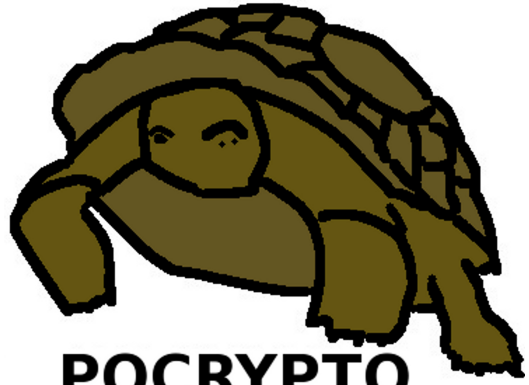
PQCRYPTO overview

Tanja Lange



28 June 2016

Scientific advisory board meeting

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 gets funded
- 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.

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 gets funded
- PQCrypto 2014.
- April 2015 NIST hosts first workshop on post-quantum cryptography
- August 2015 NSA wakes up
- September 2015: Initial recommendations by PQCRYPTO.
- PQCrypto 2016.
- 2016 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).
  - 7 presentations of PQCRYPTO.
  - 10 general presentations of post-quantum cryptography.
  - >6 presentations at (summer) schools.
  - >18 focussed presentations of scientific results.
- Lots of papers – 39 publications, 11 public preprints.
- Upcoming events: PQCrypto conference and summer school in 2017 (moved because of PQCrypto steering committee decision); expecting more than 200 participants.
- Active twitter feed `https://twitter.com/pqc_eu` with more than 700 followers.

PQCRYPTO press coverage

TU Eindhoven leads multi-million Euro project to protect data against quantum computers

April 23, 2015 (with matching releases by other partners).

At this moment all bets are off and it is unclear whether we will ever learn the outcome of this competition. Scientists at TU Eindhoven and elsewhere are developing technology that can resist attacks using quantum computers. These cryptosystems need to be in place before big quantum computers become a reality, which is expected some time after 2025. Even if the scientists win that race quantum computers can still decrypt communication that we encrypt today with current technologies if the attacker has retained this data.

- See http://pqcrypto.eu.org/press.html.
- Taken up internationally with 26 publications alone coming from the TUE announcement.

Quantum computers

A little bit, better

The Economist

After decades languishing in the laboratory, quantum computers are attracting commercial interest

Jun 20th 2015 | From the print edition

A COMPUTER proceeds one step at a time. At any particular moment, each of its bits—the binary digits it adds and

issued a call for partners in its Logical Qubits programme, to make robust, error-free qubits. In April, meanwhile, Tanja Lange and Daniel Bernstein of Eindhoven University of Technology, in the Netherlands, announced PQCRYPTO, a programme to advance and standardise "post-quantum cryptography". They are concerned that encrypted communications captured now could be subjected to quantum cracking in the future. That means strong pre-emptive encryption is needed immediately.

Quantum-proof cryptomaths does already exist. But it is clunky and so eats up computing power. PQCRYPTO's objective is to invent forms of encryption that sidestep the maths at which quantum computers excel while retaining that mathematics' slimmed-down computational elegance.

Ready or not, then, quantum computing is coming. It will start, as classical

Initial recommendations

PQCRYPTO releases initial recommendations for post-quantum cryptographic algorithms

September 07, 2015.

A consortium of cryptographers has just released initial recommendations for cryptographic algorithms to protect the Internet against future quantum computers.

Attackers armed with quantum computers will be able to decrypt credit-card numbers and passwords encrypted with RSA and elliptic-curve cryptography. PQCRYPTO is a consortium of universities and companies funded by the European Union to respond to this threat.

The new report provides initial recommendations for post-quantum encryption, authentication, and signatures. "These recommendations are chosen for confidence in their long-term security", the report says.

"We started with conservative choices to make sure that the early adopters get secure systems", says Prof. Dr. Tanja Lange from [..]

nature International weekly journal of science

NATURE | NEWS

Online security braces for quantum revolution

Encryption fix begins in preparation for arrival of futuristic computers.

Chris Cesare

08 September 2015 | Corrected: 08 September 2015

PQCRYPTO, a European consortium of quantum-cryptography researchers in academia and industry, released a preliminary report on 7 September recommending cryptographic techniques that are resistant to quantum computers (see go.nature.com/5kellc). It favoured the McEliece system, which has resisted attacks since 1978, for public-key cryptography. Tanja Lange, head of the €3.9-million (US$4.3-million) project, favours the safest possible choices for early adopters. "Sizes and speed will improve during the project," she says, "but anybody switching over now will get the best security."