Research Activities Towards (P)QC in Korea
Prof. Kwangjo Kim
IACR Fellow
Cryptology and Information Security Lab.(CAISLAB)
School of Computing, KAIST, Korea
E-mail: kkj@kaist.ac.kr https://caislab.kaist.ac.kr/kkj

Trends of ICT Security

Trends of Security

History of Modern Cryptography
Quantum Computer (1/2)

Quantum computer

Quantum Moore's Law

Quantum Computer (2/2)

Quantum Moore’s Law

Year | # of qubits
-----|-----------
2013 | 2
2014 | 5
2014 | 3
2016 | 5
2017 | 16
2017 | 20
2018 | 49
2018 | 72

PQC (Post-Quantum Cryptography)

Number theoretic hard problems

- Integer Factorization Problem
- Discrete Logarithm Problem
- Elliptic Curve Discrete Logarithm Problem

RSA

Code-based Cryptography

Lattice-based Cryptography

Post-Quantum Cryptography

Hash-based Cryptography

Isogeny-based Cryptography

Shor Algorithm (Shaded)

ICT R&D Roadmap in Korea (2019-2023) to Quantum Communication