# The crypto-apocalyose: Cybersecurity in a post-quantum world

Tanja Lange

Technische Universiteit Eindhoven

16 March 2016

# Cryptography

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

Sender
"Jefferson"


Untrustworthy network
"Eavesdropper"

Receiver
"Madison"

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

https://www.iacr.org/

https://www.iacr.org/docs/minutes/c2013mem-slides.pdf

IACR Mer

16 / 55

**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

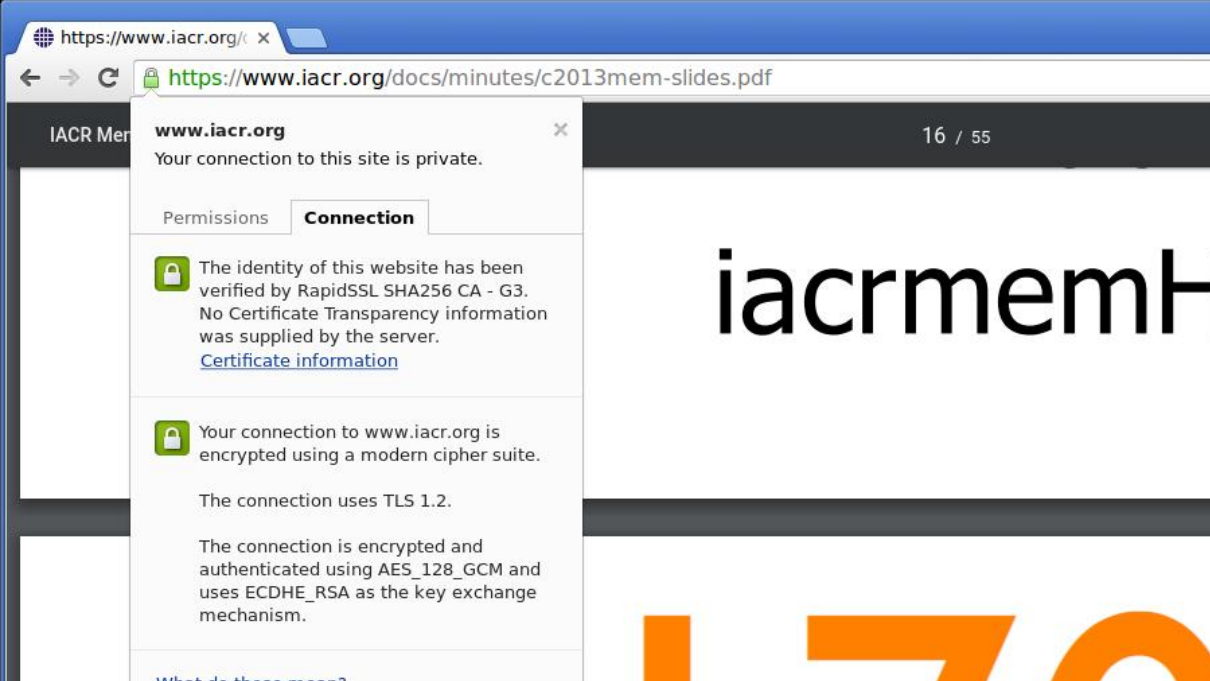
INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH

2013

1702 Members

(1580 in 2012)

1245 Regular


https://www.iacr.org/
https://www.iacr.org/docs/minutes/c2013mem-slides.pdf
IACR Mer
16 / 55
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.
iacrmemH

# Cryptographic applications in daily life

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

# Cryptographic applications in daily life

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

Snowden in Reddit AmA

> *Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.*

# Cryptographic tools

Many factors influence the security and privacy of data

- Secure storage, physical security; access control.
- Protection against alteration of data
  $\Rightarrow$ digital signatures, message authentication codes.
- Protection of sensitive content against reading
  $\Rightarrow$ encryption.

Cryptology is the science that studies mathematical techniques in order to provide secrecy, authenticity and related properties for digital information.

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.

Internet currently moving over to Bernstein's Curve25519 and joint work Ed25519 (also with Duif, Schwabe, and Yang).

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

# Cryptographic tools

Many factors influence the security and privacy of data

- Secure storage, physical security; access control.
- Protection against alteration of data
  $\Rightarrow$ digital signatures, message authentication codes.
- Protection of sensitive content against reading
  $\Rightarrow$ encryption.

