You thought your communication was secure? Quantum computers are coming!

Daniel J. Bernstein[1,2] Tanja Lange[1]

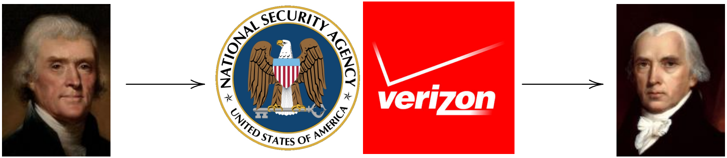
[1]Technische Universiteit Eindhoven

[2]University of Illinois at Chicago

16 April 2016

Cryptography

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

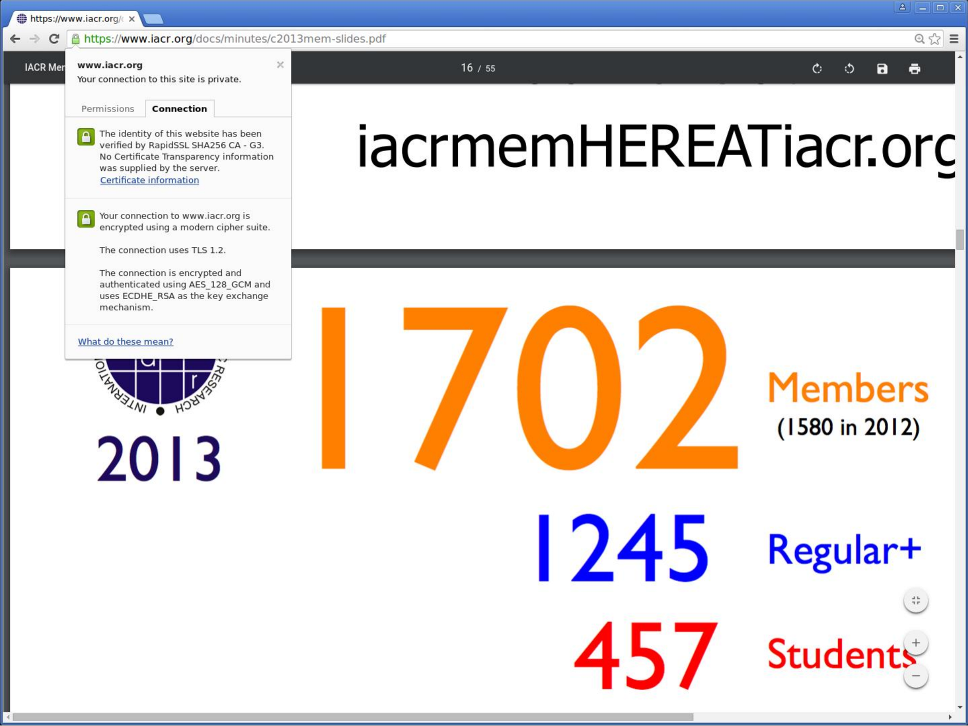


Sender
"Jefferson"

Untrustworthy network
"Eavesdropper"

Receiver
"Madison"

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



www.iacr.org

Your connection to this site is private.

