Post Quanten Kryptographie

Warum wir schon jetzt 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 Funktionieren der Netzwerk und Internet Kommunikation benötigten, asymmetrischen Kryptographie-Algorithmen wie beispielsweise *RSA* stehen in der Gefahr mithilfe eines funktionierenden Quantencomputers binnen weniger Minuten 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, digitalen Computer würde eine solche Berechnung eine längere Zeit als die Existenz des Universums dauern. Dies stellt das zentrale Sicherheits-Prinzip asymmetrischer Kryptographie dar. Wegen dieser Bedenken hat das US National Institute of Standards and Technology (NIST) seit 2016 eine Ausschreibung zur Entwicklung eines quantensicheren Algorithmus 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 die aktuellen Kryptographie Standards innerhalb der nächsten 5 Jahre ausgetauscht werden.

ABBILDUNGSVERZEICHNIS

I. EINLEITUNG

Das Thema der *Quanten Supremacy*, der Zeitpunkt zu dem ein Quantencomputer die Fähigkeit besitzt komplexe Probleme besser zu lösen als ein klassischer Computer, ist in den letzten Jahren immer wieder in einschlägigen Medien und diverse Fachpublikationen aufgetaucht. Google zum Beispiel behauptete schon wiederholt einen solchen Quantencomputer 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 Quantencomputer funktioniert, mit welchen Algorithmen, die in realer Zeit laufen, Quantencomputer die aktuellen, kryptographischen Verfahren brechen können werden. Außerdem werden wir aktuelle, neu Entwickelte quantensichere Algorithmen betrachten und wie sie sie Gefahr durch Quantencomputer mittigern werden.

II. EINFÜHRUNG IN DAS QUANTEN COMPUTING

Quanten Computing ist eine relativ junge Disziplin der Physik und Informatik. Während sich die beiden Bereiche unabhängig von einader Anfang des 20. Jahrhundert entwickelt hatten, wurden die ersten Versuche und theoretischen Überlegungen, Methoden der Informatik mithilfe von Quantenobjekten umzusetzen um 1980 gestartet. Obwohl das Quantencomputer erst seit kurzer Zeit existiert, hat es bereits bedeutende Fortschritte gemacht und

besitzt ein enormes Potenzial für Entwicklungen zum Beispiel in den Bereichen Kryptographie, Optimierungsprobleme, Simulation chemischer Prozesse und maschinelles Lernen.

A. Ein theoretischer Quantencomputer

Ein der Informatik zugrunde liegendes Prinzip ist, dass [2, S122] Informationen auf unterschiedlichen Weisen dargestellt (codiert) werden können. So kann die Zahl *fünf* zum Beispiel binär (0101) oder als Unicode Zeichen (*U+0035*) dargestellt werden. Der Inhalt der Information ist in beiden Fällen jedoch der gleiche.
Dieses Prinzip ist für die Informatik sehr wichtig. Es ermöglicht Maschinen komplexe Informationen zu speichern, mithilfe einfacher Operationen zu manipulieren und wieder in ein komplexes Format zu überführen ohne dabei an Informationsgehalt zu verlieren oder Informationen unkenntlich zu zu machen. In einem Computer werden diese Informationen in Form von *bits* darstellt die zwei Zustände, repräsentiert durch *0* und *1*, annehmen können. In einem klassischen, digitalen Computer sind diese beispielsweise durch das fließen von Strom abgebildet. Ein Quantencomputer repräsentiert Informationen in den Eigenschaften von Quanten-Objekten, beispielsweise dem Spin von Elektronen.
Um die Funktion eines Quantencomputer zu erläutern muss erst ein kurzer Blick auf einige Quantenphysikalische Phänomene geworfen werden.

1) Superpositionen: Eine Superposition ist das Fundamentale quantenphysische Phänomen das einem Quantencomputer zugrunde Liegt. Es wird meistens mithilfe des Gedankenexperiments von [3, \$5] *Schrödingers Katze* veranschaulicht: In einer Box befindet sich eine Katze und ein Gefäß mit Gift das zerstört wird und die Katze tötet wenn ein radioaktiver Zerfall gemessen wird. Von außerhalb der Box lässt sich nicht feststellen ob der Mechanismus der das Gift freisetzt aktiviert wurde. Sie befindet sich, Quantenmechanisch gesehen, in einem Zustand in dem sie sowohl Tot als auch lebendig ist. In dem Moment in dem die Box geöffnet wird, kann festgestellt werden welcher der beiden Zustände eingetroffen ist.

