Das Fraunhofer-Institut für Naturwissenschaftlich-Technische Trendanalysen berichtet über neue Technologien

Post-Quantum-Kryptografie

Für die Zukunft zu erwartende Quantencomputer werden in Teilbereichen wesentlich leistungsfähiger sein als heutige Rechner und damit eine Bedrohung für einige wichtige, derzeit genutzte Verschlüsselungsverfahren darstellen. Das betrifft auch bereits heute zu verschlüsselnde Informationen, wenn diese langfristig vertraulich bleiben und daher geschützt werden müssen. Im Rahmen der Post-Quantum-Kryptografie (PQK) beschäftigt man sich daher mit kryptografischen Methoden, deren Sicherheit gegenüber Angriffen durch sowohl klassische Computer als auch Quantencomputer gewährleistet wäre und die damit auch weiterhin z. B. einen sicheren Informationsaustausch im Internet gewährleisten würden. Dabei handelt es sich um Methoden, die auf klassischer Computertechnologie zum Einsatz gelangen können. Die PQK stellt dementsprechend selbst keine Quantentechnologie dar.

Generell lässt sich mit Hilfe von kryptografischen Verfahren u. a. die Vertraulichkeit von Informationen sicherstellen, indem unter Verwendung eines bestimmten Schlüssels ein lesbarer Klartext durch ein geeignetes Verschlüsselungsverfahren in einen unlesbaren Geheimtext umgewandelt wird. Hierbei kann grundsätzlich zwischen symmetrischen und asymmetrischen Verfahren unterschieden werden. Symmetrische Verschlüsselungsverfahren verwenden sowohl für die Verschlüsselung als auch für die Entschlüsselung denselben Schlüssel. Solche Methoden besitzen den Nachteil, dass dieser Schlüssel entsprechend geheim gehalten und daher auf einem sicheren Weg zwischen den Kommunikationspartnern ausgetauscht werden muss. Ein wichtiges Beispiel für ein herkömmliches symmetrisches Verschlüsselungsverfahren ist AES (Advanced Encryption Standard).

Asymmetrische Verschlüsselungsverfahren nutzen hingegen unterschiedliche Schlüssel für die Verschlüsselung und die Entschlüsselung. Während der sogenannte öffentliche Schlüssel allgemein bekannt ist und der Verschlüsselung dient, ist der sogenannte private Schlüssel geheim und wird zur Entschlüsselung verwendet. Wichtige herkömmliche asymmetrische Verfahren sind RSA (benannt nach den Entwicklern Rivest, Shamir, Adleman) und die Elliptische-Kurven-Kryptografie. Die Sicherheit von asymmetrischen Verschlüsselungsverfahren basiert auf mathematischen Problemstellungen, deren Lösung unter bestimmten Annahmen praktisch unmöglich ist. Hierzu zählt z. B. die Annahme, dass ein Angreifer lediglich einen klassischen Computer nutzt.

Bei Quantencomputern erfolgt im Gegensatz zu klassischen Computern die Informationsverarbeitung auf der Grundlage von quantenphysikalischen Phänomenen. Sie können daher prinzipiell deutlich leistungsfähiger sein als klassische Computer und wären dadurch in der Lage, alle zurzeit üblicherweise eingesetzten asymmetrischen kryptografischen Verfahren zu brechen. Symmetrische Verfahren wären weniger bedroht, da diese durch eine Verdoppelung der Schlüssellänge auch gegenüber Quantencomputern sicher wären (wenn der geheime Schlüssel auf einem sicheren Weg ausgetauscht wird).

Für asymmetrische kryptografische Verfahren existieren allgemein drei grundlegende Einsatzmöglichkeiten. Neben der bereits erwähnten direkten Verschlüsselung zählen hierzu noch der Schlüsselaustausch und die digitale Signatur. Während es zwar prinzipiell möglich ist, asymmetrische Verschlüsselungsverfahren zur Verschlüsselung von Nachrichten einzusetzen, ist diese Vorgehensweise jedoch deutlich rechenintensiver und damit langsamer als bei den symmetrischen Varianten. In der Praxis werden asymmetrische Verschlüsselungsverfahren daher eher für den Austausch eines geheimen Schlüssels für ein symmetrisches Verfahren genutzt. Hierbei wird zunächst nicht die eigentliche Nachricht, sondern lediglich der geheime Schlüssel zwischen den Kommunikationspartnern verschlüsselt ausgetauscht. Die Nachricht wird dann mit dem symmetrischen Verfahren und diesem geheimen Schlüssel ver- und entschlüsselt. Eine digitale Signatur dient in einer ähnlichen Weise wie eine herkömmliche Unterschrift auf Papier der Überprüfung, ob eine Nachricht tatsächlich vom korrekten Absender stammt (Authentizität) und ob an der Nachricht nachträglich Veränderungen vorgenommen wurden (Integrität).

Von großer Bedeutung für die Realisierung von Verfahren der Post-Quantum-Kryptografie ist die Einsicht, dass Quantencomputer voraussichtlich nur bei speziellen Anwendungen schneller sind als klassische Computer. Als Grundlage für derartige PQK-Verfahren müssen dementsprechend mathematische Problemstellungen verwendet bzw. gefunden werden, die nicht nur sicher gegenüber Angriffen mit Hilfe von klassischen Computern sind, sondern für die auch Quantencomputer keinen entsprechenden Vorteil gegenüber klassischen Computern aufweisen. Dabei sind in erster Linie neue asymmetrische Verfahren von Interesse, da symmetrische Verfahren, wie oben erwähnt, nur in einem erheblich geringeren Ausmaß durch Quantencomputer bedroht sind.

Einige Vorschläge für PQK-Verfahren existieren bereits heute. Diese beinhalten allerdings noch einige Herausforderungen. Eine solche Herausforderung stellt vielfach das augenblicklich noch mangelnde Vertrauen in die Sicherheit von einigen vorgeschlagenen Methoden dar. Hier ist noch mehr Erfahrung hinsichtlich der verschiedenen Verfahren erforderlich. Eine weitere Herausforderung bei manchen PQK-Vorschlägen besteht in deren im Vergleich zu herkömmlichen Verfahren geringen Effizienz, u. a. hinsichtlich der für eine ausreichende Sicherheit notwendigen Schlüssellängen. So erfordert z. B. ein PQK-Ansatz, das sogenannte McEliece-Verfahren, für eine ausreichende Sicherheit Schlüssellängen von einigen Millionen Bits, während beispielsweise für RSA nur einige Tausend Bits notwendig sind.

Augenblicklich ist noch nicht absehbar, welche Ansätze sich im Rahmen der PQK letztendlich durchsetzen werden. Generell kann es dabei zehn Jahre oder länger dauern, bis ein neues kryptografisches Verfahren ausreichend auf seine Sicherheit überprüft wurde und weit verbreitet ist. In einem ähnlichen Zeitrahmen sind auch frühestens Quantencomputer zu erwarten, die in der Lage wären, herkömmliche Verschlüsselungsverfahren wie RSA zu brechen.

Dr. Klaus Ruhlig