Post Quantum Cryptography

1 Unterschied - Klassische Computer & Quantencomputer

Wenn von einem Computer die Rede ist, dann ist heutzutage meistens ein alltäglicher Desktop oder Laptop Computer gemeint. Diese Sorte von Computer wird *klassische* Computer genannt. Klassische Computer basieren bekanntlich auf Bit, die entweder eine Eins oder eine Null sind.

Quantencomputer basieren dagegen nicht auf Bit, sondern auf sogenannten «Qubit». Der Name Qubit kommt aus der Zusammenführung der beiden Wörter «Quantum» und «Bit». Ein Qubit kann theoretisch unendlich viele Zustände inbegriffen zwischen Null und Eins annehmen. Die Quantenphysik beschreibt die eigenartigen Phänomene und Eigenschaften von sehr kleinen Teilchen, beispielsweise einzelne Atome, Photonen, Elektronen, usw.

Quantencomputer, die viele Qubit besitzen sind in der Lage spezielle Probleme zu lösen, die von klassischen Computern nur mit sehr grossem Aufwand und Zeit lösbar sind. Ist ein Problem jedoch nicht *lösbar* mit einem klassischen Computer, dann ist das Problem auch nicht lösbar mit einem Quantencomputer.

1.1 Potenzielle Anwendungen von Quantencomputer

Quantencomputer sind speziell geeignet, um gewisse Probleme oder Berechnungen zu lösen, die auf einem klassischen Computer schlichtweg zu lange dauern würden. Speziell im Bereich der Simulationen finden Quantencomputer exponentiell schneller eine Lösung als klassische Computer.

Die Anwendungen für Quantencomputer sind beinahe grenzenlos. Wichtige Beiträge könnten Quantencomputer sicherlich in den folgenden Bereichen erzielen:

- Mathematische Berechnungen
- Kryptografie / Kryptoanalyse
- Simulation von chemischen Reaktionen
- Künstliche Intelligenz
- Entwicklung von Medikamenten
- Finanzielle Modellierung
- Logistik-Optimierung
- Wettervorhersage

2 Auswirkung von Quantencomputer auf derzeitige verwendeten kryptographische Algorithmen

In den letzten Jahren ist die Forschung und Entwicklung von Quantencomputern stark fortgeschritten. Beim Einsatz von Quantencomputern im grossen Massstab, würden sie die Sicherheit vieler heute häufig eingesetzter Verschlüsselungs-Systeme bedrohen. Dabei werden Verschlüsselungsverfahren und digitale Signaturen, die auf diskreten Logarithmen und elliptischer Kurvenkryptographie basieren, am stärksten betroffen sein. Symmetrische Verschlüsselungsverfahren wie Blockchiffren und Hash-Funktionen werden hingegen nur geringfügig betroffen sein. Daher wird intensiv an der Post-Quantum-Kryptografie geforscht, um Verschlüsselungsverfahren, welche gegen Angriffe sicher sind, zu entwickeln.

Kryptographischer Algorithmus	Typ	Einsatzgebiet	Auswirkungen durch Quantencomputer Einsatz
AES	Symmetrische Schlüssel	Verschlüsselung	Sicher mit dem Einsatz grosser Schlüsselgrössen
SHA-2, SHA3		Hash Funktion	Sicher mit grösseren Zahlenwerten
RSA	Öffentliche Schlüssel	Signaturen, Schlüsseleinrichtung	Nicht mehr sicher
ECDSA, ECDSH	Öffentliche Schlüssel	Signaturen, Schlüsselaustausch	Nicht mehr sicher
DSA	Öffentliche Schlüssel	Signaturen, Schlüsselaustausch	Nicht mehr sicher

2.1 Benötigte Quantenressourcen & Empfehlungen

Die Empfehlungen beziehen sich auf die Sicherheit **bis** 2030.

Quelle: NIST SP 800-78-5: “Cryptographic Algorithms and Key Sizes for Personal Identity Verification”

2.1.1 RSA-basierte Kryptografie

Die Anzahl der Qubits, die auf einem Quantencomputer benötigt werden, um RSA zu brechen, wird auf **2n+3** (n = RSA-Bitgrösse) geschätzt, was bedeutet, dass ein Quantencomputer mit **ca. 4.000 Qubits** benötigt wird, um eine RSA-2048-Signatur zu brechen (weitere Optimierungen der Algorithmen sind zu erwarten, sodass die tatsächliche Zahl der benötigten Qubits voraussichtlich geringer sein könnte).

