Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Nationales Zentrum für Cybersicherheit NCSC

Rolf Oppliger, NCSC
(mit Unterstützung von FUB Kryptologie)

24. Februar 2016
14. August 2020 (aktualisiert)

Technologiebetrachtung

Quantencomputer und Post-Quanten-Kryptografie

1 Einleitung

In den Medien wird viel über den möglichen Bau eines Quantencomputers, die daraus für aktuelle kryptografische Verfahren resultierenden Gefahren und die Notwendigkeit von Post-Quanten-Kryptografie (PQK) berichtet. Zum Teil lösen diese Berichterstattungen Unsicherheiten und Befürchtungen über die Unzulänglichkeit der heute eingesetzten Kryptosysteme aus. Im Rahmen dieser Technologiebetrachtung soll aufgezeigt werden, was ein Quantencomputer theoretisch leisten kann, was seine Implikationen im Hinblick auf die Sicherheit moderner kryptografischer Verfahren sind und was sich hinter dem Begriff PQK verbirgt.

2 Quantencomputer

Ein herkömmlicher Computer arbeitet auf der Basis der Gesetze der klassischen Physik. Demgegenüber beruht ein Quantencomputer auf den Gesetzen der Quantenmechanik, d.h. er verarbeitet quantenmechanische Zustände nach quantenmechanischen Prinzipien, wie z.B. das Superpositionsprinzip oder das Verschränkungsprinzip. Anstelle von Bits operiert der Quantencomputer an Quantenbits, die auch etwa als Qubits oder Qbits bezeichnet werden. Dabei stellt ein Qubit das einfachste nichttriviale Quantensysteme dar, das prinzipiell unendlich viele verschiedene Zustände annehmen kann.

In der Theorie können bestimmte Probleme, auf denen die Sicherheit heute eingesetzter kryptografischer Verfahren basiert, mit Hilfe eines Quantencomputers effizienter gelöst werden als mit Hilfe konventionell arbeitender Computer. Zum Beispiel kann bei einem symmetrischen Kryptosystem der Aufwand der vollständigen Suche eines n-Bit langen Schlüssels mit Hilfe des 1996 von Lov K. Grover vorgeschlagenen Algorithmus von 2^n auf $2^{n/2}$ reduziert werden [1]. Im Falle von asymmetrischen Kryptosystemen hat Peter W. Shor 1994 Algorithmen für die Berechnung der Primfaktorzerlegung von Zahlen mit grossen Primfaktoren und das Finden diskreter Logarithmen entwickelt, welche bei Verwendung eines Quantencomputers eine polynomiale Laufzeit haben und damit im Sinne der Komplexitätstheorie effizient sind [2]. Weil fast alle heute eingesetzten asymmetrischen Kryptosysteme auf diesen zwei mathematischen Problemen basieren,

hätte der Bau eines hinreichend grossen Quantencomputers tiefreichende Auswirkungen auf deren Sicherheit.
Dabei ist ein universell einsetzbarer Quantencomputer bis heute noch ein vorwiegend theoretisches Konstrukt. In den Forschungslabors von IBM, Google, Microsoft, Intel und anderen Grossfirmen wird zwar mit grossem Aufwand an solchen Computern gearbeitet, die Zahl der verwendeten Qubits liegt dabei aber in der Grössenordnung von 50-70. Im Vergleich dazu benötigt man für den Algorithmus von Shor selbst unter idealen Bedingungen eine Anzahl Qubits, die linear mit der Bitlänge der entsprechenden Schlüssel wächst, d.h. typischerweise ein paar Tausend. Unter realen Bedingungen werden zudem noch Fehlerkorrekturverfahren benötigt, so dass die Zahl der benötigten Qubits in die Millionen gehen könnte. Nichtsdestotrotz hat Google bereits am 23. Oktober 2019 die Quantenüberlegenheit (Quantum Supremacy) proklamiert. Damit ist gemeint, dass ein Quantencomputer ein mathematisches Problem schneller gelöst hat, als dass ein konventionell arbeitender Supercomputer dies je hätte tun können. Natürlich hängt die Aussagekraft dieser Aussage sehr stark vom zugrundeliegenden Problem ab. Kurze Zeit nach der Ankündigung von Google hat auch IBM den ersten kommerziell verfügbaren „echten“ Quantencomputer angekündigt und über entsprechende Cloud-Dienste seinen Kunden verfügbar gemacht.

Ein werbewirksam auftretender Anbieter von Quantencomputern ist die Firma D-Wave Systems aus Kanada. Allerdings lassen sich deren Computer nur für eine dedizierte Aufgabe einsetzen – nämlich die Ausführung von „Annealing“ mittels Quantenphysik, d.h. „Quantum Annealing“. Experten sind sich derzeit uneinig, ob D-Wave Maschinen Optimierungsprobleme tatsächlich schneller lösen werden können als konventionelle Computer. Auf jeden Fall entspricht die Architektur einer solchen Maschine nicht der eines universellen Quantencomputers; insbesondere können auf ihr weder die Algorithmen von Shor noch der Suchalgorithmus von Grover ausgeführt werden. Zurzeit ist nicht klar, ob „Quantum Annealing“ einmal zur Faktorisierung grosser Zahlen oder zur Bestimmung diskreter Logarithmen verwendet werden kann. Zudem ist im Allgemein die Suche des Schlüssels eines symmetrischen Kryptosystems mittels „Quantum Annealing“ sehr ineffizient.

