Applied Cryptography at VTT

Erik.Hieta-aho@vtt.fi

Research topics

- Post-Quantum Cryptography
- Quantum key distribution
- Privacy
- Digital Identities
- Security Metrics
- Other activities

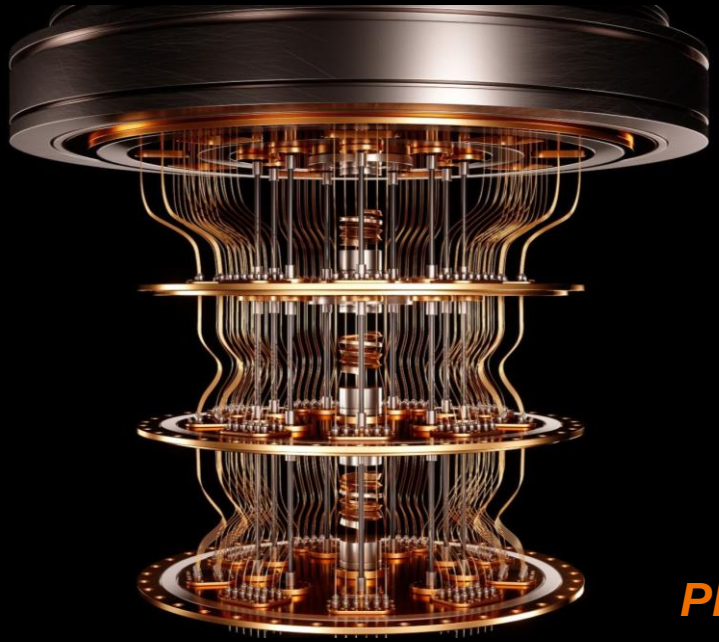
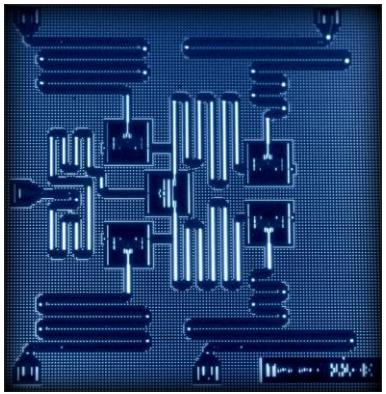


Photo: IBM

Post-Quantum Cryptography

Qubits instead of bits

- Bits are either 0 or 1
- Alternatives are computed one by one



- Qubits are both 0 and 1 until measured
- Computations are done before measurement; you can compute all alternatives at once

Public Key Infrastructure

- Public Key Infrastructure (PKI) is a tool for authenticating users and devices in the digital world
- It relies on digital signature technology, which uses public-key cryptography
- The private key of each entity is only known by that entity and is used for signing
- The key can be used as an identity for the user in digital networks

Quantum impact on PKI

- Public-key cryptography algorithms (RSA, ECC,...) are based on three different mathematical problems:
  - Factoring
  - Discrete logarithm in finite fields
  - Discrete logarithm in elliptic curves

- Shor’s algorithm on a powerful quantum computer will break all of these

Why Post-Quantum Cryptography?

- Number of useful qubits in a quantum computer doubles every year (ref. IBM)
  - Now at an order of a thousand
- At the same time number of qubits needed for break RSA2048, has reduced to about 20,000 (advances in algorithms)

- We have to make existing systems quantum-safe now
- Adversary can store communication data today and later decrypt it all with a quantum computer

Formula from Prof. Bart Preneel, KU Leuven:

$2022 + Q - x - y$

- Q is years to a practical quantum computer
- x is how long it takes to update your system with new algorithms
- y is how long the data needs to stay confidential

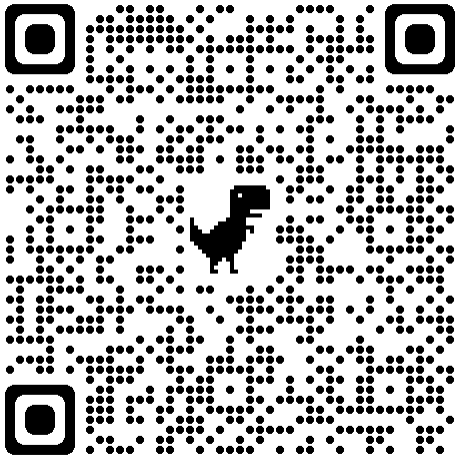
VTT: 20 qubits
running in Oct 2023

NIST PQC Standardization

- Feb 2016 – NIST PQC Competition announced
- Dec 2017 – 69 submissions accepted into 1st Round
- Jan 2019 – Round 2 candidates announced (17 KEM/PKE's + 9 signatures)
- July 2020 – Round 3 finalists announced (4 KEM + 3 Sig) plus 8 alternates
- June 2021 – 3rd PQC Standardization workshop
- July 2022 – 4 (1 KEM, 3 sig) candidates to be standardized and 4 (KEM) candidates move to 4th round.
- KYBER and Dilithium chosen to be standardized
- June 2023-New digital signatures call
- Draft standards available in 2024

