Quantencomputer – der Angriff aus der Zukunft auf unsere Daten von heute

Tanja Lange

Eindhoven University of Technology

OOP 2020

Kryptographie

Kryptographie

Absender
“Alice”

abgehörtes Netz
“Eve”

Empfänger
“Bob”

Kryptographie

Absender
“Alice”

abgehörtes Netz
“Eve”

Empfänger
“Bob”

Kryptographie

Absender
“Alice”

abgehörtes Netz
“Eve”

Empfänger
“Bob”

- Wortwörtliche Bedeutung: geheimes Schreiben.
- Funktion #1: **Vertraulichkeit** trotz Eves Spionage.
- Funktion #2: **Integrität**, z.B. Eves Sabotage erkennen.

Kryptographie

Absender
“Alice”

abgehörtes Netz
“Eve”

Empfänger
“Bob”

- Kreditkarten, EC-Karten, TANs, PINs
- ePässe, Perso mit Chip
- Online Einkäufe, Webseiten mit https

- Facebook, Gmail, WhatsApp, iMessage
- Festplattenverschlüsselung (iPhone, Bitlocker; siehe auch Apple vs. FBI)

Kryptographie

Absender
“Alice”

abgehörtes Netz
“Eve”

Empfänger
“Bob”

- Kreditkarten, EC-Karten, TANs, PINs
- ePässe, Perso mit Chip
- Online Einkäufe, Webseiten mit https
- Verschlüsselte Emails (PGP)
- Signal, Torbrowser

- Facebook, Gmail, WhatsApp, iMessage
- Festplattenverschlüsselung (iPhone, Bitlocker; siehe auch Apple vs. FBI)
- Tails, Qubes OS
- Extra Schritte um Privatsphäre und Sicherheit zu schützen

Kryptographische Software

Kryptographische Software

. . . und kann man der Hardware vertrauen?

Algorithms for Quantum Computation: Discrete Logarithms and Factoring

Peter W. Shor
AT&T Bell Labs
Room 2D-149
600 Mountain Ave.
Murray Hill, NJ 07974, USA

