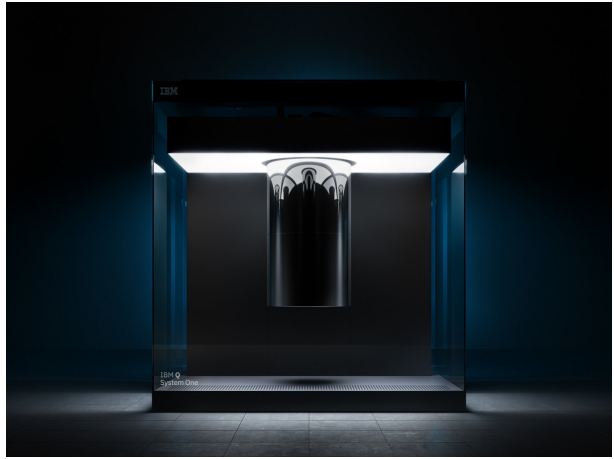
Digitale Souveränität trotz Quantencomputer

mit einem Überblick zur laufenden BMBF Förderlinie "Post-Quanten-Kryptografie"

Prof. Dr. Daniel Loebenberger, OMNISECURE 2020, Berlin, 21. Januar 2020

Motivation

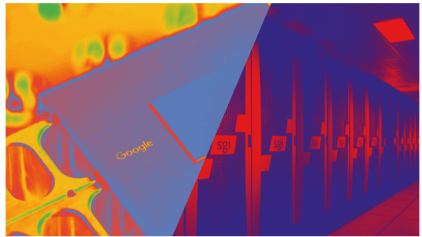


Motivation

Google: Überlegenheit von Quantencomputern bewiesen

Forscher von Google haben erstmals mit 53 Qubits gerechnet – ein gewaltiger Sprung hin zu praxistauglichen Quantenrechnern.

Lesezeit: 1 Min. In Pocket speichern 299



(Bild: Google / NASA)

24.09.2019 09:45 Uhr | Technology Review

Von Martin Giles, Arne Grävemeyer

Fraunhofer AISEC

Überblick

Quantencomputer und IT-Sicherheit

Gegenmaßnahmen

Technologische Herausforderungen

Zusammenfassung und Ausblick

Überblick

Quantencomputer und IT-Sicherheit

Gegenmaßnahmen

Technologische Herausforderungen

Zusammenfassung und Ausblick

Das Leben im Quantenzeitalter

- **Quantencomputing**
  - Quantenalgorithmen und -schaltkreise
  - Quantenvorteil
  - Quantenkryptanalyse
- **Quantenkryptographie**
  - Quantenschlüsselaustausch
  - Quantenteleportation
- **Post-Quanten Kryptographie**
  - Sichere Kryptographie im Post-Quanten Zeitalter
  - Klassische Algorithmen!

Bild: IBM

Quanten Traumata (I)

A fast quantum mechanical algorithm for database search

Lov K. Grover
3C-404A, Bell Labs
600 Mountain Avenue
Murray Hill NJ 07974
lkgrover@bell-labs.com

Summary

Imagine a phone directory containing N names arranged in completely random order. In order to find someone's phone number with a probability of $\frac{1}{2}$, any classical algorithm (whether deterministic or probabilistic) will need to look at a minimum of $\frac{N}{2}$ names. Quantum mechanical systems can be in a superposition of states and simultaneously examine multiple names. By properly adjusting the phases of various operations, successful computations reinforce each other while others interfere randomly. As a result, the desired phone number can be obtained in only $O(\sqrt{N})$ steps. The algorithm is within a small constant factor of the fastest possible quantum mechanical algorithm.

