Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Bundesamt für Cybersicherheit BACS

16. Mai 2024

Technologiebetrachtung

Quantencomputer und Post-Quanten-Kryptografie

1 Einleitung

Spätestens seit 2019 in der Fachzeitschrift *Nature* die Quantenüberlegenheit proklamiert worden ist[1], wird in den Medien viel über Quantencomputer, daraus für aktuell eingesetzte kryptografische Verfahren resultierende Gefahren und Bedrohungen, sowie die Notwendigkeit für auch gegenüber Quantencomputern sichere Kryptografie berichtet. Zum Teil lösen diese Berichterstattungen auch grosse Unsicherheiten und Befürchtungen über die Unzulänglichkeit von kryptografischen Verfahren aus. Vor diesem Hintergrund wird in diesem Ratgeber kurz aufgezeigt, was ein Quantencomputer ist, weshalb seine Existenz für die Sicherheit von bestimmten kryptografischen Verfahren problematisch ist, was sich hinter dem Begriff Post-Quanten-Kryptografie (PQK) verbirgt und wo es Handlungsbedarf gibt.

2 Quantencomputer

Während ein herkömmlicher Computer auf der Basis der Gesetze der klassischen Physik arbeitet, beruht ein Quantencomputer auf den Gesetzen der Quantenmechanik und verarbeitet quantenmechanische Zustände nach quantenmechanischen Prinzipien, wie z. B. das Superpositionsprinzip oder das Verschränkungsprinzip. Anstelle von Bits operiert er auf Quantenbits, die auch als Qubits (oder seltener Qbits) bezeichnet werden. Dabei stellt ein Qubit das einfachste nichttriviale Quantensystem dar, das prinzipiell unendlich viele verschiedene Zustände annehmen kann und sich in diesem Sinne auch simultan (bzw. «quantenparallel») in diesen Zuständen befinden kann. Daraus ergeben sich neue Möglichkeiten und Ansätze der Berechenbarkeit.

Aufgrund seiner aufwändigen Bauweise und charakteristischen Eigenschaften eignet sich ein Quantencomputer primär zum Lösen von Aufgaben, die mit herkömmlichen Computern nicht gelöst werden können bzw. zu aufwändig sind, wie z. B. Simulationsaufgaben im Bereich der Natur- und Ingenieurswissenschaften, Optimierungsaufgaben in Logistik und Finanzwirtschaft, maschinelles Lernen im Rahmen der Künstlichen Intelligenz, sowie das

[1] https://www.nature.com/articles/s41586-019-1666-5

Lösen von mathematischen Problemen, auf denen die Sicherheit von gewissen kryptografischen Verfahren beruht. Obwohl universell einsetzbare Quantencomputer bis heute noch ein vorwiegend theoretisches Konstrukt sind, wird an ihrem Bau intensiv und mit grossem Aufwand gearbeitet. Die entsprechende Forschungs- und Entwicklungsarbeit findet dabei nicht nur in den grossen Technologiefirmen statt, wie z. B. bei IBM, Google, Microsoft und Intel, sondern auch an Universitäten, Spin-Offs und in anderen neu gegründeten Firmen. Die Zahl der Qubits, die man heute verbauen kann, liegt zwar noch im Bereich von ein paar wenigen Hunderten (z. B. 433 im Falle eines 2022 von IBM vorgestellten Quantenprozessors Osprey), aber IBM plant bis 2033 den Bau eines Quantencomputers mit 100'000 Qubits.[2] Falls dieses ambitionierte Ziel erreicht werden kann, wird man im Bereich eines sogenannten kryptografisch relevanten Quantencomputers (CRQC) sein. Wie gross ein Quantencomputer sein muss, um als CRQC zu gelten, ist bis heute nicht klar. Ein Grund dafür ist, dass viele Quantenalgorithmen fehlertolerante Qubits verwenden, die auch etwa als logische Qubit bezeichnet werden. Weil die derzeit verwendeten physikalischen Qubits sehr fehleranfällig sind, besteht ein Ansatz zur Fehlerbereinigung darin, mehrere physikalische Qubits zu einem logischen Qubit zusammenzuschliessen. Dieses Verfahren nennt man Fehlerkorrektur, und in der jüngeren Vergangenheit sind viele Verbesserungen in diesem Bereich erzielt worden. Mit einem anderen Ansatz versucht man mit quantenoptischen Methoden fehlertolerante Qubits direkt zu realisieren.

