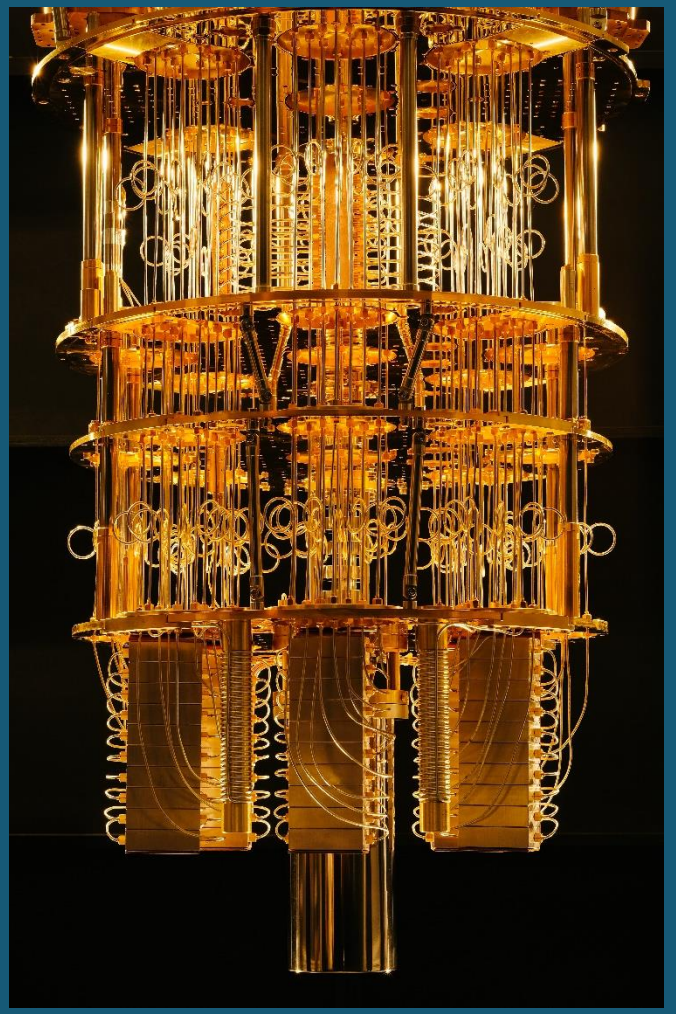
Quantum Safe Encryption Technologies

Visa Vallivaara
Senior Scientist
Applied Cryptography

Overview

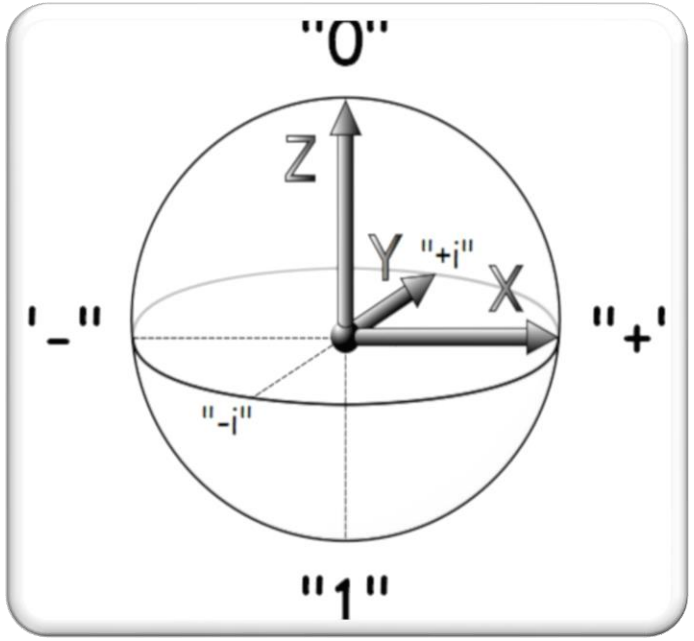
- Quantum Computing
- Post-Quantum Cryptography (PQC)
- Standardization of PQC by NIST
- PQC Finland
- Quantum Communication
- Summary

