Post-quantum cryptography: Current status and future consequences
I. Brief introduction to cryptography
II. The quantum threat and PQC
III. The future PQC standards
IV. What are the effects of PQC in practice?
Cryptography

Cryptography vs. cryptanalysis

Foundation of computer & communication security

Security is based on the secrecy of keys
Cryptography

- Foundation of computer & communication security
- Cryptography vs. cryptanalysis
- Security is based on the secrecy of keys

Cryptography

- AES
- HMAC
- SHA2
- SHA3
- SHA1
- SHA1
- MD5
- AES-GCM
- ECDH
- DSA
- RSA
- ECDSA
- SHA2
- SHA3
- SHA1
- MD5
- Secure-boot
- IPsec
- MACsec
- TLS
- ECDH
- DSA
- RSA
- ECDSA
- SHA2
- SHA3
- SHA1
- MD5
Symmetric vs. asymmetric

**Symmetric**
- Shared key $K$
  - Must be secret

**Asymmetric**
- Key-pair
  - Private key (SK) $\rightarrow$ Public key (PK)
  - Public key (PK) $\Rightarrow$ Private key (SK)

**AES**

Icons made by Freepik from Flaticon.
Asymmetric cryptography

Key exchange

Alice’s public key ➔ Combine ➔ Shared secret ➔ Bob’s private key

Digital signatures

Message ➔ Sign ➔ Message + Signature ➔ Verify ➔ Alice’s public key

Sign

Alice’s private key

Alice’s private key

Message

Message + Signature

Verify
The quantum threat

- **Shor’s algorithm** on a large-scale quantum computer
  - Discrete logarithm will be “easy” to solve
    - ECC broken
  - Factoring will be “easy” to solve
    - RSA broken

- Shor’s algorithm does not apply to symmetric cryptography

  - **Grover’s algorithm** does, but doubling the key size is enough (256 bits instead of 128 bits)
The imminent quantum threat

“Record today, break tomorrow.”
Post-quantum cryptography

- Post-Quantum Cryptography (PQC) refers to asymmetric cryptography that *cannot be broken with quantum computers*
  - Based on mathematical problems that are not affected by Shor
  - Algorithms running on *traditional computers* (≠ quantum cryptography)
- Active area of research in the cryptography community since 2000s
2016

Competition starts

69 algorithms

2017

Round 1

21 algorithms

2019

Round 2

7 finalists and 8 alternates

2020

Round 3

4 algorithms

5 July, 2022

Winners selected

2022

Round 4

4 algorithms

2023-2024

First standards

2024 ⇒

Additional standards

New signature algorithms

Embedded Conference Finland, Sept. 6, 2022
Crypto agility is a must.

FPGAs or other programmable solutions have an advantage.

- **2016**: Competition starts
- **2017 Round 1**: 69 algorithms
- **2019 Round 2**: 21 algorithms
- **2020 Round 3**: 7 finalists and 8 alternates, 4 algorithms
- **2022 Round 4**: 5 July, 2022 Winners selected, 2023-2024 First standards, 2024 Additional standards, New signature algorithms

New signature algorithms
NIST selections

**Round 3 Winners**
- **KEM**
  - CRYSTALS-Kyber (lattice)
- **Signature**
  - CRYSTALS-Dilithium (lattice)
  - Falcon (lattice)
  - SPHINCS+ (hash)

**Round 4 Candidates**
- **KEM**
- **BIKE** (code)
- **Classic McEliece** (code)
- **HQC** (code)
- **SIKE** (isogeny)
# KEM stats

