Post-Quantum - Nachtrag zum Thema Kryptographie

In der Frankfurter Allgemeinen Sonntagszeitung vom 10. Mai 2026 erregte ein Artikel meine Aufmerksamkeit, welcher revolutionäre Veränderungen im internetbasierten Datenverkehr ankündigte.

Es geht um die Sicherheit der Übertragung von verschlüsselten Daten. Als ich meine Ausführungen zur Kryptographie 2020 und 2021 schrieb, da galten asymmetrische Verschlüsselungsverfahren als das Nonplusultra im Datenverkehr. Browserdaten, Emails, Daten, die in social Media gepostet werden, Finanztransaktionen und alle anderen schützenswerten Informationen sind durch Verfahren, die auf großen Primzahlen und dem diskreten Logarithmus beruhen geschützt. Für Bitcoin-Transaktionen und Blockchains verwendet man Verfahren, die auf elliptischen Kurven basieren. Selbst für die schnellsten Computer waren Schlüssel, die auf solchen Verfahren beruhten, nur innerhalb von Jahrtausenden oder gar Jahrmillionen zu knacken. Und selbst, wenn es eng wird und die Rechenleistungen stark ansteigen würde, genügt es die Schlüssellänge etwas zu vergrößern und schon wächst die Rechenzeit zur Entschlüsselung exponentiell.

Die Idee der Quantencomputer existierte zwar schon länger, die Realisierung lag allerdings bisher noch in der Ferne.

Jetzt (30. März 2026) erschienen aber zwei Veröffentlichungen, die vermuten lassen, dass es nur noch wenige Jahre dauert, bis es einen funktionierenden Quantencomputer geben wird.

Derzeit arbeiten Computer mit Bits als kleinster Informationseinheit. Ein Bit kann zwei Zustände annehmen, die wir mit 0 und 1 bezeichnen. Sämtliche Informationen werden als Folge von Nullen und Einsen gespeichert und verarbeitet. Damit ist lässt sich einfach berechnen, wie lange es dauert, bis eine Information verarbeitet oder ein Algorithmus durchlaufen ist.

Quantencomputer dagegen arbeiten mit sog. Qubits als kleinster Informationseinheit. Ein Qubit kann zwei Zustände gleichzeitig annehmen und darüber hinaus auch noch viele weitere Zwischenzustände. Außerdem lösen Quantencomputer viele Aufgaben gleichzeitig und verarbeiten die Informationen nicht nacheinander. Ohne die Funktionsweise von Quantencomputern zu verstehen, wird dadurch bereits deutlich, dass Quantencomputer viel mehr Möglichkeiten haben, Informationen zu verarbeiten. 31 Qubits entsprechen der gleichen Speichergröße wie 32 GB eines herkömmlichen Computers. Eine Primfaktorenzerlegung einer 2048 Bit-Zahl, für die ein herkömmlicher Computer Millionen Jahre benötigt, erledigt ein Quantencomputer in wenigen Minuten.

Dies bedeutet, dass die bisher verwendeten Verfahren zur Datenverschlüsselung in absehbarer Zeit nicht mehr sicher sind. Für Quantencomputer müssen neue Programmieransätze entwickelt werden, die auf mehrdimensionalen Quantengittern

basieren. Was darunter zu verstehen ist, und wie diese Ansätze funktionieren, ist (noch) nicht Gegenstand dieser Ausführungen. Aber schon der Hinweis darauf, dass es um mehr als drei Dimensionen geht, die wir uns noch vorstellen können, lässt viel Komplexität vermuten.

Müssen wir uns nun Sorgen machen, dass unsere Daten nun bald nicht mehr sicher sind und eventuell nach James Bond Manier, von einem die Weltherrschaft anstrebenden Bösewicht, der einen Superquantencomputer einsetzen kann, ausspioniert werden können?

Mit **Post-Quantum** werden neuartige kryptographische Verfahren bezeichnet, die auch beim Einsatz von Quantencomputern sicher bleiben. An solchen Verfahren wird schon seit einigen Jahren von Geheimdiensten und nationalen oder europäischen Behörden gearbeitet. Dabei sind zu nennen das Referat Quantentechnologie und kryptographische System des Bundesamtes für Sicherheit in der Informationstechnologie (BSI) in Bonn, die Network and Information Security Group der europäischen Kommission oder das amerikanische National Institute of Standards and Technology (NIST). Außerdem arbeiten die mit Sicherheit die großen Konzerne wie Google, Meta oder andere an der Entwicklung solcher Systeme.

Es ist also davon auszugehen, dass die Welt vorbereitet ist, wenn der neue ‚Quantensprung' erfolgt.