Station 5 – Post-Quanten-Kryptografie

Hintergrund

Was ist nun Post-Quanten-Kryptografie und warum brauchen wir das?

Dazu schauen wir uns zwei Konzepte an: Was Quantencomputer überhaupt sind und welche Arten von Verschlüsselung bedroht sind. Die Erklärungen sind vereinfacht, um die Prinzipien zu erklären, dafür nehmen wir es manchmal nicht so genau.

Quantencomputer

Ein Quantencomputer arbeitet grundlegend anders als heutige Computer. Bisher rechnen wir mit Bits. Das ist die kleinste Einheit in einem Computer und hat den Wert 0 oder 1. Das lässt sich gut in Schaltkreisen abbilden, denn auch Schalter sind an oder aus. Z.B. ein Lichtschalter zu Hause. Aber auch in den Schaltkreisen eines Computers gibt es Milliarden kleiner Schalter, die ihn zusammen ermöglichen zu rechnen.

Bei einem Quantencomputer werden Quanteneffekte genutzt. Das sind Effekte, die bei kleinsten Teilchen auftreten und so in der für uns wahrnehmbaren Welt nicht auftreten. Z.B. können zwei Teilchen miteinander verschränkt sein. Ändere ich das eine, ändert sich automatisch auch das andere. Und Teilchen können gleichzeitig mehrere Zustände haben. Statt nur den Wert 0 oder 1 anzunehmen, können Quantenbits 0 und 1 gleichzeitig sein. Das wäre so, als ob das Licht gleichzeitig an und aus ist. Diesen Effekt nennt man Superposition.

Diese Superposition erlaubt es, spezielle Computer zu bauen, die manche Berechnungen deutlich schneller durchführen können als heutige Computer. Sehen wir uns das Beispiel an, herauszufinden, welche Primzahlen Teiler einer Zahl sind. Z.B. 21. Mit einem klassischen Computer bleibt mir nichts anderes übrig als der Reihe nach durchzuprobieren, ob die Zahl durch 2 teilbar ist, dann durch 3, dann durch 5 und so weiter. Das kann man ein bisschen verbessern, aber im Grunde bleibt die Berechnung für große Zahlen aufwändig und wird mit der Länge der Zahlen so schwierig, dass sie irgendwann nicht mehr zur Lebenszeit fertig wird. Ein Quantencomputer kann aber durch die Superposition die Teiler nicht nacheinander prüfen, sondern gleichzeitig. Das beschleunigt die Berechnung nicht nur, sondern sie dauert auch bei großen Zahlen nicht signifikant länger. Dafür braucht es nur mehr Quantenbits. Der Algorithmus für Quantencomputer heißt übrigens Shor-Algorithmus.

Moderne Verschlüsselungskonzepte

In der sicheren, digitalen Kommunikation gibt es momentan zwei grundlegende Konzepte. Symmetrische Verschlüsselung wie AES, bei der zum Ver- und Entschlüsseln der gleiche geheime Schlüssel verwendet wird. Und asymmetrische Verschlüsselung, bei der zwei Schlüssel existieren. Eine öffentlicher, mit dem ein Klartext verschlüsselt wird und ein geheimer, mit dem der Geheimtext wieder entschlüsselt wird.

AES (Advanced Encryption Standard) wurde im Jahr 2000 nach einem Wettbewerb zur Suche eines sicheren Verschlüsselungsverfahrens standardisiert und ist unter Expertinnen und Experten anerkannt. Momentan sind keine Angriffe bekannt, die das reine Ausprobieren sämtlicher Möglichkeiten so stark abkürzen würde, dass er nicht mehr einsetzbar wäre. Der Grover-Algorithmus halbiert die Schlüssellänge. Das kann aber mit längeren Schlüsseln ausgeglichen werden.

Bei asymmetrischen Verfahren ist es anders. Sie basieren z.B. auf der Primfaktorzerlegung. Zwei sehr große Primzahlen werden miteinander multipliziert und ergeben eine wirklich große Zahl. Diese Multiplikation ist für den Computer sehr einfach. Herauszufinden, aus welchen Primfaktoren eine Zahl besteht, ist aber sehr schwierig. Das kannst du leicht mit kleinen Zahlen ausprobieren. Was sind die beiden Primfaktoren von 77? Wenn du nicht das große Einmaleins auswendig gelernt hast, gar nicht so einfach. Aber wenn du 7 * 11 ausrechnen sollst, geht das halbwegs flott.

Z.B. bei dem asymmetrischen Verfahren RSA werden zwei 500-stellige Primzahlen multipliziert, was dann ein Produkt mit 999 oder 1000 Stellen ergibt. Die Zahl wäre so lang:

1000

Bei einer so langen Zahl die Primfaktoren zu finden ist selbst für heutige Computer sehr schwierig.

Allerdings gibt es bei Quantencomputern den Shor-Algorithmus, der das Zerlegen in Primfaktoren stark beschleunigt. Noch sind die Quantencomputer zu klein, aber es kann gerade bei Geheimdiensten in den nächsten Jahren so weit sein, dass auch solche Faktorisierungen möglich sind.

Daher wird an Alternativen geforscht, um Post-Quanten-Algorithmen zu haben, bevor die alten unsicher sind.

Ausprobieren

Die Algorithmen sind im Vergleich zu den bisher betrachteten Algorithmen deutlich komplexer, um deren Schwachstellen auszumerzen. Lass dich nicht entmutigen, wenn du sie nicht verstehst. Es hat einen Grund, warum nur wenige Kryptografinnen und Kryptografen weltweit an Wettbewerben zum Finden eines neuen Algorithmus teilnehmen. Und für einige Schritte brauchst du Potenzen und Moduluarithmetik.

Multiplikation und Faktorisierung

Probiere im Onlinefaktorisierer Msiev die vorgeschlagenen Zahlen von klein nach groß. Wie du siehst, wird die Zeit, die er braucht, um die Faktoren zu finden, exponentiell länger.

AES

In der AES-Animation des CryptTool kannst du dir prinzipiell ansehen, wie AES arbeitet. Dabei wird der Klartext in mehreren Runden immer wieder neu mit Ersetzungen und Verschiebungen bearbeitet. Wenn du möchtest, kannst du auch Schritt für Schritt die Verschlüsselung durchspielen.

RSA

Für RSA gibt es im CryptTool eine Veranschaulichung, wie RSA arbeitet und Schlüssel mit Primzahlen generiert werden. Du kannst hier die Erstellung der Schlüssel und die Verschlüsselung Schritt für Schritt durchgehen.