Auf jeden Fall wird die Entwicklung und der Bau eines CRQC einschneidender sein, als die eingangs erwähnte 2019 proklamierte Quantenüberlegenheit. Letztlich ist mit dem Begriff der Quantenüberlegenheit nur gemeint, dass ein Quantencomputer ein mathematisches Problem schneller lösen kann, als ein konventionell arbeitender Supercomputer. Natürlich hängt die Bedeutung dieser Aussage stark vom zugrundeliegenden Problem ab und ist in diesem Sinne nicht allgemeingültig. Eine ähnliche Vorsicht ist auch bei den Ankündigungen der Firma D-Wave Systems[3] geboten. Die von dieser Firma vermarkteten Computer sind zwar mit Tausenden von Qubits bestückt, allerdings handelt es sich dabei nicht um universell einsetzbare Quantencomputer. Stattdessen lassen sich die Computer von D-Wave Systems nur für bestimmte Optimierungsaufgaben einsetzen und scheinen hierfür nicht einmal leistungsfähiger als herkömmliche Computer zu sein[4].

3 Problemstellung

Wie der Name suggeriert, könnten mit einem CRQC mathematische Probleme gelöst werden, auf welchen die Sicherheit von bestimmten kryptografischen Verfahren basiert. Namentlich betrifft dies asymmetrische Kryptosysteme, die wie RSA auf dem Faktorisierungsproblem für grosse Zahlen oder wie das Diffie-Hellman Schlüsselaustauschverfahren, DSA und Kryptosysteme auf der Basis von elliptischen Kurven auf dem diskreten Logarithmusproblem basieren. So hat Peter W. Shor bereits 1994 gezeigt, wie man mit einem hinreichend grossen Quantencomputer bzw. CRQC diese mathematischen Probleme lösen und damit die auf diesen Problemen aufsetzenden Kryptosysteme brechen kann [1]. Im Gegensatz zu herkömmlichen Computern haben die Algorithmen von Shor auf einem Quantencomputer eine nur polynomiale Laufzeit und sind damit im Sinne der Komplexitätstheorie effizient.

Weil die von den Algorithmen von Shor betroffenen asymmetrischen Kryptosysteme heute fast überall im Einsatz stehen, hätte der Bau eines CRQC gravierende Auswirkungen auf

---

[2] https://www.ibm.com/quantum/blog/100k-qubit-supercomputer

[3] https://www.dwavesys.com

[4] https://dl.acm.org/doi/10.1145/3459606

deren Sicherheit. Zuweilen wird in diesem Zusammenhang auch von einem «Q-Day» gesprochen. Damit ist der Zeitpunkt gemeint, an dem CRQCs gebaut werden und Angreifenden zur Verfügung stehen.

Zur Lösung von kryptografisch relevanten Problemen benötigen Quantenalgorithmen zumindest eine Anzahl von logischen Qubits, die linear mit der Bitlänge der entsprechenden Schlüssel wächst. Im Falle von RSA sind das typischerweise ein paar Tausend. Aufgrund der heute verfügbaren Fehlerkorrekturverfahren ist die Anzahl der benötigten physikalischen Qubits ein Vielfaches davon. Wenn IBM allerdings seine Vision einhalten kann, wird der für 2033 geplante Quantencomputer (mit seinen 100'000 Qubits) für viele asymmetrische Kryptosysteme ein Problem.