Quantum Computing

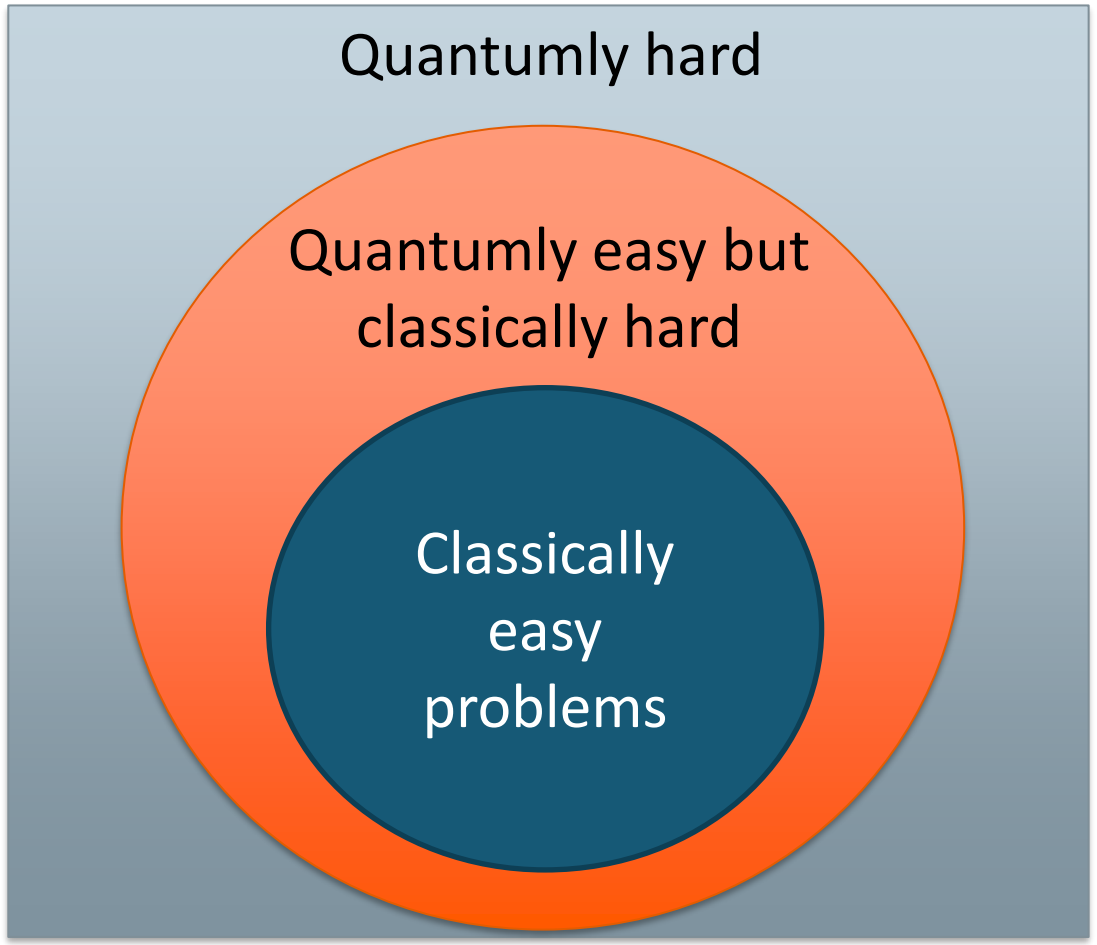


Bits and Qubits

Character	ASCII code	Binary code
null character	0	0000000
a	97	1100001
b	98	1100010
c	99	1100011
A	65	1000001
B	66	1000010
C	67	1000011
%	37	0100101
+	43	0101011
0	48	0110000
1	49	0110001
Delete	127	1111111

