XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

Wednesday, March 9, 2022

16:00 EET

State of Play of Post Quantum Cryptography

Webinar series

Cryptography under the hood

Speaker

Matti Tommiska

CEO & Co-founder, Xiphera

Definitions

Post-Quantum Cryptography (PQC)
Cryptography which cannot be "broken" by quantum computers.

Quantum computing
Computation using quantum phenomena.

Quantum cryptography
Exploits quantum mechanical phenomena for cryptographic tasks.

Public-key (asymmetric) cryptography
Algorithms used in key exchange and digital signatures.

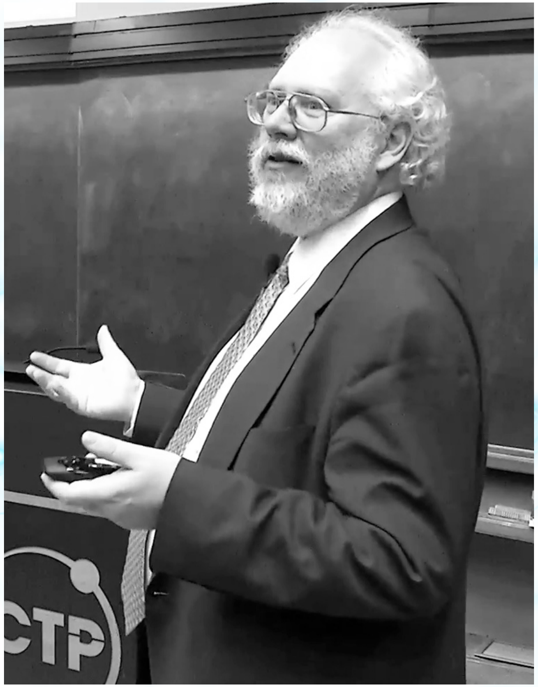
Secret-key (symmetric) cryptography
Algorithms used in encrypting and decrypting "bulk" traffic.

Effective key length
Achieved security level, not necessarily the same as key length.

Quantum Computers

- Computation based on quantum phenomena:
  - Super-position
  - Entanglement
- Qubits = “Quantum bits”
  - IBM: 127 qubits (Nov. 2021)
- “Cryptographically Relevant Quantum Computer (CRQC)”

The Quantum Threat



Peter Shor speaking after receiving the 2017 Dirac Medal from the ICTP.
Author: International Centre for Theoretical Physics
Source: https://www.youtube.com/watch?v=J7HeDX_7Heg&t=7075

- In 1994 Peter Shor introduced **Shor's algorithm**
  - A *polynomial-time* algorithm for solving integer factoring and (elliptic curve) discrete logarithms
- Shor's algorithm will break RSA and Elliptic Curve Cryptography *if CRQCs become practical*
  - Practically all Internet security relies on RSA/ECC
  - This is likely the biggest threat to contemporary cryptosystems
- Lesser concern: **Grover's algorithm** (1996)
  - Requires doubling the key length in symmetric cryptography to maintain the same security level (e.g. AES128 ⇒ AES256)

The Imminent Quantum Threat

“Record today, break tomorrow.”

NIST PQC Competition

2016
Competition starts

"Competition-like" process to standardize PQC algorithms.

2017
Round 1

69 algorithms included.

2019
Round 2

21 algorithms included.

2020
Round 3

7 finalists and 8 alternates.

2/2022
NIST reports a delay

"We hope to be able to announce the results and report not later than the end of March."

3/2022
Likely winner selected

2023-2024
First standards

3/2022
NIST announces Round 4

New algorithms (especially signatures) can be submitted for Round 4.

2024 ⇒
Additional standards

NIST PQC Finalists

Cryptotypes:

Structured lattices **Codes** **Multivariate**

Key Encapsulation Mechanisms (KEM)

