

Security in Times of Surveillance



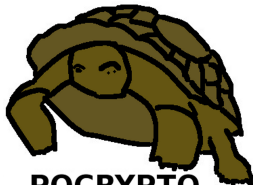
28 May 2018
TU Eindhoven
Ei/ψ

<https://www.win.tue.nl/eipsi/surveillance.html>

Post-quantum cryptography

Tanja Lange

Technische Universiteit Eindhoven



PQCRYPTO
ICT-645622

09 February 2018

SURF Security & Privacy Conference

Security in Times of Surveillance



<https://www.win.tue.nl/eipsi/surveillance.html>

Cryptography

- ▶ Motivation #1: Communication channels are spying on our data.
- ▶ Motivation #2: Communication channels are modifying our data.



- ▶ Literal meaning of cryptography: “secret writing”.
- ▶ Achieves various security goals by secretly transforming messages.

www.iacr.org
Your connection to this site is private.

Permissions **Connection**

The identity of this website has been verified by RapidSSL SHA256 CA - G3. No Certificate Transparency information was supplied by the server.
[Certificate information](#)

Your connection to www.iacr.org is encrypted using a modern cipher suite.
The connection uses TLS 1.2.

The connection is encrypted and authenticated using AES_128_GCM and uses ECDHE_RSA as the key exchange mechanism.

[What do these mean?](#)

iacrmemHEREATiacr.org



1702

Members
(1580 in 2012)

1245

Regular+

457

Students



www.iacr.org



Your connection to this site is private.

Permissions

Connection



The identity of this website has been verified by RapidSSL SHA256 CA - G3. No Certificate Transparency information was supplied by the server.

[Certificate information](#)



Your connection to www.iacr.org is encrypted using a modern cipher suite.

The connection uses TLS 1.2.

The connection is encrypted and authenticated using AES_128_GCM and uses ECDHE_RSA as the key exchange mechanism.

[What do these mean?](#)

iacrm





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 mechanical computers and have investigated their computational properties. This paper gives Las Vegas algorithms for finding discrete logarithms and factoring integers on a quantum computer that take a number of steps which is polynomial in the input size, e.g., the number of digits of the integer to be factored. These two problems are generally considered hard on a classical computer and have been used as the basis of several proposed cryptosystems. (We thus give the first examples of quantum cryptanalysis.)

[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 computation relates to classical complexity classes. We will thus first give a brief intuitive discussion of complexity classes for those readers who do not have this background. There are generally two resources which limit the ability of computers to solve large problems: time and space (i.e., memory). The field of analysis of algorithms considers the asymptotic demands that algorithms make for these resources as a function of the problem size. Theoretical computer scientists generally classify algorithms as efficient when the number of steps of the algorithms grows as a polynomial in the size of the input. The class of prob-



... but universal quantum computers are coming

- ▶ Massive research effort. Tons of progress summarized in, e.g.,
https://en.wikipedia.org/wiki/Timeline_of_quantum_computing.

... but universal quantum computers are coming

- ▶ Massive research effort. Tons of progress summarized in, e.g., https://en.wikipedia.org/wiki/Timeline_of_quantum_computing.
- ▶ Mark Ketchen, IBM Research, 2012, on quantum computing: “We’re actually doing things that are making us think like, ‘hey this isn’t 50 years off, this is maybe just 10 years off, or 15 years off.’ It’s within reach.”
- ▶ Fast-forward to 2022, or 2027. Universal quantum computers exist.

... but universal quantum computers are coming

- ▶ Massive research effort. Tons of progress summarized in, e.g., https://en.wikipedia.org/wiki/Timeline_of_quantum_computing.
- ▶ Mark Ketchen, IBM Research, 2012, on quantum computing: “We’re actually doing things that are making us think like, ‘hey this isn’t 50 years off, this is maybe just 10 years off, or 15 years off.’ It’s within reach.”
- ▶ Fast-forward to 2022, or 2027. Universal quantum computers exist.
- ▶ Shor’s algorithm solves in polynomial time:
 - ▶ Integer factorization. RSA is dead.
 - ▶ The discrete-logarithm problem in finite fields. DSA is dead.
 - ▶ The discrete-logarithm problem on elliptic curves. ECDSA is dead.
- ▶ This breaks all current public-key cryptography on the Internet!