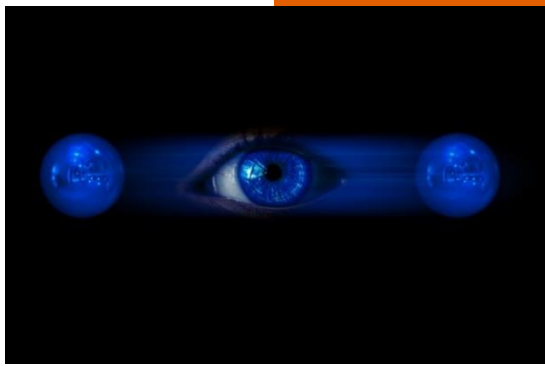


Computational Problems



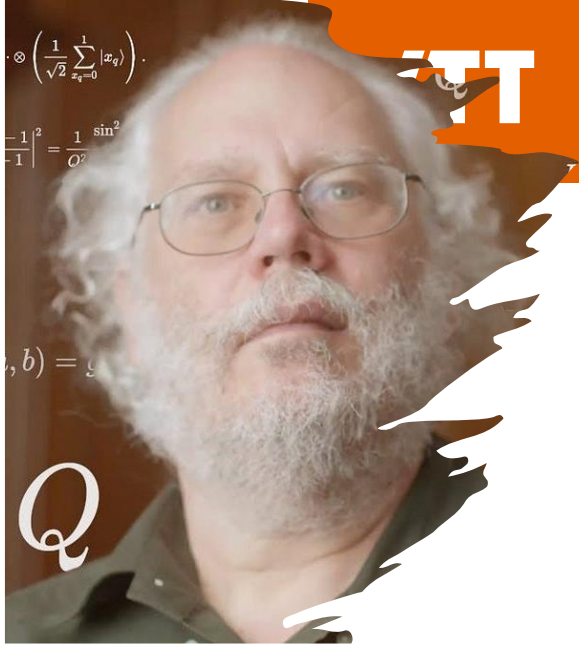
© John Preskill

Quantum Threat



- The research of quantum-computers is advancing fast
- One of the most pressing cyber security challenges is to make existing systems quantum-safe
- Current public key cryptography is based on math problems which can be broken with an effective quantum computer
- Adversary can store full communication today and later decrypt all with cryptographically relevant quantum computer
- Effective quantum computers don’t exist yet, but your secrets do

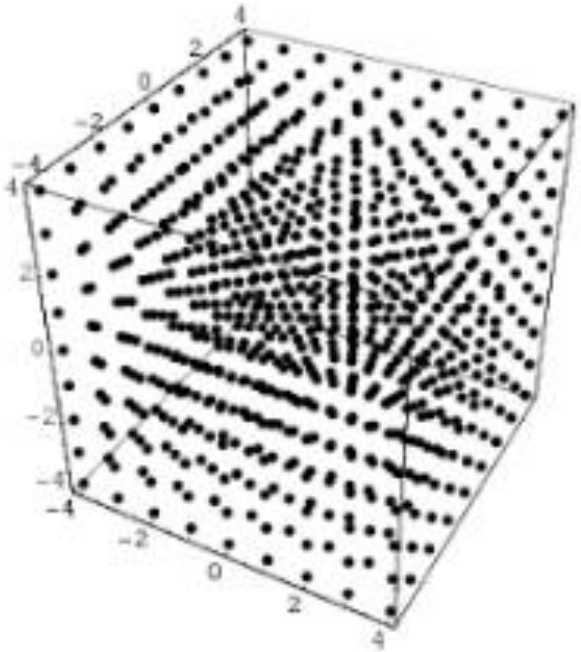
Impact on Cryptography



- Current public key cryptography is based on three different mathematical problems:
  - Factoring, discrete logarithm in finite fields and in elliptic curves
- Shor's algorithm on a suitable quantum computer will break these
  - RSA, DSA, DH and their ECC variants, ECDSA and ECDH
- Communication data is harvested today, stored, and later decrypted
- Typical applications (e.g. TLS) combine an asymmetric key agreement and symmetric encryption
- Every organization is affected

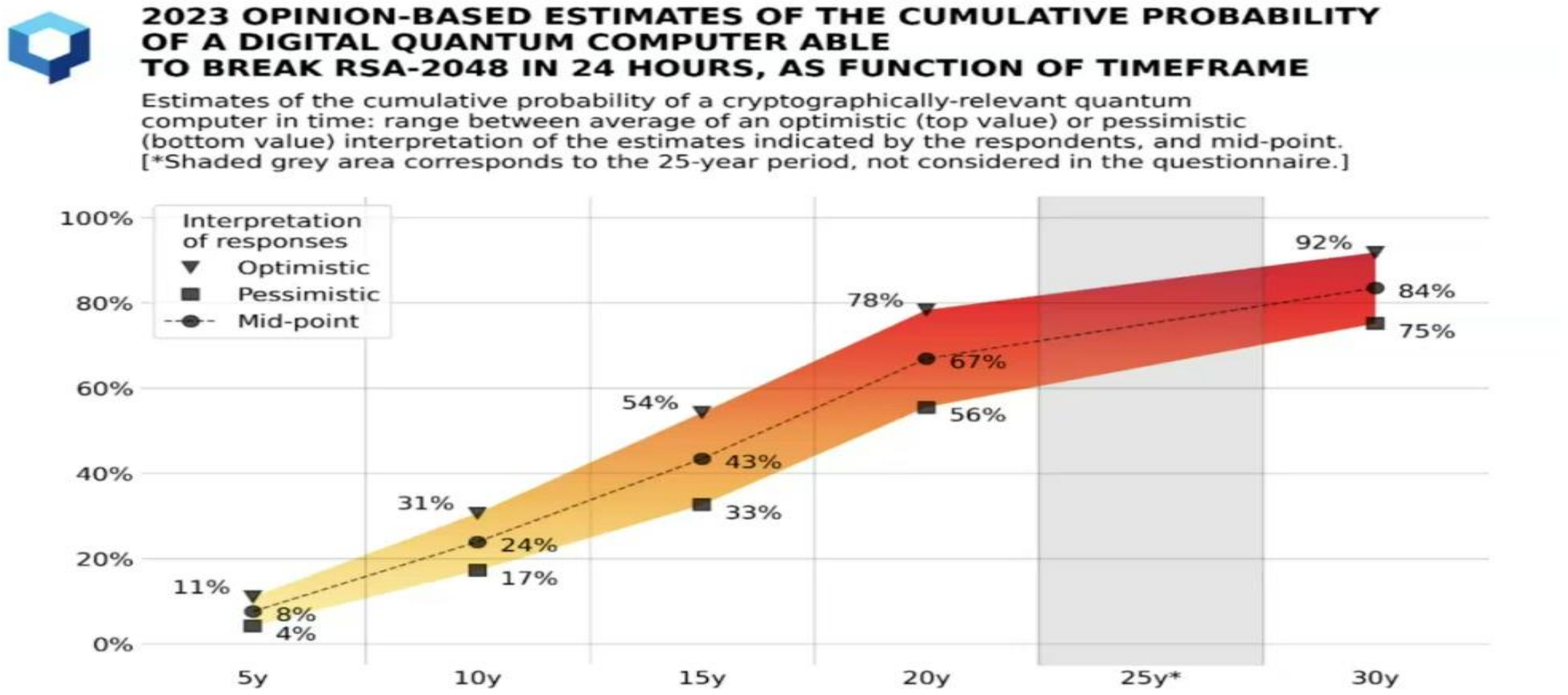
Post-Quantum Cryptography (PQC)

