Update on post-quantum cryptography

Tanja Lange

Eindhoven University of Technology

11 December 2019

Cryptography

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

Sender
"Alice"

Untrustworthy network
"Eve"

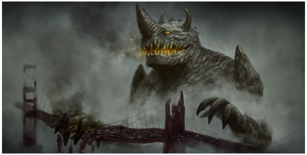
Receiver
"Bob"

- Literal meaning of cryptography: "secret writing".
- Security goal #1: **Confidentiality** despite Eve's espionage.
- Security goal #2: **Integrity**, i.e., recognizing Eve's sabotage.

Post-quantum cryptography

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

Sender
"Alice"



"Eve"
with a quantum computer

Receiver
"Bob"

- Literal meaning of cryptography: "secret writing".
- Security goal #1: **Confidentiality** despite Eve's espionage.
- Security goal #2: **Integrity**, i.e., recognizing Eve's sabotage.
- Post-quantum cryptography adds to the model that Eve has a quantum computer.

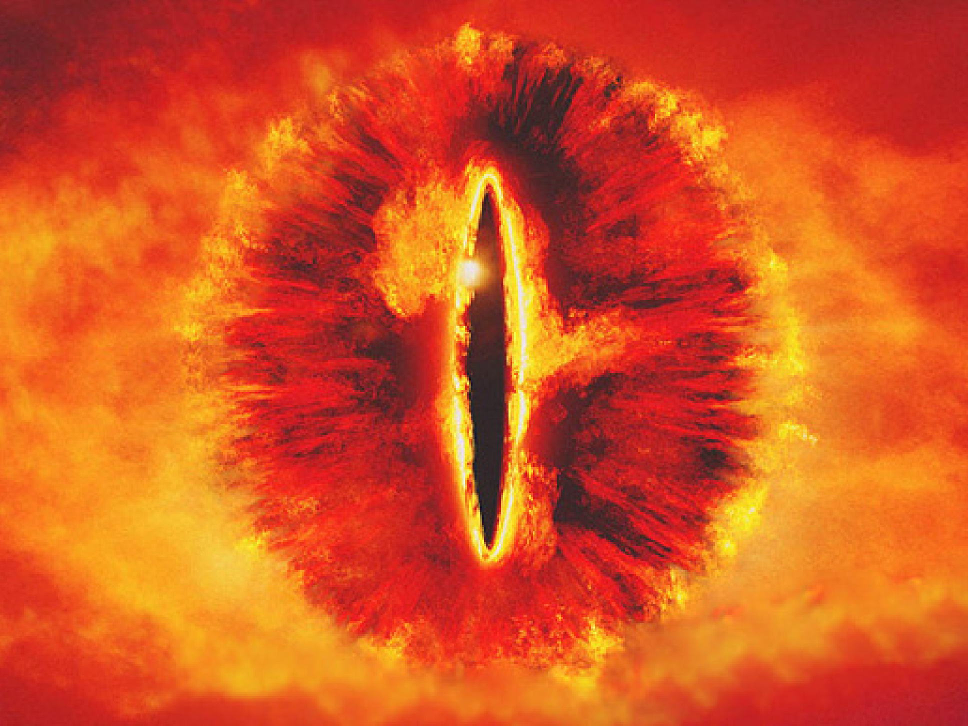
Post-quantum cryptography:
Cryptography designed
under the assumption that
the **attacker** (not the user!)
has a large quantum computer.

History of post-quantum cryptography

- 2003 Daniel J. Bernstein introduces term Post-quantum cryptography.
- PQCrypto 2006: International Workshop on Post-Quantum Cryptography.

History of post-quantum cryptography

- 2003 Daniel J. Bernstein introduces term Post-quantum cryptography.
- PQCrypto 2006: International Workshop on Post-Quantum Cryptography.
- PQCrypto 2008, PQCrypto 2010, PQCrypto 2011, PQCrypto 2013.
- 2014 EU publishes H2020 call including post-quantum crypto as topic.
- ETSI working group on "Quantum-safe" crypto.
- PQCrypto 2014.
- April 2015 NIST hosts first workshop on post-quantum cryptography
- August 2015 NSA wakes up



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.

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

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!". Or "NSA says NIST P-384 is post-quantum secure".

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!". Or "NSA says NIST P-384 is post-quantum secure". Or "NSA has abandoned ECC."

