PQCRYPTO project in the EU

Tanja Lange

3 April 2015

NIST Workshop on Cybersecurity in a Post-Quantum World
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

TU/e, technische universiteit eindhoven
BUNDES DRUCKEREI
Indra, INVENTEURS DU MONDE NUMERICA
KU LEUVEN
NXP
Radboud Universiteit
University of Haifa

Tanja Lange http://pqcrypto.eu.org

PQCRYPTO project in the EU
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?

- Events:
  - Workshop on post-quantum cryptography (Spring 2016? most likely later to avoid clashing with PQCrypto 2016)
  - Summer school on post-quantum cryptography (Spring 2017)
- More implementations, more benchmarking.
- More research manpower on post-quantum cryptography in Europe.
- Several partners have open positions.
- Find more information online at http://pqcrypto.eu.org/.
- Follow us on twitter https://twitter.com/pqc_eu.