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Status</th>
<th>Security</th>
<th>Private key (B)</th>
<th>Public key (B)</th>
<th>Ciphertext (B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECC (ECDH)</td>
<td>Pre-Quantum</td>
<td>~128</td>
<td>32</td>
<td>32</td>
<td>32</td>
</tr>
<tr>
<td></td>
<td></td>
<td>~256</td>
<td>64</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td>Kyber</td>
<td>Winner</td>
<td>~128</td>
<td>1632</td>
<td>800</td>
<td>768</td>
</tr>
<tr>
<td></td>
<td></td>
<td>~256</td>
<td>3168</td>
<td>1568</td>
<td>1568</td>
</tr>
<tr>
<td>HQC</td>
<td>Round 4</td>
<td>~128</td>
<td>40</td>
<td>2249</td>
<td>4481</td>
</tr>
<tr>
<td></td>
<td></td>
<td>~256</td>
<td>40</td>
<td>7245</td>
<td>14469</td>
</tr>
<tr>
<td>BIKE</td>
<td>Round 4</td>
<td>~128</td>
<td>2244</td>
<td>12323</td>
<td>12579</td>
</tr>
<tr>
<td></td>
<td></td>
<td>~256</td>
<td>4640</td>
<td>40973</td>
<td>41229</td>
</tr>
<tr>
<td>SIKE</td>
<td>Round 4</td>
<td>~128</td>
<td>374</td>
<td>330</td>
<td>346</td>
</tr>
<tr>
<td></td>
<td>(broken)</td>
<td>~256</td>
<td>644</td>
<td>564</td>
<td>596</td>
</tr>
<tr>
<td>Classic McEliece</td>
<td>Round 4</td>
<td>~128</td>
<td>6492</td>
<td>261120</td>
<td>128</td>
</tr>
<tr>
<td></td>
<td></td>
<td>~256</td>
<td>13932</td>
<td>10449922</td>
<td>240</td>
</tr>
</tbody>
</table>
## KEM stats

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Status</th>
<th>Security</th>
<th>Private key (B)</th>
<th>Public key (B)</th>
<th>Ciphertext (B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECC (ECDH)</td>
<td>Pre-Quantum</td>
<td>~128</td>
<td>32</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td></td>
<td></td>
<td>~256</td>
<td>64</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>Kyber</td>
<td>Winner</td>
<td>~128</td>
<td>1632</td>
<td>3168</td>
<td>3168</td>
</tr>
<tr>
<td></td>
<td></td>
<td>~256</td>
<td>1568</td>
<td>1568</td>
<td>1568</td>
</tr>
<tr>
<td>HQC</td>
<td>Round 4</td>
<td>~128</td>
<td>40</td>
<td>2244</td>
<td>2244</td>
</tr>
<tr>
<td></td>
<td></td>
<td>~256</td>
<td>40</td>
<td>4640</td>
<td>4640</td>
</tr>
<tr>
<td>BIKE</td>
<td>Round 4</td>
<td>~128</td>
<td>2244</td>
<td>12323</td>
<td>12579</td>
</tr>
<tr>
<td></td>
<td></td>
<td>~256</td>
<td>4640</td>
<td>40973</td>
<td>41229</td>
</tr>
<tr>
<td>SIKE</td>
<td>Round 4</td>
<td>~128</td>
<td>374</td>
<td>330</td>
<td>330</td>
</tr>
<tr>
<td></td>
<td></td>
<td>~256</td>
<td>644</td>
<td>596</td>
<td>596</td>
</tr>
<tr>
<td>Classic McEliee</td>
<td>Round 4</td>
<td>~128</td>
<td>6492</td>
<td>261120</td>
<td>128</td>
</tr>
<tr>
<td></td>
<td></td>
<td>~256</td>
<td>13932</td>
<td>10449922</td>
<td>240</td>
</tr>
</tbody>
</table>

- **Significantly larger keys & ciphertexts**
- **Larger communication and storage overhead**
- **Latencies will stay similar or even become slightly faster**

