

Post-Quantum Cryptography and Standardization

Tanja Lange

Eindhoven University of Technology

May 21, 2024

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-

Post-quantum cryptography:

Post-quantum cryptography:

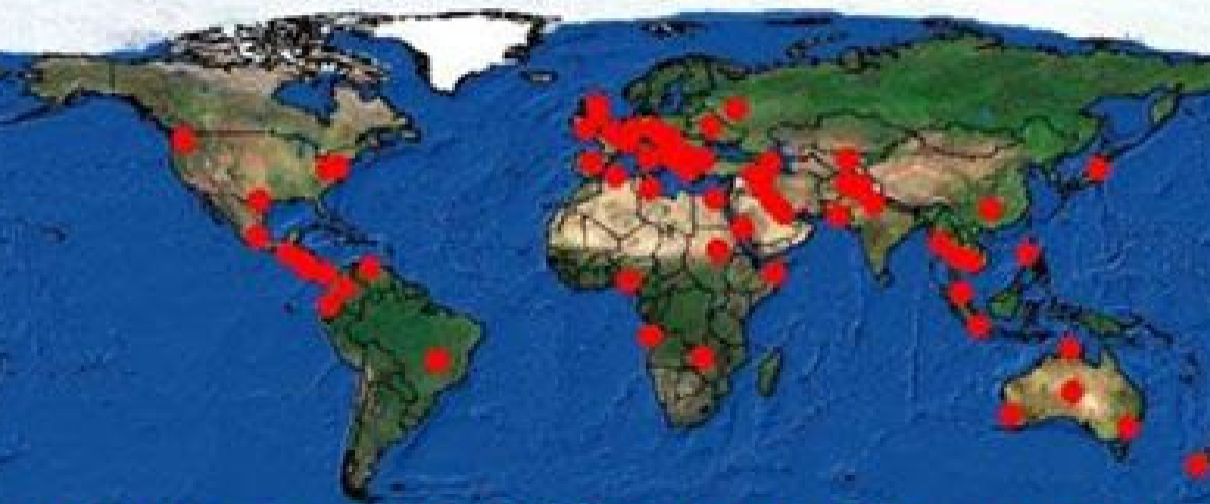
Algorithmic cryptography with attack
model quantum cryptanalysis

Why now?

Why now?

Store now, decrypt later

Where is X-KEYSCORE?



2018 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>

2018 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.”

2018 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.nationalacademies.org/read/25196/chapter/1>.

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 and signatures.
- ▶ Lattice-based encryption and signatures.
- ▶ Multivariate-quadratic encryption and signatures.
- ▶ Symmetric cryptography.

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

Stateful hash-based signatures

- ▶ 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 plaintext.
- ▶ Old idea: 1979 Lamport one-time signatures.
- ▶ 1979 Merkle extends to more signatures.

Pros:

- ▶ Post quantum
- ▶ Only need secure hash function
- ▶ Security well understood
- ▶ Fast

Cons:

- ▶ Biggish signature though some tradeoffs possible
- ▶ Stateful, i.e., ever reusing a subkey breaks security. Adam Langley “for most environments it’s a huge foot-cannon.”

Stateful hash-based signatures

- ▶ 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 plaintext.
- ▶ Old idea: 1979 Lamport one-time signatures.
- ▶ 1979 Merkle extends to more signatures.

Pros:

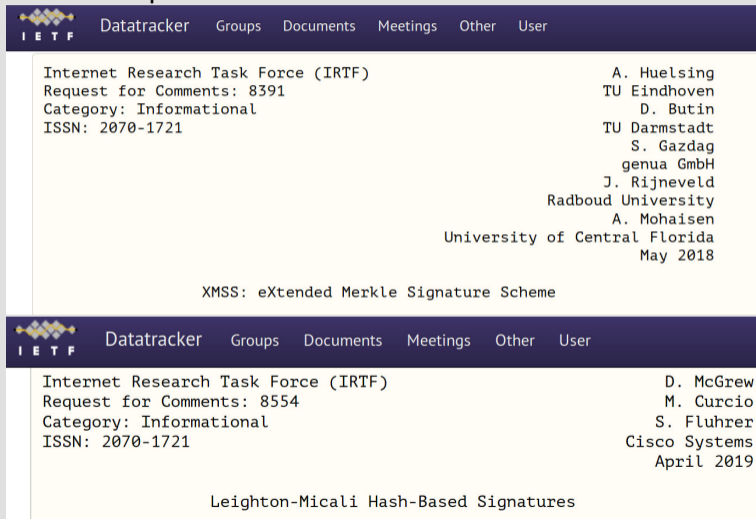
- ▶ Post quantum
- ▶ Only need secure hash function
- ▶ Security well understood
- ▶ Fast
- ▶ We can count: OS update, code signing, . . . naturally keep state.

Cons:

- ▶ Biggish signature though some tradeoffs possible
- ▶ Stateful, i.e., ever reusing a subkey breaks security. Adam Langley “for most environments it’s a huge foot-cannon.”

