The H2020 PQCRYPTO project, an update

Andreas Hülsing, TU/e

PQCRYPTO
ICT-645622

14 September 2017

5th 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

TU/e technische universiteit eindhoven

BUNDESDRUCKEREI

DTU Danmarks Tekniske Universitet

Inria INVENTEURS DU MONDE NUMÉRIQUE

KU LEUVEN

NXP

50 Jahre RUB

Radboud Universiteit

TECHNISCHE UNIVERSITÄT DARMSTADT

University of Haifa

ACADEMIA SINICA

PQCRYPTO ICT-645622

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/.
- Final reports next summer.
- Follow us on twitter https://twitter.com/pqc_eu.

Initial recommendations (September 2015)

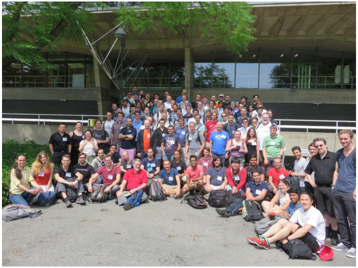
- **Symmetric encryption** Thoroughly analyzed, 256-bit keys:
  - AES-256
  - Salsa20 with a 256-bit key

  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-, ...

The last year



- ECRYPT-CSA executive school in Eindhoven, $\sim$ 40 people.
- PQCRYPTO school in Eindhoven (at TU/e)
  120 Participants, 21 lectures,
  videos & slides online:
  https://2017.pqcrypto.org/school/schedule.html
- PQCrypto 2017, Utrecht
  67 submissions, 23 papers accepted;
  226 participants; videos to come.
  https://2017.pqcrypto.org/conf

Selected research results

(only minimally subjective)

Post-quantum signatures with formal security arguments

The quantum accessible ROM

- ROM: every party gets access to *ideal* hash function.
- Hash-function has public description.
- Assuming quantum adversaries we need to give quantum access!

Results

- Picnic: Signatures from symmetric key primitives.[1]
- SOFIA: Signatures based on MQ-based identification.[2]

---

[1] Chase, Derler, Goldfeder, Orlandi, Ramacher, Rechberger, Slamanig, Zaverucha. Post-Quantum Zero-Knowledge and Signatures from Symmetric-Key Primitives. ia.cr/2017/279

[2] Chen, Hülsing, Rijneveld, Samardjiska, Schwabe. SOFIA: MQ-based signatures in the QROM. ia.cr/2017/680

Hash function security

Common belief

- Grover is provably optimal $\Rightarrow$ Attacks gain at most a square-root factor.
- Only in the worst case if function is random!

Constructive results

- Also only square-root speed-up in average case (for random function).[3]
- Sponges are collapsing, CR, SPR, OW, if block function is random function or OW-permutation.[4]

Destructive result

- Can parallelize Grover search for 1 out of t images on p small cores to achieve $\sqrt{N/pt^{1/2}}$ runtime.[5]

---

[3] Hülsing, Rijneveld, Song. Mitigating Multi-Target Attacks in Hash-based Signatures. PKC'16. (OW / SPR, CR was shown by Zhandry)

[4] Czajkowski, Groot Bruinderink, Hülsing, Schaffner, Unruh. Post-quantum security of the sponge construction. QCRYPT'17.

[5] Banegas, Bernstein. Low-communication parallel quantum multi-target preimage search SAC'17

Lattice-based KEMs

Scheme	PQ sec.	ct?		Cycles		Bytes
CCA2-secure KEMs						
Streamlined NTRU Prime 4591^{761}	137	yes	**K**:	6 115 384	**sk:**	1600
			E:	59 600	**pk:**	1218
			D:	97 452	**c:**	1047
spLWE-KEM	128	?	**K**:	$\approx$ 336 700	**sk:**	?
(128-bit PQ parameters)			**E**:	$\approx$ 813 800	**pk:**	?
			D:	$\approx$ 785 200	**c:**	804
Kyber	161	yes	**K**:	77 892	**sk:**	2400
(AVX2 optimized)			**E**:	119 652	**pk:**	1088
			D:	125 736	**c:**	1184
NTRU-KEM	123	yes	**K**:	307 914	**sk:**	1422
			E:	48 646	**pk:**	1140
			D:	67 338	**c:**	1281
CCA2-secure public-key encryption						
NTRU ees743ep1	159	no	**K**:	1 194 816	**sk:**	1 120
			E:	57 440	**pk:**	1 027
			D:	110 604	**c:**	980
Lizard	128	no	**K**:	$\approx$ 97 573 000	**sk:**	466 944
(recommended parameters)			**E**:	$\approx$ 35 000	**pk:**	2 031 616
			D:	$\approx$ 80 800	**c:**	1 072

Table: Source: Hülsing, Rijneveld, Schanck, Schwabe. High-speed key encapsulation from NTRU. CHES 2017. (See source for references and more details)

Finding short vectors

Not enough study in literature

- SVP: find shortest nonzero vector in a lattice.
- Big improvements in attack speed in last several years.
- Breaking SVP breaks lattice-based crypto.
- Lattice-based crypto uses additional structure: ideal lattices, approximation vectors, FHE.
- Fast quantum attack recently developed against Gentry's original FHE system.[6]

Destructive results

- Fast non-quantum attack against a reasonable FHE system.[7]

---

[6] Eisenträger, Kitaev, Hallgren, Song, STOC'14; Campbell, Groves, Shepherd, 2014; Biasse, Song, SODA'16.

[7] Bauch, Bernstein, de Valence, Lange, van Vredendaal, Short generators without quantum computers: the case of multiquadratics. Eurocrypt'17.

Discrete Gaussian sampling

- Important building block in lattice-based crypto.
- Used to "hide" secrets.
- Hard to do fast, constant-time implementation.

Destructive results

- Many existing samplers vulnerable to side-channel attacks.[8]

Constructive results

- Can switch to *rounded Gaussians* for signatures.
- Sample continuous Gaussian and round to nearest Integer.
- *Rounded Gaussians* can be sampled efficiently in constant-time.

---

[8] Pessl, Groot Bruinderink, Yarom. To BLISS-B or not to be – Attacking strongSwan's Implementation of Post-Quantum Signatures. CCS'17

Coming soon

- **NIST (Not-)Competition**
  - Several submissions in progress.
  - Signatures, KEX and KEM.
  - Not just plain published schemes but optimized variants.
- **Nature article on post-quantum crypto**
  - Really soon: today's issue
- **XMSS RFC**

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.