This paper applies quantum computing to a mundane problem in information processing and presents an algorithm that is significantly faster than any classical algorithm can be. The problem is this: there is an unsorted database containing N items out of which just one item satisfies a given condition - that one item has to be retrieved. Once an item is examined, it is possible to tell whether or not it satisfies the condition in one step. However, there does not exist any sorting on the database that would aid its selection. The most efficient classical algorithm for this is to examine the items in the database one by one. If an item satisfies the required condition stop; if it does not, keep track of this item so that it is not examined again. It is easily seen that this algorithm will need to look at an average of $\frac{N}{2}$ items before finding the desired item.

https://arxiv.org/abs/quant-ph/9605043

Fraunhofer AISEC

Quanten Traumata (II)

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

https://arxiv.org/abs/quant-ph/9508027

Angriffsflächen heute

Ein **N**icht-**s**pezifizierter **A**ngreifer (NSA) speichert Daten
und findet den Schlüssel später.

Bild: National Security Agency

Tempus Fugit

nach Michele Mosca, University of Waterloo

Ab wann müssen wir uns Sorgen machen?

- Wie lange benötigt man sichere Verschlüsselung? (***x*** Jahre)
- Wie lange dauert die Anpassung der Infrastruktur? (***y*** Jahre)
- Wie lange dauert es einen praktikablen Quantencomputer zu bauen? (***z*** Jahre)

Überblick

Quantencomputer und IT-Sicherheit

Gegenmaßnahmen

Technologische Herausforderungen

Zusammenfassung und Ausblick

Post-Quanten Kryptographie

Verschiedene Richtungen:

- Gitter-basierte Kryptographie
- Code-basierte Kryptographie
- Multivariate Systeme
- Hash-basierte Signaturen
- Weitere Technologien (e. g. Isogenie-basiert, . . .)

$\Rightarrow$ Wie kann man die Verfahren in praktische Anwendungen überführen?

Förderprogramm des BMBF

Selbstbestimmt und sicher in der digitalen Welt von 2015 bis 2020

- Teil der Hightech-Strategie der Bundesregierung
- Konkrete Ausschreibung: „Post-Quanten-Kryptografie“
- Aktuell sind sieben Projekte bewilligt
- Ggf. kommen noch (wenige) weitere hinzu

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Überblick laufender Projekte

(laut Webseite des BMBF, Zugriff am 17. Januar 2020)

- Aquorypt: Quantencomputerresistente Kryptografie in die Anwendung bringen
- FLOQI: Ein Schlüsselkasten für sichere Kommunikation im Internet der Dinge
- KBLS: Kryptobibliothek Botan: Langlebige Sicherheit für IT-Anwendungen und Dienste
- SIKRIN-KRYPTOV: Sicherung von hydraulischen Anlagen in kritischen Infrastrukturen
- PQC4MED: Daten in der medizinischen Versorgung für die PQ-Ära schützen
- QuaSiModO: Quantensichere virtuelle private Netzwerke
- QuantumRISC: Kryptografie der nächsten Generation für eingebettete Systeme

Überblick laufender Projekte

(laut Webseite des BMBF, Zugriff am 17. Januar 2020)

- Aquorypt: Quantencomputerresistente Kryptografie in die Anwendung bringen
- FLOQI: Ein Schlüsselkasten für sichere Kommunikation im Internet der Dinge
- KBLS: Kryptobibliothek Botan: Langlebige Sicherheit für IT-Anwendungen und Dienste
- SIKRIN-KRYPTOV: Sicherung von hydraulischen Anlagen in kritischen Infrastrukturen
- PQC4MED: Daten in der medizinischen Versorgung für die PQ-Ära schützen
- QuaSiModO: Quantensichere virtuelle private Netzwerke
- QuantumRISC: Kryptografie der nächsten Generation für eingebettete Systeme