Obwohl ein Quantencomputer grundsätzlich auch zum Brechen symmetrischer Kryptografie eingesetzt werden kann, sind die Auswirkungen auf die Sicherheit der entsprechenden Verfahren weniger gravierend. Lov K. Grover hat 1996 einen Algorithmus vorgeschlagen, mit dem der Aufwand einer vollständigen Suche eines n-Bit langen Schlüssels von 2^n auf $2^{n/2}$ reduziert werden kann [2]. Damit sind zwar grundsätzlich auch Pseudozufallsgeneratoren, Nachrichtenauthentifikationscodes und symmetrische Verschlüsselungen verwundbar, aber diese Verwundbarkeit kann relativ einfach mit einer Verdoppelung der Schlüssellänge kompensiert werden. Die Sicherheit der symmetrischen Kryptografie ist damit durch die Existenz eines CRQC nur marginal betroffen. Zudem ist der Algorithmus von Grover optimal, d. h. es ist hier mit keiner Verbesserung zu rechnen.

Selbst wenn ein CRQC heute noch nicht gebaut werden kann, besteht das Problem, dass ein grossangelegtes Sammeln verschlüsselter Daten stattfinden kann, um diese Daten dann in Zukunft mit einem CRQC entschlüsseln zu können. Man spricht in diesem Zusammenhang von einem «Harvest Now, Decrypt Later»- bzw. HNDL-Angriff, und die mögliche Existenz von HNDL-Angriffen stellt aus heutiger Sicht das primäre Motiv dar, weshalb man möglichst schnell praktikable Lösungsansätze und entsprechende Lösungen finden sollte.

4 Lösungsansätze

Angesichts der grossen Forschungs- und Entwicklungsaktivitäten, mit welchen die erwähnten Technologiefirmen den Bau universeller Quantencomputer vorantreiben, sowie der Möglichkeit von HNDL-Angriffen, ist es sinnvoll, sich Gedanken darüber zu machen, wie man Kryptosysteme konstruieren kann, die resistent gegenüber Quantencomputern sind. Dieses Teilgebiet der Kryptografie wird als PQK bezeichnet und erlebt zurzeit ein sehr grosses Interesse. Dabei bezieht sich PQK auf die asymmetrische Kryptografie. Im Bereich der symmetrischen Kryptografie gibt es kaum Handlungsbedarf, weil – wie oben erwähnt – alle heute eingesetzten Kryptosysteme weiterhin genutzt werden können, wenn die Schlüssellänge verdoppelt wird.[5] Diese Verdoppelung kompensiert die Implikationen des Algorithmus von Grover, d. h. die resultierende Sicherheit bleibt somit in etwa gleich. Konkret bedeutet dies, dass z. B. AES-256 anstelle von AES-128 eingesetzt werden soll. Die Nachteile im praktischen Einsatz sind – falls überhaupt vorhanden – sehr bescheiden (insbesondere hängt der Durchsatz bei der Ver- und Entschlüsselung nicht entscheidend von der Schlüssellänge ab).

Das Ziel der PQK besteht also darin, asymmetrische Verfahren und Kryptosysteme zu konstruieren, welche auf anerkannt schwierigen, auch mittels Quantencomputer praktisch unlösbaren mathematischen Problemen basieren und trotzdem effizient implementierbar sind.

[5] Natürlich ist eine solche Verdoppelung nur bis zu einer bestimmten Schlüssellänge sinnvoll und erforderlich. Ab 256 Bit ist eine Verdoppelung auf jeden Fall nicht mehr erforderlich.

Das US-amerikanische National Institute of Standards and Technology (NIST) führt dazu seit 2017 einen international stark beachteten Wettbewerb[6] durch und hat 2022 die ersten vier Gewinner für die asymmetrische Verschlüsslung bzw. den Schlüsseltransport (KEM[7]) sowie für digitale Signaturen bekanntgegeben. Auf diesen Algorithmen beruhende Standards werden momentan von NIST ausgearbeitet und befinden sich in der finalen Bereinigung. Es handelt sich dabei um den FIPS 203 für ML-KEM und FIPS 204 für ML-DSA. Die Grundlagen dafür sind die auf Gittern basierten Algorithmen CRYSTALS-Kyber und CRYSTALS-Dilithium. Der auf Hash-Funktionen basierende Algorithmus SPHINCS+ ist die Grundlage für den FIPS 205 SLH-DSA. Der ebenfalls auf Gitter basierenden Signaturalgorithmus FALCON wird zu einem späteren Zeitpunkt standardisiert. Für KEMs geht der Wettbewerb zusätzlich mit mehreren codebasierten Algorithmen in eine weitere Runde. Zu guter Letzt hat das NIST für digitale Signaturen im 2023 einen zweiten Wettbewerb gestartet. Damit ist im Moment nicht klar ist, ob und wann auch noch andere Verfahren als mögliche Standards mit ins Spiel kommen werden. Neben dem NIST arbeiten auch weitere Organisationen, wie z. B. die Internet Engineering Task Force (IETF), das European Telecommunications Standards Institute (ETSI) und die International Organization for Standardization (ISO), an der Standardisierung von PQK-Algorithmen.