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

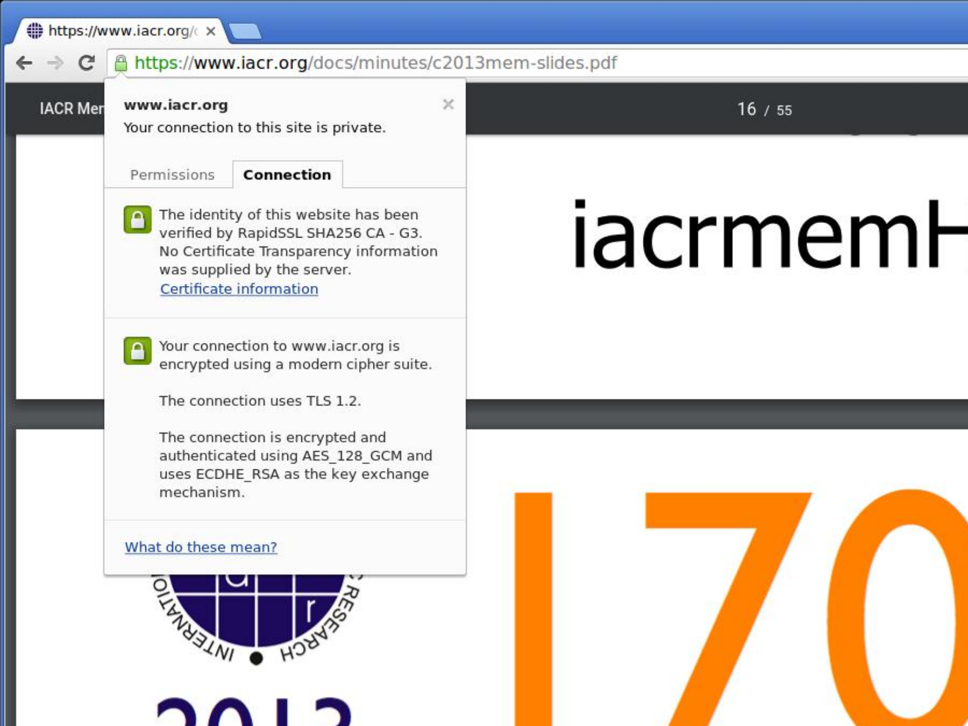
2013

1702 Members

(1580 in 2012)

1245 Regular+

457 Students



www.iacr.org

Your connection to this site is private.

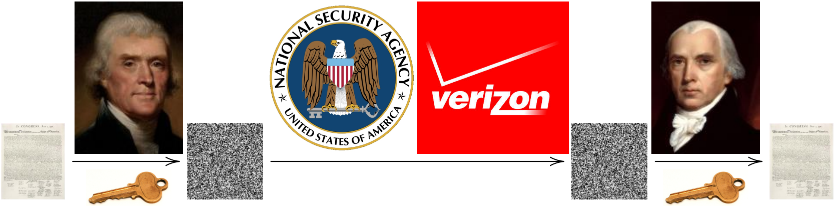
The identity of this website has been verified by RapidSSL SHA256 CA - G3. No Certificate Transparency information was supplied by the server.

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

The connection uses TLS 1.2.

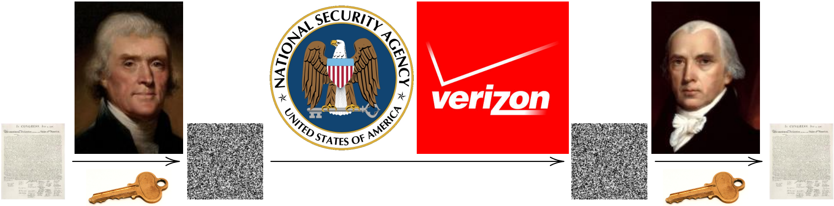
The connection is encrypted and authenticated using AES_128_GCM and uses ECDHE_RSA as the key exchange mechanism.

Secret-key encryption



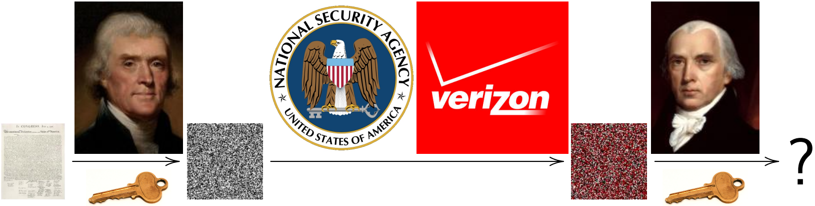
- Prerequisite: Jefferson and Madison share a secret key 🔑.
- Prerequisite: Eve doesn't know 🔑.
- Jefferson and Madison exchange any number of messages.
- Security goal #1: **Confidentiality** despite Eve's espionage.