Überblick

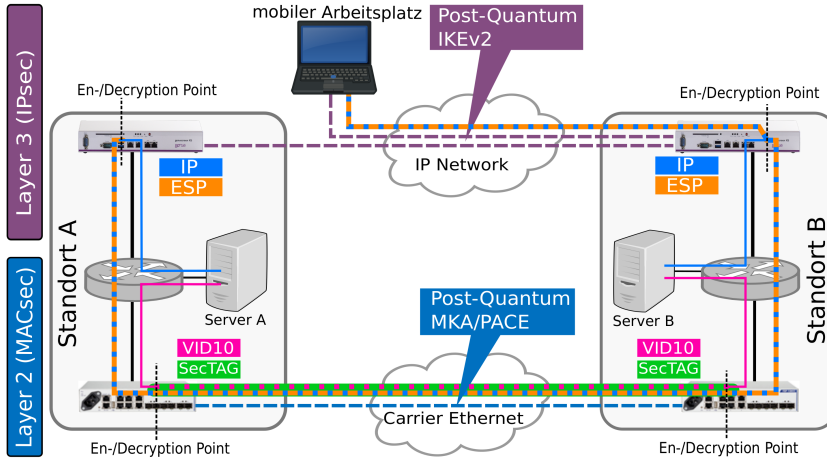
Quantencomputer und IT-Sicherheit

Gegenmaßnahmen

Technologische Herausforderungen

Zusammenfassung und Ausblick

Beispiel: Projekt QuaSiModO



Fraunhofer AISEC

Algorithmenwahl

- Laufendes Standardisierungverfahren der NIST
- Zahlreiche kryptographische Primitive
- Unterschiedliche technische Anforderungen
- Prozess nicht abgeschlossen, Ausgang ungewiss!
- (mehr dazu im nächsten Vortrag)

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Algorithmenwahl

- Laufendes Standardisierungverfahren der NIST
- Zahlreiche kryptographische Primitive
- Unterschiedliche technische Anforderungen
- Prozess nicht abgeschlossen, Ausgang ungewiss!
- (mehr dazu im nächsten Vortrag)

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Auswahl verschiedener Verfahren für prototypische Implementierungen!

Auswirkungen unterschiedlicher Anforderungen der PQ-Primitive

Beispiel: Classic McEliece

Definition (MTU)

Die Maximum Transmission Unit (MTU) beschreibt die maximale Paketgröße eines Protokolls der Vermittlungsschicht des OSI-Modells.

Auswirkungen unterschiedlicher Anforderungen der PQ-Primitive

Beispiel: Classic McEliece

Definition (MTU)

Die Maximum Transmission Unit (MTU) beschreibt die maximale Paketgröße eines Protokolls der Vermittlungsschicht des OSI-Modells.

Problem:

- IPv4: 68 Bytes (minimum MTU)
- IPv6: 1280 Bytes (minimum MTU)
- Classic McEliece public key: $\approx$ 1 MB

Auswirkungen unterschiedlicher Anforderungen der PQ-Primitive

Beispiel: Classic McEliece

Definition (MTU)

Die Maximum Transmission Unit (MTU) beschreibt die maximale Paketgröße eines Protokolls der Vermittlungsschicht des OSI-Modells.

Problem:

- IPv4: 68 Bytes (minimum MTU)
- IPv6: 1280 Bytes (minimum MTU)
- Classic McEliece public key: $\approx$ 1 MB

$\Rightarrow$ Anpassung der Netzprotokolle ggf. ebenfalls nötig!

Überblick

Quantencomputer und IT-Sicherheit

Gegenmaßnahmen

Technologische Herausforderungen

Zusammenfassung und Ausblick

Zusammenfassung

- Quantencomputer stellen eine disruptive Technologie dar
- Wesentliche Auswirkungen auf die Kryptographie zu erwarten
- Dadurch entsprechende Implikationen für IT-Sicherheit im allgemeinen
- Post-Quanten Kryptographie widersteht Quantencomputern
- Erfahrungen aus der praktischen Anwendung nötig
- Daher gibt es verschiedene laufende bzw. anlaufende Projekte

„We live in exciting times! The best, however, is yet to come.“
(Anthony Annunziata, IBM Research, Oktober 2019)

Kontaktinformation

Prof. Dr. Daniel Loebenberger

Fraunhofer Institut für
Angewandte und Integrierte Sicherheit AISEC
Standort Weiden

Adresse: Hermann-Brenner-Platz 1
92637 Weiden i.d.Opf.
Internet: http://www.aisec.fraunhofer.de

E-Mail: daniel.loebenberger@aisec.fraunhofer.de