Using Post Quantum Cryptography for Self-Sovereign Identity Today

Erik Hieta-aho, PhD

Senior Scientist
Applied Cryptography

VTT – Technical Research Centre of Finland

VTT is a large research institute in Finland

Work on security and privacy technologies: research and implementation

Our team has experts in applied cryptography

VTT in numbers
Creating impact over 80 years

284 M€
operating income

2,355
employees

450
patent families

50+
start-ups*

45%
of the net turnover from abroad

1,135
customers

488
scientific articles

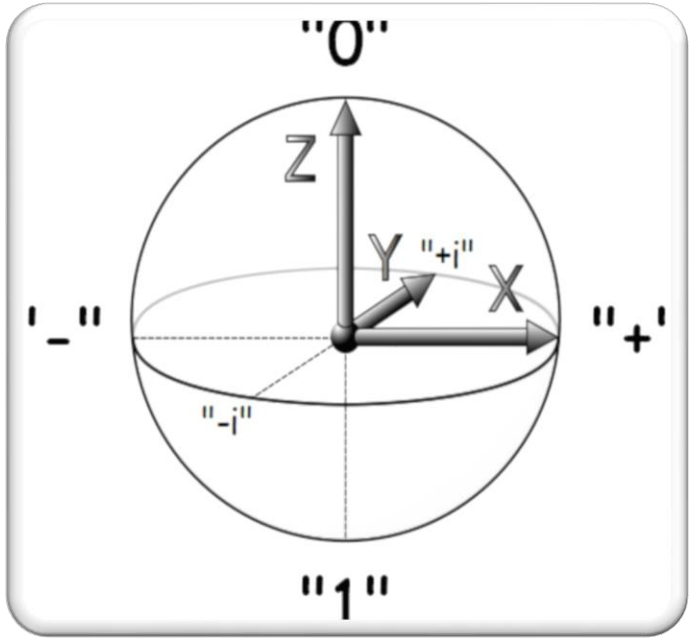
75
Net promoter score (NPS)