- Classic McEliece
- CRYSTALS-KYBER
- NTRU
- Saber

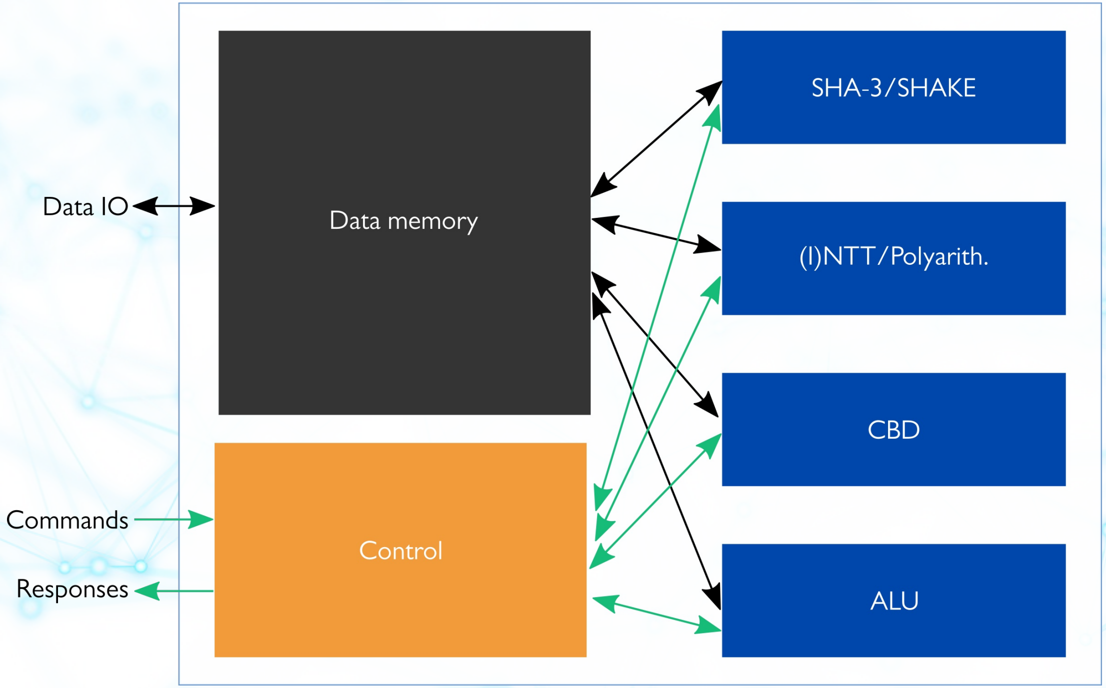
KeyGen() → (pk, sk)
Encapsulate(pk) → (ct, ss)
Decapsulate(pk, sk, ct) → (ss)

Signature schemes

- CRYSTALS-DILITHIUM
- FALCON
- Rainbow

KeyGen() → (pk, sk)
Sign(sk, msg) → (sig)
Verify(sig, msg, pk) → (msg)

Example: CRYSTALS-KYBER



Algorithm 5 KYBER.CPAPKE.Enc(pk, m, r): encryption

Input: Public key $pk \in \mathcal{B}^{12 \cdot k \cdot n/8+32}$
Input: Message $m \in \mathcal{B}^{32}$
Input: Random coins $r \in \mathcal{B}^{32}$
Output: Ciphertext $c \in \mathcal{B}^{d_u \cdot k \cdot n/8 + d_v \cdot n/8}$

$N := 0$
$\hat{\mathbf{t}} := \mathsf{Decode}_{12}(pk)$
$\rho := pk + 12 \cdot k \cdot n/8$
for i from 0 to $k-1$ **do**
  for j from 0 to $k-1$ **do**
    $\hat{\mathbf{A}}^T[i][j] := \mathsf{Parse}(\mathsf{XOF}(\rho, i, j))$
  end for
end for
for i from 0 to $k-1$ **do**
  $\mathbf{r}[i] := \mathsf{CBD}_{\eta_1}(\mathsf{PRF}(r, N))$
  $N := N + 1$
end for
for i from 0 to $k-1$ **do**
  $\mathbf{e}_1[i] := \mathsf{CBD}_{\eta_2}(\mathsf{PRF}(r, N))$
  $N := N + 1$
end for
$e_2 := \mathsf{CBD}_{\eta_2}(\mathsf{PRF}(r, N))$
$\hat{\mathbf{r}} := \mathsf{NTT}(\mathbf{r})$
$\mathbf{u} := \mathsf{NTT}^{-1}(\hat{\mathbf{A}}^T \circ \hat{\mathbf{r}}) + \mathbf{e}_1$
$v := \mathsf{NTT}^{-1}(\hat{\mathbf{t}}^T \circ \hat{\mathbf{r}}) + e_2 + \mathsf{Decompress}_q(\mathsf{Decode}_1(m), 1)$
$c_1 := \mathsf{Encode}_{d_u}(\mathsf{Compress}_q(\mathbf{u}, d_u))$
$c_2 := \mathsf{Encode}_{d_v}(\mathsf{Compress}_q(v, d_v))$
return $c = (c_1 \| c_2)$

