Post-Quantum Cryptography

Tanja Lange

Technische Universiteit Eindhoven

21 April 2017

Cryptographic applications in daily life

- Mobile phones connecting to cell towers.
- Credit cards, EC-cards, access codes for banks.
- Any webpage with `https`: Internet commerce, tax declarations, webmail.
- Encrypted file system on iPhone (see Apple vs. FBI).
- Facebook, WhatsApp, iMessage on iPhone.

Cryptographic applications in daily life

- Mobile phones connecting to cell towers.
- Credit cards, EC-cards, access codes for banks.
- Any webpage with `https`: Internet commerce, tax declarations, webmail.
- Encrypted file system on iPhone (see Apple vs. FBI).
- Facebook, WhatsApp, iMessage on iPhone.
- PGP encrypted email, Signal, Tor, Tails, Qubes OS, Subgraph OS.

Cryptographic applications in daily life

- Mobile phones connecting to cell towers.
- Credit cards, EC-cards, access codes for banks.
- Any webpage with `https`: Internet commerce, tax declarations, webmail.
- Encrypted file system on iPhone (see Apple vs. FBI).
- Facebook, WhatsApp, iMessage on iPhone.
- PGP encrypted email, Signal, Tor, Tails, Qubes OS, Subgraph OS.

Currently used crypto (check the lock icon in your browser) starts with RSA, Diffie-Hellman (DH) in finite fields, or elliptic curve DH, followed by AES or ChaCha20.

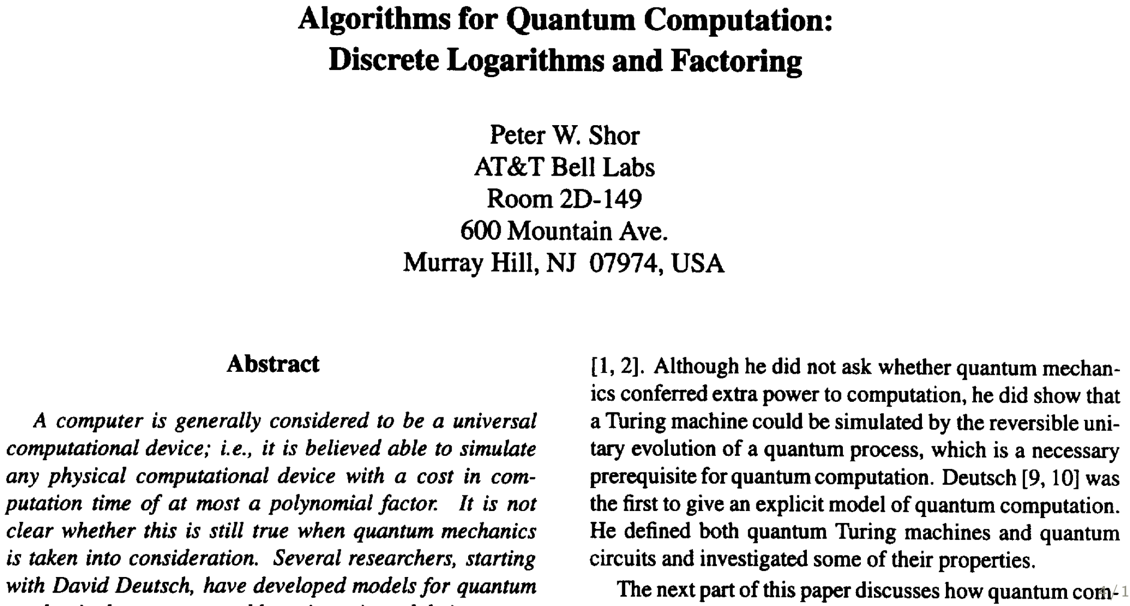
Security is getting better, but lots of bugs and no secure hardware

Cryptographic applications in daily life

- Mobile phones connecting to cell towers.
- Credit cards, EC-cards, access codes for banks.
- Any webpage with `https`: Internet commerce, tax declarations, webmail.
- Encrypted file system on iPhone (see Apple vs. FBI).
- Facebook, WhatsApp, iMessage on iPhone.
- PGP encrypted email, Signal, Tor, Tails, Qubes OS, Subgraph OS.

Currently used crypto (check the lock icon in your browser) starts with RSA, Diffie-Hellman (DH) in finite fields, or elliptic curve DH, followed by AES or ChaCha20.

Security is getting better, but lots of bugs and no secure hardware
. . . not to mention anti-security measures such as backdoors.



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-

Universal quantum computers are coming, and are scary

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

Universal quantum computers are coming, and are scary

- 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!
- 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: “Were 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.”

Universal quantum computers are coming, and are scary

- 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!
- 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: "Were 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."
- 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

- Locked briefcases, quantum key distribution, etc.
- Horrendously expensive.
- "Information protection for rich people."

Physical cryptography: a return to the dark ages

- Locked briefcases, quantum key distribution, etc.
- Horrendously expensive.
- “Information protection for rich people.”
- “Provably secure”—under highly questionable assumptions.
- Broken again and again. Much worse track record than normal crypto.
- Easy to screw up. Easy to backdoor. Hard to audit.