Secret-key authenticated encryption



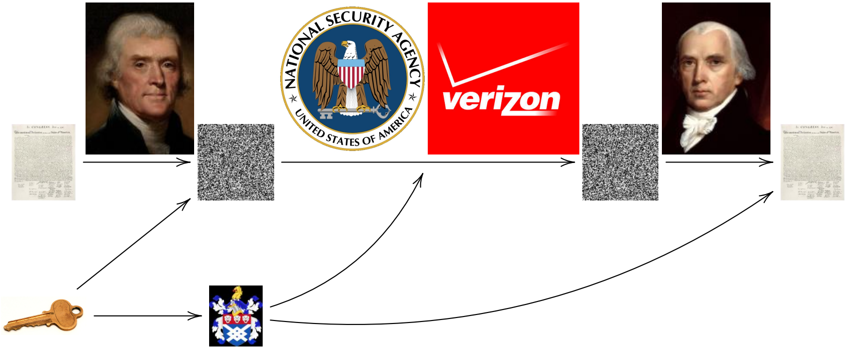
- Prerequisite: Jefferson and Madison share a secret key 🔑.
- Prerequisite: Eve doesn't know 🔑.
- Jefferson and Madison exchange any number of messages.
- Security goal #1: **Confidentiality** despite Eve's espionage.
- Security goal #2: **Integrity**, i.e., recognizing Eve's sabotage.

Secret-key authenticated encryption



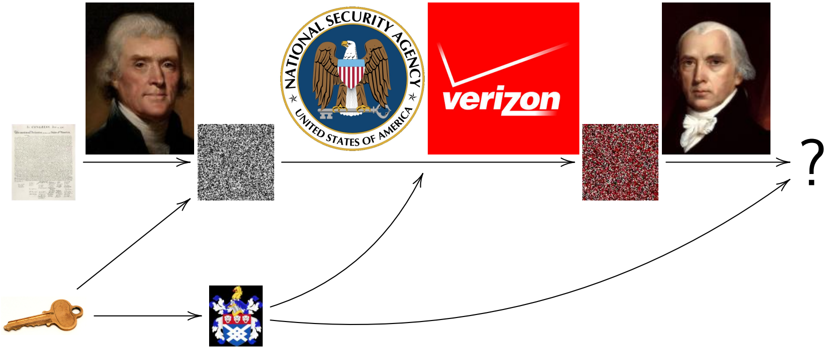
- Prerequisite: Jefferson and Madison share a secret key 🔑.
- Prerequisite: Eve doesn't know 🔑.
- Jefferson and Madison exchange any number of messages.
- Security goal #1: **Confidentiality** despite Eve's espionage.
- Security goal #2: **Integrity**, i.e., recognizing Eve's sabotage.

Public-key signatures



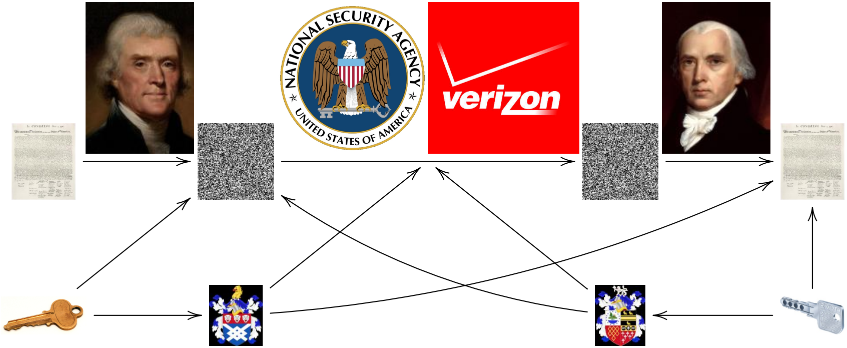
- Prerequisite: Jefferson has a secret key 🔑 and public key 🛡.
- Prerequisite: Eve doesn't know 🔑. Everyone knows 🛡.
- Jefferson publishes any number of messages.
- Security goal: Integrity.

Public-key signatures



- Prerequisite: Jefferson has a secret key 🔑 and public key 🛡.
- Prerequisite: Eve doesn't know 🔑. Everyone knows 🛡.
- Jefferson publishes any number of messages.
- Security goal: Integrity.