Standardization progress of hash-based signatures

- ▶ CFRG has published 2 RFCs: [RFC 8391 XMSS](#) and [RFC 8554 LMS](#)



The image shows two screenshots of the IETF Datatracker website. The top screenshot displays the details for RFC 8391, titled 'XMSS: eXtended Merkle Signature Scheme'. The bottom screenshot displays the details for RFC 8554, titled 'Leighton-Micali Hash-Based Signatures'. Both screenshots show the document title, request for comments number, category, ISSN, and the authors' names and affiliations.

Top Screenshot (RFC 8391):

Internet Research Task Force (IRTF)
Request for Comments: 8391
Category: Informational
ISSN: 2070-1721

A. Huelsing
TU Eindhoven
D. Butin
TU Darmstadt
S. Gazdag
genua GmbH
J. Rijnveld
Radboud University
A. Mohaisen
University of Central Florida
May 2018

XMSS: eXtended Merkle Signature Scheme

Bottom Screenshot (RFC 8554):

Internet Research Task Force (IRTF)
Request for Comments: 8554
Category: Informational
ISSN: 2070-1721

D. McGrew
M. Curcio
S. Fluhrer
Cisco Systems
April 2019

Leighton-Micali Hash-Based Signatures

Standardization progress of hash-based signatures

- ▶ CFRG has published 2 RFCs: [RFC 8391 XMSS](#) and [RFC 8554 LMS](#)
- ▶ NIST has published [NIST SP 800-208](#) Recommendation for Stateful Hash-Based Signature Schemes covering XMSS and LMS..



Standardization progress of hash-based signatures

- ▶ CFRG has published 2 RFCs: [RFC 8391 XMSS](#) and [RFC 8554 LMS](#)
- ▶ NIST has published [NIST SP 800-208](#) Recommendation for Stateful Hash-Based Signature Schemes covering XMSS and LMS..



- ▶ ISO SC27 JTC1 WG2 has [14888-4 Stateful hash-based mechanisms](#) under publication.

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

NIST Post-quantum “competition”

- ▶ 30 November 2017: NIST receives 82 submissions.
- ▶ 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.

NIST Post-quantum “competition”

- ▶ 30 November 2017: NIST receives 82 submissions.
- ▶ 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.
- ▶ 22 July 2020: NIST narrows further to 15 Round 3 candidates – Finalists: 4 KEMs, 3 signatures; alternates: 5 KEMs, 3 signatures.

NIST Post-quantum “competition”

- ▶ 30 November 2017: NIST receives 82 submissions.
- ▶ 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.
- ▶ 22 July 2020: NIST narrows further to 15 Round 3 candidates – Finalists: 4 KEMs, 3 signatures; alternates: 5 KEMs, 3 signatures.
- ▶ 2021 “Late December”: NIST announces selection.

NIST Post-quantum “competition”

- ▶ 30 November 2017: NIST receives 82 submissions.
- ▶ 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.
- ▶ 22 July 2020: NIST narrows further to 15 Round 3 candidates – Finalists: 4 KEMs, 3 signatures; alternates: 5 KEMs, 3 signatures.
- ▶ ~~2021~~ 2022 “not later than the end of March” NIST announces selection.

NIST Post-quantum “competition”

- ▶ 30 November 2017: NIST receives 82 submissions.
- ▶ 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.
- ▶ 22 July 2020: NIST narrows further to 15 Round 3 candidates – Finalists: 4 KEMs, 3 signatures; alternates: 5 KEMs, 3 signatures.
- ▶ ~~2021~~ 2022 “not later than the end of March” July NIST announces winners.

NIST Post-quantum “competition”

- ▶ 30 November 2017: NIST receives 82 submissions.
- ▶ 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.
- ▶ 22 July 2020: NIST narrows further to 15 Round 3 candidates – Finalists: 4 KEMs, 3 signatures; alternates: 5 KEMs, 3 signatures.
- ▶ ~~2021~~ 2022 “not later than the end of March” July NIST announces winners.
- ▶ Start of 4th round for 4 more KEMs.

NIST Post-quantum “competition”

- ▶ 30 November 2017: NIST receives 82 submissions.
- ▶ 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.
- ▶ 22 July 2020: NIST narrows further to 15 Round 3 candidates – Finalists: 4 KEMs, 3 signatures; alternates: 5 KEMs, 3 signatures.
- ▶ ~~2021~~ 2022 “not later than the end of March” July NIST announces winners.
- ▶ Start of 4th round for 4 more KEMs.
- ▶ 24 August 2023: NIST posts draft FIPS standards for
 - ▶ FIPS 203 ML-KEM (Kyber), based on lattices
 - ▶ FIPS 204 ML-DSA (Dilithium), based on lattices
 - ▶ FIPS 205 SLH-DSA (SPHINCS+), based on hash functions

A draft for Falcon (lattices) is still forthcoming.