Aus heutiger Sicht wäre es falsch, alle aktuell eingesetzten asymmetrischen Verfahren durch PQK-Verfahren zu ersetzen, weil erst die Zukunft zeigen wird, wie sicher diese wirklich sind (viele PQK-Verfahren und -Algorithmen beruhen auf noch relativ jungen und noch nicht vollständig verstandenen kryptografischen Ideen). Stattdessen sind eine Ergänzung und eine Komplementierung dieser Verfahren sinnvoll und zweckmässig. Man spricht in diesem Zusammenhang auch von «hybriden» Verfahren oder von sogenannt «hybriden Combinern». So kombinieren die Ende-zu-Ende verschlüsselnden Messenger-Dienste Signal und iMessage z. B. das konventionelle Diffie-Hellman Schlüsselaustauschverfahren auf der Basis von elliptischen Kurven mit Kyber, und auch im Bereich der digitalen Signaturen und entsprechenden Zertifikaten ist in Zukunft mit hybriden Ansätzen zu rechnen.

Explizit keine Lösungsansätze für die im Rahmen dieses Kurzratgebers diskutierte Problemstellung stellen die Quantenkryptografie (bzw. die Quantenschlüsselvereinbarung als hauptsächliche und eigentlich auch einzige Anwendung der Quantenkryptografie) und Quantenzufallsgeneratoren dar. Beide Technologien sind thematisch verwandt und können im Rahmen von kommerziellen Produkten auch eingesetzt werden. Allerdings ist die Quantenkryptografie mit so vielen praktischen Problemen behaftet, dass weder die US-amerikanische National Security Agency[8] (NSA) noch ein Zusammenschluss aus vier europäischen Behörden[9] den Einsatz propagieren. Weil Quantenzufallsgeneratoren auch nur eine von vielen technischen Umsetzungsmöglichkeiten für Zufallsgeneratoren darstellen, gibt es auch hier kaum einen Mehrwert, der für einen zwingenden Einsatz sprechen würde.

---

[6] https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

[7] Die Abkürzung KEM steht für «Key Encapsulation Mechanism». Damit ist ein Mechanismus gemeint, der es erlaubt, einer Partei einen kryptografischen Schlüssel sicher zukommen zu lassen. Dabei wird der zu transportierende Schlüssel zufällig ausgewählt und mit dem öffentlichen Schlüssel der Partei so verpackt (oder «enkapsuliert»), dass er nur mit dem entsprechenden privaten Schlüssel wieder ausgepackt werden kann. Gesucht wäre eigentlich ein Schlüsselaustauschverfahren, das ähnlich wie Diffie-Hellman (auch nicht interaktiv) eingesetzt werden kann, ein solches steht aber bis heute nicht zur Verfügung. Ersatzweise werden deshalb KEMs eingesetzt.

[8] https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

[9] https://cyber.gouv.fr/en/actualites/uses-and-limits-quantum-key-distribution

5 Empfehlungen und weiteres Vorgehen

Der Bau eines CRQC stellt aus technischer Sicht eine grosse Herausforderung dar und steht entsprechend nicht unmittelbar bevor. Dennoch bietet sich aufgrund der Möglichkeit von breit angelegten HNDL-Angriffen der Einsatz von PQK bereits an. Dabei ist ein behutsames und wohlüberlegtes Vorgehen angebracht.[10] Der schnelle Einsatz von kurzfristigen und möglicherweise auch übereilten Lösungen, respektive Lösungsansätzen, würde sich eher negativ auf die Sicherheit auswirken, auch wenn damit vordergründig Resistenz vor von Quantencomputern ausgehenden Angriffen erzielt werden könnte. Eine entsprechende Migration ist ein langer Prozess, der vor dem Hintergrund der aktuell stattfindenden Standardisierung von PQK-Algorithmen entsprechend geplant werden muss.[11]