Empfehlung: Mindestens eine Bitgrösse von 2048 Bit.

2.1.2 ECC / ECDSA

Die Anzahl der Qubits, um ECC / ECDSA zu brechen, beträgt „ungefähr“ **6n**. Das bedeutet, dass ein Quantencomputer mit **ca.1.500 Qubits** eine ECC-P256-Signatur brechen kann.

Empfehlung: Kurven P-256 und P-384.

2.1.3 Symmetrische Verschlüsselung

Quantencomputer **halbieren** die effektive Sicherheit von symmetrischen Verschlüsslungsverfahren der eigentlichen Schlüssellänge. Somit wird bei einem symmetrischen Verschlüsselungsverfahren von beispielsweise AES-256 die effektive Sicherheit auf die von AES-128 reduziert.

Empfehlung: Bitgrösse von 128, 192 und 256 Bit.

3 Quantum-Safe-Cryptography (QSC) / Post-quantum-cryptography (PQC)

Die US-Behörde National Institute of Standards and Technology (NIST) hat im Dezember 2016 ein Standardisierungsprozess für die Post-Quantum Public-Key-Verschlüsselungs-Algorithmen gestartet. Die vorgeschlagenen Algorithmen wurden in mehreren Runden auf ihre Sicherheit und Einsatztauglichkeit bewertet, welche im NIST «Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process» aufgeführt sind. Von ursprünglich 69 zulässigen Eingaben wurden nach der dritten Prüfungsrunde (Juli 2022) 4 Algorithmen standardisiert und 1 weiterer Algorithmus als Alternative bestimmt.

Algorithmus	Details	Verwendungszweck	Anmerkung
CRYSTALS-Kyber	**Dieser Algorithmus ist ein Schlüsselkapselungsmechanismus (KEM), der sich für allgemeine Verschlüsselung, beispielsweise zur Sicherung von Websites, eignet.**	**Asymmetrischer Schlüsselaustausch.**	**Primärer Algorithmus für asymmetrische Verschlüsselung.**
CRYSTALS-Dilithium	**Dies ist ein modulgitterbasierter digitaler Signaturstandard, der für digitale Signaturen verwendet wird.**	**Digitale Signatur.**	**Primärer (genereller) Signatur Algorithmus.** **Gitter-basiert.**
FALCON	**Dieser Algorithmus wird für digitale Signaturen verwendet.**	**Digitale Signatur.**	**Signatur Algorithmus für kleinere Signaturen.** **Gitter-basiert.**
SPHINCS+	**Zustandsloser, hashbasierter digitaler Signaturstandard.**	**Digitale Signatur.**	**Ersatz für digitale Signaturen.** **Hash-basiert, bzw. vertraut der Sicherheit von Hashes.**
HQC	**Dieser Algorithmus ist ein Backup für ML-KEM und verwendet einen anderen mathematischen Ansatz.**	**Asymmetrischer Schlüsselaustausch.**	**Ersatz für asymmetrische Verschlüsselung, falls CRYSTALS-Kyber kompromittiert wird.**

Für die SG-PKI gilt es die Entwicklung der Standardisierung zu verfolgen, um dies in die zukünftige Entwicklung einbeziehen zu können. Zusätzlich muss ein Augenmerk auf die Umsetzung der entsprechenden Sicherheitslösungen gelegt werden, dies insbesondere auch auf die Lösungen, welche von den Herstellern dazu präsentiert werden.

3.1 Level 1-5 bei Dilithium

Level 3 bei CRYSTALS-Dilithium bezeichnet eine Sicherheitsstufe, die vom NIST (National Institute of Standards and Technology) im Rahmen der Standardisierung quantensicherer Algorithmen definiert wurde. Die Levels orientieren sich an der Stärke klassischer symmetrischer Algorithmen (wie AES).

Level 3 bietet ein gutes Gleichgewicht zwischen Sicherheit und Performance.