Public-key authenticated encryption ("DH" data flow)



- Prerequisite: Jefferson has a secret key 🔑 and public key 🛡.
- Prerequisite: Madison has a secret key 🔑 and public key 🛡.
- Jefferson and Madison exchange any number of messages.
- Security goal #1: Confidentiality.
- Security goal #2: Integrity.

Many more security goals studied in cryptography

- Protecting against denial of service.
- Stopping traffic analysis.
- Securely tallying votes.
- Searching encrypted data.
- Much more.

Cryptographic applications in daily life

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

Cryptographic applications in daily life

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

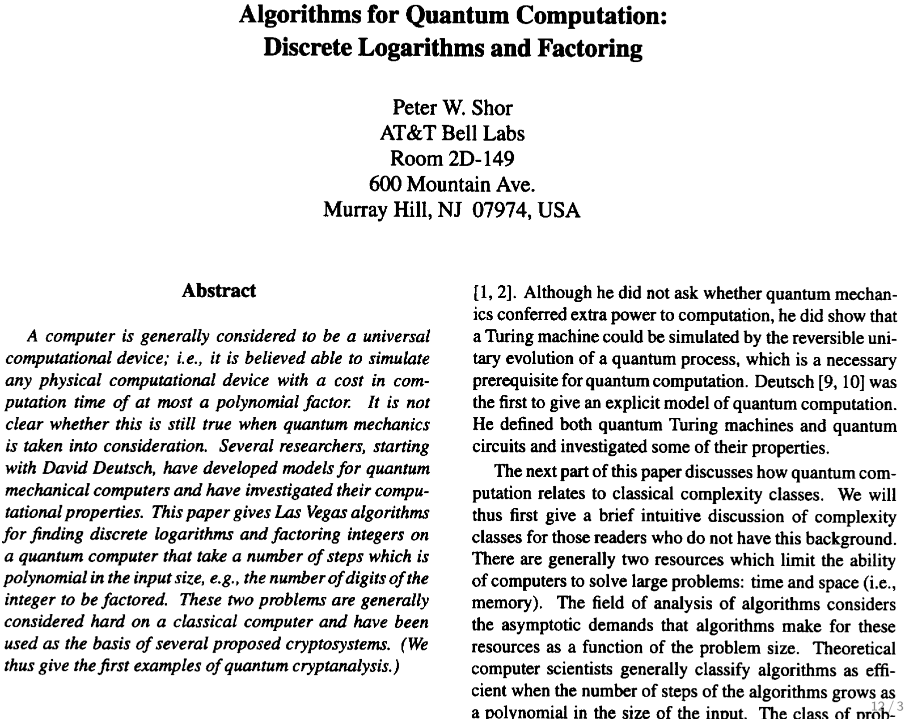
Many factors influence the security and privacy of data:

- Secure storage, physical security; access control.
- Protection against alteration of data
  ⇒ public-key signatures, message-authentication codes.
- Protection of sensitive content against reading
  ⇒ encryption.

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 Curve25519 (Bernstein) and Ed25519 (Bernstein, Duif, Lange, Schwabe, and Yang).

Security is getting better. Some obstacles: bugs; untrustworthy hardware; anti-security measures such as UK snooper's charter.



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-

D:wave
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 . . .

- 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

- 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!

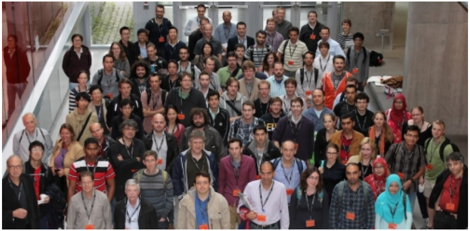
Post-quantum crypto is crypto that resists attacks by quantum computers.

- 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.