Algorithm 6 KYBER.CPAPKE.Dec(sk, c): decryption

Input: Secret key $sk \in \mathcal{B}^{12 \cdot k \cdot n/8}$
Input: Ciphertext $c \in \mathcal{B}^{d_u \cdot k \cdot n/8 + d_v \cdot n/8}$
Output: Message $m \in \mathcal{B}^{32}$

$\mathbf{u} := \mathsf{Decompress}_q(\mathsf{Decode}_{d_u}(c), d_u)$
$v := \mathsf{Decompress}_q(\mathsf{Decode}_{d_v}(c + d_u \cdot k \cdot n/8), d_v)$
$\hat{\mathbf{s}} := \mathsf{Decode}_{12}(sk)$
$m := \mathsf{Encode}_1(\mathsf{Compress}_q(v - \mathsf{NTT}^{-1}(\hat{\mathbf{s}}^T \circ \mathsf{NTT}(\mathbf{u})), 1))$
return m

CRYSTALS-KYBER

Main operations are

- Number Theoretic Transform (NTT)
- Polynomial arithmetic
- Samplings from Centered Binomial Distributions (CBD)
- SHA-3/SHAKE computations (PRF, XOF)

PQC vs. current algorithm differences

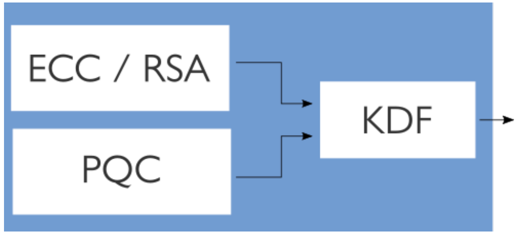
- PQC key lengths significantly longer
- Latency examples
  - KYBER ja SABER generally slightly faster than current ECC
  - Classic McEliece likely fastest of all
  - For example, SIKE is slow

KEMs: Key and Ciphertext Sizes (in bytes)

Algorithm	Status	Security	Private key	Public key
ECC	Pre-Quantum	1	32	32
		5	64	64
Classic McEliece	Finalist	1	6492	261120
		5	13932	1044992
Kyber	Finalist	1	1632	800
		5	3168	1568
NTRU	Finalist	1	935	699
		5	1590	1230
Saber	Finalist	1	1568	672
		5	3040	1312
SIKE	Alternate	1	374	330
		5	644	564

Recommendations

- Government agencies have given recommendations
  - BSI (Germany):
    - Classic McEliece or FrodoKEM (NIST alternate, lattice scheme)
  - ANSSI (France):
    - Post-quantum defense-in-depth as soon as possible for products requiring a long-lasting protection of information
    - FrodoKEM, Kyber, Dilithium or Falcon
- Hybrid key exchange in TLS 1.3 (draft IETF)
- Multiple key exchanges in IKEv2 (draft IETF)
- "hybridation" = co-existence of PQC and ECC/RSA



Key Take-aways

Systems designed today should have the ability to support PQC in the future.

Co-existence of classical and PQC algorithms.

Reprogrammability of FPGA is an advantage.

Fixed solutions (ASIC, TPM) lack crypto agility.

2-3 years from algorithms to standards.

Quantum Cryptography for niche applications.

XIPHERA

Thank you!

www.xiphera.com
info@xiphera.com
matti.tommiska@xiphera.com

Next webinar

June 8, 2022

Register at

www.xiphera.com /webinars.php

XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

www.xiphera.com
info@xiphera.com
matti.tommiska@xiphera.com

Appendix

- https://www.ssi.gouv.fr/publication/anssi-views-on-the-post-quantum-cryptography-transition/
- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/P283_QC_Studie-V_1_2.pdf?__blob=publicationFile&v=1
- https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography
- Quantum computers
  - Credit: Shutterstock