... but universal quantum computers are coming

- ▶ Massive research effort. Tons of progress summarized in, e.g., https://en.wikipedia.org/wiki/Timeline_of_quantum_computing.
- ▶ Mark Ketchen, IBM Research, 2012, on quantum computing: “We’re actually doing things that are making us think like, ‘hey this isn’t 50 years off, this is maybe just 10 years off, or 15 years off.’ It’s within reach.”
- ▶ Fast-forward to 2022, or 2027. Universal quantum computers exist.
- ▶ Shor’s algorithm solves in polynomial time:
 - ▶ Integer factorization. RSA is dead.
 - ▶ The discrete-logarithm problem in finite fields. DSA is dead.
 - ▶ The discrete-logarithm problem on elliptic curves. ECDSA is dead.
- ▶ This breaks all current public-key cryptography on the Internet!
- ▶ Also, Grover’s algorithm speeds up brute-force searches.
- ▶ Example: Only 2^{64} quantum operations to break AES-128;
 2^{128} quantum operations to break AES-256.



Physical cryptography: a return to the dark ages

- ▶ Imagine a lockable-briefcase salesman proposing a “locked-briefcase Internet” using “provably secure locked-briefcase cryptography”:
 - ▶ Alice puts secret information into a lockable briefcase.
 - ▶ Alice locks the briefcase.
 - ▶ A courier transports the briefcase from Alice to Bob.
 - ▶ Bob unlocks the briefcase and retrieves the information.
 - ▶ There is a mathematical proof that the information is hidden!
 - ▶ Throw away algorithmic cryptography!



Physical cryptography: a return to the dark ages

- ▶ Imagine a lockable-briefcase salesman proposing a “locked-briefcase Internet” using “provably secure locked-briefcase cryptography”:
 - ▶ Alice puts secret information into a lockable briefcase.
 - ▶ Alice locks the briefcase.
 - ▶ A courier transports the briefcase from Alice to Bob.
 - ▶ Bob unlocks the briefcase and retrieves the information.
 - ▶ There is a mathematical proof that the information is hidden!
 - ▶ Throw away algorithmic cryptography!
- ▶ Most common reactions from security experts:
 - ▶ This would make security much worse.



Physical cryptography: a return to the dark ages

- ▶ Imagine a lockable-briefcase salesman proposing a “locked-briefcase Internet” using “provably secure locked-briefcase cryptography”:
 - ▶ Alice puts secret information into a lockable briefcase.
 - ▶ Alice locks the briefcase.
 - ▶ A courier transports the briefcase from Alice to Bob.
 - ▶ Bob unlocks the briefcase and retrieves the information.
 - ▶ There is a mathematical proof that the information is hidden!
 - ▶ Throw away algorithmic cryptography!
- ▶ Most common reactions from security experts:
 - ▶ This would make security much worse.
 - ▶ This would be insanely expensive.



Physical cryptography: a return to the dark ages

- ▶ Imagine a lockable-briefcase salesman proposing a “locked-briefcase Internet” using “provably secure locked-briefcase cryptography”:
 - ▶ Alice puts secret information into a lockable briefcase.
 - ▶ Alice locks the briefcase.
 - ▶ A courier transports the briefcase from Alice to Bob.
 - ▶ Bob unlocks the briefcase and retrieves the information.
 - ▶ There is a mathematical proof that the information is hidden!
 - ▶ Throw away algorithmic cryptography!
- ▶ Most common reactions from security experts:
 - ▶ This would make security much worse.
 - ▶ This would be insanely expensive.
 - ▶ We should not dignify this proposal with a response.



Security advantages of algorithmic cryptography

- ▶ Keep secrets heavily shielded inside authorized computers.
- ▶ Reduce trust in third parties:
 - ▶ Reduce reliance on closed-source software and hardware.
 - ▶ Increase comprehensiveness of audits.
 - ▶ Increase comprehensiveness of formal verification.
 - ▶ Design systems to be secure even if **keys are public**.
Critical example: **signed** software updates.
- ▶ Understand security as thoroughly as possible:
 - ▶ Publish comprehensive specifications.
 - ▶ Build large research community with clear security goals.
 - ▶ Publicly document attack efforts.
 - ▶ Require systems to convincingly survive many years of analysis.