Auf ein Quantenteilchen übertragen heißt das: Es kann sich in einem Undefinierten Zustand befinden, der **Superposition** aus allen möglichen Zuständen. Erst wenn *nachgeschaut* also der Zustand gemessen wird, kollabiert die Superposition in einen der möglichen Zustände. Eine Superposition kann durch die Wahrscheinlichkeit mit der jeder der Zustände eintreten kann beschrieben werden. Ein Elektron mit den Zuständen Spin up (75%) und Spin down (25%) kollabiert also wenn der Spin gemessen wird zu $3/4$ der Fälle als Spin up und $1/4$ als Spin down. Mathematisch kann eine Superposition ψ also als Linearkombination ihrer Zustände betrachtet werden.

$$|\psi\rangle = \alpha\,|1\rangle + \beta\,|0\rangle \tag{1}$$

Diese Linearkombination kann auch grafisch als Vektor auf einer Kugel dargestellt werden (siehe Graphik 1), es ist zu beachten, dass der Vector z nicht den Spin, sondern die Linearkombination darstellt.

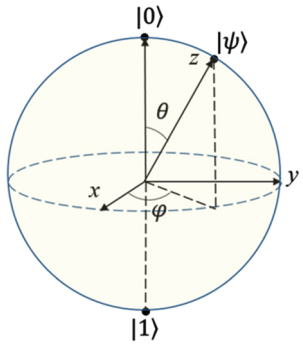

Abbildung 1. Spin eines Elektrons in Superposition [4]

2) Quantenverschränkung:

B. Implementierung eines Quantencomputers

III. RSA

IV. Shors-Algorithmus

Die Faktorisierung großer Zahlen **bernsteinPostquantumCryptography2017** ist ein fundamentales mathematisches Problem, bei dem eine gegebene Zahl in ihre Primfaktoren zerlegt wird. Dieses Problem ist von zentraler Bedeutung für die Kryptographie, da viele

asymmetrische Verschlüsselungsverfahren, wie beispielsweise RSA, auf der Schwierigkeit der Faktorisierung großer Zahlen beruhen.

Das Problem der Primfaktorzerlegung besteht darin, eine öffentliche Zahl N in zwei oder mehr geheime Primzahlen p und q zu zerlegen: N = pq. Für kleine Zahlen kann die Faktorisierung durch Ausprobieren möglicher Primfaktoren relativ einfach sein. Allerdings wird die Faktorisierung bei großen Zahlen exponentiell schwieriger, da es keine effizienten klassischen Algorithmen gibt, welche dies in Polynomialzeit bewältigen können.

Die Sicherheit vieler asymmetrischer Verschlüsselungsverfahren, wie beispielsweise das RSA-Verfahren, beruht auf der Schwierigkeit der Faktorisierung großer Zahlen. Wenn ein Angreifer in der Lage wäre, die Primfaktoren einer Zahl zu finden, könnte er den geheimen Schlüssel einer Verschlüsselungsmethode berechnen und die Sicherheit des Systems kompromittieren.

Shors Algorithmus **shorAlgorithmsQuantumComputation1994** gilt als einer der bedeutendsten Quantenalgorithmen, der die Faktorisierung großer Zahlen in Polynomialzeit ermöglicht. Auch wenn dieser Algorithmus einen Quantencomputer mit vielen, stabilen Qubits voraussetzt, stellt diese revolutionäre Entdeckung bereits heute eine enorme Bedrohung für die moderne Kryptographie dar. Zum einen wird effektiv an CQ geforscht, die Anzahl stabiler Qubits in QC steigen. Wenn der Quantencomputer seinen Durchbruch in unserer Gsellschaft erreicht hat, müssen wir darauf vorbereitet sein und uns bereits heute mit den Konsequenzen auseinander setzen. Zum anderen werden verschlüsselten Daten bereits heute gespeichert um sie in der Zukunft entschlüsseln zu können und im Nachinein an wichtige, vertrauliche Informationen zu gelangen. In der Kryptographie spricht man von dem Prinzip: SSafe now, decrypt later".