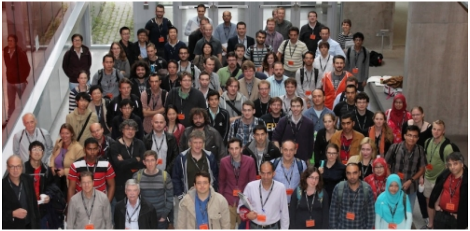
- PQCrypto 2006: International Workshop on Post-Quantum Cryptography.
- PQCrypto 2008.
- PQCrypto 2010.
- PQCrypto 2011.
- PQCrypto 2013.
- PQCrypto 2014.



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.
- New 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.

Post-quantum becoming mainstream

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

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

- PQCrypto 2017 planned, will be in Utrecht, Netherlands.

Confidence-inspiring crypto takes time to build

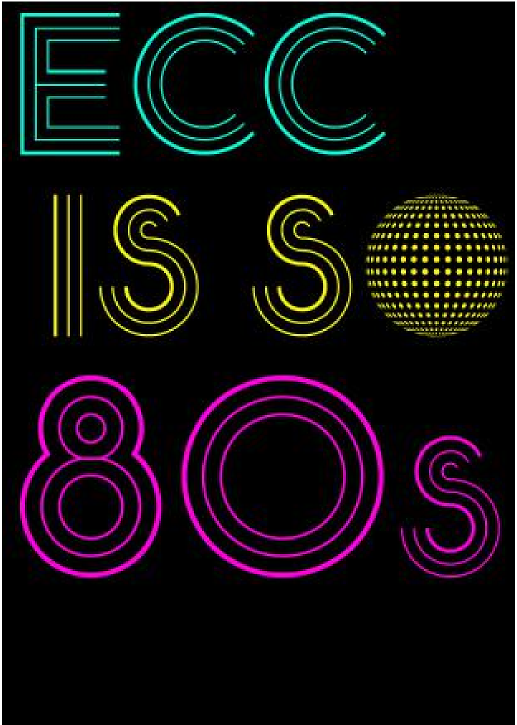
- Many stages of research from cryptographic design to deployment:
  - Explore space of cryptosystems.
  - Study algorithms for the attackers.
  - Focus on secure cryptosystems.

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**.
- Post-quantum research can't wait for quantum computers!

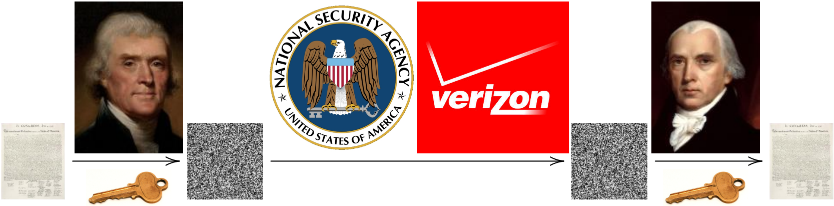

ECC
IS SO
80s

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 . . .

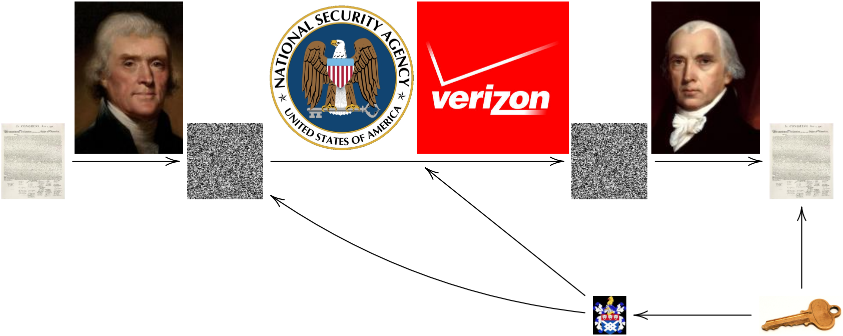
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL
Where is X-KEYSCORE?
KEYSC

Post-quantum secret-key authenticated encryption



- Very easy solutions if secret key 🔑 is long uniform random string:
  - "One-time pad" for encryption.
  - "Wegman–Carter MAC" for authentication.
- AES-256: Standardized method to expand 256-bit 🔑 into string indistinguishable from long 🔑.
- AES introduced in 1998 by Daemen and Rijmen. Security analyzed in papers by dozens of cryptanalysts.
- No credible threat from quantum algorithms. Grover costs 2^{128}.

