The Impacts of Post Quantum Cryptography
Quantum Computing will decimate the security infrastructure of the digital economy

Dr. Michele Mosca
Founder of the Institute for Quantum Computing, University of Waterloo
The Impacts of Post Quantum Cryptography

The Impacts of Quantum Computing on Applications and Use Cases

- **Impersonation**
  - Attacker “calculates” secret credentials of your PIV or EMV card from publicly available information and authenticates as you
  - Attacker approves requests and/or signs documents in your name

- **Fake identities**
  - Issuance of fake certificates (i.e. identities) in the name of your organization’s PKI

- **Document / data manipulation**
  - Attacker manipulates documents w/o invalidating their signature
  - Attacker manipulates blockchains, e.g. Bitcoin to steel your money

- **Eavesdropping**
  - Record key agreement (e.g. TLS) today, break it in 15 years to decrypt confidential information
The Impacts of Post Quantum Cryptography

Standardization of Quantum Safe Cryptography

<table>
<thead>
<tr>
<th>Quantum Safe Cryptography</th>
<th>Digital Signature</th>
<th>Public-Key Encryption</th>
<th>Key Agreement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash-based signatures (e.g. SPHINCS+)</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lattices (e.g. Dilithium, Kyber, NewHope, Frodo)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Error Correcting Codes (e.g. Classic McEliece)</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Elliptic Curve Isogenies (e.g. SIKE)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Multivariate (e.g. Rainbow)</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

- Some stateful hash-based signatures are accepted as quantum safe
  - eXtended Merkle Signature Scheme XMSS
  - Leighton-Micali Hierarchical Signature System HSS
The Impacts of Post Quantum Cryptography

The Impacts of Post Quantum Cryptography – e.g. Signature Algorithms

NIST ROUND 3 – SIGNATURE FINALISTS vs. RSA / ECC
The Impacts of Post Quantum Cryptography

- **Key size and certificate size**
  - Memory capacity of a PIV card / EMV card chip

- **Communication overhead**
  - Latency

- **Signature creation / verification time**
  - Real-time requirements in grid control systems

- **Power consumption**
  - Battery lifetime of a smart gas meter

---

**Subject** = DE, UTIMACO, Dieter Bong

**Public Key** = 7E 03 2A …

**Valid not after**
30.09.2023

**Signature** = 2B 40 75 …
The Impacts of Post Quantum Cryptography

Make yourself familiar with Post Quantum Cryptography

- Know more about PQC
  - Read Post-Quantum Crypto for dummies

- Test and evaluate PQC
  - Download Q-Safe simulator
    https://support.hsm.utimaco.com/hsm-simulator

Need to implement quantum-safe algorithms?
Get in touch and try our Q-safe HSM simulator!
The Impacts of Post Quantum Cryptography

The Road to Mass Adoption of Post Quantum Cryptography
Thank you for your attention!