The H2020 PQCRYPTO project

Andreas Hülsing

PQCRYPTO
ICT-645622

05 October 2015

3rd 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

Impact of PQCRYPTO

- All currently used public-key systems on the Internet are broken by quantum computers.
- Today's encrypted communication can be (and is being!) stored by attackers and can be decrypted later with quantum computer – think of medical records, legal proceedings, and state secrets.
- Post-quantum secure cryptosystems exist but are under-researched – we can recommend secure systems now, but they are big and slow

Impact of PQCRYPTO

- All currently used public-key systems on the Internet are broken by quantum computers.
- Today's encrypted communication can be (and is being!) stored by attackers and can be decrypted later with quantum computer – think of medical records, legal proceedings, and state secrets.
- Post-quantum secure cryptosystems exist but are under-researched – we can recommend secure systems now, but they are big and slow hence the logo.

Impact of PQCRYPTO

- All currently used public-key systems on the Internet are broken by quantum computers.
- Today's encrypted communication can be (and is being!) stored by attackers and can be decrypted later with quantum computer – think of medical records, legal proceedings, and state secrets.
- Post-quantum secure cryptosystems exist but are under-researched – we can recommend secure systems now, but they are big and slow hence the logo.
- PQCRYPTO will design a portfolio of high-security post-quantum public-key systems, and will improve the speed of these systems, adapting to the different performance challenges of mobile devices, the cloud, and the Internet.
- PQCRYPTO will provide efficient implementations of high-security post-quantum cryptography for a broad spectrum of real-world applications.

Work packages

Technical work packages

- WP1: Post-quantum cryptography for small devices
  Leader: Tim Güneysu, co-leader: Peter Schwabe
- WP2: Post-quantum cryptography for the Internet
  Leader: Daniel J. Bernstein, co-leader: Bart Preneel
- WP3: Post-quantum cryptography for the cloud
  Leader: Nicolas Sendrier, co-leader: Lars Knudsen

Non-technical work packages

- WP4: Management and dissemination
  Leader: Tanja Lange
- WP5: Standardization
  Leader: Walter Fumy

WP1: Post-quantum cryptography for small devices

- Find post-quantum secure cryptosystems suitable for small devices in power and memory requirements (e.g. smart cards with 8-bit or 16-bit or 32-bit architectures, with different amounts of RAM, with or without coprocessors).
- Develop efficient implementations of these systems.
- Investigate and improve their security against implementation attacks.
- Deliverables include reference implementations and optimized implementations for software for platforms ranging from small 8-bit microcontrollers to more powerful 32-bit ARM processors.
- Deliverables also include FPGA and ASIC designs and physical security analysis.

WP2: Post-quantum cryptography for the Internet

- Find post-quantum secure cryptosystems suitable for busy Internet servers handling many clients simultaneously.
- Develop secure and efficient implementations.
- Integrate these systems into Internet protocols.
- Deliverables include software library for all common Internet platforms, including large server CPUs, smaller desktop and laptop CPUs, netbook CPUs (Atom, Bobcat, etc.), and smartphone CPUs (ARM).
- Aim is to get high-security post-quantum crypto ready for the Internet.

WP3: Post-quantum cryptography for the cloud

- Provide 50 years of protection for files that users store in the cloud, even if the cloud service providers are not trustworthy.
- Allow sharing and editing of cloud data under user-specified security policies.
- Support advanced cloud applications such as privacy-preserving keyword search.
- Work includes public-key and symmetric-key cryptography.
- Prioritize high security and speed over key size.

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/.
- Follow us on twitter https://twitter.com/pqc_eu.

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-, ...

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/.
- Follow us on twitter https://twitter.com/pqc_eu.