Post Quanten Kryptographie

Warum wir neue Verschlüsselungsalgorithmen brauchen

Thomas Jakkel
MatNr. 1001594
01jath1bif@hft-stuttgart.de

Lukas Reinke
MatNr. 1001213
01relu1bif@hft-stuttgart.de

***Zusammenfassung*—Quantenkryptographie wird als ernsthafte Gefahr für die aktuell gängigen Kryptographie-Verfahren gesehen. Speziell die, für das sichere Funktionierende der Netzwerk-Kommunikation benötigten, asymmetrischen Kryptographie-Algorithmen wie beispielsweise *RSA* stehen in der Gefahr mithilfe eines Quantencomputers innerhalb von Stunden gebrochen zu werden. Ein solcher Computer birgt somit eine Gefahr für die gesamte heutige Informationssicherheit.**

Schon 1994 bewies der amerikanische Mathematiker *Peter Shor* in der Theorie, wie mithilfe eines Quantencomputers die Primfaktorzerlegung großer Zahlen in realer Zeit erfolgen kann. Mit einem klassischen, binären Computer wäre dies nicht in der Lebenszeit des Universums möglich, was das kern Sicherheits-Prinzip asymmetrischer Kryptographie darstellt. Wegen dieser Bedenken hat das US National Institute of Standards and Technology (NIST) seit 2016 eine Ausschreibung zur Entwicklung eines quantensicheren aufgestellt. Der aktuelle Favorit, ein Verfahren auf basis mehrdimensionaler Vektorfelder, soll, soweit sich keine Schwachstellen herausstellen, schon in den nächsten Jahren in der Netzwerk Kryptographie etabliert werden und somit die Kommunikation schon vor der Existenz eines potentiellen Quantencomputers absichern. Es ist also gut möglich, dass wir die aktuellen Kryptographie Standards innerhalb der nächsten 5 Jahre austauschen werden.

Abbildungsverzeichnis

Abkürzungsverzeichnis

I. Einleitung

Das Thema der *Quanten Supremacy*, der Zeitpunkt zu dem ein Quantencomputer (QC) die Fähigkeit komplexe Probleme zu lösen besser beherrscht als ein klassischer Computer, ist in den letzten Jahren immer wieder in einschlägigen Medien und diverse Fachpublikationen aufgetaucht. Google zum Beispiel behauptet hat schon wiederholt behauptet einen solchen QC zu besitzen, was jedoch in diversen Publikationen bezweifelt wurde [1]. Wenig Zweifel besteht jedoch, dass ein solcher Computer in absehbarer Zeit einsatzbereit sein wird. Im Folgenden wird beschieden wie ein QC funktioniert, mit welchen Algorithmen, die in realer Zeit laufen, QC die aktuellen, kryptographischen Verfahren brechen können werden. Außerdem werden wir aktuelle, neu Entwickelte quantensichere Algorithmen betrachten und wie sie sie Gefahr durch QC mittigern werden.

Literaturverzeichnis

[1] a. cho adrian, *Ordinary computers can beat Google's quantum computer after all — Science — AAAS*, Aug. 2022. Adresse: https://www.science.org/content/article/ordinary-computers-can-beat-google-s-quantum-computer-after-all (besucht am 14. 04. 2023).