TEAPQC

Transition Easily and Automatically to Post-Quantum Cryptography

Visa Vallivaara visa.vallivaara@vtt.fi
Senior Scientists of Applied Cryptography

Successful R&I in Europe 2024

02/02/2024 **VTT – beyond the obvious**

If your Expected Outcome, Scope or Special Conditions ...

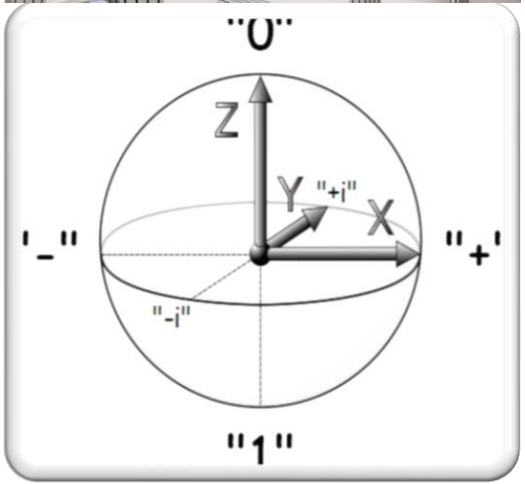
- ...has a term...
  - "security" or "cybersecurity"
  - "privacy"
  - "best practices" or "future", or...
- … requires connecting two or more devices over Internet... or ...
- … aims at high-TRL...

… then please put everything else aside for a moment:

here may be something to make your proposal stronger.

Quantum Threat

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



Quantumly hard

Quantumly easy but classically hard

Classically easy problems

Post-Quantum Cryptography (aka 'quantum resilience')

- All the applications, systems and projects that we plan now should be designed to be quantum safe to be future-proof
- Current public key cryptography is based on math problems which can be broken with an effective quantum computer
- IBM has roadmap for an error corrected quantum computer in 2029
- USA will enforce migration to PQC algorithms by 2030
- **Harvest now and decrypt later** threat (e.g. health data)
- NIST PQC standard will be ready during 2024 but implementing and using the algorithms correctly is challenging

… today, PQC is mandatory for future-proofness of everything

VTT Applied Cryptography team Expertise

- Post-Quantum Cryptography (**PQC**)
- Homomorphic encryption and Light Weight Cryptography (LWC)
- Quantum key distribution (QKD)
- Cyber security related quantum research
- Privacy preserving technologies

- Interested to participate in consortiums who need experts in **future-proof cyber security** and cryptographic solutions
- Ready to coordinate HORIZON-CL3-2024-CS-01-02: **Post-quantum cryptography transition - TEAPQC**
  - Effective crypto inventory, automatization of different steps in the migration, long term crypto analysis, sidechannel analysis

Key References

PQC Publications:

- **Implementing Post-quantum Cryptography** for Developers
  - Hekkala, Muurman, Halunen, Vallivaara, in SN Computer Science 2023
- **Quantum-Safe Signing** of Notification Messages in Intelligent Transport Systems
  - Nikula, Halunen, Vallivaara, EAI AC3 2022
- Applying a **cryptographic metric** to post-quantum lattice-based signature algorithms
  - Rautell, Latvala, Vallivaara, Halunen, ARES 2022

Research Projects:

- Coordinator of **PQC Finland**: www.pqc.fi
  - National research project with 9 partners and budget about 6 M€ during 1.2020-6.2022
- Coordinator of national EuroQCI research project NaQCI.fi: www.naqci.fi
- Partner country project director in NATO SPS research project
  - "Secure Communication via Classical and Quantum Technologies", 2023-2025.
- National coordinator of Secur-e-Health ITEA project

visa.vallivaara@vtt.fi