*Embedded Conference Finland, Sept. 6, 2022*
## Signature stats

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Status</th>
<th>Security</th>
<th>Private key (B)</th>
<th>Public key (B)</th>
<th>Signature (B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECC (ECDSA)</td>
<td>Pre-Quantum</td>
<td>~128</td>
<td>32</td>
<td>32</td>
<td>64</td>
</tr>
<tr>
<td></td>
<td></td>
<td>~256</td>
<td>64</td>
<td>64</td>
<td>128</td>
</tr>
<tr>
<td>Dilithium</td>
<td>Winner</td>
<td>~128</td>
<td>2544</td>
<td>1312</td>
<td>2420</td>
</tr>
<tr>
<td></td>
<td></td>
<td>~256</td>
<td>4880</td>
<td>2592</td>
<td>4595</td>
</tr>
<tr>
<td>Falcon</td>
<td>Winner</td>
<td>~128</td>
<td>1281</td>
<td>897</td>
<td>666</td>
</tr>
<tr>
<td></td>
<td></td>
<td>~256</td>
<td>2305</td>
<td>1793</td>
<td>1280</td>
</tr>
<tr>
<td>SPHINCS⁺ (s)</td>
<td>Winner</td>
<td>~128</td>
<td>64</td>
<td>32</td>
<td>7856</td>
</tr>
<tr>
<td></td>
<td></td>
<td>~256</td>
<td>128</td>
<td>64</td>
<td>29792</td>
</tr>
<tr>
<td>SPHINCS⁺ (f)</td>
<td>Winner</td>
<td>~128</td>
<td>64</td>
<td>32</td>
<td>17088</td>
</tr>
<tr>
<td></td>
<td></td>
<td>~256</td>
<td>128</td>
<td>64</td>
<td>49856</td>
</tr>
</tbody>
</table>
## Signature stats

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Status</th>
<th>Security</th>
<th>Private key (B)</th>
<th>Public key (B)</th>
<th>Signature (B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECC (ECDSA)</td>
<td>Pre-Quantum</td>
<td>~128</td>
<td>32</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td></td>
<td></td>
<td>~256</td>
<td>64</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>Dilithium</td>
<td>Winner</td>
<td>~128</td>
<td>2544</td>
<td>2592</td>
<td>4595</td>
</tr>
<tr>
<td></td>
<td></td>
<td>~256</td>
<td>4880</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Falcon</td>
<td>Winner</td>
<td>~128</td>
<td>1281</td>
<td>897</td>
<td>666</td>
</tr>
<tr>
<td></td>
<td></td>
<td>~256</td>
<td>2305</td>
<td>1793</td>
<td>1280</td>
</tr>
<tr>
<td>SPHINCS⁺ (s)</td>
<td>Winner</td>
<td>~128</td>
<td>64</td>
<td>32</td>
<td>7856</td>
</tr>
<tr>
<td></td>
<td></td>
<td>~256</td>
<td>128</td>
<td>64</td>
<td>29792</td>
</tr>
<tr>
<td>SPHINCS⁺ (f)</td>
<td>Winner</td>
<td>~128</td>
<td>64</td>
<td>32</td>
<td>17088</td>
</tr>
<tr>
<td></td>
<td></td>
<td>~256</td>
<td>128</td>
<td></td>
<td>49856</td>
</tr>
</tbody>
</table>

- **Significantly larger keys & signatures**
- **Larger communication and storage overhead**
- **PQC signature landscape will change when new algorithms enter Round 4**
Why hybrid systems?

- We **cannot fully trust** that the new PQC schemes are secure
  - **Example:** NIST Round 3 finalist Rainbow and Round 4 candidate SIKE were broken!
- Many recommend using a **hybrid system**
  - **Combine PQC with ECC**
  - ANSSI (France) recommends it at least until 2030
- ECC will not go away for a long time!

Source: ANSSI (2022)
Hybrid systems: PQC + ECC
Hybrid systems: PQC + ECC

- ECDH(E)
- PQC-KEM
- KDF
Hybrid systems: PQC + ECC

- ECDH(E)
- PQC-KEM
- KDF
- ECDSA-Sign
- Document
- ok?
Hybrid systems: PQC + ECC

- ECDH(E)
- PQC-KEM
- KDF

Document
- PQC-Sign
- ECDSA-Sign

Both ok?
Hybrid systems: PQC + ECC

ECC overhead compared to PQC is small

Increased footprint may be the biggest problem

Both ok?
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.