**Quantencomputer – Segen oder Fluch?**

Dr. sc. techn. Iwan Schnyder, Dipl. El.-Ing. ETH / MAS FHO BAE

*Gegenwärtig existiert ein Wettlauf mit der Zeit, wer den ersten komplett funktionsfähigen Quantencomputer besitzt. Denn: Quantencomputer werden nicht nur sehr leistungsfähig sein, sondern haben auch grosses Potenzial, fast alle heute üblichen Verschlüsselungsalgorithmen zu lösen.*

Quantencomputer sind viel leistungsfähiger als heutige Computer, weil sie im Gegensatz zu diesen nicht auf den Gesetzen der traditionellen Halbleiterphysik basieren, sondern quantenmechanische Effekte nutzen. Dabei spielen die sogenannten Qubits als Mass für die Leistungsfähigkeit von Quantencomputern eine massgebende Rolle. Diese Qubits entsprechen den einzelnen Bits von konventionellen Computern.

Vieles ist ähnlich wie bei den konventionellen und uns bekannten Computern. Doch aufgrund der quantenmechanischen Effekte können die einzelnen Qubits nicht nur einen, sondern mehrere Zustände gleichzeitig speichern. Damit steigt die theoretische Anzahl der Operationen, die ein System aus mehreren Qubits gleichzeitig durchführen kann, exponentiell, wie die einfache Formel 2(Anzahl Qubits) zeigt. Konkret bedeutet dies: Bei einem Quantenregister mit 10 Qubits sind dies 1'024 Operationen, bei 32 Qubits 4'294'967'296 Operationen und bei 64 Qubits 18'446'744'073'709'551'616 Operationen – in derselben Zeit.

**Die zwei Seiten der Medaille**

Die aktuelle Theorie zu Quantencomputer besagt: Dank dieser Effekte und der riesigen Rechenleistung lassen sich gewisse Probleme der Informatik erheblich effizienter und damit schneller lösen, etwa die Suche in extrem grossen Datenbanken oder die Faktorisierung grosser Zahlen. In einer Disziplin haben Quantencomputer sogar das Potenzial, die digitale Welt nicht nur weiter zu beschleunigen, sondern regelrecht zu revolutionieren: Verfügen sie über eine ausreichende Anzahl Qubits und somit über genügend Rechenleistung, ist es möglich, dass diese Computer die Verschlüsselungsalgorithmen der heute sicheren Kommunikation im Internet und in der Datenverschlüsselung mit Leichtigkeit aushebeln.

**Was bedeutet das?**

Die aktuell vorherrschende Meinung «Quantencomputer könnten gar alle Verschlüsselungsverfahren lösen» trifft heute unglücklicherweise zu. Denn betroffen sind alle heute üblichen Verfahren wie beispielsweise das RSA-Krypto-System. Diese Verfahren beruhen auf zwei unterschiedlichen asymmetrischen Rechenoperationen, die in der einen Richtung einfach auszuführen sind, in der anderen aber nur sehr schwer. Die eine der beiden Rechenoperationen ist die Zerlegung grosser Zahlen in ihre Primfaktoren. Die zweite ist die Berechnung eines diskreten Logarithmus einer ganzen Zahl. Beide Verfahren eignen sich für die Public-Key-Verschlüsselung, weil man die codierten Nachrichten nur lesen kann, wenn sich die öffentlich sichtbare Zahl zerlegen lässt. Etwas, was nur die Kommunikationspartner können, die über den privaten Schlüssel verfügen. Für beide Operationen hat der

Mathematiker Peter Shor bereits 1994 nachgewiesen, dass Quantencomputer mit ausreichend Qubits die Berechnungen in beide Richtungen in überschaubarer Zeit lösen können.

**Wie der Gefahr begegnen?**

Es gibt bereits erste neue Verschlüsselungsverfahren, die auch vor der Rechenleistung eines Quantencomputers sicher zu sein scheinen. Verschiedene Algorithmen gelten als quantensicher, wobei das lediglich heisst: Derzeit ist noch kein Quantenverfahren bekannt, das sie knacken kann. Denn eine mathematisch unterlegte Sicherheit existiert nicht. Welches Verfahren die beste Alternative ist, diskutieren Forscherinnen und Forscher immer noch und auch die US-amerikanische Standardisierungsbehörde NIST prüft verschiedene neue Verschlüsselungsverfahren. Die Chancen stehen also gut, sich vor der Quantenapokalypse auf neue, sicherere (Internet)Kommunikation und Methoden zur Datenverschlüsselung zu einigen.

Unglücklicherweise ist der Wechsel von Verschlüsselungsverfahren jedoch eine komplexe und aufwändige Angelegenheit, müssen doch ganze IT- und Kommunikationssysteme quantencomputerresistent gemacht werden. Das sind Umstellungen, die lange dauern. Dabei müssen viele sensitive Daten, die wir heute erzeugen, wie beispielsweise Gesundheitsdaten, für lange Zeit vor Zugriffen und Manipulation Dritter sicher sein und nicht rückwirkend von einem Quantencomputer «geknackt» werden können.

Bis diese Verbesserungen implementiert und wirksam sind, können die einzelnen Unternehmen nicht viel mehr tun, als die eigenen ICT-Systeme auf dem aktuellsten Stand der Technik zu halten, periodische Backups der wichtigsten Daten zu erstellen und diese physisch an einem anderen Ort zu speichern, am besten getrennt vom Internet. Zudem sollten sehr sensible Daten nicht in einer Cloud, sondern in einer eigenen kontrollierten ICT-Umgebung aufbewahrt sein. Der Vorteil: Die Daten – verschlüsselt oder nicht – lassen sich auf diese Weise nicht von Dritten kopieren, um sie dann zu entschlüsseln und zu verwerten, sobald die erforderliche Rechenleistung von Quantencomputern für die Entschlüsselung verfügbar ist.