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

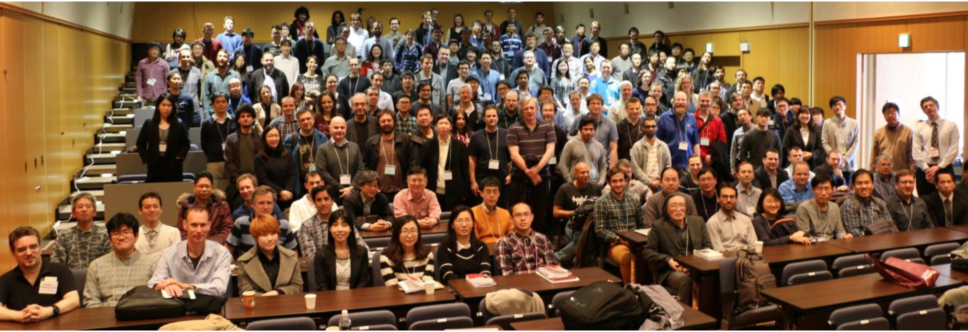
> *IAD will initiate a transition to quantum resistant algorithms in the not too distant future.*

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!". Or "NSA says NIST P-384 is post-quantum secure". Or "NSA has abandoned ECC." Or "The NSA can break lattices and wants you to use them."

Post-quantum becoming mainstream

- PQCrypto 2016: 22–26 Feb in Fukuoka, Japan, $>$ 200 people



- 2016: Every agency posts something (NCSC UK, NCSC NL, NSA).
- 2016: After public input, NIST calls for submissions to "Post-Quantum Cryptography Standardization Project". Solicits submissions on signatures and encryption (deadline Nov 2017).


pq
PQCrypto 2018
The Ninth International Conference on Post-Quantum Cryptography
Fort Lauderdale, Florida, April 9-11, 2018
Hilton

National Academy of Sciences (US)

4 December 2018: 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."

National Academy of Sciences (US)

4 December 2018: 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."

Systems expected to survive

- Code-based encryption: short ciphertexts and large public keys. Security based on the hardness of decoding random codes.
- Hash-based signatures: very solid security and small public keys. Require only a secure hash function (hard to find second preimages).
- Isogeny-based encryption: new kid on the block, promising short keys and ciphertexts and non-interactive key exchange. Systems rely on hardness of finding isogenies between elliptic curves over finite fields.
- Lattice-based encryption and signatures: possibility for balanced sizes. Security relies on finding short vectors in some (typically special) lattice.
- Multivariate-quadratic signatures: short signatures and large public keys. Systems rely on hardness of solving systems of multi-variate equations over finite fields.

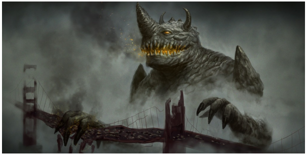
These are categories of mathematical problems;
individual systems may be insecure if the problem is not used correctly.

Post-quantum secret-key authenticated encryption

$$m \xrightarrow[k]{} c \longrightarrow c \xrightarrow[k]{} m$$

- Very easy solutions if secret key k is long uniform random string:
  - “One-time pad” for encryption.
  - “Wegman–Carter MAC” for authentication.
- AES-256: Standardized method to expand 256-bit k into string indistinguishable from long k.
- 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}.
- Some recent results assume attacker has quantum access to computation, then some systems are weaker . . . but I’d know if my laptop had turned into a quantum computer.

Post-quantum secret-key authenticated encryption



$$m \xrightarrow[k]{} c \xrightarrow{\qquad\qquad\qquad} c \xrightarrow[k]{} m$$

- Very easy solutions if secret key k is long uniform random string:
  - "One-time pad" for encryption.
  - "Wegman–Carter MAC" for authentication.
- AES-256: Standardized method to expand 256-bit k into string indistinguishable from long k.
- 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}.
- Some recent results assume attacker has quantum access to computation, then some systems are weaker ... but I'd know if my laptop had turned into a quantum computer.

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.

Overview from Dustin Moody's (NIST) talk at Asiacrypt 2017:

	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**

1.5 years ago in the NIST competition . . .

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.

1.5 years ago . . . there were already attacks

By end of 2017: 8 out of 69 submissions attacked.

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 less security than claimed; some really broken; some attack scripts.

Do cryptographers have any idea what they're doing?

By end of 2018: 22 out of 69 submissions attacked.

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 less security than claimed; some really broken; some attack scripts.

Some attempts to explain the situation

"What's safe is lattice-based cryptography." — Are you sure about that?

Some attempts to explain the situation

"What's safe is lattice-based cryptography." — Are you sure about that?

Lattice-based submissions: Compact LWE. CRYSTALS-DILITHIUM. CRYSTALS-KYBER. Ding Key Exchange. DRS. EMBLEM and R.EMBLEM. FALCON. FrodoKEM. HILA5. KINDI. LAC. LIMA. Lizard. LOTUS. NewHope. NTRUEncrypt. NTRU-HRSS-KEM. NTRU Prime. Odd Manhattan. OKCN/AKCN/CNKE. pqNTRUSign. qTESLA. Round2. SABER. Titanium.