Cryptology is the science that studies mathematical techniques in order to provide secrecy, authenticity and related properties for digital information.

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.

Internet currently moving over to Bernstein's Curve25519 and joint work Ed25519 (also with Duif, Schwabe, and Yang).

Security is getting better, but lots of bugs and no secure hardware – let alone anti-security measures such as the Dutch "Hackvoorstel".

# 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 compu-*

[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-


D-Wave
D-Wave
D-Wave

# D-Wave quantum computer isn't universal . . .

- Can't store stable qubits.
- Can't perform basic qubit operations.
- Can't run Shor's algorithm.
- Can't run other quantum algorithms we care about.

# D-Wave quantum computer isn't universal . . .

- Can't store stable qubits.
- Can't perform basic qubit operations.
- Can't run Shor's algorithm.
- Can't run other quantum algorithms we care about.
- Hasn't managed to find any computation justifying its price.
- Hasn't managed to find any computation justifying 1% of its price.

## . . . but universal quantum computers are coming, and are scary

- 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, and are scary

- 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."
- Fast-forward to 2022, or 2027. Universal quantum computers exist.

# . . . but universal quantum computers are coming, and are scary

- 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."
- 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, and are scary

- 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."
- 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

- Locked briefcases, quantum key distribution, etc.
- Horrendously expensive.

# Physical cryptography: a return to the dark ages

- Locked briefcases, quantum key distribution, etc.
- Horrendously expensive.
- "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.
- "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.
- PQCrypto 2016: 22–26 Feb.
- PQCrypto 2017 planned.

# 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.
- PQCrypto 2016: 22–26 Feb.
- PQCrypto 2017 planned.
- New EU project, 2015–2018: PQCRYPTO, Post-Quantum Cryptography for Long-term Security.

PQCRYPTO
ICT-645622

# 2016: more than 200 participants

# 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 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.

NIST is calling for post-quantum proposals; expect a small competition.

# Confidence-inspiring crypto takes time to build

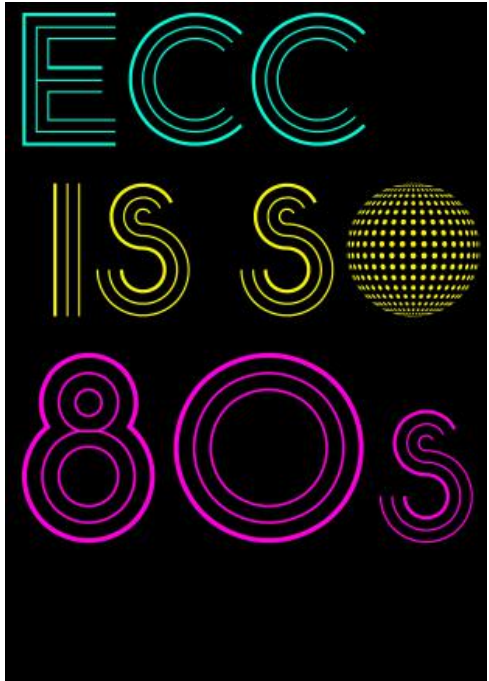
- Many stages of research from cryptographic design to deployment:
  - Explore space of cryptosystems.
  - Study algorithms for the attackers.
  - Focus on secure cryptosystems.

# 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 ...


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

  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-, ...

# 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

- General crypto/security links.
  - TRU/e Master in Cyber Security
  - Talks: Security in Times of Surveillance 2014, 2015 and Post-Snowden Cryptography
  - Bits of Freedom's campaign against the Hackvoorstel
  - Last week tonight: Encryption by John Oliver
  - Thomas Jefferson and Apple versus the FBI post by Daniel J. Bernstein
  - EFF and 46 Technology Experts Ask Court To Throw Out Unconstitutional Apple Order
- PQCrypto 2016 with slides and videos from lectures (incl. winter school)
- `https://pqcrypto.org`: Our survey site.
  - Many pointers: e.g., PQCrypto 2016.
  - Bibliography for 4 major PQC systemss.
- `https://pqcrypto.eu.org`: PQCRYPTO EU project.:
  - Expert recommendations.
  - Free software libraries. (Coming soon)
  - More benchmarking to compare cryptosystems. (Coming soon)
  - 2017: workshop and spring/summer school.
  - `https://twitter.com/pqc_eu`: PQCRYPTO Twitter feed.