Even higher urgency for long-term confidentiality

- ▶ Attacker can break currently used encryption (ECC, RSA) with a quantum computer.
- ▶ Even worse, today's encrypted communication is being stored by attackers and will be decrypted years later with quantum computers. All data can be recovered in clear from recording traffic and breaking the public key scheme.
- ▶ How many years are you required to keep your data secret? From whom?



- ▶ Signature schemes can be replaced once a quantum computer is built – but there will not be a public announcement

Even higher urgency for long-term confidentiality

- ▶ Attacker can break currently used encryption (ECC, RSA) with a quantum computer.
- ▶ Even worse, today's encrypted communication is being stored by attackers and will be decrypted years later with quantum computers. All data can be recovered in clear from recording traffic and breaking the public key scheme.
- ▶ How many years are you required to keep your data secret? From whom?



- ▶ Signature schemes can be replaced once a quantum computer is built – but there will not be a public announcement . . . and an important function of signatures is to protect operating system upgrades.
- ▶ Protect your upgrades *now* with post-quantum signatures.

Confidence-inspiring crypto takes time to build

- ▶ Many stages of research from cryptographic design to deployment:
 - ▶ Explore space of cryptosystems.
 - ▶ Study algorithms for the attackers.
 - ▶ Focus on secure cryptosystems.

Confidence-inspiring crypto takes time to build

- ▶ Many stages of research from cryptographic design to deployment:
 - ▶ Explore space of cryptosystems.
 - ▶ Study algorithms for the attackers.
 - ▶ Focus on secure cryptosystems.
 - ▶ Study algorithms for the users.
 - ▶ Study implementations on real hardware.
 - ▶ Study side-channel attacks, fault attacks, etc.
 - ▶ Focus on secure, reliable implementations.
 - ▶ Focus on implementations meeting performance requirements.
 - ▶ Integrate securely into real-world applications.

Confidence-inspiring crypto takes time to build

- ▶ Many stages of research from cryptographic design to deployment:
 - ▶ Explore space of cryptosystems.
 - ▶ Study algorithms for the attackers.
 - ▶ Focus on secure cryptosystems.
 - ▶ Study algorithms for the users.
 - ▶ Study implementations on real hardware.
 - ▶ Study side-channel attacks, fault attacks, etc.
 - ▶ Focus on secure, reliable implementations.
 - ▶ Focus on implementations meeting performance requirements.
 - ▶ Integrate securely into real-world applications.
- ▶ Example: ECC introduced **1985**; big advantages over RSA. Robust ECC started to take over the Internet in **2015**.
- ▶ Can't wait for quantum computers before finding a solution!

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

- ▶ **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-, ...

NIST Post-Quantum “Competition”

December 2016, after public feedback: NIST [calls for submissions](#) of post-quantum cryptosystems to standardize.

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

“Complete and proper” submissions

21 December 2017: NIST posts [69 submissions](#) from 260 people.

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. pqNTRUSign. NTRU-HRSS-KEM. NTRU Prime. NTS-KEM. Odd Manhattan. OKCN/AKCN/CNKE. Ouroboros-R. Picnic. 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” submissions

21 December 2017: NIST posts [69 submissions](#) from 260 people.

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. pqNTRUSign. NTRU-HRSS-KEM. NTRU Prime. NTS-KEM. Odd Manhattan. OKCN/AKCN/CNKE. Ouroboros-R. Picnic. 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.

Some attack scripts already posted causing **total break** or **serious tweaks**. Many more receiving detailed analysis.

Further resources

- ▶ <https://2017.pqcrypto.org/school>: PQCRYPTO summer school with 21 lectures on video + slides + exercises.
- ▶ <https://2017.pqcrypto.org/exec>: Executive school (12 lectures), less math, more overview. So far slides, soon videos.
- ▶ <https://2017.pqcrypto.org/conference>: PQCrypto 2017; the latest results on post-quantum crypto.
- ▶ <https://pqcrypto.org>: Our survey site.
 - ▶ Many pointers: e.g., to PQCrypto conferences;
 - ▶ Bibliography for 4 major PQC systems.
- ▶ <https://pqcrypto.eu.org>: PQCRYPTO EU project.
Coming soon:
 - ▶ Expert recommendations.
 - ▶ Free software libraries.
 - ▶ More benchmarking to compare cryptosystems.
- ▶ https://twitter.com/pqc_eu: PQCRYPTO Twitter feed.
- ▶ <https://twitter.com/PQCryptoConf>: PQCrypto conference Twitter feed.