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 Funktionieren 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 zentrale 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 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 wir die aktuellen Kryptographie Standards innerhalb der nächsten 5 Jahre austauschen werden.

Abbildungsverzeichnis

Abkürzungsverzeichnis

QC Quantencomputer

I. Einleitung

Das Thema der *Quanten Supremacy*, der Zeitpunkt zu dem ein Quantencomputer (QC) 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 QC zu besitzen, was jedoch in diversen Publikationen bezweifelt wurde **cho˙ordinary˙2022**. 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.

II. Shors-Algorithmus

Die Faktorisierung großer Zahlen [1, S189] 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 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 [2] 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 [3, S.]

III. CHATGPT

Titel: Quantensichere Verschlüsselungsalgorithmen

Abstract: Diese wissenschaftliche Ausarbeitung untersucht das Thema der quantensicheren Verschlüsselungsalgorithmen. Angesichts des bevorstehenden Zeitalters der Quantencomputer gewinnt die Entwicklung von Algorithmen, die immun gegen Shors Algorithmus sind, zunehmend an Bedeutung. Der Schwerpunkt liegt auf der Post-Quantum-Kryptografie sowie neuen, sicheren Algorithmen wie der Lattice-Kryptografie. Die Ausarbeitung gibt einen Überblick über die Herausforderungen, die mit der Quantencomputertechnologie verbunden sind, und erläutert, wie die genannten Algorithmen eine vielversprechende Lösung bieten.

Einleitung Die Quantencomputertechnologie hat das Potenzial, herkömmliche asymmetrische Kryptosysteme, die auf der Faktorisierung großer Zahlen basieren, zu brechen. Shors Algorithmus, ein quantenbasiertes Algorithmus zur Faktorisierung, könnte herkömmliche Verschlüsselungsalgorithmen wie RSA und elliptische Kurvenkryptografie unsicher machen. Um zukünftige Sicherheitsrisiken zu bewältigen, müssen neue Ansätze entwickelt werden.

Quantencomputer und Shors Algorithmus 2.1 Grundlagen der Quantencomputer 2.2 Shors Algorithmus 2.3 Herausforderungen für die herkömmliche Kryptografie

Post-Quantum-Kryptografie 3.1 Grundprinzipien der Post-Quantum-Kryptografie 3.2 Schlüsselaustauschverfahren 3.3 Signaturverfahren 3.4 Kryptosysteme basierend auf Gittern 3.5 Kryptosysteme basierend auf Codes 3.6 Kryptosysteme basierend auf Gittern im R-LWE-Problem 3.7 Vergleich der post-quantum Kryptosysteme

Lattice-Kryptografie 4.1 Einführung in die Lattice-Kryptografie 4.2 Lattice-basierte Verschlüsselung 4.3 Lattice-basierte Signaturverfahren 4.4 Lattice-basierte Schlüsselaustauschverfahren 4.5 Vorteile und Herausforderungen der Lattice-Kryptografie

Fallstudie: NIST Post-Quantum Cryptography Standardization 5.1 Auswahlprozess 5.2 Ausgewählte Kandidatenalgorithmen 5.3 Kategorien von Kryptosystemen 5.4 Evaluationskriterien 5.5 Aktueller Stand der Standardisierung

Fazit Die Entwicklung quantensicherer Verschlüsselungsalgorithmen ist von entscheidender Bedeutung, um den zukünftigen Bedrohungen durch Quantencomputer standzuhalten. Post-Quantum-Kryptografie und Lattice-Kryptografie sind viel-

versprechende Ansätze, um die Sicherheit unserer Kommunikation auch im Zeitalter der Quantencomputer zu gewährleisten. Es ist wichtig, dass Forschung und Standardisierung in diesem Bereich fortgesetzt werden, um sichere und effiziente Lösungen zu gewährleisten.

IV. 2.1 Grundlagen der Quantencomputer

Quantencomputer stellen eine neue Art von Computern dar, die auf den Prinzipien der Quantenmechanik basieren. Im Gegensatz zu klassischen Computern, die Bits verwenden, die entweder den Zustand 0 oder 1 repräsentieren können, nutzen Quantencomputer sogenannte Qubits. Qubits können jedoch Superpositionen von Zuständen haben, was bedeutet, dass sie gleichzeitig in verschiedenen Zuständen existieren können. Dies ermöglicht es Quantencomputern, Informationen auf eine Weise zu verarbeiten, die klassischen Computern nicht möglich ist. Die Superposition ermöglicht es Qubits, mehrere mögliche Zustände gleichzeitig darzustellen. Wenn ein Qubit in einen bestimmten Zustand gemessen wird, kollabiert die Superposition, und das Qubit nimmt einen bestimmten Zustand an. Die Wahrscheinlichkeit, dass das Qubit in einem bestimmten Zustand gemessen wird, wird durch die Amplituden der Superposition bestimmt. Ein weiteres Schlüsselkonzept in der Quantenmechanik ist die Verschränkung. Verschränkte Qubits können in einer Weise miteinander verbunden sein, dass der Zustand eines Qubits von dem Zustand anderer Qubits abhängt, unabhängig von der Entfernung zwischen ihnen. Diese Verschränkung ermöglicht es Quantencomputern, parallel arbeiten zu können und komplexe Berechnungen effizient durchzuführen [1].