Post-Quantum Cryptography



- PQC is based on different mathematical problems
- Lattice, code-based and hash-based
- Larger keys and/or signatures/ciphertexts than current PKI
- Most of these cannot be simply plugged in on existing systems and protocols
- Need for rethinking the systems and careful planning on which algorithms work best in different use cases

Expert estimates of the likelihood of a quantum computer breaking RSA-2048 in 24 hours (different time frames)



Source: Global Risk Institute 2023

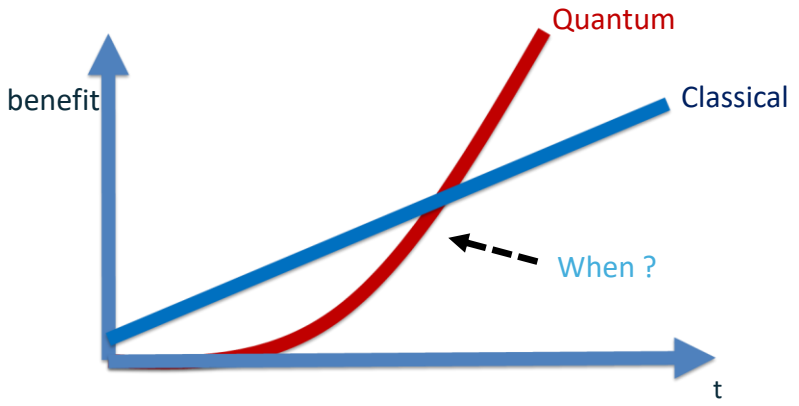
Biden Signs Post-Quantum Cybersecurity Guidelines Into Law

The new law holds the US Office of Budget and Management to a road map for transitioning federal systems to NIST-approved PQC.

Karen Spiegelman
Features Editor

December 22, 2(

Why already 2024?



Use the formula

2024 + Q – x –y,

where Q is # of years to first large scale quantum computer

x is # of years it takes to switch algorithms in your industry (3-12 years)

y is # of years data needs to be **confidential**

So for example Q = 20, x = 5 and y = 15 means you need to start to prepare today!

Thanks to prof. Bart Preneel for the formula! (https://twitter.com/AnomalRoil/status/1192463323104763904?s=20)

Standardization of PQC by NIST

National Institute of Standards and Technology
U.S. Department of Commerce

NIST PQC Standardization

- NIST started the standardization of PQC 2017
  - Dec 2017 – Round 1 started with 69 accepted submissions
  - Jan 2019 – Round 2 continued with 17 KEM and 9 signature candidates
  - July 2020 – Round 3 divided to finalists (4 KEM + 3 Sig) plus 8 alternates
  - July 2022 – Announcing 4 candidates to be standardized, plus round 4 candidates
  - April 10-12, 2024 – 5th PQC Standardization Conference

Attacks after 2rd Round

- NOV 2020 – GEMSS ATTACK
  - Improved Key Recovery of the HFEv- Signature Scheme
  - All parameters sets fall below claimed security levels
- FEB 2022 – RAINBOW ATTACK
  - "Breaking rainbow takes a weekend on a laptop" (Level 1)
- APR 2022 – ATTACK ON STRUCTURED LATTICE SCHEMES
  - Lattice Reduction Meets Key-Mismatch
  - Relevant to Kyber, Saber, Dilithium and likely NTRU
- APR 2022 – ATTACK ON SPHINCS+ (Fixed)
  - Breaking Category Five SPHINCS+ with SHA-256

