Long-term Secure Hash-Based Digital Signatures

ETSI Quantum Safe Workshop 2017

Quantum Computer vs asymmentric Crypto

- Shor's algorithm (1994) shows that QC can solve **certain** mathematical problems in "polynomial time"
  - Factorisation problem (RSA)
  - Discrete Logarithm problem (DSA, Diffie-Hellman)
  - Discrete Logarithm problem on Elliptic Curves (ECDSA, EC Diffie-Hellman)
- A QC does **not** solve just any problem in "almost no time"
  - It solves special classes of problems, typically optimisation problems
- Symmetric algorithms and hash functions are **not** under the same threat
  - 256-bit AES could still be safe in 2050 according to an ETSI Report

Progress on Quantum Computers

- 3 qbits in 1998, now 20 qbits, UCSB+Google announced 50 for EoY
- Scaleup remains major challenge:
- IBM think that hybrid architecture is a good approach. Error rate and connectivity also influence expected performance of a QC. Chemistry and optimisation problems are likely candidates for 50-60 physical qbits, like analog computers in 1950s
- Oxford: Error rates are improving, still ECC: 1000 phys for 1 logical qbit -> At least 10^6 physical qbits are needed to attack RSA-1024
- Waterloo: Even with optimal ECC, execution and control take time -> “Constants in front of Os or Omegas matter!” SHA-256 is currently considered 166 bit QC-secure (not just 128 bit via Grover). Author is not aware of special QC algorithms like Shor to crack hash functions or AES

QRA – PQC – QSC … resistant algos

- Quantum-Resistant Algorithms (QRA) aka
- Post-Quantum Cryptography (PQC) aka
- Quantum-Safe Cryptography (QSC)
- ETSI has working group to assess quantum-safe primitives and more…
- NIST has a call for algorithms open, very first round of mutual comparisons and assessments, expected to run for several years
- Academia is very active, proposing algorithms from different classes
  - Lattice-based
  - Multivariate-based
  - Code-based
  - **Hash-based (signatures only, but IRTF standardisation nearly completed)**
  - Isogeny-based

Summary

- QC scale up remains hard to predict
- Standardisation of QRA has just begun
- So which QRA to target for implementation?
  - One overall proposal agreed by many participants:
  - Implement today's standard algo, but reprogrammable
  - Secure reprogrammability *with most conservative QRA digital signature* to achieve best possible long-term security:
  - hash-based signatures using so-called "Merkle-trees"

QRA details backup slide

- H2020 SAFEcrypto focuses on lattice-based algos, one of their use cases is SC TT&C (Thales, UniBelfast, workshop planned in January)
- H2020 PQCrypto does research, benchmarking, FOSS libraries
- French Implementation Initiative called RISQ, includes ANSSI
- IRTF is standardizing hash-based signaturesCisco and Genua are active on hash-based signatures as well
- Waterloo also has FOSS libraries, more specialised talks here
- QRA for one-pass, e.g. secure email: Key Encapsulation Mechanism
- US effort to implement Lattice-QRA on FPGA/SoC, will release design