Some attempts to explain the situation

“What’s safe is lattice-based cryptography.” — Are you sure about that?

Lattice-based submissions: Compact LWE. CRYSTALS-DILITHIUM. CRYSTALS-KYBER. Ding Key Exchange. DRS. EMBLEM and R.EMBLEM. FALCON. FrodoKEM. HILA5. KINDI. LAC. LIMA. Lizard. LOTUS. NewHope. NTRUEncrypt. NTRU-HRSS-KEM. NTRU Prime. Odd Manhattan. OKCN/AKCN/CNKE. pqNTRUSign. qTESLA. Round2. SABER. Titanium.

Many recent papers improving lattice attacks.
e.g. D’Anvers–Vercauteren–Verbauwhede papers in November+December: “On the impact of decryption failures on the security of LWE/LWR based schemes”; “The impact of error dependencies on Ring/Mod-LWE/LWR based schemes”.

Some attempts to explain the situation

"What's safe is using the portfolio from the European PQCRYPTO project." — Are you sure about that?

Some attempts to explain the situation

“What’s safe is using the portfolio from the European PQCRYPTO project.” — Are you sure about that?

The portfolio: BIG QUAKE. BIKE. Classic McEliece. CRYSTALS-DILITHIUM. CRYSTALS-KYBER. DAGS. FrodoKEM. Gui. KINDI. LUOV. MQDSS. NewHope. NTRU-HRSS-KEM. NTRU Prime. Picnic. qTESLA. Rainbow. Ramstake. SABER. SPHINCS+.

Some attempts to explain the situation

"What's safe is using the portfolio from the European PQCRYPTO project." — Are you sure about that?

The portfolio: BIG QUAKE. BIKE. Classic McEliece. CRYSTALS-DILITHIUM. CRYSTALS-KYBER. DAGS. FrodoKEM. Gui. KINDI. LUOV. MQDSS. NewHope. NTRU-HRSS-KEM. NTRU Prime. Picnic. qTESLA. Rainbow. Ramstake. SABER. SPHINCS+.

69 submissions = **denial-of-service attack against security evaluation**. Maybe cryptanalysts focused on submissions from outside the project.

Do cryptographers have any idea what they're doing?

By end of 2018: 22 out of 69 submissions attacked.

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 less security than claimed; some really broken; some attack scripts.

NIST round two

30 January 2019: 26 candidates retained for second round.

. BIKE. . Classic McEliece. .
CRYSTALS-DILITHIUM. CRYSTALS-KYBER. .
. . . . .
. FALCON. FrodoKEM. GeMSS. .
. . . HILA5. . . HQC.
. LAC. LAKE. LEDAkem. LEDApkc. . . .
LOCKER. . LUOV. . . MQDSS.
NewHope. NTRUEncrypt. . NTRU-HRSS-KEM. NTRU
Prime. NTS-KEM. . .
Ouroboros-R. Picnic. . . .
. qTESLA. . Rainbow. . .
. Round2. RQC. . SABER. SIKE. SPHINCS+. .
Three Bears. . .

Some less security than claimed; some really broken; some attack scripts.
Merges: HILA5 & Round2; LAKE, LOCKER, & Ouroboros-R;
LEDAkem & LEDApkc; NTRUEncrypt & NTRU-HRSS-KEM.

How to learn more and get involved

- NIST welcomes input on use cases.
- ISO JTC 1/ SC 27 WG 2 will soon post a standing document on PQC.
- Last page has a bunch of links.

On the fast track: hash-based signatures

IETF Datatracker Groups Documents Meetings Other User

```
Internet Research Task Force (IRTF)                          A. Huelsing
Request for Comments: 8391                                 TU Eindhoven
Category: Informational                                         D. Butin
ISSN: 2070-1721                                            TU Darmstadt
                                                               S. Gazdag
                                                              genua GmbH
                                                            J. Rijneveld
                                                      Radboud University
                                                             A. Mohaisen
                                          University of Central Florida
                                                                May 2018

              XMSS: eXtended Merkle Signature Scheme
```

Pros:

- Security well understood
  1979 Lamport, 1979 Merkle
- Only need secure hash function
- Small public key, fast

Cons:

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

On the fast track: hash-based signatures

Datatracker Groups Documents Meetings Other User

```
Internet Research Task Force (IRTF)                          A. Huelsing
Request for Comments: 8391                                 TU Eindhoven
Category: Informational                                         D. Butin
ISSN: 2070-1721                                            TU Darmstadt
                                                               S. Gazdag
                                                              genua GmbH
                                                            J. Rijneveld
                                                      Radboud University
                                                             A. Mohaisen
                                          University of Central Florida
                                                                May 2018

              XMSS: eXtended Merkle Signature Scheme
```

Pros:

- Security well understood
  1979 Lamport, 1979 Merkle
- Only need secure hash function
- Small public key, fast
- We can count: OS update, code signing, . . . do keep state.