Algorithms to be Standardized

Public-Key Encryption/KEMs

- **CRYSTALS-KYBER**

Digital Signatures

- **CRYSTALS-Dilithium**
- FALCON
- SPHINCS+

PQC Fourth Round Candidates

- Key-Establishment Mechanisms (KEMs)
  - BIKE
  - Classic McEliece
  - HQC
  - ~~SIKE(Broken)~~
- NIST requested additional (quantum-resistant) digital signature proposals to be considered in the PQC standardization process
  - Schemes that are not based on structured lattices are of greatest interest

Detailed Crypto overview

	Features			Speed			Memory		
	QUANTUM-SAFE?	STANDARD-ISED	CONFIDENCE[1]	KEY GEN	ENCRYP-TION/ SIGNING	DECRYP-TION/ VERI-FICATION	PUB KEY	PRIV KEY	CIPHERTEXT/ SIGNATURE
RSA (KE)									
Elliptic-curve (KE)									
CR.-KYBER (KE)									
FrodoKEM (KE)									
McEliece (KE)									
BIKE (KE)									
HQC (KE)									
CR.-DILITHIUM (DSS)									
FALCON (DSS)									
SPHINCS+ (DSS)									

Strengths and weaknesses of various traditional as well as post-quantum primitives.

PQC Finland

PQC Finland project

- Post-Quantum Cryptography project: www.pqc.fi
- A Co-Innovation project funded by Busines Finland
- Duration: 1.1.2020-30.6.2022, Budjet: 6M€
- Research: VTT, Aalto- and Helsinki University
- Industry: SSH, Bittium, Insta, Sectra, Advenica and Tosibox; important security companies applying PQC in their solutions
- In steering group: Traficom, DVV and Defence Forces; important government stakeholders related to national security
- There was close collaboration with NIST through research exchange

PQC Finland Consortium

Aalto-yliopisto

Policy brief

- ”Kvanttiturvalliset salausmenetelmät Suomessa”,
  Latvala, Vallivaara and Mellin
- Published 16.9.2022
- Introduction to quantum threat, pqc advices and good practices for decision makers
- The current state and future preparedness of quantum-safe encryption methods in Finland.

Implementing PQC

- Master thesis -> conference paper -> journal paper by Julius Hekkala.
- “Implementing Post-quantum Cryptography for Developers”, Hekkala, Muurman, Halunen, Vallivaara, in SN Computer Science
- We integrated and tested three lattice-based post-quantum algorithms into a fork of Crypto++, a C++ cryptography library.
  - https://github.com/juliushekkala/cryptopp-pqc
- The complex mathematical ideas behind the algorithms make implementation challenging

Quantum safe signing in smart vehicles

- Master thesis & conference paper by Sara Nikula
- "Quantum-Safe Signing of Notification Messages in Intelligent Transport Systems", Nikula, Halunen, and Vallivaara, in EAI AC3 2022
- In the intelligent transport system the signatures are created by using elliptic curve cryptography, which is not quantum safe
- We integrated three quantum-safe signature algorithms
  - CRYSTALS-Dilithium, FALCON and (Rainbow)
- Our results show that quantum-safe digital signature algorithms could be used in intelligent transport systems, with only moderate changes to performance in signing and verification

Continuation project: BlimPQC

- Preparations for new Co-Innovation project: **BLimPQC: Beyond the Limits of Post-Quantum Cryptography**
- Under Bittium's "veturi" ecosystem: Seamless and Secure Connectivity
- The project will answer to new challenges both in research and implementation
- Research: VTT, Aalto, Helsinki Uni. and Oulu Uni.
- Industry: Bittium, SSH, Xiphera, Jutel, Icareus, and Ericsson

Huoltovarmuuskeskus
Försörjningsberedskapscentralen
National Emergency Supply Agency

