Post-Quantum Cryptography
Quantum Computer

- Ongoing practical research and development paves the way for building large-scale quantum computers.
- Small scale quantum computers already exist.
- In about 10-20 years, large-scale quantum computers could become a reality.
IBM unveils its first commercial quantum computer

January 2019
Gartner Hype Cycle 2018

Hype Cycle for Emerging Technologies, 2018

garter.com/SmarterWithGartner

Source: Gartner (August 2018)
© 2018 Gartner, Inc. and/or its affiliates. All rights reserved.
Global Initiatives (just examples)

- Quantum Flagship
- National Quantum Initiative Act
- Centre For Quantum Computation and Com. Technology
- National Laboratory for Quantum Information Sciences
Companies

- Too many to list…
Capabilities of Quantum Computers

- Quantum computers will be able to perform computations much faster.
- Search algorithms can be performed in square root time (Grover’s algorithm).
- Factorization and discrete logs can be computed in polynomial time (Shor’s algorithm)
How is Cryptography Affected?

Symmetric:
- Generic square root quantum search algorithms apply.
- Need to double the key length.

Public-Key:
- Schemes, whose security is based on integer factorization (RSA), can be broken in quantum polynomial time.
- Schemes, based on DLOG problem, can be broken in quantum polynomial time.
- All of the currently standardized asymmetric cryptography (RSA, ECC) can be efficiently broken by a quantum adversary!
- No ‘easy fix’ as for symmetric cryptography.
## How is Cryptography Affected?

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Key length</th>
<th>Security Level Conventional Computer</th>
<th>Security Level Quantum Computer</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA-1024</td>
<td>1024 bits</td>
<td>80 bits</td>
<td>0 bits</td>
</tr>
<tr>
<td>RSA-2048</td>
<td>2048 bits</td>
<td>112 bits</td>
<td>0 bits</td>
</tr>
<tr>
<td>ECC-256</td>
<td>256 bits</td>
<td>128 bits</td>
<td>0 bits</td>
</tr>
<tr>
<td>ECC-384</td>
<td>384 bits</td>
<td>256 bits</td>
<td>0 bits</td>
</tr>
<tr>
<td>AES-128</td>
<td>128 bits</td>
<td>128 bits</td>
<td>64 bits</td>
</tr>
<tr>
<td>AES-256</td>
<td>256 bits</td>
<td>256 bits</td>
<td>128 bits</td>
</tr>
</tbody>
</table>
Problem | Quantum Computer Threat # Today

Record Now, Decrypt Later

https://www.sciencenews.org/article/google-moves-toward-quantum-supremacy-72-qubit-computer
Transition Period


- How long does your information need to be secure ($x$)
- How long to deploy quantum safe solutions ($y$)
- How long until a large-scale quantum computer ($z$)

If $x + y > z$ then worry
Prepare for the Quantum Computer

1. Create a Crypto Inventory
   - Know your vulnerabilities

2. Move to a Crypto Agile System
   - Do the effort once
   - Use standard crypto for now

3. Risk Assessment
   - When do I need to worry?

4. Move to PQC
   - Use today's PQC algorithms

5. Move to NIST standards
   - NIST published its standards

N. Monitor Crypto Threats
   - Ready for future crypto challenges
Post-Quantum Cryptography
Quantum Safe Cryptosystems

**Code Based Cryptosystems**
Security is based on the difficulty of decoding linear codes. It is famous for being the oldest public key encryption scheme that is potentially quantum safe.

**Hash Based Cryptosystems**
Security is based on hash functions. The most famous schemes are XMSS and SPHINCS.

**Lattice Based Cryptosystems**
Security is based on the shortest vector problem in a lattice. The most famous schemes include NTRU or cryptosystems based on Learning With Errors (LWE).

**Isogeny Based Cryptosystems**
Security is based on the problem to find an isogeny between supersingular elliptic curves. The most famous scheme is SIDH.

**Multivariate Based Cryptosystems**
Security is based on the problem of solving a set of non-linear equations. The most famous scheme is the Hidden Field Equations cryptosystems.
Lattice-Based

- Many lattice-based approaches exist, depending on the underlying hard problem: Closest Vector Problem (CVP), Learning With Errors (LWE), Ring-LWE (RLWE) and others
- Used for signatures, encryption, KEM
Code-Based

- Based on error-correcting codes
- The hard problem is based on hardness of decoding general linear code (NP-hard)
- Used for signatures, encryption, KEMs
Isogeny-Based

- Supersingular elliptic curve isogeny cryptography
- Extension of elliptic curve cryptography
- Hard problem is based on the difficulty of computing the isogeny between curves

- Used for key encapsulation
Hash-Based

- One-time and few-time signatures form the building blocks
- Use a tree structure
- Security only depends on the security of the underlying hash function
- Used for signatures
Multivariate-Based

- Based on multivariate polynomials over a finite field $F$
- Uses affine transformations and affine endomorphisms
- Hard problem is solving the system of multivariate polynomial equations
- Used for signatures
NIST Competition