Example project: PQC Finland
www.pqc.fi

- A Co-Innovation project funded by Business Finland under the Digital Trust program
- Duration: 1.1.2020-30.6.2022 with total budget ~ 6 M€
- Nine partners in the consortium
  - VTT, Aalto University and Helsinki University
  - SSH, Bittium, Insta, Sectra, Advenica and Tosibox
  - Collaboration with NIST through research exchange
  - Government stakeholders
- Final seminar held on Friday 6.5.2022.
- Policy brief in Finnish
  - Latvala, Vallivaara, Mellin, 2022: *Kvanttiturvalliset salausmenetelmät Suomessa* https://publications.vtt.fi/julkaisut/muut/2022/Kvanttiturvalliset-salausmenetelm%C3%A4t-Suomessa.pdf

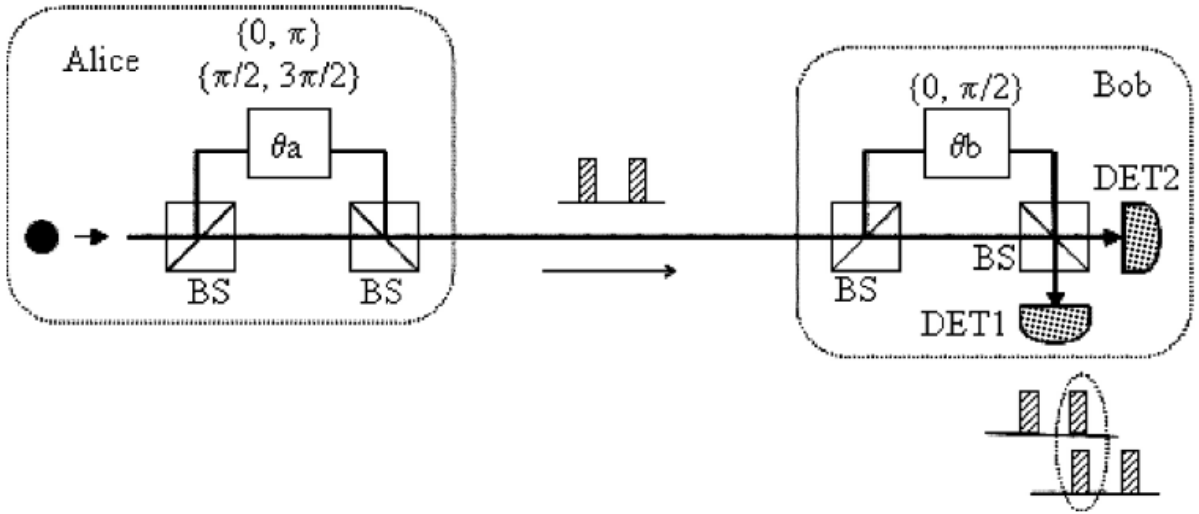


Calls of interest

- HORIZON-JU-SNS-2024-STREAM-B
  - 01-01: **System Architecture**
    - Resilient Security, Trustworthy and Privacy
  - 01-08: **Reliable AI for 6G Communications Systems and Services**
    - Security Metrics for quantum safety

Recently started and other research

Quantum communications 2022–

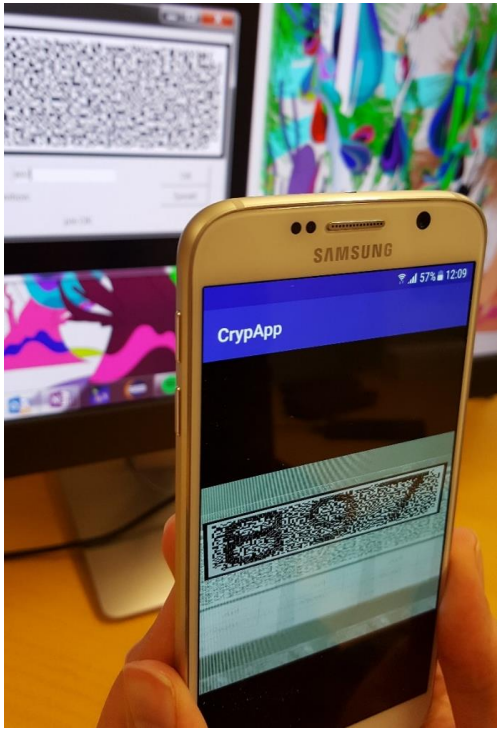


Ref: Inoue, K. (2006) Quantum Key Distribution Technologies

Cryptography for privacy

Regarding privacy, personal data and business data are parallels: Methods are similar. Controlling visibility is pivotal. Human factors apply equally.

- Processing encrypted data
  - privacy, while maintaining usability of data
- Human-understandable and user-friendly cryptography
  - Otherwise, end-users and employees become weakest links
- Digital identities with privacy
  - Tracking people or operational units made (next to) impossible
- Anonymous recommendations and service personalization
  - Token-based lightweight distributed engine with excellent scalability
- R&D&I on the use of cryptography in any domain
  - e.g. developing metrics for cryptosystems in critical operations



VTT

beyond

the obvious

Erik Hieta-aho
Erik.hieta-aho@vtt.fi
+358 50 462 4005

Ville Ollikainen (team leader)
ville.ollikainen@vtt.fi
+358 40 084 1116

@VTTFinland

www.vtt.fi