In PKI-Umgebungen wird **Dilithium Level 3** häufig für digitale Signaturen empfohlen, wenn **langfristige Sicherheit** und **quantenresistenter Schutz** erforderlich sind.

Level	Sicherheitsäquivalent (klassisch)	Verwendungsempfehlung
Level 1	~ AES-128	Basis-Sicherheit für allgemeine Anwendungen
Level 3	~ AES-192	**Erhöhte Sicherheit**, z.B. für Behörden, Industrie
Level 5	~ AES-256	Höchste Sicherheit, z.B. für nationale Sicherheit

4 Harvest-Now-Decrypt-Later

Harvest-Now-Decrypt-Later (HNDL) bezeichnet das Problem, dass derzeit sicher verschlüsselte Daten gesammelt und zu einem späteren Zeitpunkt mit leistungsstarken Quantencomputern entschlüsselt werden können.

Dies birgt insbesondere für langfristig sensible Daten ein hohes Risiko, da sie auch Jahre oder Jahrzehnte nach ihrer Erfassung noch schützenswert sein können. Daher ist es essenziell, bereits heute darauf zu achten, welche Daten verschlüsselt werden und wie lange diese sicher bleiben müssen. Beispielsweise sind personenbezogene Daten, staatliche Geheimnisse oder geschäftskritische Informationen besonders kritisch, da ein zukünftiger Verlust der Vertraulichkeit schwerwiegende Folgen haben könnte.

5 Migrations-Timeline

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.

(Quelle: Technologiebetrachtung: Quantencomputer und Post-Quanten-Kryptografie)

Ein hybrider Ansatz eignet sich besonders für Signaturen, da klassische Signaturen und PQC-Signaturen parallel und isoliert voneinander verwendet werden können. Beide Signaturen können dabei unabhängig voneinander validiert werden, wodurch sowohl die Sicherheit der etablierten klassischen Verfahren als auch die Vorteile der neuen PQC-Ansätze kombiniert werden.

5.1 Mosca's Theorem

Mosca’s Theorem beschreibt das Risiko, dass heutige Verschlüsselungsverfahren durch zukünftige Quantencomputer gebrochen werden könnten. Es betont die Notwendigkeit, frühzeitig auf Post-Quanten-Kryptografie (PQC) umzustellen, insbesondere für langfristig vertrauliche Daten. Die Dringlichkeit wird durch die folgende Formel bestimmt: **X + Y > Z.**

- **X**: Die Zeit, in der Daten sicher bleiben müssen.
- **Y**: Die Dauer der PQC-Migration.
- **Z**: Die Zeit, bis Quantencomputer klassische Verschlüsselung brechen können.

Falls die Summe von **X** und **Y** größer als **Z** ist, besteht Handlungsbedarf, um die langfristige Sicherheit zu gewährleisten.

5.1.1 Beispiel zu Mosca's theorem

Als Beispiel nehmen wir Daten der Schweizer Armee, welche militärische Strategien, Kommunikationsprotokolle, kritische Infrastruktur, etc. beinhalten. Diese Daten der Schweizer Armee müssen **10 Jahre** (= **X**) sicher verschlüsselt bleiben. Eine Migration zu PQC dauert aufgrund der Beschaffung, Umstellung, etc. ungefähr **5 Jahre** (= **Y**). Unter der Annahme, dass ein Durchbruch in der Quantenforschung gelingt, könnte ein Quantencomputer, der die aktuelle Verschlüsselung brechen kann, in **10 Jahren** (= **Z**) verfügbar sein. Damit lässt sich mit Mosca’s Theorem aufzeigen, dass die Daten nicht lange genug sicher sind, da: **X+Y>Z 15 > 10.**

Dieses Szenario zeigt, dass eine frühzeitige und beschleunigte Migration zu PQC notwendig ist, um sicherzustellen, dass sensible militärische Daten nicht durch einen unerwartet frühen Durchbruch in der Quantenforschung kompromittiert werden.

6 Die Physik eines Quantencomputers

Während klassische Computer sich stets in einem von zwei Zuständen Zustand befinden, können Quantencomputer alle beliebigen Zustände gleichzeitig annehmen. Die Ausgabe, bzw. die Antwort auf eine Berechnung des Quantencomputers ist jeweils wieder nur ein einzelner Zustand.

