4th PQC ASIA Forum 2019
Chongqing., China May 7, 2019

# Research Activities Towards (P)QC in Korea


**Prof. Kwangjo Kim**

**IACR Fellow**

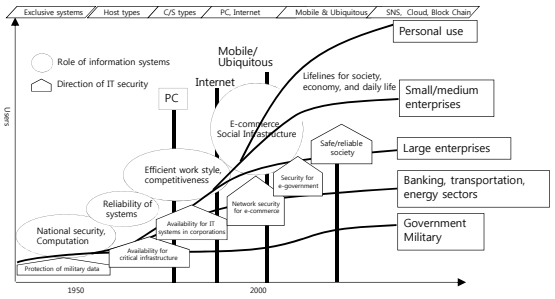
**Cryptology and Information Security Lab.(CAISLAB)**

**School of Computing, KAIST, Korea**

**E-mail: kkj@kaist.ac.kr https://caislab.kaist.ac.kr/kkj**

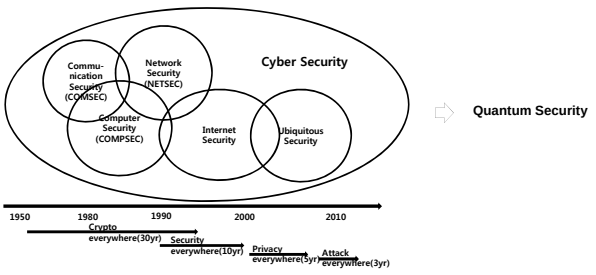



## Trends of ICT Security



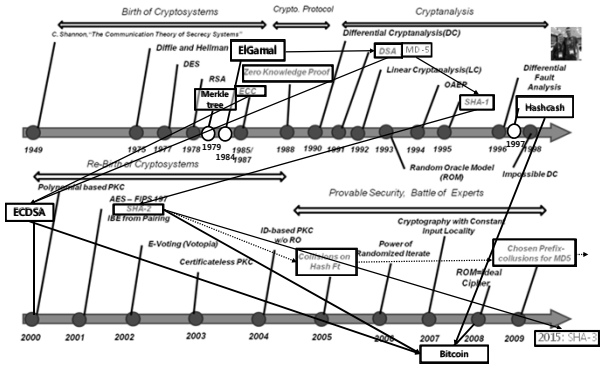



## Trends of Security






## History of Modern Cryptography



## Quantum Computer (1/2)

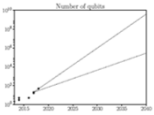

- Quantum mechanics applies to all systems from micro to macro scale and enables superposition and entanglement.
- Reversible computing: if no information is erased, computation may in principle be achieved which is thermodynamically reversible, and require no release of heat [Lan61].

(1) D. Aggarwal et al. "Quantum attacks on Bitcoin, and how to protect against them", arXiv 1710:10377v1. Oct. 28, 2017



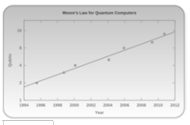
## Quantum Computer (2/2)

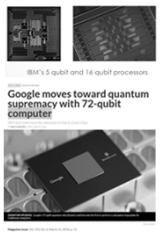
### Quantum Moore's Law




(1)

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






(1) D. Aggarwal et al. "Quantum attacks on Bitcoin, and how to protect against them", arXiv 1710:10377v1. Oct. 28, 2017



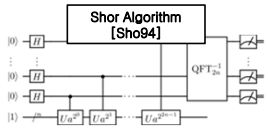
## PQC(Post-Quantum Cryptography)

Number theoretic hard problems

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

RSA

Shor Algorithm [Sho94]



Code-based Cryptography

Lattice-based Cryptography

Post Quantum Cryptography

MQE-based Cryptography

Hash-based Cryptography

Isogeny-based Cryptography



## ICT R&D Roadmad in Korea (2019-2013) to Quantum Communication