3 Post-Quanten-Kryptografie (PQK)

Angesichts der grossen Forschungsbudgets, mit denen die oben erwähnten Grossfirmen den Bau universeller Quantencomputer vorantreiben, ist es durchaus sinnvoll, sich heute bereits Gedanken darüber zu machen, wie man Kryptosysteme konstruieren kann, damit diese sowohl resistent gegenüber Quantencomputern als auch klassischen Computern sind. Dieses Teilgebiet der Kryptografie wird als PQK bezeichnet und erlebt zurzeit ein sehr grosses Interesse.

Im Falle symmetrischer Kryptosysteme können alle heute eingesetzten Systeme auch weiterhin genutzt werden, wenn nur die Schlüssellänge verdoppelt wird. Diese Verdoppelung kompensiert die Implikationen des Algorithmus von Grover, d.h. die resultierende Sicherheit bleibt dann in etwa gleich. Konkret bedeutet das, dass z.B. AES-256 anstelle von AES-128 eingesetzt werden kann. Die Nachteile im praktischen Einsatz sind – falls überhaupt vorhanden – sehr bescheiden.

PQK betrifft also primär die asymmetrische Kryptografie. Ziel ist es, Verfahren zu finden, welche auf einem anerkannt schwierigen, auch mittels Quantencomputer praktisch unlösbaren mathematischen Problem basieren und eine effiziente Implementierung zulassen. Das U.S. amerikanische NIST führt dazu seit 2017 einen Wettbewerb

durch[1]. Aus den anfänglich 69 zulässigen Eingaben hat das NIST bereits 54 ausgeschieden und untersucht seit Juli 2020 in Runde drei noch 7 Finalisten und 8 alternative Algorithmen weiter.

4 Quantenschlüsselvereinbarung

Die Schlüsselvereinbarung ist ein spezielles kryptografisches Problem, das mit Hilfe der asymmetrischen Kryptografie effizient und elegant gelöst werden kann. Ein alternativer Lösungsansatz beruht auf quantenmechanischen Effekten. Im Gegensatz zu Quantencomputer können solche quantenbasierten Systeme für die Schlüsselvereinbarung heute bereits gebaut werden. Allerdings ist das Thema kontrovers, weil solche Systeme für den praktischen Einsatz mit erheblichen Nachteilen und Schwierigkeiten behaftet sind. Zum Beispiel können solche Systeme für die Schlüsselvereinbarung nur auf der physischen Schicht realisiert werden, so dass der Einsatz einzig der Link-Verschlüsselung vorbehalten bleibt und die beteiligten Partner gemäss heutigem Stand höchstens wenige 100 km voneinander entfernt sein dürfen. Zudem erfordert dieser quantenmechanische Ansatz die Existenz eines zusätzlichen authentischen Kanals. Für vernetzte und verteilte Systeme, den hauptsächlichen Anwendungsfall von asymmetrischer Kryptografie, ist die quantenmechanische Alternative denn auch kaum praktikabel. Dennoch gibt es Firmen, die sich ausschliesslich der Vermarktung solcher Systeme widmen, wie z.B. die in Genf ansässige ID Quantique[2] (IDQ).

5 Schlussfolgerungen und Ausblick

Aus physikalischer Sicht stellt der Bau eines hinreichend grossen Quantencomputers eine grosse Herausforderung dar. Zurzeit deutet nichts darauf hin, dass ein für kryptanalytische Zwecke einsetzbarer Quantencomputer gebaut werden kann. Entsprechend sind die Bestrebungen zur PQK noch nicht unmittelbar wichtig. Nichtsdestotrotz sind sie sinnvoll und müssen auch aus der Sicht der Bundesverwaltung weiter verfolgt werden. Die im Rahmen der PQK entwickelten Alternativen zu herkömmlichen asymmetrischen Kryptosystemen könnten nämlich auch dann wichtig werden, wenn aufgrund zahlentheoretischer Fortschritte effizientere Algorithmen zur Primfaktorenzerlegung oder zum Lösen von diskreten Logarithmen gefunden werden. Solche Fortschritte sind jedenfalls nicht unwahrscheinlicher als der Bau eines hinreichend grossen universellen Quantencomputers.

Beim Einsatz herkömmlicher asymmetrischer Kryptosysteme besteht immer das Risiko, dass heute verschlüsselte Informationen in Zukunft entweder mit der Realisierung eines Quantencomputers oder aufgrund zahlentheoretischer Fortschritte entschlüsselt werden können. Das ist insbesondere dann problematisch, wenn die zu schützenden Informationen langfristig geheim gehalten werden müssen. Aus diesem Grund empfiehlt die kryptologische Fachstelle des Bundes (FUB Kryptologie) bereits heute, zumindest für den Schutz von als GEHEIM klassifizierten Informationen ausschliesslich symmetrische Kryptosysteme mit einer Schlüssellänge von mindestens 256 Bit zu verwenden. Zusätzlich verfolgt dieselbe Fachstelle die Forschung und Entwicklung im Bereich Quantencomputer und PQK.

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

Referenzen

[1] 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

[2] 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