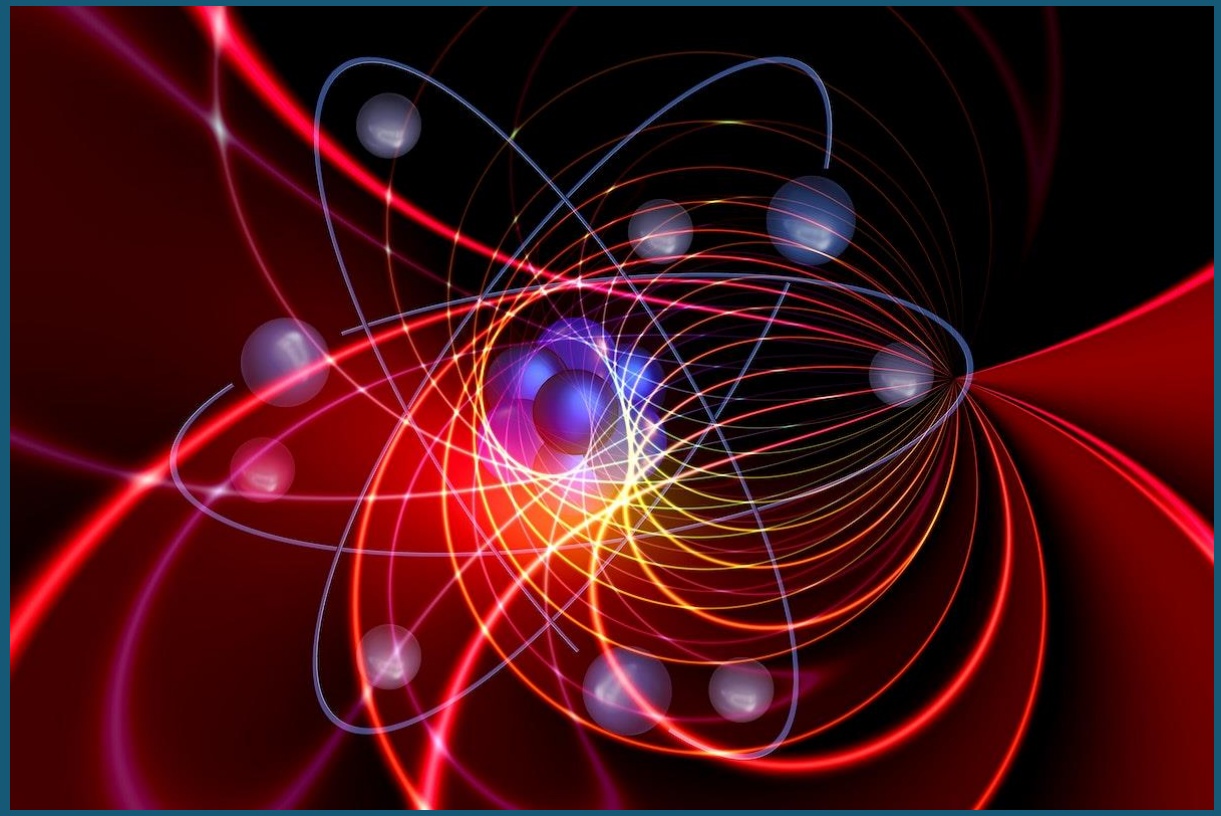
VTT

PQC for National Emergency Supply organisations

- ”Kvanttilaskennan tietoturvavaikutuksiin varautuminen”
- Ongoing research project for HVK digipooli Jan 2024-May 2024, 30k€

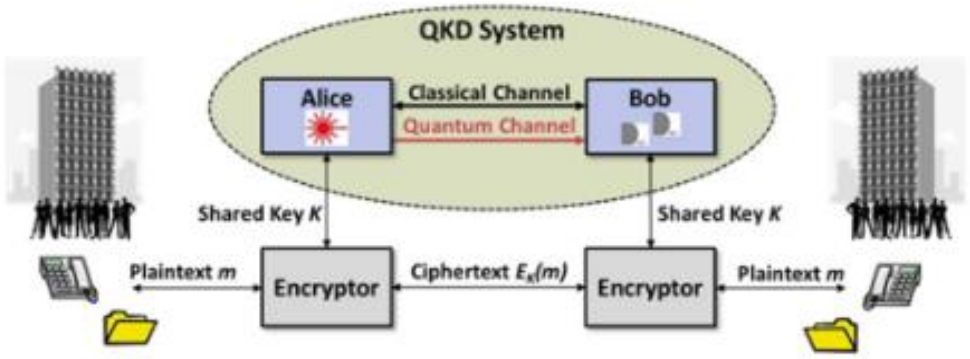
1. Diagnosis
   - What is the stance towards PQC migration?
   - Risk assessment and inventory of crypto assets
2. Planning
   - PQC Roadmap
3. Execution
   - Cryptographic agility
   - Hybrid solutions

