Report – Security in a Post- Quantum World

S. Bai, J.-F. Biasse, E. Persichetti

Transition from first-generation PKC to PQC

- Quantum computers will break first generation PKC (RSA, ECC).
- Transition to a new suite of “Post-Quantum Cryptography” (PQC) algorithms is necessary.
- In 2017, NIST started a standardization process of PQC schemes for basic functionalities (encryption, digital signatures).
  - Currently in 3rd round (results expected Summer 2022).
  - Finalists: 3 signatures and 4 KEMs.
  - At the end of round 3, a first set of schemes will be recommended for standardization.

Current and future research in PQC

- Schemes based on Euclidean lattices are predominant in 3rd round finalists (5 out of 7).
  - Security of lattice-based schemes needs to be studied further.
  - Develop alternative solutions to lattices (further NIST rounds).
- More effort in cryptanalysis is needed from the scientific community.
  - Ex: a devastating attack was found recently on a 3rd round finalist.
  - New PQC schemes have not been scrutinized as much as first-generation PKC schemes (RSA, ECC).
- Side-channel analysis of PQC proposals is important.

Current and future research in PQC

- Trade-offs between security and performance of implementations.
- Development of PQC schemes with properties adapted to specific applications.
  - Ex: lightweight PQC.
  - Ex: specific environment scenarios such as IoT.
- Design of PQC schemes with advanced functionalities (Identity based encryption, homomorphic encryption …).
- Deployment of hybrid 1st gen. PKC/PQC schemes.
- Crypto agility at the protocol level.

Quantum Computing meets PQC

- To analyze the security of PQC schemes, we need to investigate quantum algorithms.
  - Quantum resource estimation of existing algorithms.
  - Need new/improved quantum attacks.
  - Actual implementation of quantum attacks.
  - Hybrid classical/quantum attacks.
- Revisit notions of security in light of capabilities of quantum adversaries (e.g. QROM).