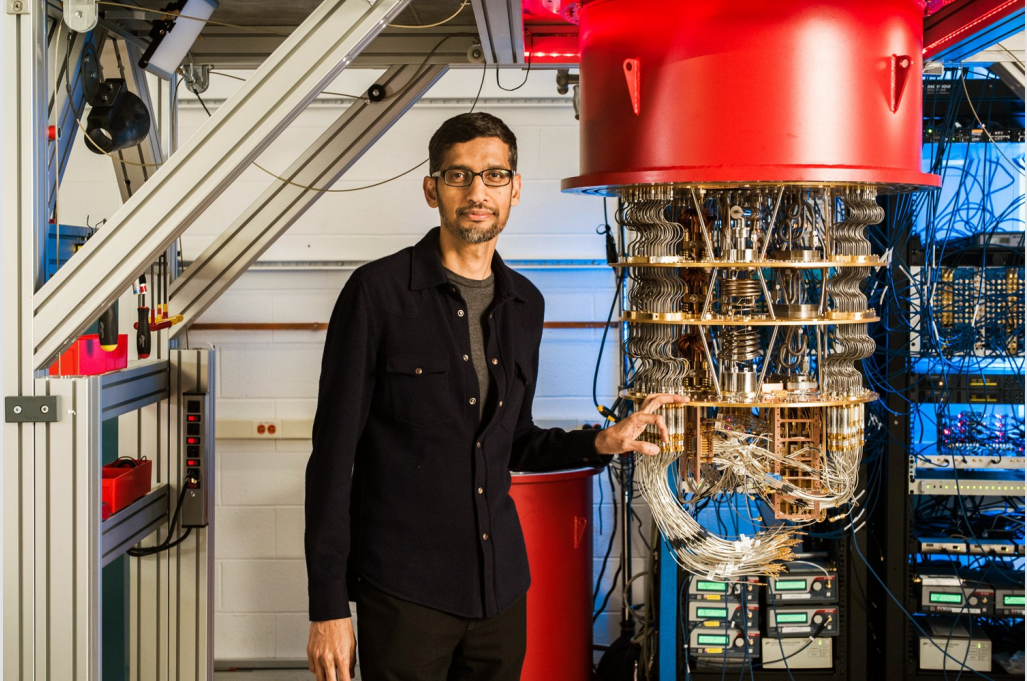
Abstract

A computer is generally considered to be a universal computational device; i.e., it is believed able to simulate any physical computational device with a cost in computation time of at most a polynomial factor. It is not clear whether this is still true when quantum mechanics is taken into consideration. Several researchers, starting with David Deutsch, have developed models for quantum

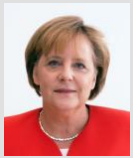
[1, 2]. Although he did not ask whether quantum mechanics conferred extra power to computation, he did show that a Turing machine could be simulated by the reversible unitary evolution of a quantum process, which is a necessary prerequisite for quantum computation. Deutsch [9, 10] was the first to give an explicit model of quantum computation. He defined both quantum Turing machines and quantum circuits and investigated some of their properties.

The next part of this paper discusses how quantum com-


IBM Q



Weit verbreitete Systeme



Absender
“Alice”

abgehörtes Netz
“Eve”

Empfänger
“Bob”

Kryptographie mit symmetrischen Schlüsseln
AES-128. **AES-192**. **AES-256**. **AES-GCM**. **ChaCha20**. **HMAC-SHA-256**. **Poly1305**. **SHA-2**. **SHA-3**. **Salsa20**.
Kryptographie mit öffentlichen Schlüsseln
BN-254. **Curve25519**. **DH**. **DSA**. **ECDH**. **ECDSA**. **EdDSA**. **NIST P-256**. **NIST P-384**. **NIST P-521**. **RSA encrypt**. **RSA sign**. **secp256k1**.

Weit verbreitete Systeme

Absender
“Alice”

abgehörtes Netz
“Eve” mit Quantencomputer

Empfänger
“Bob”

Kryptographie mit symmetrischen Schlüsseln

AES-128. **AES-192**. **AES-256**. **AES-GCM**. **ChaCha20**. **HMAC-SHA-256**. **Poly1305**. **SHA-2**. **SHA-3**. **Salsa20**.

Kryptographie mit öffentlichen Schlüsseln

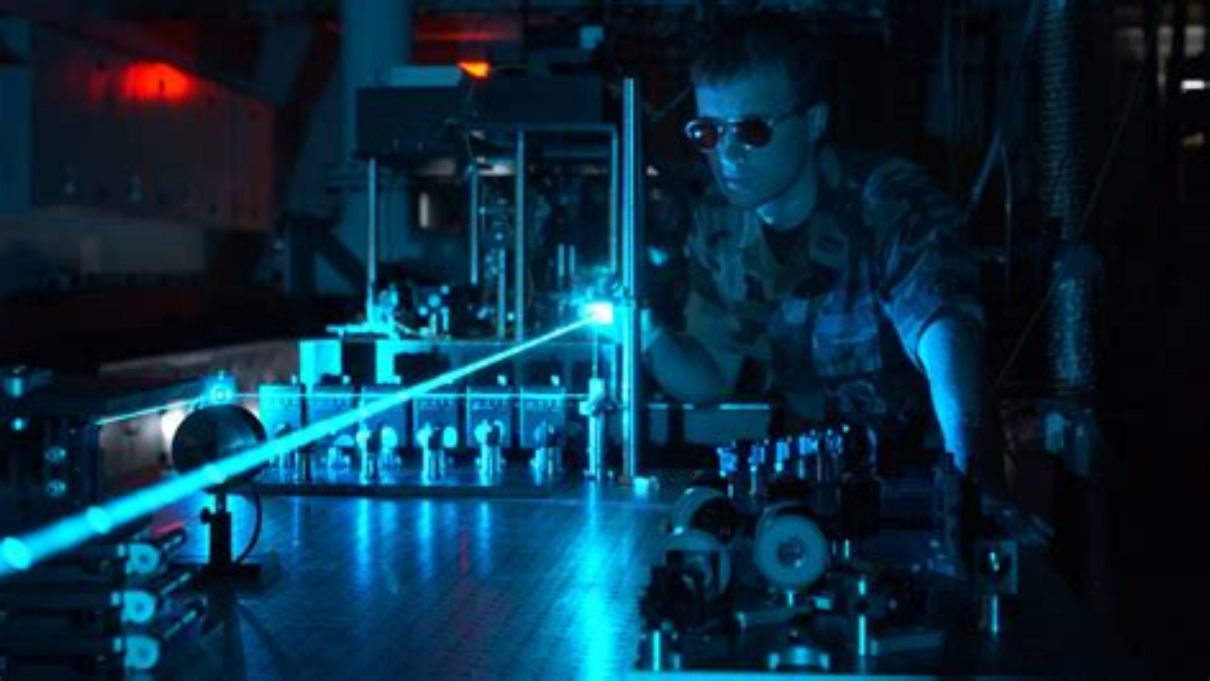
BN-254. **Curve25519**. **DH**. **DSA**. **ECDH**. **ECDSA**. **EdDSA**. **NIST P-256**. **NIST P-384**. **NIST P-521**. **RSA encrypt**. **RSA sign**. **secp256k1**.