Post-quantum public-key encryption: code-based



- Jefferson uses Madison's public key to encrypt.
- Madison uses his secret key to decrypt.
- Code-based crypto proposed by McEliece in 1978 using Goppa codes.
- Almost as old as RSA, but much stronger security history.
- Many further improvements, e.g. Niederreiter system for smaller keys.

Security analysis

- Some papers studying algorithms for attackers:
  1962 Prange; 1981 Omura; 1988 Lee–Brickell; 1988 Leon; 1989 Krouk;
  1989 Stern; 1989 Dumer; 1990 Coffey–Goodman; 1990 van Tilburg;
  1991 Dumer; 1991 Coffey–Goodman–Farrell; 1993 Chabanne–Courteau;
  1993 Chabaud; 1994 van Tilburg; 1994 Canteaut–Chabanne;
  1998 Canteaut–Chabaud; 1998 Canteaut–Sendrier;
  2008 Bernstein–Lange–Peters; 2009 Bernstein–Lange–Peters–van Tilborg;
  2009 Bernstein (post-quantum); 2009 Finiasz–Sendrier;
  2010 Bernstein–Lange–Peters; 2011 May–Meurer–Thomae;
  2011 Becker–Coron–Joux; 2012 Becker–Joux–May–Meurer;
  2013 Bernstein–Jeffery–Lange–Meurer (post-quantum);
  2015 May–Ozerov.

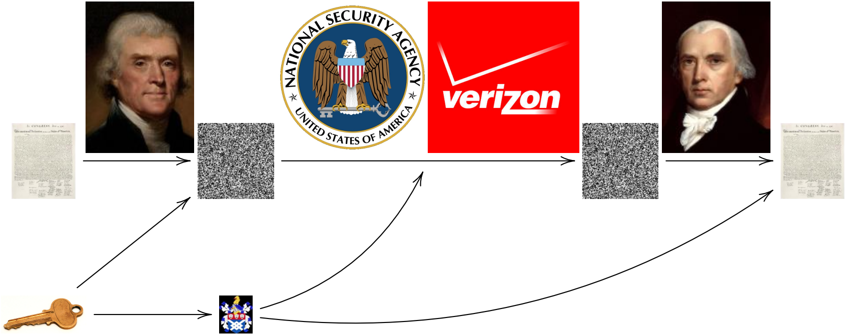
Security analysis

- Some papers studying algorithms for attackers:
  1962 Prange; 1981 Omura; 1988 Lee–Brickell; 1988 Leon; 1989 Krouk;
  1989 Stern; 1989 Dumer; 1990 Coffey–Goodman; 1990 van Tilburg;
  1991 Dumer; 1991 Coffey–Goodman–Farrell; 1993 Chabanne–Courteau;
  1993 Chabaud; 1994 van Tilburg; 1994 Canteaut–Chabanne;
  1998 Canteaut–Chabaud; 1998 Canteaut–Sendrier;
  2008 Bernstein–Lange–Peters; 2009 Bernstein–Lange–Peters–van Tilborg;
  2009 Bernstein (post-quantum); 2009 Finiasz–Sendrier;
  2010 Bernstein–Lange–Peters; 2011 May–Meurer–Thomae;
  2011 Becker–Coron–Joux; 2012 Becker–Joux–May–Meurer;
  2013 Bernstein–Jeffery–Lange–Meurer (post-quantum);
  2015 May–Ozerov.
- 256 KB public key for 2^{146} pre-quantum security.
- 512 KB public key for 2^{187} pre-quantum security.
- 1024 KB public key for 2^{263} pre-quantum security.