- Submission deadline: Nov 30, 2017
- 69 round 1 candidates
- April 2018: first NIST PQC Workshop
- Second round began January 2019
- August 2019: second NIST PQC Workshop
- 2020/2021 - Select algorithms or start a 3rd Round
- 2022-2024 - Draft standards available

- Note: Standard organizations such as ETSI, IETF, ISO, and X9 are all working on recommendations.
### NIST Competition

**Submissions**

<table>
<thead>
<tr>
<th>Category</th>
<th>Signatures</th>
<th>KEM/Encryption</th>
<th>Overall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lattice-based</td>
<td>5</td>
<td>21</td>
<td>26</td>
</tr>
<tr>
<td>Code-based</td>
<td>2</td>
<td>17</td>
<td>19</td>
</tr>
<tr>
<td>Multivariate</td>
<td>7</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>Symmetric/Hash-based</td>
<td>3</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>Isogeny-based</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Other</td>
<td>2</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>19</strong></td>
<td><strong>45</strong></td>
<td><strong>64</strong></td>
</tr>
</tbody>
</table>
NIST Competition

- Round 2

<table>
<thead>
<tr>
<th></th>
<th>Signatures</th>
<th>KEM/Encryption</th>
<th>Overall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lattice-based</td>
<td>3</td>
<td>9</td>
<td>12</td>
</tr>
<tr>
<td>Code-based</td>
<td>0</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Multivariate</td>
<td>4</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>Symmetric/Hash-based</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Isogeny-based</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Other</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>9</strong></td>
<td><strong>17</strong></td>
<td><strong>26</strong></td>
</tr>
</tbody>
</table>

Benchmarks

- https://bench.cr.yp.to/supercop.html
- https://www.safecrypto.eu/pqclounge/
## Signature Algorithm

- CPU cycles and bytes

<table>
<thead>
<tr>
<th>Category</th>
<th>Scheme</th>
<th>Key generation</th>
<th>Sign</th>
<th>Verify</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash-based</td>
<td>Sphincs++-SHA256-128f</td>
<td>7'170'350</td>
<td>238'582</td>
<td>9'951'241</td>
<td>16'976</td>
</tr>
<tr>
<td>Lattice</td>
<td>Dilithium</td>
<td>227'254</td>
<td>910'911</td>
<td>291'116</td>
<td>2'044</td>
</tr>
<tr>
<td>Multivariate</td>
<td>MQDSS-48</td>
<td>2'579'234</td>
<td>252'403'091</td>
<td>185'066'255</td>
<td>32'886</td>
</tr>
<tr>
<td>Code</td>
<td>pqsigRM412</td>
<td>18'062'152'610</td>
<td>33'057'982'128</td>
<td>301'873'276</td>
<td>528</td>
</tr>
</tbody>
</table>
Key Encapsulation Mechanism

- CPU cycles

<table>
<thead>
<tr>
<th>Category</th>
<th>Scheme</th>
<th>Key generation</th>
<th>Encapsulation</th>
<th>Decapsulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Isogeny ECC</td>
<td>SIKEp503</td>
<td>82'329'570</td>
<td>133'880'410</td>
<td>142'428'861</td>
</tr>
<tr>
<td>Lattice</td>
<td>NewHope512-CCA</td>
<td>513'054</td>
<td>776'525</td>
<td>874'199</td>
</tr>
<tr>
<td>Multivariate</td>
<td>DME-(3,2,48)</td>
<td>445'585'460</td>
<td>2'114'390</td>
<td>10'845'706</td>
</tr>
<tr>
<td>Code</td>
<td>Classic McEliece 6960119</td>
<td>2'406'818'088</td>
<td>1'756'816</td>
<td>498'750'958</td>
</tr>
</tbody>
</table>
PQC and PKI
PKI

- Quantum computing strikes at the heart of the security of the global public key infrastructure
- All certificates become obsolete
- Root CAs operate for 20+ years
- Transition to new cryptosystem takes 10+ years (see SHA-1)
Multiple Public-Key Algorithm X.509 Certificates

- X.509 Extensions
- Adds a PQC algorithm and signature to the certificate

```
[ ... omitted for brevity ... ]
X509v3 extensions:
  X509v3 Basic Constraints:
    CA:FALSE
  Netscape Cert Type:
    SSL Server
  Netscape Comment:
    OpenSSL Generated Server Certificate
[ ... omitted for brevity ... ]
Alt-Signature-Algorithm:
  sha512WithHSS

Subject-Alt-Public-Key-Info:
  Leighton-Micali Hierarchical Signature System
  Public Key:
    00:00:00:01:00:00:00:00:00:00:00:00:00:03:1c:ba:ef:
    [ ... omitted for brevity ... ]
  Winternitz Value: 3 (0x3)
  Tree Height: 7 (0x7)

Alt-Signature-Value:
  Signature:
    30:82:0a:74:[ ... omitted for brevity ... ]

Signature Algorithm: ecdsa-with-SHA256
  30:45:02:21: [ ... omitted for brevity ... ]
```

https://datatracker.ietf.org/doc/draft-truskovsky-lamps-pq-hybrid-x509/
Conclusion

- Quantum Computer risk is real
- Do your risk assessment
- Move towards crypto agile systems
- Be ready in case QC becomes real