Post-Quanten Kryptographie

Post-Quanten Kryptographie

Kryptographie mit Angriffs-Modell Quantencomputer

Zurück in die Steinzeit?



Post-Quanten Kryptographie

Algorithmische Kryptographie

mit Angriffs-Modell

Quantencomputer

Was bleibt?

- Systeme basierend auf Codierungstheorie
- Signaturen basierend auf Hash-Funktionen
- Systeme basierend auf Isogenien zwischen elliptischen Kurven
- Systeme basierend auf Gittern
- Systeme basierend auf multi-variaten Gleichungen
- Symmetrische Kryptographie

Dies sind grobe Kategorien, konkrete Systeme können trotzdem vollständig unsicher sein!

Was bleibt?

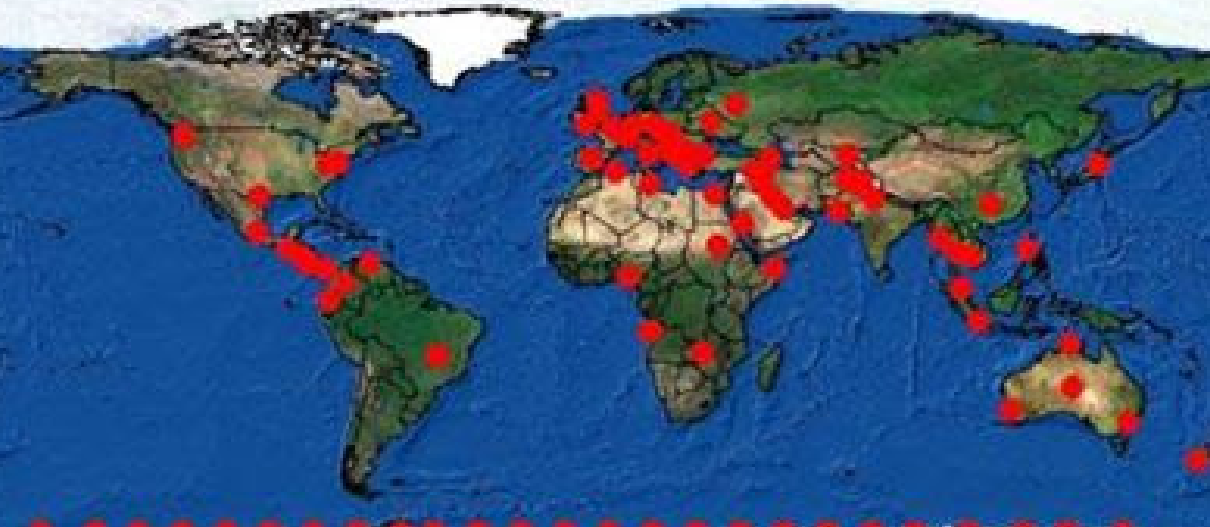
- Systeme basierend auf Codierungstheorie
- Signaturen basierend auf Hash-Funktionen
- Systeme basierend auf Isogenien zwischen elliptischen Kurven
- Systeme basierend auf Gittern
- Systeme basierend auf multi-variaten Gleichungen
- Symmetrische Kryptographie