Security analysis

- Some papers studying algorithms for attackers:
  1962 Prange; 1981 Omura; 1988 Lee–Brickell; 1988 Leon; 1989 Krouk;
  1989 Stern; 1989 Dumer; 1990 Coffey–Goodman; 1990 van Tilburg;
  1991 Dumer; 1991 Coffey–Goodman–Farrell; 1993 Chabanne–Courteau;
  1993 Chabaud; 1994 van Tilburg; 1994 Canteaut–Chabanne;
  1998 Canteaut–Chabaud; 1998 Canteaut–Sendrier;
  2008 Bernstein–Lange–Peters; 2009 Bernstein–Lange–Peters–van Tilborg;
  2009 Bernstein (post-quantum); 2009 Finiasz–Sendrier;
  2010 Bernstein–Lange–Peters; 2011 May–Meurer–Thomae;
  2011 Becker–Coron–Joux; 2012 Becker–Joux–May–Meurer;
  2013 Bernstein–Jeffery–Lange–Meurer (post-quantum);
  2015 May–Ozerov.
- 256 KB public key for 2^{146} pre-quantum security.
- 512 KB public key for 2^{187} pre-quantum security.
- 1024 KB public key for 2^{263} pre-quantum security.
- Post-quantum (Grover): below 2^{263}, above 2^{131}.

Post-quantum public-key signatures: hash-based



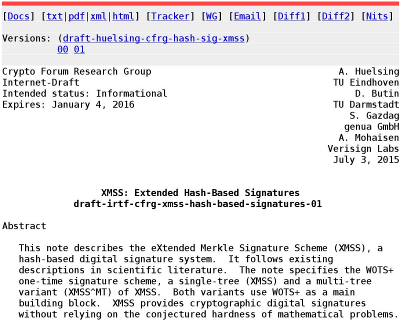
- Secret key , public key .
- Only one prerequisite: a good hash function, e.g. SHA3-512, . . .
  Hash functions map long strings to fixed-length strings.

  Signature schemes use hash functions in handling .
- Old idea: 1979 Lamport one-time signatures.
- 1979 Merkle extends to more signatures.

Pros and cons

Pros:

- Post quantum
- Only need secure hash function
- Small public key
- Security well understood
- Fast
- Proposed for standards: https://tools.ietf.org/html/draft-irtf-cfrg-xmss-hash-based-signatures-01



[Docs] [txt|pdf|xml|html] [Tracker] [WG] [Email] [Diff1] [Diff2] [Nits]

Versions: (draft-huelsing-cfrg-hash-sig-xmss)
00 01

```
Crypto Forum Research Group                                  A. Huelsing
Internet-Draft                                             TU Eindhoven
Intended status: Informational                                  D. Butin
Expires: January 4, 2016                                  TU Darmstadt
                                                              S. Gazdag
                                                             genua GmbH
                                                            A. Mohaisen
                                                          Verisign Labs
                                                           July 3, 2015
```

XMSS: Extended Hash-Based Signatures
draft-irtf-cfrg-xmss-hash-based-signatures-01

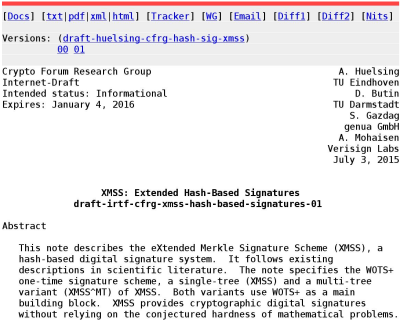
Abstract

This note describes the eXtended Merkle Signature Scheme (XMSS), a hash-based digital signature system. It follows existing descriptions in scientific literature. The note specifies the WOTS+ one-time signature scheme, a single-tree (XMSS) and a multi-tree variant (XMSS^MT) of XMSS. Both variants use WOTS+ as a main building block. XMSS provides cryptographic digital signatures without relying on the conjectured hardness of mathematical problems.