Shors Algorithmus bietet eine effiziente Lösung für die Faktorisierung großer Zahlen auf einem Quantencomputer. Dieser Quantenalgorithmus...

A. *Faktorisierung großer Zahlen*

Die teuerste Operation **gidneyHowFactor20482021**

V. Leitfrage: Warum wir schon jetzt neue Verschlüsselungsalgorithmen brauchen

Nachdem wir uns in dieser Arbeit hauptsächlich mit dem WIE Quantencomputer die aktuelle asymmetrische Kryptografie brechen können und wie mit diesem Problem auf einer technischen Ebene umgegangen werden kann, gilt es noch eine weitere Frage zu beantworten. Warum müssen wir uns schon jetzt mit dieser potentiellen Gefahr auseinandersetzen? Ein großteil der vorgestellen Konzepte und Algorithmen sind nur theoretischer Natur und aktuelle Quantencomputer sind nicht in der Lage zum Beispiel RSA zu decodieren. Warum also hat das NIST seine Ausschreibung für einen Quantensichern Algorithmus gestartet? Warum sollte die Gefahr eines Quantencomputers auf die Kryptographie schon jetzt ernst genommen werden?
Zum einen gilt es die Frage zu beantworten wann es wahrscheinlich es ist, dass ein Quantencomputer in der Lage ist eine mit RSA-2048 bit verschlüsselte Nachricht zu entschlüsseln. Das theoretische minimum an benötigte Qbits hierfür liegt laut Abschätzungen der Schweizer IT-Sicherheitsfirma *Kudelski Security* bei 6190 logischen Qbits [5]. Dies berücksichtigt jedoch Faktoren wie Implementierungs-Details und Fehlerkorrektur nicht. Einer anderen Schätzung zufolge würden eher um die 10.000 reale Qbits benötigt[6]. Wie Lange wird es dauern bis ein Quantencomputer mit einer solchen Anzahl an Qbits Realität ist?
Schaut man auf die *Timeline* der Firma IBM (siehe Grafik 3) so sieht man, dass der aktuelle entwicklungsstand ein Quantencomputer mit 433 Qbits ist. Dies stellt schon ein enormes Wachstum zu den 27 Qbits in 2019 dar. Der Plan ist es bis 2025 auf ungefähr 4000 Qbits zu gelangen und nach 2026 10.000 und mehr Qbits anzupeilen [7].
Diese Vorhersage deckt sich auch mit den Ansichten führende Experten in dem Gebiet der Quantenkryptografie. Bei einer Befragung des *Global Risk Intites* an der 47 Forschende teilnahmen ergab sich die folgenden Ergebnisse. Es wird für sehr wahrscheinlich

gehalten, dass in den nächsten 15 bis 20 Jahren ein Quantencomputer in der Lage sein wird RSA-2048 zu brechen mindestens aber in 30 Jahren soll dies mit nahezu vollständiger Sicherheit möglich sein [8].

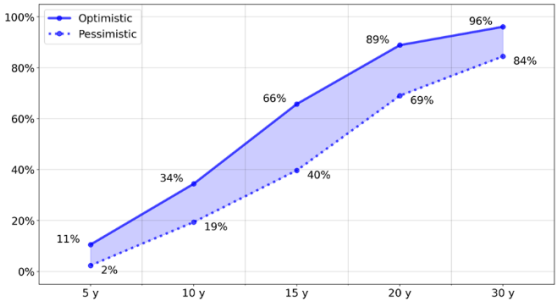

Abbildung 2. Wahrscheinlichkeit wann laut Experten des Quantencomputing RSA-2048 durch einen Quantencomputer gebrochen sein kann [8]

Wenn

Literaturverzeichnis

[1] a. cho adrian. „Ordinary computers can beat Google's quantum computer after all — Science — AAAS.“ (2. Aug. 2022), Adresse: https://www.science.org/content/article/ordinary-computers-can-beat-google-s-quantum-computer-after-all (besucht am 14. 04. 2023).

[2] A. Steane, „Quantum computing,“ *Reports on Progress in Physics*, Jg. 61, Nr. 2, S. 117, Feb. 1998, ISSN: 0034-4885. DOI: 10.1088/0034-4885/61/2/002. Adresse: https://dx.doi.org/10.1088/0034-4885/61/2/002 (besucht am 19. 03. 2023).