NIST Post-quantum “competition”

- ▶ 30 November 2017: NIST receives 82 submissions.
- ▶ 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.
- ▶ 22 July 2020: NIST narrows further to 15 Round 3 candidates – Finalists: 4 KEMs, 3 signatures; alternates: 5 KEMs, 3 signatures.
- ▶ ~~2021~~ 2022 “not later than the end of March” July NIST announces winners.
- ▶ Start of 4th round for 4 more KEMs.
- ▶ 24 August 2023: NIST posts draft FIPS standards for
 - ▶ FIPS 203 ML-KEM (Kyber), based on lattices
 - ▶ FIPS 204 ML-DSA (Dilithium), based on lattices
 - ▶ FIPS 205 SLH-DSA (SPHINCS+), based on hash functionsA draft for Falcon (lattices) is still forthcoming.
- ▶ 2024?: NIST/FIPS issues standards for PQC.

Beyond NIST

- ▶ Internet Engineering Task Force (IETF) is working on drafts for various schemes

- ▶ Kyber
- ▶ Classic McEliece,
- ▶ NTRU (currently expired),
- ▶ Streamlined NTRU Prime (currently expired),

and methods for combining them with elliptic-curve crypto

- ▶ General KEM combiners,
- ▶ Kyber+Curve25519 hybrid called X-Wing,
- ▶ Combiner for Kyber/McEliece/NTRU Prime + ECC called Chempat,
- ▶ NTRU Prime+X25519,

as well as some specific to protocols, e.g. McEliece for SSH.

Beyond NIST

- ▶ Internet Engineering Task Force (IETF) is working on drafts for various schemes

- ▶ Kyber
- ▶ Classic McEliece,
- ▶ NTRU (currently expired),
- ▶ Streamlined NTRU Prime (currently expired),

and methods for combining them with elliptic-curve crypto

- ▶ General KEM combiners,
- ▶ Kyber+Curve25519 hybrid called X-Wing,
- ▶ Combiner for Kyber/McEliece/NTRU Prime + ECC called Chempat,
- ▶ NTRU Prime+X25519,

as well as some specific to protocols, e.g. McEliece for SSH.

- ▶ ISO 18033-2 Asymmetric ciphers, Amendment 2 in working-draft stage, reportedly covering Classic McEliece, FrodoKEM, and Kyber/ML-KEM.

Where to go from here?

- ▶ Some deployment needs interoperability and agreements/standards. This is certainly true for the financial industry. But much data and traffic could be protected now already.

Where to go from here?

- ▶ Some deployment needs interoperability and agreements/standards. This is certainly true for the financial industry. But much data and traffic could be protected now already.
- ▶ Migration needs testing phase and safety nets. Dangerous to remove pre-quantum crypto now & no harm keeping.
- ▶ Lots of recommendations available already, to highlight two from the European Union Agency for Cybersecurity (ENISA)
 - ▶ Current state and quantum mitigation
 - ▶ Post-Quantum Cryptography – Integration study(Disclaimer: I contributed to these documents.)
- ▶ Several positive signs of awareness and progress in migration.



Adoption & Usage

Worldwide



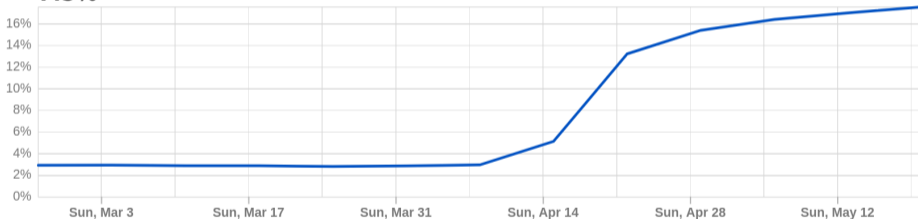
Last 3 months



Post-Quantum Encryption Adoption

Post-Quantum encrypted share of HTTPS request traffic ?

— PQ Encrypted

7.5%

That's 16.9% of all HTTPS connections, not just TLS 1.3.

PQC support now default in Chrome and Edge; can turn on in Firefox.

<https://radar.cloudflare.com/adoption-and-usage?dateRange=12w>

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

Further information

- ▶ NIST PQC competition.
- ▶ Quantum Threat Timeline, 2019; 2021 update.
- ▶ Status of quantum computer development (by German BSI).
- ▶ ENISA studies: Post-quantum cryptography: Integration study, Post-quantum cryptography: current state and quantum mitigation
- ▶ YouTube channel Tanja Lange: Post-quantum cryptography.
- ▶ <https://2017.pqcrypto.org/school>: PQCRYPTO summer school with 21 lectures on video; slides; exercises.
- ▶ Less math, more perspective: <https://2017.pqcrypto.org/exec> and <https://pqcschool.org>.
- ▶ <https://pqcrypto.org> our overview page.
- ▶ PQCrypto 2016, 2017, 2018, 2019, 2020, 2021, 2022, 2023, 2024 (upcoming) slides + videos.
- ▶ PQCRYPTO recommendations.