Dies sind grobe Kategorien, konkrete Systeme können trotzdem vollständig unsicher sein!
NIST (National Institute of Standards and Technology) hält einen Wettbewerb zu Standards in Post-Quanten Kryptographie.

Warum jetzt?

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Where is X-KEYSCORE?



Es eilt für Langzeitsicherheit!

- Heute fangen Angreifer alle Nachrichten ab und speichern sie. Viele Jahre später können sie diese mit einem Quantumcomputer entschlüsseln.
  Dies bringt Menschenrechtler, Journalisten, Patientendossiers (ärztliche Schweigepflicht), nationale Sicherheit, Rechtsakten, . . . in Gefahr.

- Signatursysteme können später ersetzt werden, wenn es einen großen Quantencomputer gibt – aber das wird sicher geheim gehalten

Es eilt für Langzeitsicherheit!

- Heute fangen Angreifer alle Nachrichten ab und speichern sie. Viele Jahre später können sie diese mit einem Quantumcomputer entschlüsseln.
  Dies bringt Menschenrechtler, Journalisten, Patientendossiers (ärztliche Schweigepflicht), nationale Sicherheit, Rechtsakten, . . . in Gefahr.

- Signatursysteme können später ersetzt werden, wenn es einen großen Quantencomputer gibt – aber das wird sicher geheim gehalten . . . und eine der Hauptfunktionen von Signaturen sind Updates für Betriebssysteme.
- Wir müssen also *jetzt schon* Upgrades mit Post-Quanten Signaturen sichern.

Bericht der National Academy of Sciences (US)

Don't panic. "Key Finding 1: Given the current state of quantum computing and recent rates of progress, it is highly unexpected that a quantum computer that can compromise RSA 2048 or comparable discrete logarithm-based public key cryptosystems will be built within the next decade."

Bericht der National Academy of Sciences (US)

Don't panic. "Key Finding 1: Given the current state of quantum computing and recent rates of progress, it is highly unexpected that a quantum computer that can compromise RSA 2048 or comparable discrete logarithm-based public key cryptosystems will be built within the next decade."

Panic. "Key Finding 10: Even if a quantum computer that can decrypt current cryptographic ciphers is more than a decade off, the hazard of such a machine is high enough—and the time frame for transitioning to a new security protocol is sufficiently long and uncertain—that prioritization of the development, standardization, and deployment of post-quantum cryptography is critical for minimizing the chance of a potential security and privacy disaster."

Initial recommendations of long-term secure post-quantum systems

Daniel Augot, Lejla Batina, Daniel J. Bernstein, Joppe Bos,
Johannes Buchmann, Wouter Castryck, Orr Dunkelman,
Tim Güneysu, Shay Gueron, Andreas Hülsing,
Tanja Lange, Mohamed Saied Emam Mohamed,
Christian Rechberger, Peter Schwabe, Nicolas Sendrier,
Frederik Vercauteren, Bo-Yin Yang

Erste Empfehlungen von PQCRYPTO

- **Symmetrische Verschlüsselung** Grover erfordert 256-Bit Schlüssel:
  - AES-256
  - Salsa20 mit 256-Bit Schlüssel

  Forschung: Serpent-256, ...
- **Symmetrische Authentisierung** Informationstheoretische MACs (weder Shor noch Grover finden Anwendung):
  - GCM mit 96-Bit nonce und 128-Bit Ausgabe
  - Poly1305
- **Public-key Verschlüsselung** McEliece mit binären Goppa Codes:
  - Länge $n = 6960$, Dimension $k = 5413$, $t = 119$ Fehler

  Forschung: QC-MDPC, Stehlé-Steinfeld NTRU, ...
- **Public-key Signaturen** Hash-basiert (minimale Annahmen):
  - XMSS mit Parametern aus dem CFRG Draft
  - SPHINCS-256

  Forschung: HFEv-, ...