Quantum Communication



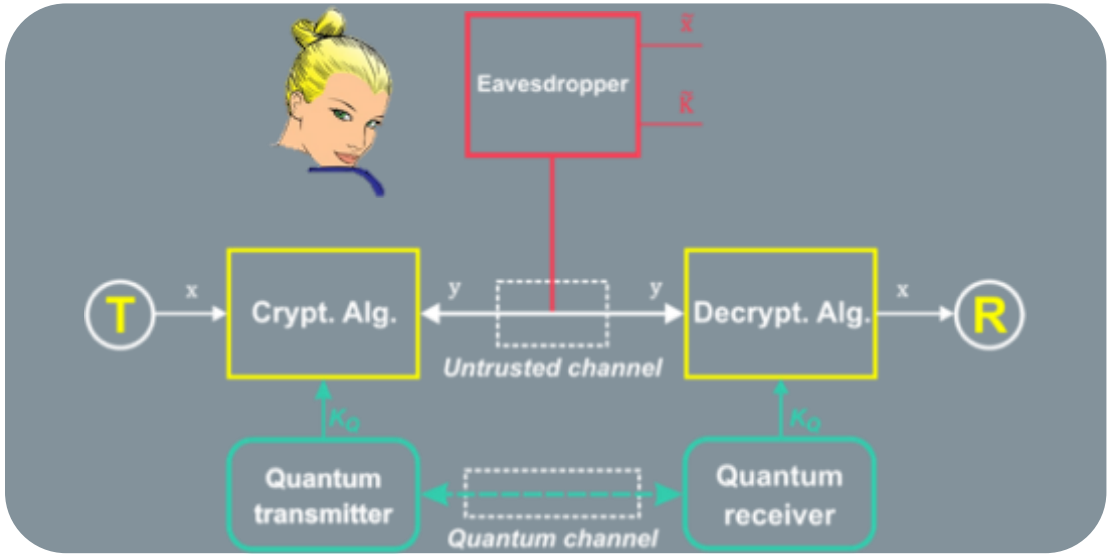
Alternative solution: Quantum Communication

- In quantum communication random symmetric keys are generated and shared securely without having to use asymmetric cryptography to secure the channel or having to communicate in person to exchange them.
- It provides a secure channel to send completely random keys.
- This can be done by quantum random number generation (QRNG) and quantum key distribution (QKD).



Quantum Key Distribution(QKD)

- Exploit quantum mechanics laws for establishing secure keys
- Single photons/weak coherent pulses transmission for generation of quantum keys
- Classical channel for encrypted messages
- Using One time Pad (OTP) encryption (or others encryption algorithm)
  Alice and Bob can share secret messages
- PQC and Quantum Communication can complement each other in PQC/QKD hybrid solutions



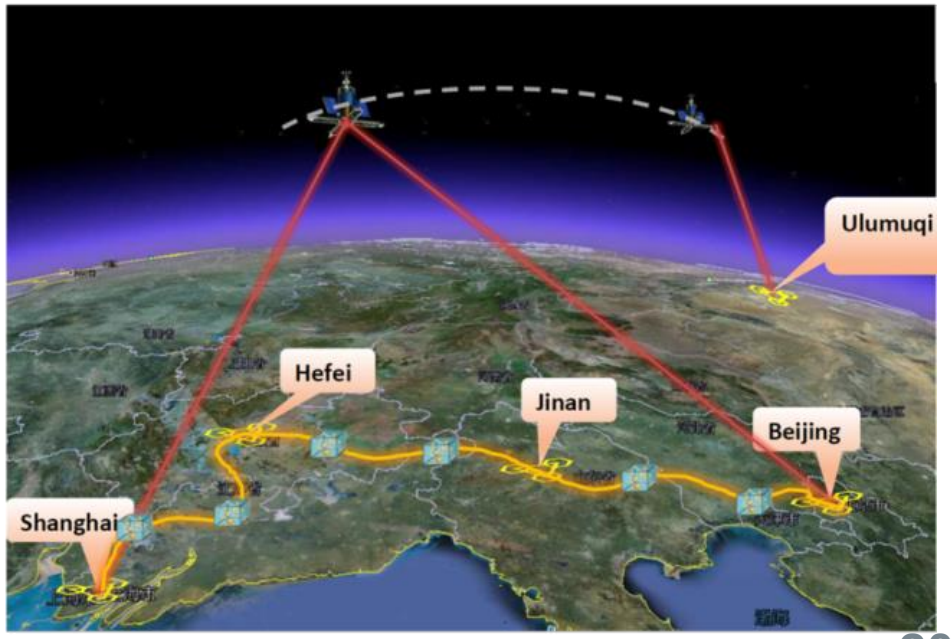
Potential applications

- Critical infrastructures (e.g. the Smart Grid)
- Financial institutions
- National defense (with major **limitations**)
- QKD networks deployed in
  - Asia: China, South Korea, Japan
  - Europe: Austria, Italy, UK, Switzerland
  - America: USA (DARPA, Los Alamos)
- Max key rate: 10 Mbps (10 Km)
- Max distance: 405 km (6.5 bps)

