Post-quantum cryptography: schemes and standards

Tanja Lange

Department of Mathematics and Computer Science & QT/e
Eindhoven University of Technology

Cryptography

Post-quantum cryptography:

Post-quantum cryptography:

Cryptography designed under the assumption
that the **attacker** (not the user!)
has a large quantum computer.

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

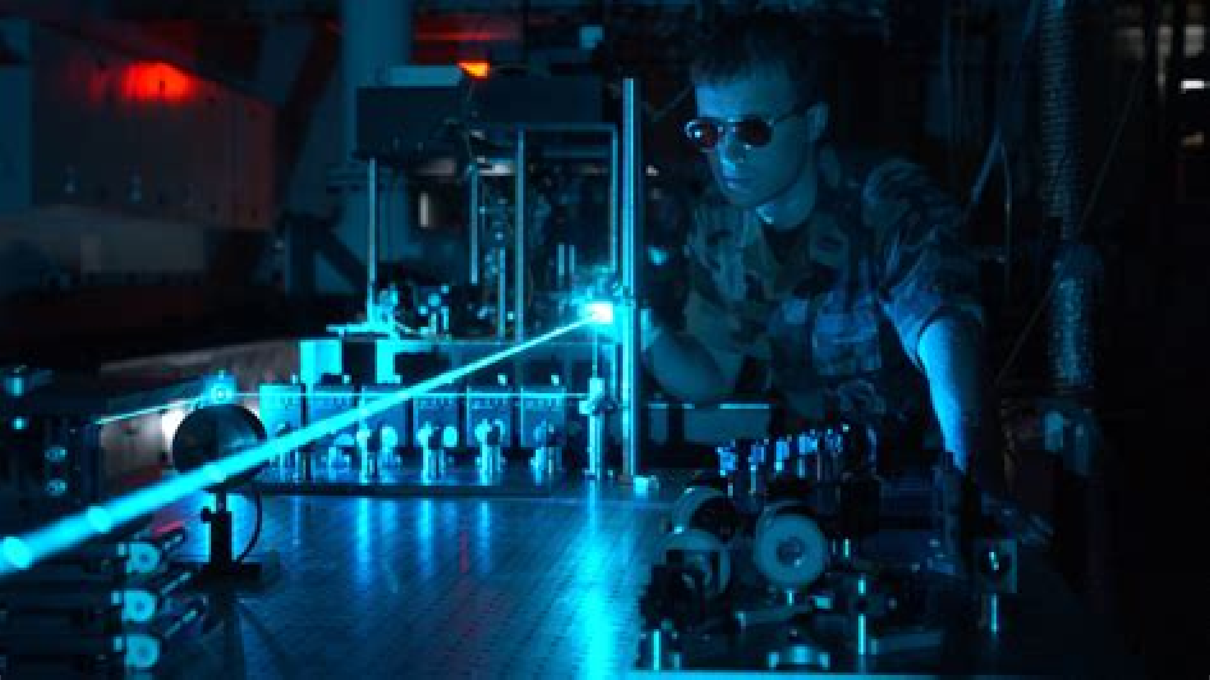
Abstract

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-

Back to the stone age?



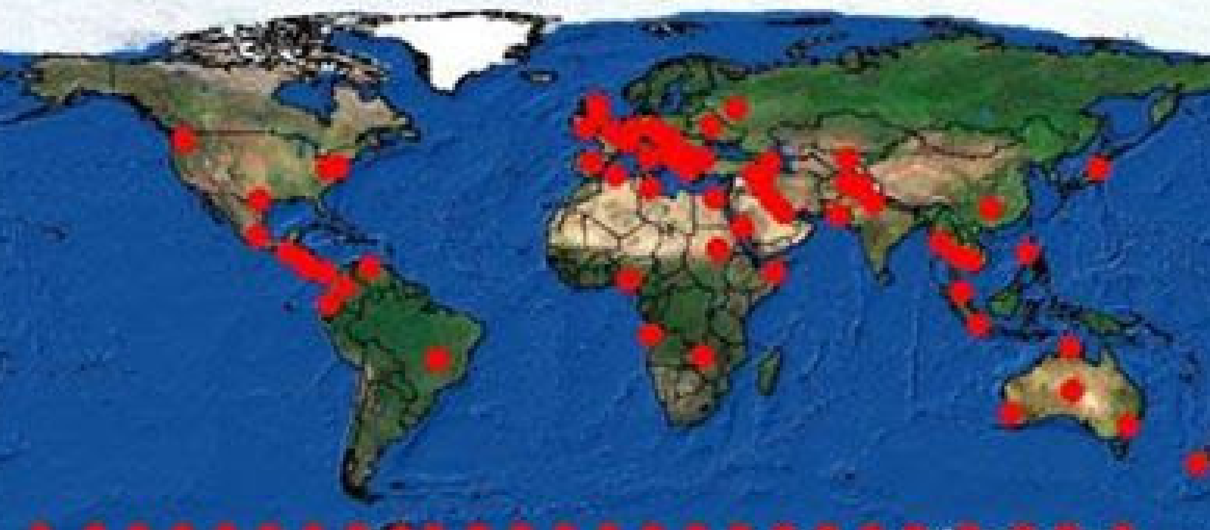
Post-quantum cryptography:

Post-quantum cryptography:

<u>Algorithmic</u> cryptography with attack model quantum cryptanalysis

Why now?

Where is X-KEYSCORE?



National Academy report on quantum computing

The National Academies of SCIENCES ENGINEERING MEDICINE THE NATIONAL ACADEMIES PRESS

This PDF is available at http://nap.edu/25196 SHARE

Quantum Computing: Progress and Prospects (2018)

DETAILS

202 pages | 6 x 9 | PAPERBACK
ISBN 978-0-309-47969-1 | DOI 10.17226/25196

http://www8.nationalacademies.org/onpinews/newsitem.aspx?RecordID=25196

National Academy report on quantum computing

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."

National Academy report on quantum computing

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."

Full report at `https://nap.edu/25196` (scroll down for free pdf).

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

Initial recommendations (2015)

- **Symmetric encryption** Thoroughly analyzed, 256-bit keys:
  - AES-256
  - Salsa20 with a 256-bit key

  Evaluating: Serpent-256, ...
- **Symmetric authentication** Information-theoretic MACs:
  - GCM using a 96-bit nonce and a 128-bit authenticator
  - Poly1305
- **Public-key encryption** McEliece with binary Goppa codes:
  - length $n = 6960$, dimension $k = 5413$, $t = 119$ errors

  Evaluating: QC-MDPC, Stehlé-Steinfeld NTRU, ...
- **Public-key signatures** Hash-based (minimal assumptions):
  - XMSS with any of the parameters specified in CFRG draft
  - SPHINCS-256

  Evaluating: HFEv-, ...

Categories of post-quantum cryptography

- Code-based encryption and signatures.
- Hash-based signatures.
- Isogeny-based encryption.
- Lattice-based encryption and signatures.
- Multivariate-quadratic encryption and signatures.
- Symmetric cryptography.

These are broad categories. For deployment concrete instantiations are needed.

NIST Post-quantum “competition”

30 November 2017: NIST receives 82 submissions.

	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**

NIST Post-quantum “competition”

30 November 2017: NIST receives 82 submissions.

	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**

21 December 2017: NIST publishes 69 submissions from 260 researchers.

NIST Post-quantum “competition”

30 November 2017: NIST receives 82 submissions.

	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**

21 December 2017: NIST publishes 69 submissions from 260 researchers.

30 January 2019: NIST narrows the field to 26 Round-2 candidates – 17 encryption systems and 9 signature systems.

Standardization progress of hash-based signatures

- CFRG has published 2 RFCs: RFC 8391 and RFC 8554

Datatracker Groups Documents Meetings Other User

```
Internet Research Task Force (IRTF)                          A. Huelsing
Request for Comments: 8391                                 TU Eindhoven
Category: Informational                                        D. Butin
ISSN: 2070-1721                                            TU Darmstadt
                                                             S. Gazdag
                                                            genua GmbH
                                                          J. Rijneveld
                                                    Radboud University
                                                           A. Mohaisen
                                         University of Central Florida
                                                              May 2018

                 XMSS: eXtended Merkle Signature Scheme
```

Datatracker Groups Documents Meetings Other User

```
Internet Research Task Force (IRTF)                            D. McGrew
Request for Comments: 8554                                     M. Curcio
Category: Informational                                       S. Fluhrer
ISSN: 2070-1721                                            Cisco Systems
                                                              April 2019

                 Leighton-Micali Hash-Based Signatures
```

Standardization progress of hash-based signatures

- CFRG has published 2 RFCs: RFC 8391 and RFC 8554
- NIST has gone through two rounds of requests for public input, most are positive and recommend standardizing XMSS and LMS. Only concern is about statefulness in general.

Standardization progress of hash-based signatures

- CFRG has published 2 RFCs: RFC 8391 and RFC 8554
- NIST has gone through two rounds of requests for public input, most are positive and recommend standardizing XMSS and LMS. Only concern is about statefulness in general.

- ISO SC27 JTC1 WG2 has started a study period on stateful hash-based signatures.

Post-quantum cryptography is ready
for deployment
on today's CPUs and Internet