Mehr Information

- https://pqcrypto.org: Übersichtsseite von Daniel J. Bernstein & mir.
- PQCrypto 2016, PQCrypto 2017, PQCrypto 2018 mit Folien der Vorträge.
- https://pqcrypto.eu.org: PQCRYPTO EU Projekt.
  - Unsere Empfehlungen.
  - Freie Software-Bibliotheken (libpqcrypto, pqm4, pqhw).
  - Etliche Berichte, wissenschaftliche Artikel, (Übersichts-)Vorträge.
- https://2017.pqcrypto.org/school: PQCRYPTO Sommer-Schule mit 21 Vorlesungen auf Video, mit Folien und Übungsaufgaben.
- https://2017.pqcrypto.org/exec und https://pqcschool.org/index.html: Executive school (weniger Mathe, mehr Überblick.)
- https://csrc.nist.gov/Projects/post-quantum-cryptography/Post-Quantum-Cryptography-Standardization: NIST PQC Wettbewerb.
- Quantum Threat Timeline vom Global Risk Institute.

Bonus Folien

NIST Einreichung SPHINCS+

- Signatur basierend auf Hash-Funktionen.
- Benötigt nur eine sichere Hashfunktion, keine weiteren Annahmen.
- Basiert auf Ideen von Lamport (1979) und Merkle (1979).
- Weiterentwicklung von SPHINCS mit
  - verbesserter Mehrfach-Signatur,
  - kleineren Schlüsseln,
  - Möglichkeit für kleinere Signaturen (30kB statt 41kB) wenn "nur" 2^{50} gebraucht werden.
- Drei Versionen (verschiedene Hash-Funkionen)
  - SPHINCS+-SHA3 (mit SHAKE256),
  - SPHINCS+-SHA2 (mit SHA-256),
  - SPHINCS+-Haraka (mit Haraka, einer Hash-Funktion für kurze Eingaben).

Mehr Info unter https://sphincs.org/.

NIST Einreichung Classic McEliece

- Asymptotische Sicherheit unverändert trotz 40 Jahren Kryptanalyse.
- Kurze Verschlüsselungen / geringe Bandbreite.
- Einfache und effiziente Umwandlung von OW-CPA PKE zu IND-CCA2 KEM.
- Freie Software und FPGA Implementierungen.
- Keine Patente.

Metric	**mceliece6960119**	**mceliece8192128**
Public-key size	1047319 bytes	1357824 bytes
Secret-key size	13908 bytes	14080 bytes
Ciphertext size	226 bytes	240 bytes
Key-generation time	813812960 cycles	898881136 cycles
Encapsulation time	156624 cycles	172576 cycles
Decapsulation time	298472 cycles	316888 cycles

Mehr Info unter https://classic.mceliece.org.

NIST Einreichung NTRUPrime

- Gitter-basiertes Verschlüsselungssystem – deutlich kleinere Schlüssel.
- NTRUPrime gibt weniger Struktur an den Angreiffer:
  - Alle Rechnungen passieren modulo einer Primzahl statt einer Zweierpotenz.
  - Ringe benutzen $x^p - x - 1$, mit p prim, statt $x^n - 1$ oder $x^n + 1$.
  - Keine (nichttrivialen) Unterringe oder körper.
- Keine Fehler in der Entschlüsselung.

Metric	**Streamlined NTRU Prime** 4591^{761}	**NTRU LPRime** 4591^{761}
Public-key size	1158 bytes	1039 bytes
Secret-key size	1763 bytes	1294 bytes
Ciphertext size	1039 bytes	1167 bytes
Key-generation time	951684 cycles	45912 cycles
Encapsulation time	52996 cycles	75076 cycles
Decapsulation time	68996 cycles	91952 cycles

Mehr Info unter https://ntruprime.cr.yp.to/.