Post-Quanten-Kryptographie für Langzeitsicherheit

Tanja Lange

Technische Universiteit Eindhoven

8. Handelsblatt Jahrestagung Cybersecurity

Kryptographie

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-

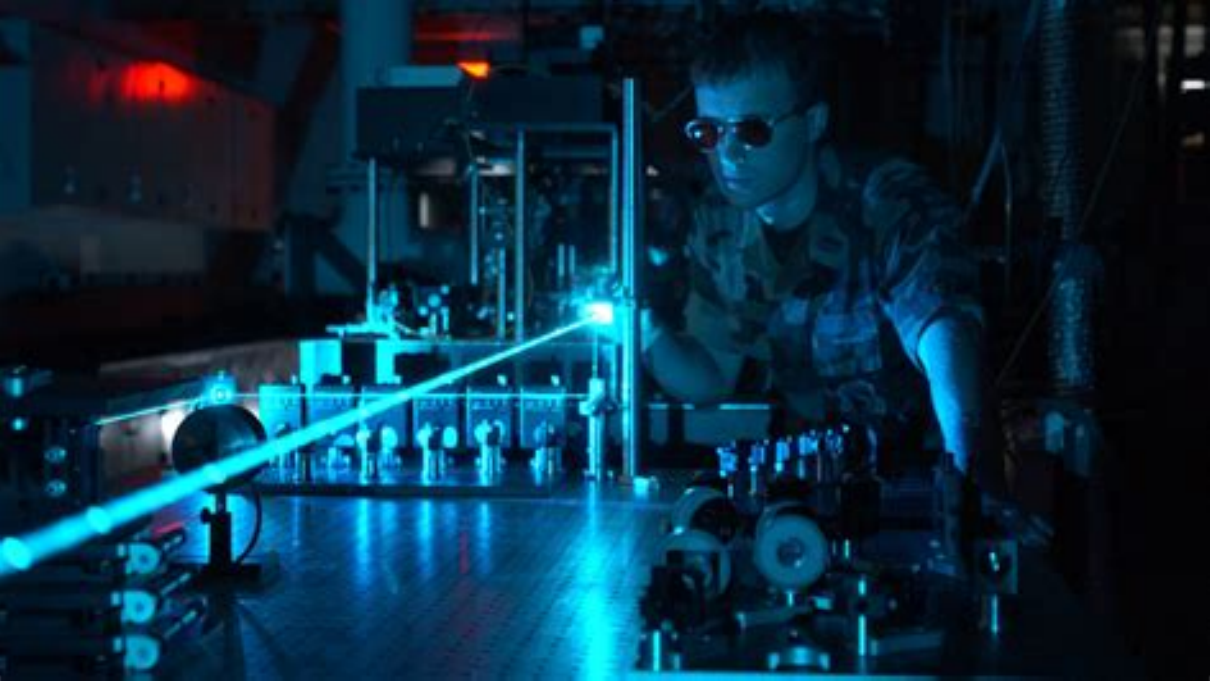

IBM Q

Post-Quanten Kryptographie

Post-Quanten Kryptographie

Kryptographie mit Angriffs-Modell Quantencomputer

Zurück in die Steinzeit?



Post-Quanten Kryptographie

Algorithmische Kryptographie

mit Angriffs-Modell

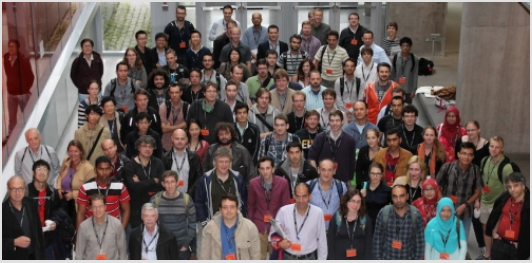
Quantencomputer

Wer arbeitet an Post-Quanten Kryptographie?

- PQCrypto 2006: International Workshop on Post-Quantum Cryptography.

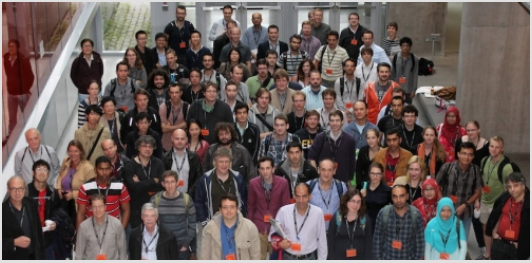
Wer arbeitet an Post-Quanten Kryptographie?