Die drei wichtigsten Phänomene, die ein Quantencomputer dafür benutzt, sind die Superposition, die Verschränkung und die Interferenz.

6.1 Grundlagen

6.1.1 Superposition

Die Superposition beschreibt ein System, wo mehrere Zustände gleichzeitig existieren können. Erst sobald man einen Zustand misst, kollabiert das System in einen definitiven Zustand.

Das berühmte Gedankenexperiment «Schrödingers Katze» des Physikers Erwin Schrödinger beschreibt dieses Phänomen:

In einer verschlossenen Kiste befindet sich eine Katze. Ebenfalls in der Kiste befinden sich ein Geigerzähler, ein unstabiles Element und ein mit Gift gefüllter Behälter. Sobald das unstabile Element zerfällt, misst der Geigenzähler dies und der Behälter wird zerstört, womit sich das Gift in der Kiste ausbreitet, und die Katze tötet.

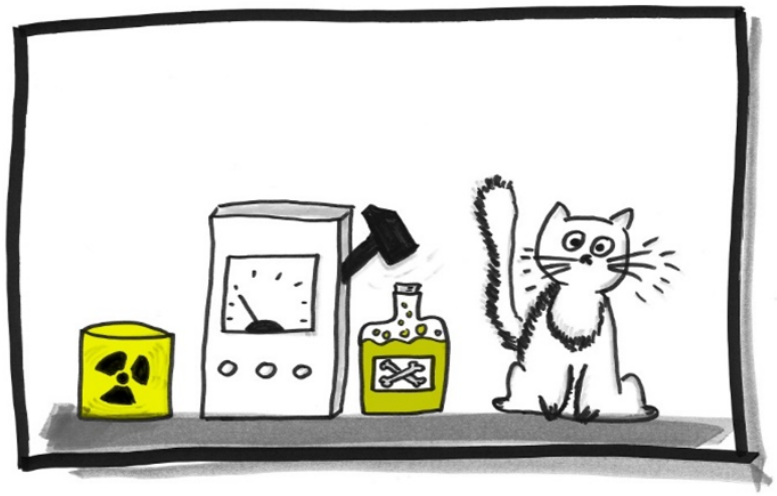

Abbildung: Gedankenexperiment "Schrödingers Katze".

Solange die Kiste verschlossen bleibt ist unklar, ob das Element noch nicht zerfallen ist, was bedeuten würde, dass die Katze noch lebend ist, oder ob das Element bereits zerfallen ist, was bedeuten würde, dass die Katze tot ist. Die verschlossene Kiste beschreibt so eine Superposition der beiden Zustände der Katze – den Zustand «die Katze ist lebendig» (50% Wahrscheinlichkeit) und den Zustand «die Katze ist tot» (50% Wahrscheinlichkeit). Der Zustand kollabiert in einen der beiden Zustände, sobald man eine Messung durchführt, indem man beispielsweise die Kiste öffnet und kontrolliert, ob die Katze noch lebt oder bereits gestorben ist.

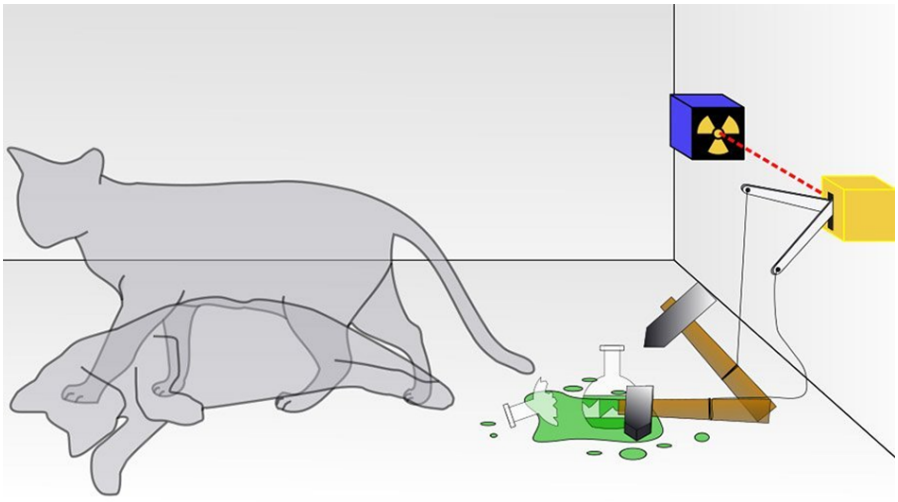

Abbildung: Die Katze befindet sich in der Superposition der beiden Zustände lebendig und tot.

