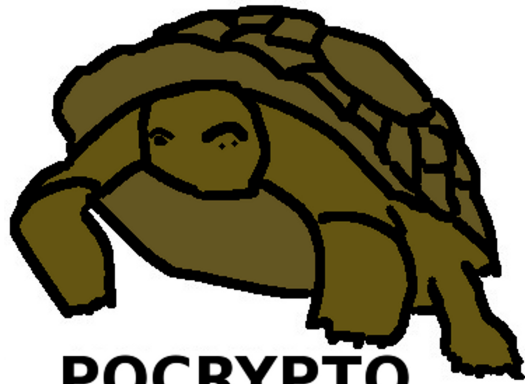
Post-quantum cryptography for long-term security
PQCRYPTO ICT-645622

Daniel J. Bernstein and Tanja Lange



11-15 April 2016

ISO 27 meeting in Tampa

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

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.

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. PQCRYPTO applies and is funded.
- PQCrypto 2014.
- April 2015: NIST hosts first workshop on post-quantum cryptography.
- August 2015: NSA makes announcement on post-quantum importance.
- September 2015: Initial recommendations by PQCRYPTO.
- PQCrypto 2016.
- New: NIST announces competition for post-quantum systems.

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: Wouter Castryck
- WP3: Post-quantum cryptography for the cloud
  Leader: Nicolas Sendrier, co-leader: Christian Rechberger

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.

General PQCRYPTO achievements

- September 2015: Initial recommendations for post-quantum cryptographic algorithms
  Consolidated recommendations for symmetric encryption & authentication and for public-key encryption and signatures.
  Widely picked up and discussed, incl. mention in Nature.
- Presentations (slides are online, some talks have videos).
  - presentations of PQCRYPTO.
  - general presentations of post-quantum cryptography.
  - presentations at (summer) schools.
  - focussed presentations of scientific results.
- Lots of papers with available pdf files.
- Upcoming events: PQCrypto conference and summer school in 2017; expecting more than 200 participants.
- Active twitter feed, follow us as `https://twitter.com/pqc_eu`.