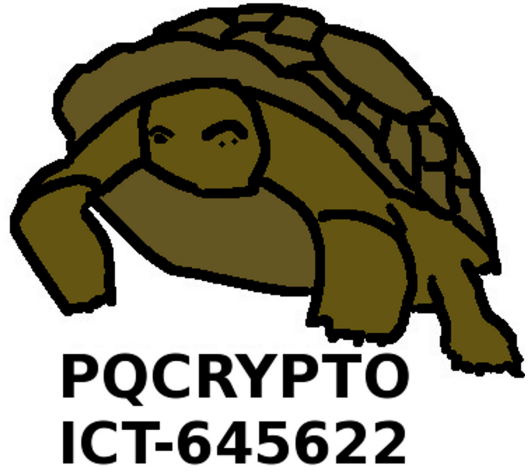
The H2020 PQCRYPTO project, an update

Andreas Hülsing, TU/e

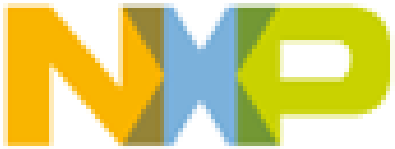


20 September 2016

4th ETSI/IQC Workshop on Quantum-Safe Cryptography

Post-Quantum Cryptography for Long-term Security

- Project funded by EU in Horizon 2020.
- Starting date 1 March 2015, runs for 3 years.
- 11 partners from academia and industry, TU/e is coordinator



What does PQCRYPTO mean for you?

- Expert recommendations for post-quantum secure cryptosystems.
- Recommended systems will get faster/smaller as result of PQCRYPTO research.
- More benchmarking to compare cryptosystems.
- Cryptographic libraries will be made freely available for several computer architectures.
- Find more information online at http://pqcrypto.eu.org/.
- Soon many deliverables.
- Follow us on twitter https://twitter.com/pqc_eu.

Initial recommendations (September 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-, ...

What happened since then?

- $>$ 52 publications
- 1 Internet Draft
- $>$ 44 presentations
- 1 Workshop

Selected highlights

(only minimally subjective)

Hash-based signatures

Stateful

- Internet Draft **XMSS: Extended Hash-Based Signatures**.
- Accompanying paper with security reduction & analysis of generic quantum attacks.
- Several reference implementations available.

Stateless

- **ARMed SPHINCS**: Implementation on ARM Cortex M3.
- Short, fixed-size input hash functions:
  - **Haraka**
  - **Simpira**

Lattice-based key exchange

NewHope

- Lattice-based KEX.
- Better suited error distribution, improved error-reconciliation mechanism, quantum-secure parameters, constant-time high speed implementation.
- Winner of the 2016 Internet Defense Prize (100,000 USD).
- Test deployment in Google Chrome.

More recent

- Frodo: Take off the ring!
- NewHope-Simple.

Code-based encryption

QcBits

- Fast, constant-time implementation of QC-MDPC encryption (but only 80-bit pre-quantum security).
- Asiacrypt2016 paper by Johansson, Stankovski, Guouses uses decryption failures to break QC-MDPC encryption.
- For QCBits, decryption failures less frequent than 10^{-8} (but can be constructed).
- New theoretical result reducing error probability to 2^{-128}.

McBits Single Message

- Fast, constant-time implementation of Niederreiter with binary Goppa codes.
- not published yet.

MQ-based signatures

MQ-DSS

- First signature scheme with security reduction from MQ-Problem (and hash function / PRF properties).
- Parameters for 128bit security against quantum attacks.
- High-speed constant-time implementation.

Of course there is more...

- Several works on cryptanalysis.
- Several works on implementations.
- Several works on quantum security.
- And of course several more works on constructions...

PQCrypto 2017, June 26-28

- Conference location Utrecht,
  now looking for bigger venue ;-)
- **Dates:**
  - School: June 19-23,
  - Executive school: June 22-23,
  - Conference: June 26-28.
- AMS airport Schiphol is 30 min by train (4 $\times$ per hour)
- Other airports: Rotterdam, Eindhoven, Düsseldorf.
- Direct ICEs from FRA.
- School location will be Eindhoven.
  Travel time Eindhoven–Utrecht: 50 min.

Utrecht, the Netherlands

Utrecht is easy to reach

Utrecht, the Netherlands

Utrecht is home to Miffy

Miffy is called Nijntje in the Netherlands. http://nijntjemuseum.nl is located in the museums district of Utrecht.

Technische Universiteit Eindhoven

Eindhoven, the Netherlands

Thank you

- All papers can be found online at http://pqcrypto.eu.org/papers.html.
- For previous works, author lists etc.pp. see papers.
- Find more information online at http://pqcrypto.eu.org/.
- Follow us on twitter https://twitter.com/pqc_eu.