Pros and cons

Pros:

- Post quantum
- Only need secure hash function
- Small public key
- Security well understood
- Fast
- Proposed for standards: https://tools.ietf.org/html/draft-irtf-cfrg-xmss-hash-based-signatures-01



```
[Docs] [txt|pdf|xml|html] [Tracker] [WG] [Email] [Diff1] [Diff2] [Nits]

Versions: (draft-huelsing-cfrg-hash-sig-xmss)
          00 01

Crypto Forum Research Group                                  A. Huelsing
Internet-Draft                                             TU Eindhoven
Intended status: Informational                                  D. Butin
Expires: January 4, 2016                                  TU Darmstadt
                                                              S. Gazdag
                                                             genua GmbH
                                                            A. Mohaisen
                                                          Verisign Labs
                                                           July 3, 2015


                   XMSS: Extended Hash-Based Signatures
              draft-irtf-cfrg-xmss-hash-based-signatures-01

Abstract

   This note describes the eXtended Merkle Signature Scheme (XMSS), a
   hash-based digital signature system.  It follows existing
   descriptions in scientific literature.  The note specifies the WOTS+
   one-time signature scheme, a single-tree (XMSS) and a multi-tree
   variant (XMSS^MT) of XMSS.  Both variants use WOTS+ as a main
   building block.  XMSS provides cryptographic digital signatures
   without relying on the conjectured hardness of mathematical problems.
```

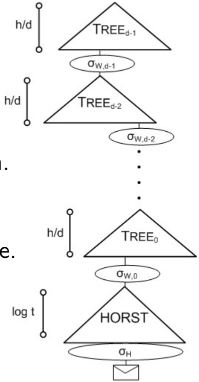
Cons:

- Biggish signature
- Stateful
  Adam Langley "for most environments it's a huge foot-cannon."

ELIMINATE
THE STATE

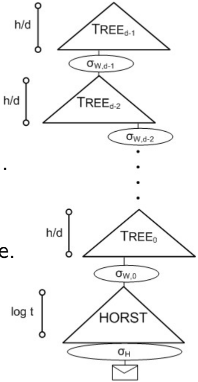
Stateless hash-based signatures

- Idea from 1987 Goldreich:
  - Signer builds huge tree of certificate authorities.
  - Signature includes certificate chain.
  - Each CA is a hash of master secret and tree position. This is deterministic, so don't need to store results.
  - **Random** bottom-level CA signs message. Many bottom-level CAs, so one-time signature is safe.

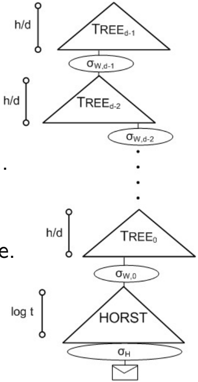


Stateless hash-based signatures

- Idea from 1987 Goldreich:
  - Signer builds huge tree of certificate authorities.
  - Signature includes certificate chain.
  - Each CA is a hash of master secret and tree position. This is deterministic, so don't need to store results.
  - **Random** bottom-level CA signs message. Many bottom-level CAs, so one-time signature is safe.
- 0.6 MB: Goldreich's signature with good 1-time signature scheme.
- 1.2 MB: average Debian package size.
- 1.8 MB: average web page in Alexa Top 1000000.



Stateless hash-based signatures



- Idea from 1987 Goldreich:
  - Signer builds huge tree of certificate authorities.
  - Signature includes certificate chain.
  - Each CA is a hash of master secret and tree position. This is deterministic, so don't need to store results.
  - **Random** bottom-level CA signs message. Many bottom-level CAs, so one-time signature is safe.
- 0.6 MB: Goldreich's signature with good 1-time signature scheme.
- 1.2 MB: average Debian package size.
- 1.8 MB: average web page in Alexa Top 1000000.
- 0.041 MB: SPHINCS signature, new optimization of Goldreich. Modular, guaranteed as strong as its components (hash, PRNG). Well-known components chosen for 2^{128} post-quantum security. sphincs.cr.yp.to

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.
  - Talks: Security in Times of Surveillance 2014, 2015 and Post-Snowden Cryptography
  - Last week tonight: Encryption by John Oliver
  - Thomas Jefferson and Apple versus the FBI post by 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 systems.
- `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.