Dabei wird an verschiedenen Fronten an der Standardisierung von PQK-Algorithmen und am Einbau dieser Algorithmen in Sicherheitsprotokollen und Produkten gearbeitet. Auf Signal und iMessage ist bereits hingewiesen worden. Auch Google hat bereits Mitte der 2010er-Jahre versucht, Frodo (ein Vorgängeralgorithmus von Kyber) in TLS einzubauen und arbeitet seither an verschiedenen PQK-Erweiterungen für seine Produkte.[12] Ähnliches gilt auch für Microsoft, Cloudflare und andere Technologiefirmen. Grundsätzlich gilt, dass je offener ein System ist, es umso schwieriger und zeitaufwändiger ist, dieses System mit PQK zu ergänzen. In diesem Sinne stellt auch die Nutzung von PQK in standardisierten Sicherheitsprotokollen für das Internet (z. B. IPsec, TLS, …) eine grosse Herausforderung für die IETF und ihre Arbeitsgruppen dar.

Alle Bestrebungen zu PQK dienen letztlich der kryptografischen Agilität und müssen auch vor diesem Hintergrund betrachtet werden. Dabei sind Systeme und Anwendungen so zu konzipieren und zu implementieren, dass unterschiedliche kryptografische Verfahren und Algorithmen bedient und unterstützt werden können. Diese Form der Agilität ist heute bereits wichtig und wird in Zukunft wohl noch wichtiger werden. Kryptografische Agilität setzt eine dafür ausgerichtete Software-Architektur voraus. Bei Hardware-Implementierungen, die typischerweise bei erhöhten Performance- und/oder Sicherheitsanforderungen zum Einsatz kommen, sind die Möglichkeiten der Agilität in der Regel eingeschränkt. Dabei ist es in jedem Fall sinnvoll, die verbauten kryptografischen Komponenten, Verfahren und Algorithmen in einer Software (SBOM) bzw. Cryptography Bill of Materials (CBOM) zu dokumentieren. Diese Art der Inventarisierung ist auch unabhängig vom Thema PQK vor dem Hintergrund zunehmender «Supply Chain»-Angriffe wichtig.

Abkürzungen

AES	Advanced Encryption Standard
BACS	Bundesamt für Cybersicherheit
CBOM	Cryptography Bill of Materials
CRQC	Cryptographically Relevant Quantum Computer
DSA	Digital Signature Algorithm
ETSI	European Telecommunications Standards Institute
FIDO2	Fast IDentity Online

[10] Adi Shamir hat das anlässlich der RSA Konferenz 2023 im Rahmen eines Panels zum Thema «Migrating to Post-Quantum Schemes» einen den Sachverhalt treffend umschreibenden Ratschlag gegeben: «If you want to switch to post-quantum algorithms, walk, don't run» (https://www.rsaconference.com/library/presentation/usa/2023/Panel%20Migrating%20to%20Post-Quantum%20Schemes).

[11] https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography

[12] https://bughunters.google.com/blog/5108747984306176/google-s-threat-model-for-post-quantum-cryptography

FIPS	Federal Information Processing Standards (US)
HNDL	Harvest Now, Decrypt Later
IETF	Internet Engineering Task Force
IPsec	Internet Protocol Security
ISO	International Organization for Standardization
KEM	Key Encapsulation Mechanism
ML	Module Lattice
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PQK	Post-Quanten-Kryptografie
RSA	Rivest, Shamir, Adleman
SBOM	Software Bill of Materials
SLH	Stateless Hash
TLS	Transport Layer Security
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport

Referenzen

[1] Peter W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science, November 1994, Santa Fe, NM, pp. 124–134

[2] Lov K. Grover, *A Fast Quantum Mechanical Algorithm for Database Search*, In: Proceedings of the 28th Annual ACM Symposium on the Theory of Computing, May 1996, pp. 212–219