- PQCrypto 2006: International Workshop on Post-Quantum Cryptography.
- PQCrypto 2008.
- PQCrypto 2010.
- PQCrypto 2011.
- PQCrypto 2013.
- PQCrypto 2014.



Wer arbeitet an Post-Quanten Kryptographie?

- PQCrypto 2006: International Workshop on Post-Quantum Cryptography.
- PQCrypto 2008.
- PQCrypto 2010.
- PQCrypto 2011.
- PQCrypto 2013.
- PQCrypto 2014.
- EU Projekt, 2015–2018: PQCRYPTO, Post-Quantum Cryptography for Long-term Security.



NSA Ankündigungen

August 11, 2015

> *IAD recognizes that there will be a move, in the not distant future, to a quantum resistant algorithm suite.*

NSA Ankündigungen

August 11, 2015

IAD recognizes that there will be a move, in the not distant future, to a quantum resistant algorithm suite.

August 19, 2015

IAD will initiate a transition to quantum resistant algorithms in the not too distant future.

Post-Quantum wird Mainstream

- PQCrypto 2016: 22.–26. Feb in Fukuoka, Japan, mit über 240 Teilnehmern

- NIST kündigt einen Wettbewerb für neue Post-Quanten Standards an.


PQCrypto 2018
The Ninth International Conference on Post-Quantum Cryptography
Fort Lauderdale, Florida, April 9-11, 2018

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 Post-Quanten "Wettbewerb"

30. November 2017: NIST bekommt 82 Einreichungen.

	Signatures	KEM/Encryption	Overall
Lattice-based	4	24	28
Code-based	5	19	24
Multi-variate	7	6	13
Hash-based	4		4
Other	3	10	13
Total	**23**	**59**	**82**

“Complete and proper” Einreichungen

21. Dezember 2017: NIST veröffentlicht 69 Einreichungen von 260 Forschern.

BIG QUAKE. **BIKE**. **CFPKM**. **Classic McEliece**. **Compact LWE**. **CRYSTALS-DILITHIUM**. **CRYSTALS-KYBER**. **DAGS**. **Ding Key Exchange**. **DME**. **DRS**. **DualModeMS**. **Edon-K**. **EMBLEM and R.EMBLEM**. **FALCON**. **FrodoKEM**. **GeMSS**. **Giophantus**. **Gravity-SPHINCS**. **Guess Again**. **Gui**. **HILA5**. **HiMQ-3**. **HK17**. **HQC**. **KINDI**. **LAC**. **LAKE**. **LEDAkem**. **LEDApkc**. **Lepton**. **LIMA**. **Lizard**. **LOCKER**. **LOTUS**. **LUOV**. **McNie**. **Mersenne-756839**. **MQDSS**. **NewHope**. **NTRUEncrypt**. **NTRU-HRSS-KEM**. **NTRU Prime**. **NTS-KEM**. **Odd Manhattan**. **OKCN/AKCN/CNKE**. **Ouroboros-R**. **Picnic**. **pqNTRUSign**. **pqRSA encryption**. **pqRSA signature**. **pqsigRM**. **QC-MDPC KEM**. **qTESLA**. **RaCoSS**. **Rainbow**. **Ramstake**. **RankSign**. **RLCE-KEM**. **Round2**. **RQC**. **RVB**. **SABER**. **SIKE**. **SPHINCS+**. **SRTPI**. **Three Bears**. **Titanium**. **WalnutDSA**.