Cannot have both at the same time

IDQ
FROM VISION TO TECHNOLOGY

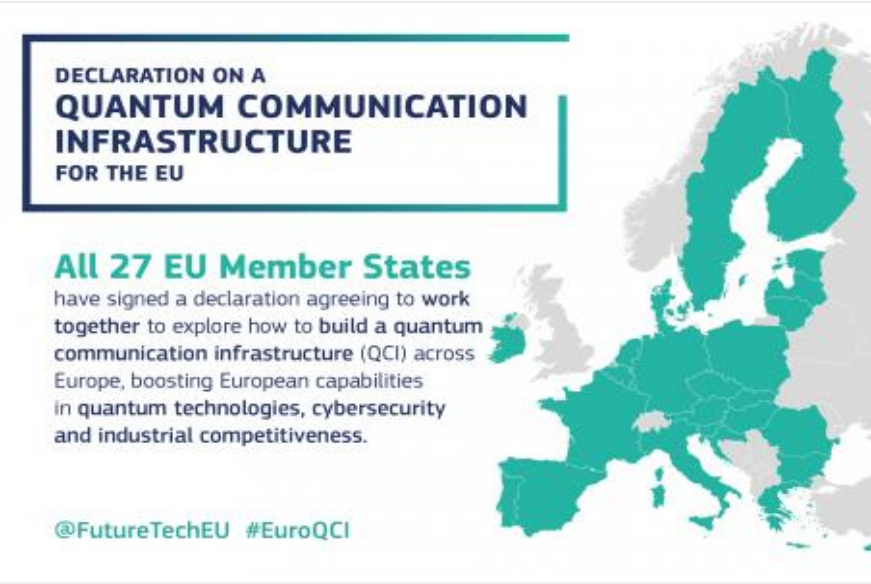
TOSHIBA
Leading Innovation



VTT – beyond the obvious

National **Q**uantum **C**ommunication **I**nfrastructure in **Fi**nland **NaQCI.fi**

- **NaQCI.fi** is the Finnish consortium joining to the EuroQCI (“European Quantum Communication Infrastructure”)
  - VTT, CINIA, ERVE, CSC, - Coordinator: Kari Seppänen/VTT
- The expected outcome of the project is clear plans for a cost-effective deployment of the national quantum communication infrastructure
- The main goal of the NaQCI.fi project is to test and gain experience on QKD technology both for Metropolitan and Long-Distance links in Finland.
- Total funding 8.2 m€, duration 1.2023-6.2026



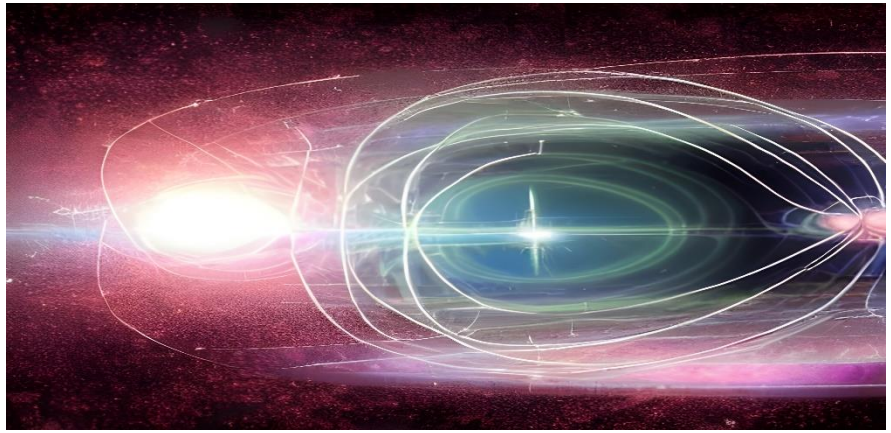
Secure Communication via Classical and Quantum Technologies

- Funded by **NATO** Science for Peace and Security (SPS) Programme
- Total budget 350 000 EUR and duration 2023-2025.
  - Kick-off at VTT on 30.3.2023
- NATO country Project Director: Dr. Rainer Steinwandt
  - Partner country Project Director: Visa Vallivaara
- Participants:
  - The University of Alabama in Huntsville, USA
  - VTT Technical Research Centre of Finland
  - Universidad Rey Juan Carlos, Spain
  - Academy of Sciences and University of Technology in Bratislava, Slovakia

Summary

Summary

- Quantum computing will some day break our current PKI, e.g. key exchange and digital signatures
- Harvest now decrypt later threat
- Quantum safe solutions exist and NIST PQC standard is coming
- In Finland we have studied and implemented PQC solutions
- Quantum communication is theoretically safe but not yet practical.



beyond

the obvious

Visa.vallivaara@vtt.fi
Visa Vallivaara | LinkedIn