Empfehlungen in der Technischen Richtlinie TR-02102-1 (Kryptographische Verfahren: Empfehlungen und Schlüssellängen) auf den Zeitraum bis 2024 begrenzt. Ab dann ist damit zu rechnen, dass Quantenrechner zumindest einen Teil der gängigen Verschlüsselungstechnologien obsolet machen.

Crypto Agility bietet zudem einen weiteren Vorteil: Sie schlägt eine Brücke zwischen Verschlüsselungstechniken, die noch nicht „quantensicher" sind und solchen, die bereits den neuen Anforderungen genügen. Das gilt für Chips, Geheimnisse und Software-Code. Erste Hybrid-Ansätze, die PQC und bislang gängige Kryptografie-Verfahren verwenden, sind in Entwicklung. Google hat bei seinem PQC-Algorithmus NewHope diese Vorgehensweise gewählt.

Zentrale Rolle von Software Development Kits

Die Frage ist allerdings, wie sich Crypto Agility in der Praxis umsetzen lässt. Problematisch ist beispielsweise, dass ein Großteil der Verschlüsselungs-Hardware auf dem Markt keine flexible Anpassung an neue Gegebenheiten ermöglicht. Das Einspielen neuer Firmware oder die Implementierung neuer Algorithmen ist nicht oder nur mit hohem Aufwand möglich.

Dass dies nicht sein muss, belegen die Hardware-Sicherheitsmodule von Utimaco in Verbindung mit dem Utimaco Software Development Kit (SDK). Eine solche Entwicklungsumgebung ermöglicht es bereits heute, Lösungen zu entwickeln, die für die Post-Quanten-Ära tauglich sind.[8]

8 https://hsm.utimaco.com/solutions/applications/post-quantum-crypto-agility/

Mit dem SDK können Nutzer eigene Algorithmen, eine maßgeschneiderte Schlüsselableitung oder komplexe Protokolle erstellen. Zudem lassen sich neue PQC-Algorithmen und entsprechende Schlüssel in ein Hardware-Sicherheitsmodul integrieren – ein flexibler und zukunftssicherer Ansatz. Dies ist einer der Gründe, weshalb Großunternehmen die Lösungen von Utimaco einsetzen.

Letztlich ist ein Software Development Kit vor dem Hintergrund der Post-Quanten-Kryptografie unverzichtbar. Das gilt sowohl für Umgebungen, in denen eine symmetrische Verschlüsselung zum Einsatz kommt, als auch für solche, die asymmetrische Verfahren verwenden.

Denn bei der symmetrischen Kryptografie gilt es, viele Schlüssel zu verwalten und Key Derivation Functions (KDF) in einer sicheren Umgebung zu implementieren. Letzteres lässt sich am besten mit einem SDK bewerkstelligen. Ein Beispiel für eine solche Umgebung ist das Home Location Register (HLR) im Bereich Mobilfunk, wo mithilfe des SDK die Schlüsselableitungen im HSM umgesetzt werden. Um solche symmetrischen Kryptografie-Verfahren für das PQC-Zeitalter „fit" zu machen, gilt es, zumindest die Schlüssellängen zu verdoppeln.

Bei asymmetrischen Verschlüsselungsverfahren gibt es noch keine standardisierte PQC-Lösung. Hier werden voraussichtlich erst 2023 neue Algorithmen von der NIST als „sicher" identifiziert werden. Unternehmen, die mit Public-Key-Infrastrukturen (PKI) arbeiten, um ihre IoT-Geräte zu identifizieren und zu authentisieren, werden eine Zeitlang Schlüssel auf der Basis von heutigen und zukünftigen, quanten-sicheren Algorithmen parallel nutzen (müssen). Hierfür ist Flexibilität auf mehreren Ebenen gefordert – diese bietet unter anderem das Utimaco Software Development Kit und die dazugehörige Scripting-Lösung, mit dessen Hilfe neue Algorithmen in eingesetzte HSM implementiert werden können.

> Unsere HSM sind zukunftssicher, weil sich auf einfache Weise neue Verschlüsselungstechnologien und Algorithmen nachrüsten lassen. Das gilt auch für Verfahren, die Attacken mit Quantenrechnern widerstehen.
>
> *Malte Pollmann, CEO von Utimaco*

Die Hardware-Sicherheitsmodule von Utimaco in Verbindung mit einem Software Development Kit (SDK) ermöglicht es bereits heute, Lösungen zu entwickeln, die für die Post-Quanten-Ära tauglich sind (Bildquelle: Utimaco)

Anwendungsszenario: PQC und Hardware-Sicherheitsmodule

Ein Anwendungsszenario einer Post-Quanten-Kryptografielösung in Verbindung mit Hardware-Sicherheitsmodulen (HSM) hat Microsoft vorgestellt.[9] Es basiert auf dem Signatur-Verfahren Picnic von Microsoft und der HSM-Lösung von Utimaco. Dabei kamen zwei Software-Komponenten zum Einsatz:

- Eine Host-Anwendung auf einem Windows-PC und
- Firmware-Module von Microsoft in einem HSM der Reihe SecurityServer Se50 LAN V4 von Utimaco.

Mithilfe dieser Elemente gelang es Microsoft im Rahmen eines Research-Projektes zu quantensicheren Algorithmen, eine Public-Key-Infrastruktur (PKI) mit Signaturen aufzubauen, die nicht mithilfe von Quantencomputern kompromittiert werden kann. Der Einsatz neuer Schlüssel und von Signaturen, die mithilfe eines bislang neuartigen Algorithmus erzeugten wurden, stellte für das HSM kein Problem dar.

Als großer Vorteil der Lösung von Utimaco erwies sich, dass sich Firmware von externen Anbietern wie Microsoft auf die Systeme aufspielen lässt. Dadurch ist es möglich, bei Bedarf neue kryptografische Algorithmen zu implementieren. Sollten sich beispielsweise bestimmte Verschlüsselungstechniken als anfällig gegenüber Attacken mit Quantenrechnern erweisen, lassen sich neue Firmware-Module mit entsprechender Software auf der Hardware installieren.

Wollen Sie mehr über Post-Quantum Crypto erfahren?

Wenn dieses Whitepaper Ihr Interesse geweckt hat und Sie mehr über Post-Quantum Crypto, Crypto Agility und die Implementierung von neuen Algorithmen in HSM wissen möchten, lesen Sie unser „Post-Quantum Crypto for Dummies“ Buch.

Verfügbar ab dem 16. April 2018 auf der RSA Conference in San Francisco oder kurze Zeit später auf unserer Webseite unter hsm.utimaco.com/downloads/.

Möchten Sie unser HSM ausprobieren oder selber neue Algorithmen implementieren?

Legen Sie los, in dem Sie unseren Simulator herunterladen. Sie finden ihn über hsm.utimaco.com/downloads/utimaco-portal/hsm-simulator/

Startklar?
Laden Sie unseren HSM-Simulator herunter

Melden Sie sich an!

Los geht's

9 https://github.com/Microsoft/Picnic/blob/master/spec/design-v1.0.pdf