“Complete and proper” Einreichungen

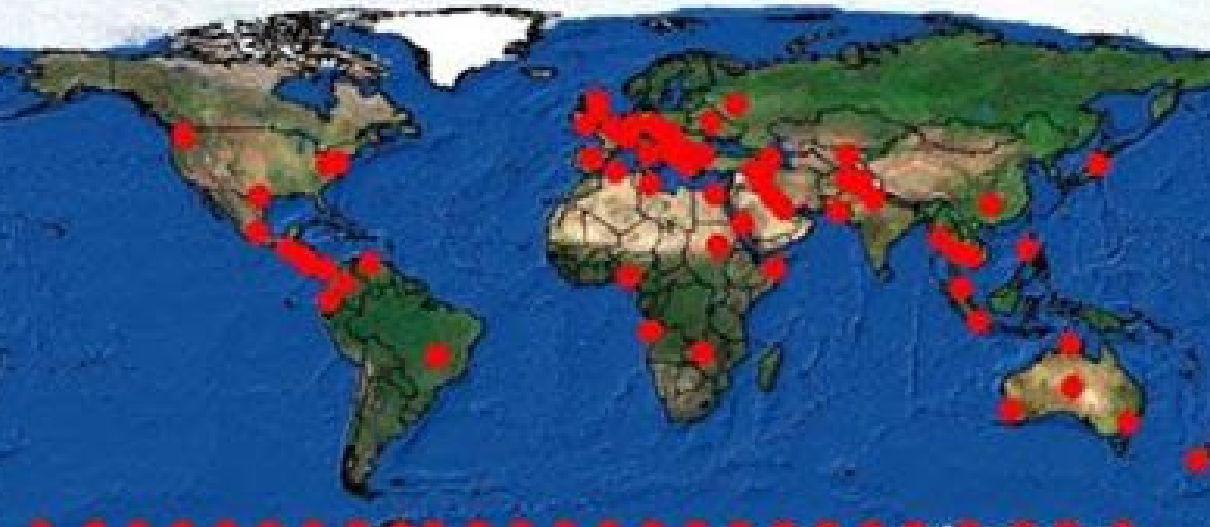
21. Dezember 2017: NIST veröffentlicht 69 Einreichungen von 260 Forschern.

BIG QUAKE. **BIKE**. **CFPKM**. **Classic McEliece**. **Compact LWE**. **CRYSTALS-DILITHIUM**. **CRYSTALS-KYBER**. **DAGS**. **Ding Key Exchange**. **DME**. **DRS**. **DualModeMS**. **Edon-K**. **EMBLEM and R.EMBLEM**. **FALCON**. **FrodoKEM**. **GeMSS**. **Giophantus**. **Gravity-SPHINCS**. **Guess Again**. **Gui**. **HILA5**. **HiMQ-3**. **HK17**. **HQC**. **KINDI**. **LAC**. **LAKE**. **LEDAkem**. **LEDApkc**. **Lepton**. **LIMA**. **Lizard**. **LOCKER**. **LOTUS**. **LUOV**. **McNie**. **Mersenne-756839**. **MQDSS**. **NewHope**. **NTRUEncrypt**. **NTRU-HRSS-KEM**. **NTRU Prime**. **NTS-KEM**. **Odd Manhattan**. **OKCN/AKCN/CNKE**. **Ouroboros-R**. **Picnic**. **pqNTRUSign**. **pqRSA encryption**. **pqRSA signature**. **pqsigRM**. **QC-MDPC KEM**. **qTESLA**. **RaCoSS**. **Rainbow**. **Ramstake**. **RankSign**. **RLCE-KEM**. **Round2**. **RQC**. **RVB**. **SABER**. **SIKE**. **SPHINCS+**. **SRTPI**. **Three Bears**. **Titanium**. **WalnutDSA**.

Warum jetzt?

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

Where is X-KEYSCORE?



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

- 1 & 2 Juli 2019: Executive summer school in Eindhoven.
- 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-)Vortäge.
- https://2017.pqcrypto.org/school: PQCRYPTO Sommer-Schule mit 21 Vorlesungen auf Video, mit Folien und Übungsaufgaben.
- https://2017.pqcrypto.org/exec: Executive school (12 Vorträge), weniger Mathe, mehr Überblick. Bislang nur Folien, hoffentlich bald Videos.
- https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions: NIST PQC Wettbewerb.

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	1108833108 cycles	1173074192 cycles
Encapsulation time	153940 cycles	188520 cycles
Decapsulation time	318088 cycles	343756 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	1218 bytes	1047 bytes
Secret-key size	1600 bytes	1238 bytes
Ciphertext size	1047 bytes	1175 bytes
Key-generation time	5925834 cycles	44940 cycles
Encapsulation time	45468 cycles	80596 cycles
Decapsulation time	94744 cycles	113272 cycles

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