Das Problem ist in diesem Fall, dass man mikroskopische Zustände der Superposition nicht auf die makroskopische Welt übertragen kann. Quantenmechanische Gesetze *können* nicht auf unsere bekannte Alltagswelt übertragen werden. Die kleinsten Partikel folgen allerdings den Gesetzen der Quantenmechanik.

Man sollte an dieser Stelle anmerken, dass Erwin Schrödinger dieses Gedankenexperiment in der Form eines Paradoxons aufstellte, um die Absurdität darzulegen, dass sich makroskopische Gegenstände (beispielsweise eine Katze) nicht in einer Superposition befinden können.

6.1.2 Verschränkung

Sind zwei Partikel miteinander verschränkt, dann ändert sich beim Ändern des Zustandes eines Partikels zwingend ebenso der Zustand des anderen Partikels. Die Messung des Zustandes eines Partikels bietet somit direkt Informationen beider Partikel an. Ebenso kann man den Zustand vielen verschränkten Partikel beeinflussen, indem man nur den Zustand eines einzelnen Partikels beeinflusst.

Eine der Möglichkeiten, um mehrere Partikel in einen verschränkten Zustand zu bringen, ist die Partikel auf sehr tiefe Temperaturen zu kühlen und sie nahe beieinander zu halten. Die individuellen Quantenzustände überlappen sich schliesslich, was zur Folge hat, dass es unmöglich ist die einzelnen Partikel voneinander zu unterscheiden. Sie werden dann als ein einzelnes einheitliches System angesehen.

6.1.3 Interferenz

In der Realität wird der Zustand eines Qubit als eine Quanten-Wellenfunktion abgebildet. Wellenfunktionen beschreiben die fundamentalen mathematischen Eigenschaften der Quantenmechanik. Hat ein Computer mehrere verschränkte Qubit, dann addieren sich die individuellen Wellenfunktionen in eine einheitliche Wellenfunktion, welche den gesamten Zustand des Quantencomputers, bzw. der Qubit beschreibt.

Die einheitliche Wellenfunktion des Quantencomputers beschreibt schlussendlich die Wahrscheinlichkeitsverteilung der verschiedenen Zustände, in der sich der Computer befindet.

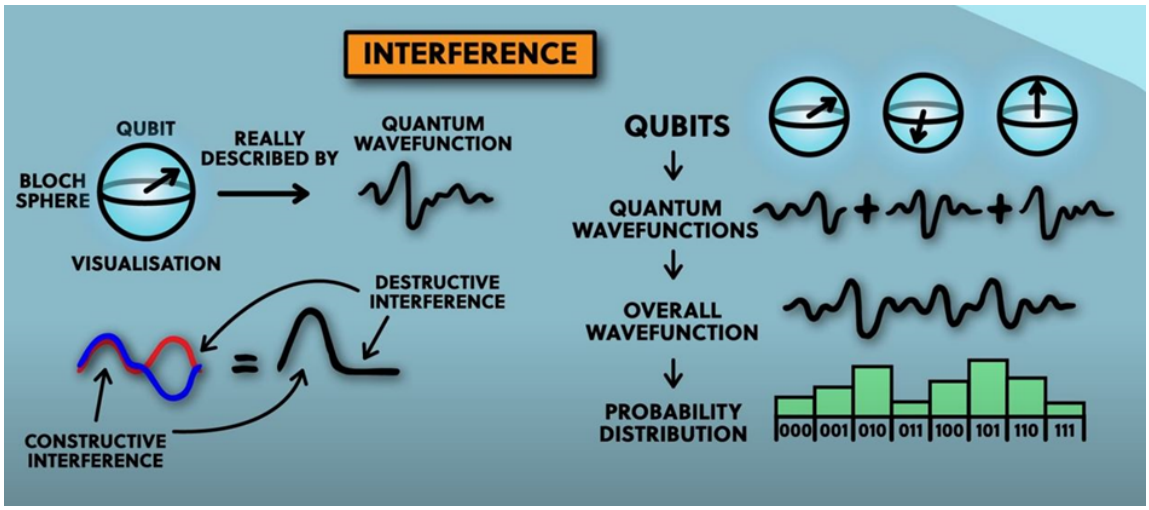

Abbildung: Interferenz in einem Quantencomputer

Obwohl sich der Quantencomputer in allen möglichen Zuständen befindet, wird bei einer Messung immer nur ein einzelner Zustand als Rückgabewert erfolgen.