V. 2.2 Shors Algorithmus

Shors Algorithmus, entwickelt von Peter Shor im Jahr 1994, ist ein wegweisender quantenbasierter Algorithmus, der das Potenzial hat, die Faktorisierung großer Zahlen in Polynomialzeit zu lösen. Die Faktorisierung ist ein mathematisches Problem, das für klassische Computer sehr zeitaufwendig ist und exponentiell mit der Größe der zu faktorisierenden Zahl wächst. Shors Algorithmus hingegen kann dieses Problem effizient auf einem Quantencomputer lösen. Der Algorithmus basiert auf zwei Hauptteilen: der Quantenphasenschätzung und der Quantenfouriertransformation. Die Quantenphasenschätzung wird verwendet, um periodische Eigenschaften einer Funktion zu bestimmen, während die Quantenfouriertransformation diese Informationen in die Faktorisierung der Zahl umwandelt. Durch die Ausnutzung der Superposition und Verschränkung von Qubits kann Shors Algorithmus effizient die Faktorisierung durchführen und somit das RSA-Verschlüsselungsverfahren und andere kryptografische Verfahren angreifen, die auf der Schwierigkeit der Faktorisierung basieren [3]. Der Algorithmus verwendet Quantenoperationen, um die periodische Funktion zu analysieren und die Primfaktoren der Zahl zu bestimmen. Shors Algorithmus ist in der Lage, große Zahlen in polynomieller Zeit zu faktorisieren, was für klassische Computer praktisch unmöglich ist. Dies macht ihn zu einer ernsthaften Bedrohung für die Sicherheit vieler herkömmlicher Verschlüsselungsalgorithmen, da die Faktorisierung ein zentraler Bestandteil ihrer Sicherheit ist [4].
Die Leistungsfähigkeit von Shors Algorithmus liegt in der Ausnutzung der einzigartigen Eigenschaften von Quantencomputern, insbesondere der Superposition und Verschränkung von Qubits. Dadurch kann der Algorithmus exponentiell schneller arbeiten als klassische Algorithmen. Während ein klassischer Algorithmus für die Faktorisierung einer N-Bit-Zahl eine Laufzeit von

$$O(2^N/2)$$

hat, kann Shors Algorithmus dies in Polynomialzeit mit einer Laufzeit von

$$O((N^3)(logN)(loglogN))$$

erreichen [5].
Es ist wichtig anzumerken, dass die Effizienz von Shors Algorithmus stark von der Verfügbarkeit leistungsfähiger Quantencomputer abhängt. Aktuelle Quantencomputer sind noch nicht in der Lage, die erforderliche Anzahl von Qubits und die notwendige Kohärenz aufrechtzuerhalten, um die Faktorisierung großer Zahlen durchzuführen. Jedoch sind

Fortschritte in der Quantentechnologie zu beobachten, und es wird erwartet, dass in Zukunft Quantencomputer mit ausreichender Leistung verfügbar sein werden, um Shors Algorithmus erfolgreich anzuwenden.

VI. 2.3 Herausforderungen für die herkömmliche Kryptografie

Die Entwicklung von Quantencomputern stellt eine ernsthafte Herausforderung für die herkömmliche asymmetrische Kryptografie dar. Viele der heute verwendeten Kryptosysteme basieren auf mathematischen Problemen, die für klassische Computer schwer zu lösen sind, wie die Faktorisierung großer Zahlen oder das diskrete Logarithmusproblem. Shors Algorithmus bietet jedoch einen effizienten Weg, um diese Probleme auf Quantencomputern zu lösen. Sobald ausreichend leistungsfähige Quantencomputer verfügbar sind, könnten diese herkömmlichen Verschlüsselungsalgorithmen in kurzer Zeit gebrochen werden, was erhebliche Auswirkungen auf die Sicherheit von Kommunikationssystemen und sensiblen Daten hätte. Daher ist es von entscheidender Bedeutung, quantensichere Verschlüsselungsalgorithmen zu entwickeln, die gegen Angriffe durch Quantencomputer beständig sind. Ein vielversprechender Ansatz für die Quantenkryptografie ist die Lattice-Kryptografie. Diese basiert auf Gitterproblemen und bietet eine mathematische Grundlage für die Entwicklung quantensicherer Verschlüsselungsalgorithmen. Lattice-Kryptografie hat das Potenzial, Sicherheit gegenüber Angriffen durch Quantencomputer zu bieten, da die zugrunde liegenden Probleme schwer zu lösen sind, selbst für Quantencomputer [6].

VII. 4 Lattice-Kryptographie

Lattice-Kryptographie ist ein Bereich der post-quanten Kryptographie, der auf mathematischen Strukturen namens Gittern basiert. Diese Form der Kryptographie zielt darauf ab, Sicherheit gegen Angriffe durch Quantencomputer zu bieten, indem sie auf Probleme abzielt, die auch für Quantencomputer schwierig zu lösen sind.