Cons:

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

Standardization progress

- CFRG has published 2 RFCs: RFC 8391 and RFC 8554

IETF Datatracker Groups Documents Meetings Other User

```
Internet Research Task Force (IRTF)                          A. Huelsing
Request for Comments: 8391                                 TU Eindhoven
Category: Informational                                         D. Butin
ISSN: 2070-1721                                             TU Darmstadt
                                                               S. Gazdag
                                                              genua GmbH
                                                            J. Rijneveld
                                                      Radboud University
                                                             A. Mohaisen
                                         University of Central Florida
                                                                May 2018

               XMSS: eXtended Merkle Signature Scheme
```

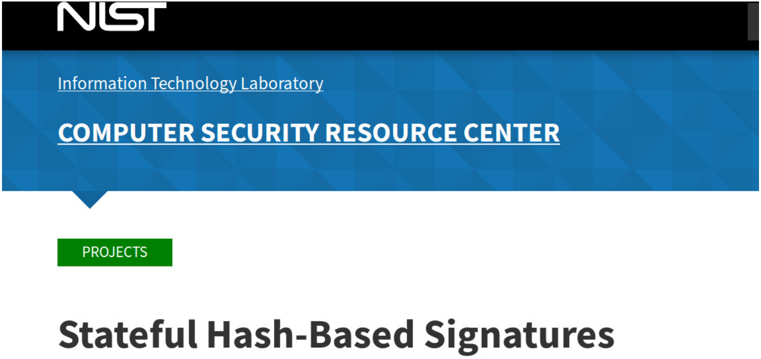
IETF Datatracker Groups Documents Meetings Other User

```
Internet Research Task Force (IRTF)                            D. McGrew
Request for Comments: 8554                                     M. Curcio
Category: Informational                                       S. Fluhrer
ISSN: 2070-1721                                            Cisco Systems
                                                              April 2019

               Leighton-Micali Hash-Based Signatures
```

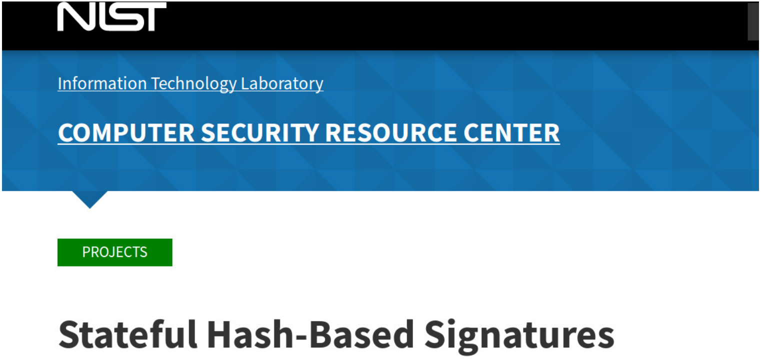
Standardization progress

- CFRG has published 2 RFCs: RFC 8391 and RFC 8554
- NIST has gone through two rounds of requests for public input, most are positive and recommend standardizing XMSS and LMS. Only concern is about statefulness in general.



Standardization progress

- CFRG has published 2 RFCs: RFC 8391 and RFC 8554
- NIST has gone through two rounds of requests for public input, most are positive and recommend standardizing XMSS and LMS. Only concern is about statefulness in general.



- ISO SC27 JTC1 WG2 has started a study period on stateful hash-based signatures.

Links

- NIST PQC competition https://csrc.nist.gov/Projects/Post-Quantum-Cryptography
- Executive summer school on PQC in Eindhoven https://pqcschool.org/index.html.
- PQCRYPTO EU project https://pqcrypto.eu.org:
  - Expert recommendations.
  - Free software libraries (libpqcrypto, pqm4, pqhw).
  - Lots of reports, scientific papers, (overview) presentations.
- PQCRYPTO summer school 2017 with 21 lectures on video + slides + exercises. https://2017.pqcrypto.org/school:
- Executive school 2017 (12 lectures), less math, more overview. https://2017.pqcrypto.org/exec
- PQCrypto 2019 conference.
- PQCrypto 2018 conference.
- PQCrypto 2017 conference.
- PQCrypto 2016 with slides and videos from lectures + school.
- https://pqcrypto.org: Our survey site.
  - Many pointers: e.g., PQCrypto conference series.
  - Bibliography for 4 major PQC systems.