Mit speziell konzipierten Algorithmen kann man durch konstruktive Interferenz die Wahrscheinlichkeit der korrekten Antwort erhöhen und durch dekonstruktive Interferenz die Wahrscheinlichkeit der inkorrekten Antworten senken. Wird nach der Interferenz der Zustand des Quantencomputers gemessen, ist es wahrscheinlich, dass die korrekte Antwort als Rückgabewert erfolgt. Es kann jedoch durchaus vorkommen, dass durch eine Messung per Zufall die inkorrekte Antwort als Rückgabewert erfolgt.

Das Phänomen der Interferenz trifft man (anders als das Phänomen der Superposition und der Verschränkung) ebenfalls in der makroskopischen Welt an – beispielsweise bei Schallwellen.

Kopfhörer haben heutzutage oft eine Funktion eingebaut, die sich «Noise-cancelling» (Englisch für "Geräusch-Unterdrückung") nennt. Dabei wird destruktive Interferenz verwendet um unerwünschte Töne (meistens Umgebungslärm) zu unterdrücken. Ein Mikrofon misst dabei die Audiosignale der Umgebung und sendet direkt über die Kopfhörer das inverse Audiosignal. Somit heben sich die Schallwellen gegenseitig auf.

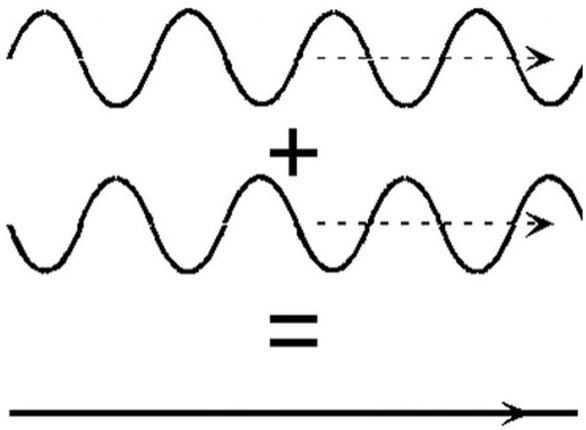

Abbildung: Destruktive Interferenz, beispielsweise bei Schallwellen. Das resultierende Signal ist ohne Amplitude.

6.2 Probleme bei der Entwicklung von Quantencomputer

Warum es bis heute noch keine grossen, bzw. leistungsstarke Quantencomputer gibt hat diverse Gründe. Die Zwei grössten Entwicklungshürden, die es zu überwinden gilt, sind die Isolation und die Fehlertoleranz.

6.2.1 Isolation

Quantencomputer müssen von der Aussenwelt isoliert sein. Ist dies nicht der Fall, dann wird die Information der Qubit schnell durch die Interaktion mit der Aussenwelt unerwünscht verändert oder die Information geht gänzlich verloren. Im besten Fall will man, dass die Qubit untereinander verschränkt sind, nicht aber mit anderen Partikeln. Dieses Problem wird als «Dekohärenz» bezeichnet.

Schlussendlich besteht das grundsätzliche Problem, dass Qubit aus sehr kleinen Partikeln bestehen und man weitere Partikel braucht, um diese Teilchen zu beeinflussen. Es gibt theoretische Möglichkeiten, um Störungen zu vermindern, beispielsweise könnten viele verschränkte Qubit (100 – 1' 000 Qubit) ein einzelnes Fehlerfreies Qubit repräsentieren.