[3] E. Schrödinger, „Die gegenwärtige Situation in der Quantenmechanik,“ *Naturwissenschaften*, Jg. 23, Nr. 48, S. 807–812, 1. Nov. 1935, ISSN: 1432-1904. DOI: 10.1007/BF01491891. Adresse: https://doi.org/10.1007/BF01491891 (besucht am 10. 06. 2023).

[4] „cpb_27_9_090308_f8.jpg (JPEG Image, 462 × 527 pixels).“ (), Adresse: https://cpb.iphy.ac.cn/article/2018/1953/cpb_27_9_090308/cpb_27_9_090308_f8.jpg (besucht am 10. 06. 2023).

[5] T. Gagliardoni. „Quantum attack resource estimate: Using shor's algorithm to break RSA vs DH/DSA VS ECC,“ Kudelski Security Research. (24. Aug. 2021), Adresse: https://research.kudelskisecurity.com/2021/08/24/quantum-attack-resource-estimate-using-shors-algorithm-to-break-rsa-vs-dh-dsa-vs-ecc/ (besucht am 11. 06. 2023).

[6] L. Ziegler, „Online security, cryptography, and quantum computing,“ *Forum Lectures*, 29. Jan. 2015. Adresse: https://digitalcommons.csbsju.edu/forum_lectures/119.

[7] „IBM Quantum Computing — Roadmap.“ (1. Okt. 2015), Adresse: https://www.ibm.com/quantum/www.ibm.com/quantum/roadmap (besucht am 11. 06. 2023).

[8] „2021 quantum threat timeline report: Global risk institute,“ Global Risk Institute. (), Adresse: https://globalriskinstitute.org/publication/2021-quantum-threat-timeline-report-global-risk-institute-global-risk-institute/ (besucht am 16. 04. 2023).

VI. Anhang

A. *IBM Quantencomputing roadmap*

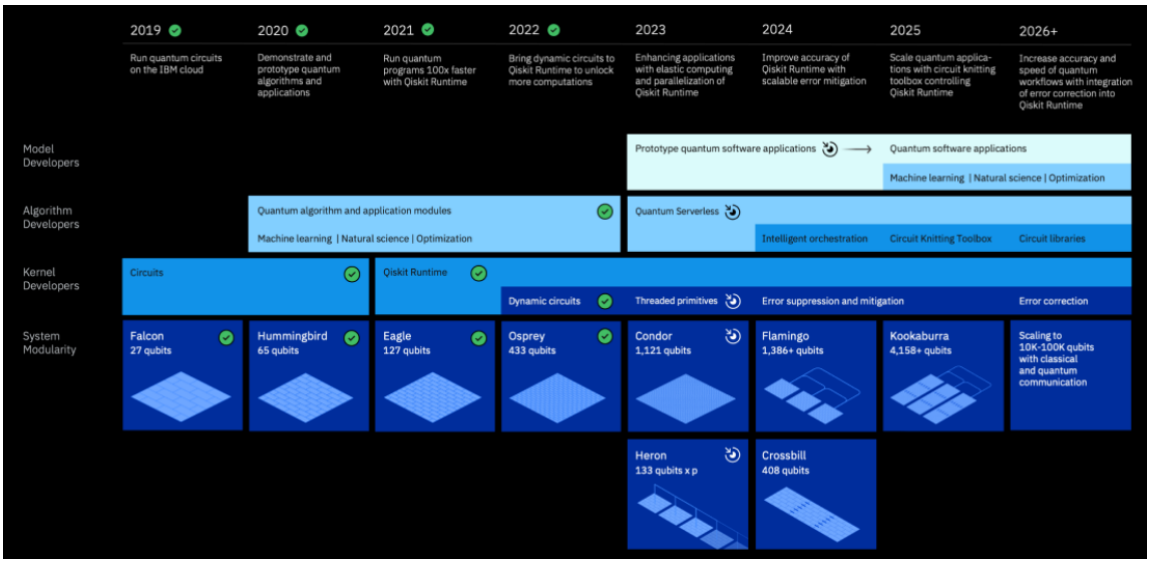

Abbildung 3. Rodmap der Firma IBM für ihren Quantencomputer [7]