How can quantum technologies be integrated into a future proof security infrastructure

Fabien Adouani
IT SA 2019
Quantum Everywhere

Quantum Encryption
Quantum Supremacy
Quantum Resistant
Quantum Mechanics
Quantum-Safe
Quantum Key Distribution
Quantum Computing
Quantum Crypto Algorithm
Qubits
Qubert
QKD
Post-Quantum
What is Quantum?

What does Quantum mean?

Its was originates from "quantum mechanics," a basic theory in physics. It’s a fundamental theory in physics which describes nature at the smallest scales of atoms and subatomic particles.

What is a Quantum Computing

A machine that performs calculations based on the laws of quantum mechanics, which is the behavior of particles at the sub-atomic level.

Quantum mechanics

\[
i\hbar \frac{\partial}{\partial t} |\psi(t)\rangle = \hat{H} |\psi(t)\rangle
\]

Schrödinger equation
Principles of Quantum Computing

Classical Computing - Bits  Quantum Computing - Qubits

Traditional computers are based on a binary system (0 or 1) per bit. One bit can have only two states “on” or “off”.

More information can be represented by a single qubit. A qubit can take on the properties of 0 and 1 simultaneously at any one moment.
The Benefits of Quantum Computing

Because of this property of qubit its calculation abilities are exponentially higher in magnitude.

- **Time**: Solves problems in much fewer steps and at a faster speed
- **Complexity**: Could process massive amount of complex data.
- **Accuracy**: Capability to convey more accurate answers.

- With around 49 qubits computers can outperform even the fastest supercomputer today. **Quantum Supremacy**
The Applications of Quantum Computing

- **Molecular and Biomedical Simulations**
  - Researchers at Harvard University used a D-Wave One quantum computer to solve the puzzle of how some proteins fold in 2012.

- **Machine Learning and AI**
  - Big data is out there to be analyzed, but we need more powerful computers to process the petabytes of unanalyzed data.

- **Financial Services**
  - Complex financial modeling and risk management within the financial industry as well.

- **Unwanted access to the encrypted data**
  - By breaking current public key cryptography (DH, RSA, ECC…)
Current Crypto Algorithms

- The challenge with currently popular algorithms is that their security relies on one of three hard mathematical problems:
  - the integer factorization problem — the decomposition of a composite number into a product of smaller integers.
  - the discrete logarithm problem
  - the elliptic-curve discrete logarithm issue.

- These problems can be easily solved on a sufficiently powerful quantum computer running Shor's algorithm.
## Current Crypto Algorithms

<table>
<thead>
<tr>
<th>Name of method</th>
<th>Application</th>
<th>Resilience against Quantum Computer</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA</td>
<td>Encryption, signature</td>
<td>✗</td>
</tr>
<tr>
<td>ECC</td>
<td>Encryption, signature</td>
<td>✗</td>
</tr>
<tr>
<td>AES 256</td>
<td>Encryption</td>
<td>✓</td>
</tr>
<tr>
<td>Hash-based</td>
<td>Authentication</td>
<td>✓</td>
</tr>
<tr>
<td>Lattice-based (NTRU)</td>
<td>Encryption; signature</td>
<td>✓</td>
</tr>
<tr>
<td>Code-based (Mc Eliece)</td>
<td>Encryption</td>
<td>✓</td>
</tr>
<tr>
<td>Multivariate polynomials</td>
<td>Encryption; signature</td>
<td>✓</td>
</tr>
<tr>
<td>Supersingular elliptic curve isogenies</td>
<td>Encryption; possibly signature</td>
<td>✓</td>
</tr>
</tbody>
</table>

Reference: ETSI – Standard Organization 2017
Quantum-Safe Solutions
Post-Quantum Algorithms

- Post-Quantum or Quantum Resistant Algorithm
  - refers to cryptographic algorithms that are believed to be secure against an attack by a quantum computer.

- Currently post-quantum cryptography research is mostly focused on six different approaches (ETSI):
  - Lattice-based cryptography
  - Multivariate cryptography
  - Hash-based cryptography
  - Code-based cryptography
  - Supersingular elliptic curve isogeny cryptography
  - Symmetric key quantum resistance (AES and SNOW)
Photons travelling through a semi-transparent mirror. The mutually exclusive events (reflection/transmission) are detected and associated to ‘0’ or ‘1’ bit values respectively.

- Speed of output and full availability
- Reliability & trust (Metas, CTL and AIS31)
- Unpredictable output
- High Quality entropy and keys
Quantum Key Distribution

- A secure communication method which implements a cryptographic protocol involving components of quantum mechanics.
- A shared random secret key known only by two parties, which can then be used to encrypt and decrypt messages.
- The key can be used with any chosen encryption algorithm to encrypt and decrypt - standard communication channel.
- Detect Unwanted third party, a results from a fundamental aspect of quantum mechanics: the process of measuring a quantum system in general disturbs the system.
ID Quantique – Path to Quantum Safety

Quantum Random Number Generation (QRNG)
- Instantly strengthen your crypto key material
- Feed higher quality entropy into key generation servers, HSMs, Linux & crypto applications and connected devices

Crypto agility and Post Quantum Crypto
- Be crypto-agile to move to next generation Post Quantum Crypto
- Be QKD ready (ready to upgrade to quantum cryptography)
- Protect your investments for today and for tomorrow

Quantum Key Distribution (QKD)
- Quantum Cryptography for secure transmission
- Provide forward secrecy & anti-eavesdropping of private key exchange/back up
- Use QKD today for backend IP protection
Recommendations

- **Start to Encrypt now**
  - AES 256 or Hash-based cryptography

- **Know your Crypto Assets**
  - Situation assessment (Algorithm, length of the keys etc.)

- **Think Agility**
  - Solution that will evolve in time – crypto agility

- **One size do not fit them all**
  - Adapt the solution to the case
  - The value of your data in time
  - Hybrid systems can improve security for sensitive data (Post quantum crypto with QKD)
Thank you
Post Quantum Safe: auch in Zukunft sichere Daten