Physical cryptography: a return to the dark ages

- Locked briefcases, quantum key distribution, etc.
- Horrendously expensive.
- "Information protection for rich people."
- "Provably secure"—under highly questionable assumptions.
- Broken again and again. Much worse track record than normal crypto.
- Easy to screw up. Easy to backdoor. Hard to audit.
- Very limited functionality: e.g., no public-key signatures.

Is there any hope? Yes!

Post-quantum crypto is crypto that resists attacks by quantum computers.

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

Is there any hope? Yes!

Post-quantum crypto is crypto that resists attacks by quantum computers.

- PQCrypto 2006: International Workshop on Post-Quantum Cryptography.
- PQCrypto 2008.

Is there any hope? Yes!

Post-quantum crypto is crypto that resists attacks by quantum computers.

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

Is there any hope? Yes!

Post-quantum crypto is crypto that resists attacks by quantum computers.

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

Is there any hope? Yes!

Post-quantum crypto is crypto that resists attacks by quantum computers.

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

PQCRYPTO
ICT-645622

NSA announcements

August 11, 2015

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

NSA announcements

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.*

NSA announcements

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.*

NSA comes late to the party and botches its grand entrance.

NSA announcements

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.*

NSA comes late to the party and botches its grand entrance.

Worse, now we get people saying “Don’t use post-quantum crypto, the NSA wants you to use it!”.

Post-quantum becoming mainstream

- PQCrypto 2016: 22–26 Feb in Fukuoka, Japan, with more than 200 participants

- NIST is calling for post-quantum proposals for competition, due November.

Confidence-inspiring crypto takes time to build

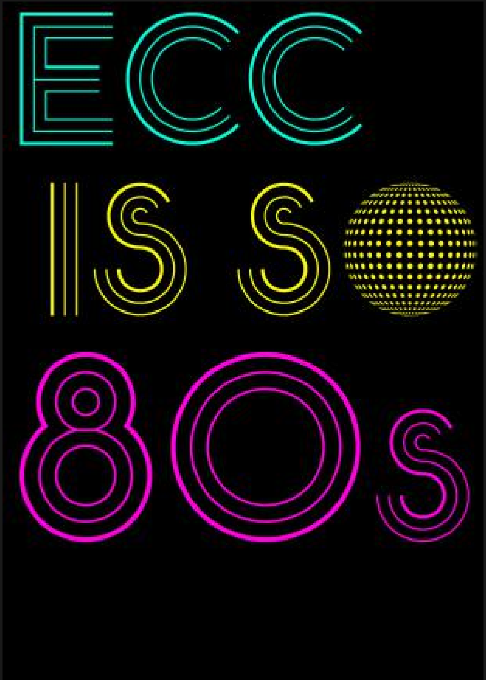
- Many stages of research from cryptographic design to deployment:
  - Explore space of cryptosystems.
  - Study algorithms for the attackers.
  - Focus on secure cryptosystems.

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 is starting to take over the Internet in **2015**.
- Post-quantum research can't wait for quantum computers!


ECC
IS SO
80s

Even higher urgency for long-term confidentiality

- Today's encrypted communication is being stored by attackers and will be decrypted years later with quantum computers. Danger for human-rights workers, journalists, security research, lawyers, diplomats, health records ...

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

Where is X-KEYSCORE?

- 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.

Next slide:
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. Key size: 1MB

  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-, . . .

Code-based Crypto

Parity check matrix, e.g. $n = 7, k = 4$:

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Many special constructions discovered in 65 years of coding theory:

- For special matrices H, given $\mathbf{s} = H \cdot \mathbf{e}$ find $\mathbf{e}$ with few non-zero entries.
- For random matrices H, finding $\mathbf{e}$ given $\mathbf{s}$ is hard.

Code-based Crypto

Parity check matrix, e.g. $n = 7, k = 4$:

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

Many special constructions discovered in 65 years of coding theory:

- For special matrices H, given $\mathbf{s} = H \cdot \mathbf{e}$ find $\mathbf{e}$ with few non-zero entries.
- For random matrices H, finding $\mathbf{e}$ given $\mathbf{s}$ is hard.
- Use this difference in complexities for encryption
  with some trapdoor to move from random matrix to good matrix as secret.

Many more post-quantum suggestions

- QC-MDPC: variant with much smaller keys, but is it secure?
- Many more code-based systems. Some broken, some not.
- NTRU: 1990s "lattice-based" system, similar to QC-MDPC. Security story less stable than code-based cryptography.
- Many more lattice-based systems. Some broken, some not. e.g., 2014 quantum break of 2009 Smart–Vercauteren system.
- Many multivariate-quadratic systems. Some broken, some not. Highlight: very small signatures.
- More exotic possibility that needs analysis: isogeny-based crypto. Highlight: supports DH.

Further resources

Summer school on post-quantum crypto
Eindhoven, 19–23 June 2017
https://2017.pqcrypto.org/school/index.html

Executive school on post-quantum crypto
Eindhoven, 22–23 June 2017
https://2017.pqcrypto.org/exec/index.html

PQCrypto 2017
Utrecht, 26–28 June 2017
https://2017.pqcrypto.org/conference/index.html

https://pqcrypto.org: Our survey site.

https://pqcrypto.eu.org: PQCRYPTO EU project.