6.2.2 Fehlertoleranz

Da sich ebenso bei klassischen Computern teilweise aufgrund von Interaktionen mit der Aussenwelt ein Fehler einschleichen kann, haben viele Operationen bei klassischen Computern eine Fehlerkorrektur implementiert. Fehlerkorrekturen sind bei Quantencomputer jedoch fast unmöglich – teilweise sind Fehlerkorrekturen sogar aufgrund von physikalischen Gesetzen unmöglich, beispielsweise aufgrund des «No-Cloning-Theorem» (Englisch für "nicht-Klonbarkeit"). Das No-Cloning-Theorem besagt, dass es unmöglich ist ein System zu bauen, welches Qubit kopiert, ohne das bestehende Qubit zu verändern.

Inzwischen gibt es diverse Möglichkeiten um einen Quantencomputer (zumindest theoretisch) zu realisieren, alle mit ihren Vor- und Nachteilen. Es bleibt aber weiterhin unklar, welche Option sich als die beste herausstellen wird.

7 Quantenalgorithmen

7.2 Grover's Algorithmus

Der Grover-Algorithmus kann eine Suche nach einem bestimmten Element im Gegensatz zu klassischen Computern exponentiell (quadratisch) ausführen.

Ist beispielsweise eine unstrukturierte Liste mit **n** Elementen gegeben, dann müsste man mit einem klassischen Computer jedes einzelne Element durchgehen und überprüfen, ob es das gesuchte ist. Im Durchschnitt wird die Hälfte der gesamten Liste überprüft, bis das gesuchte Element gefunden wird, im schlimmsten Fall – falls sich das gesuchte Element am Ende der Liste befindet – die ganze Liste, also **n** Schritte.

Ein Quantencomputer könnte mithilfe von Grovers Algorithmus ein gesuchtes Element in einer Liste mit **n** Elementen in $\mathbf{n^{1/2}}$ (quadratische Wurzel) Schritten finden. Ein Element kann beispielsweise ein Schlüssel sein. Die Suchkomplexität wäre daher für einen 128-Bit Schlüssel nicht $\mathbf{2^{128}}$, sondern die quadratische Wurzel von $\mathbf{2^{128} = 2^{64}}$.

Symmetrische Algorithmen sind jedoch, trotz Grovers Algorithmus, meistens quanten-resistent. Grovers Algorithmus verkürzt die effektive Länge eines symmetrischen Schlüssels auf die Hälfte. Um die bestehende Sicherheit weiterhin zu garantieren, kann man einfach die Schlüssellänge verdoppeln.

7.3 Shor's Algorithmus

Mit klassischen Computern ist es sehr einfach zwei beliebig grosse Zahlen miteinander zu multiplizieren. Jedoch ist es sehr schwierig mit klassischen Computern eine beliebig grosse Zahl zu faktorisieren.

Peter Shor publizierte im Jahr 1994 einen Algorithmus («Shor's Algorithmus»), der es in annehmbarer Zeit ermöglicht Zahlen zu faktorisieren. Um den Algorithmus effizient ausführen zu können, wird allerdings ein leistungsfähiger Quantencomputer benötigt.

Ein Quantencomputer verwendet dabei die Eigenschaft der Superposition, um viele Berechnungen parallel auszuführen. Mithilfe der destruktiven Interferenz schliessen sich alle falschen Antworten gegenseitig aus und die überbleibende Zahl liefert einen Weg, um den privaten RSA-Schlüssel zu berechnen.

Im Jahr 2019 veröffentlichte der YouTube-Kanal «minutephysics» das Video How Quantum Computers Break Encryption | Shor's Algorithm Explained. Es erklärt Shor's Algorithmus mit zusätzlichen Details und mathematischen Berechnungen.

Da Quantencomputer noch in der frühen Entwicklung sind und das Problem der Entwicklung von Quantenprozessoren vieler Qubit weiterhin noch besteht, ist die Grösse der Zahlen, welche faktorisiert werden konnten bisher noch sehr tief. Diverse Labore sind in der Lage die Zahl 15 mit Shor's Algorithmus zu faktorisieren.

Der offizielle Rekord (Stand 2021) für die Faktorisierung der grössten Zahl mit Shor's Algorithmus liegt lediglich bei 21, welche im Jahr 2012 durchgeführt wurde.

Es gibt diverse Berichte über die Faktorisierung von grösseren Zahlen mit Quantencomputern, welche jedoch bei näherer Betrachtung nur aufgrund spezieller Relationen von den unterliegenden Faktoren möglich waren.