VIII. 4.1 Grundlagen der Lattice-Kryptographie

In der Lattice-Kryptographie werden Verschlüsselungssysteme auf der Grundlage mathematischer Gitterstrukturen entwickelt. Ein Gitter ist eine diskrete, periodische Anordnung von Punkten im Raum. In der Kryptographie werden meistens Gitter in mehrdimensionalen Vektorräumen verwendet.
Ein grundlegendes Problem in der Lattice-Kryptographie ist das Shortest Vector Problem (SVP), bei dem man den kürzesten Vektor in einem Gitter finden muss. Ein weiteres Problem ist das Learning With Errors (LWE), bei dem man die Lösung eines linearen Gleichungssystems mit fehlerbehafteten Variablen in einem Gitter finden muss.
Die Sicherheit von Lattice-Kryptographie basiert auf der Annahme, dass das Finden des kürzesten Vektors in einem Gitter oder das Lösen von linearen Gleichungssystemen mit fehlerbehafteten Variablen in einem Gitter schwierig ist. Diese Annahme wurde umfassend untersucht und es wurden verschiedene Varianten und Verbesserungen von Lattice-Kryptographie entwickelt.[7]

IX. 4.2 Lattice-basierte Verschlüsselungsalgorithmen

Lattice-Kryptographie bietet verschiedene Arten von Verschlüsselungsalgorithmen, die als post-quanten sicher gelten. Einer der bekanntesten Algorithmen ist der NTRU (Nth degree truncated polynomial ring) Algorithmus, der auf Polynomringen basiert und für Public-Key-Verschlüsselung und digitale Signaturen eingesetzt wird.
Der NTRU-Algorithmus zeichnet sich durch seine Effizienz und seine starke Sicherheit aus. Er basiert auf der Schwierigkeit, den kürzesten Vektor in einem Gitter zu finden. Die Sicherheit des NTRU-Algorithmus hängt von der Wahl geeigneter Parameter ab, um sicherzustellen, dass das SVP schwierig zu lösen ist.
Ein weiterer wichtiger Algorithmus ist der Learning With Errors (LWE)-basierte Verschlüsselungsalgorithmus. Dieser Algorithmus

nutzt die Schwierigkeit, Lösungen für lineare Gleichungssysteme mit fehlerbehafteten Variablen in Gittern zu finden, um sichere Verschlüsselung zu ermöglichen. LWE-basierte Verschlüsselungsalgorithmen haben gezeigt, dass sie widerstandsfähig gegen Angriffe durch Quantencomputer sind.[8]

X. 4.3 Sicherheit von Lattice-Kryptographie

Die Sicherheit von Lattice-Kryptographie beruht auf der Schwierigkeit mathematischer Probleme in Gittern. Quantencomputer haben Schwierigkeiten, bestimmte Gitterprobleme effizient zu lösen, was bedeutet, dass Lattice-Kryptographie gegen Angriffe von Quantencomputern resistent sein kann.
Es wurden verschiedene Sicherheitsparameter und -annahmen für Lattice-Kryptographie entwickelt, um die Sicherheit der verwendeten Algorithmen zu gewährleisten. Die Wahl der richtigen Parameter und die Überprüfung der Sicherheitsannahmen sind entscheidend, um eine ausreichende Sicherheit in Lattice-Kryptographie-Verfahren zu gewährleisten.[9]

XI. 4.4 Implementierung und Anwendung von Lattice-Kryptographie

Lattice-Kryptographie findet Anwendung in verschiedenen Bereichen, wie zum Beispiel in der sicheren Datenübertragung, der Authentifizierung, der Schlüsselaustauschprotokolle und der digitalen Signaturen. Die Implementierung von Lattice-Kryptographie erfordert spezielle mathematische Algorithmen und sorgfältige Parameterwahl, um Sicherheit und Effizienz zu gewährleisten.
Es gibt bereits einige Implementierungen von Lattice-Kryptographie in der Praxis. Zum Beispiel hat das NIST (National Institute of Standards and Technology) einen Wettbewerb für post-quanten Kryptographie veranstaltet, bei dem auch lattice-basierte Verfahren untersucht wurden. Dies zeigt, dass Lattice-Kryptographie bereits eine praktische Relevanz hat und als vielversprechende Lösung für die Sicherheit in einer post-quanten Welt betrachtet wird.[4][5]

Literaturverzeichnis

[1] D. J. Bernstein und T. Lange, „Post-quantum cryptography,“ *Nature*, Jg. 549, Nr. 7671, S. 188–194, Sep. 2017, ISSN: 1476-4687. DOI: 10 . 1038 / nature23461. (besucht am 16. 04. 2023).

[2] P. Shor, „Algorithms for Quantum Computation: Discrete Logarithms and Factoring,“ in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, Nov. 1994, S. 124–134. DOI: 10.1109/SFCS.1994.365700.

[3] C. Gidney und M. Ekerå, „How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits,“ *Quantum*, Jg. 5, S. 433, Apr. 2021, ISSN: 2521-327X. DOI: 10.22331/q-2021-04-15-433. arXiv: 1905.09749 [quant-ph]. (besucht am 16. 04. 2023).