VTT Group (2023). *) Rolling data

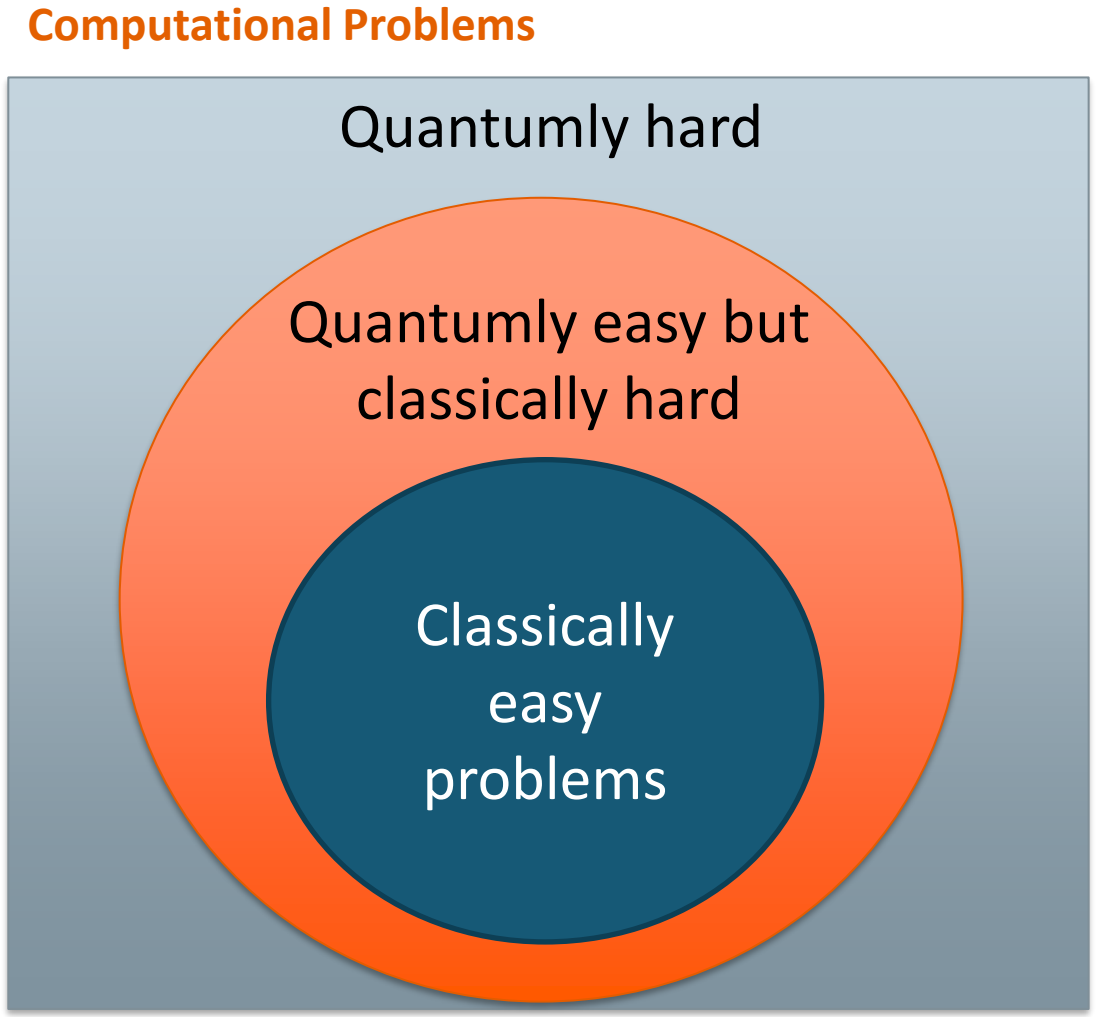
Quantum Computing and Shor’s Algorithm

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

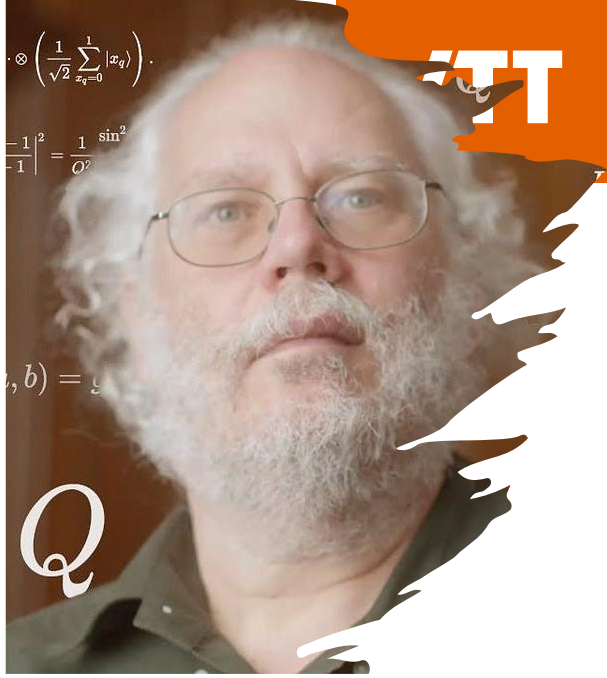


Quantumly easy problems



© John Preskill

Quantum threat on Cryptography



- Current public key cryptography is based on three different mathematical problems:
  - Factoring, discrete logarithm in finite fields and elliptic curves
- Shor's algorithm on a suitable quantum computer will break these
- At risk: RSA, Diffie-Helman and Elliptic Curve
- Data can be stolen today, stored, and later broken with quantum
- Grover's algorithm would roughly halve symmetric key lengths
- Typical applications (e.g. TLS) combine an asymmetric key agreement and symmetric encryption

Quantum Computing status

Quantum Research seems to be accelerating

- While recently attending theQuantum World Congress, there were multiple companies claiming 2029 to be the year that error corrected quantum computers will be viable and practical.
  - Quantinuum – Fully fault tolerant and universal quantum computer in 2029- 100s of logical qubits
  - IBM – 2029 error corrected logical qubits, 100M gates
  - Microsoft claimed that we are now in the setting of reliable quantum computing.
  - Google Quantum AI – focused on logical qubit design

Gartner

Search

Advanced

Ask Peers | Conferences | Magic Quadrants | Hype Cycles | Events and Webinars | Initiatives

Top Strategic Technology Trends for 2025: Postquantum Cryptography

21 October 2024 - ID G00818769 - 7 min read

By Mark Horvath, Sarah Almond, **and 1 more**

Initiatives: Technology Innovation and Strategy

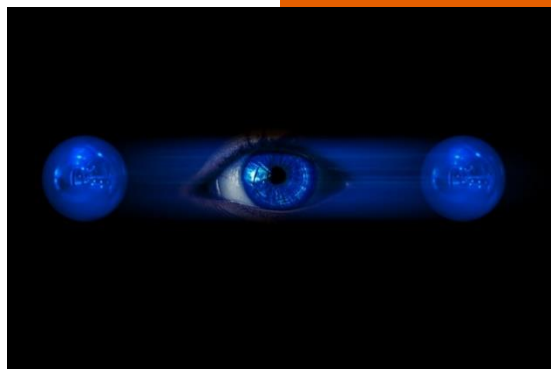
Conventional cryptography is under threat from quantum computing, which will render it unsafe to use by 2029. This research describes why IT leaders should prepare to move to postquantum cryptography as a matter of urgency to protect their data and how to begin the process.


IBM Quantum
System Two
RTE 01
RTE 02
RTE 03
RTE 04


IBM Quantum
System Two
IBM Quantum
System Two
IBM

Post-Quantum Cryptography (PQC)

PQC Algorithms



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

Standardization of PQC by NIST

- 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
  - Aug 2024 – Announced the first 3 standards FIPS 203, 204 and 205
  - Round four continuing evaluation of BIKE, HQC, and McEliece.

NIST Digital signature schemes

- Another competition for digital signature schemes that are based on hardness problems that aren't lattice-based.
  - In 2023 there were **40 signature schemes** accepted in round 1.
  - Recently NIST announced that they have **accepted 14** of the 40 signatures into round two of evaluation. This second phase of evaluation and review is estimated to last 12-18 months.
  - CROSS, FAEST, HAWK, LESS, MAYO, Mirath (merger of MIRA/MiRitH), MQOM, PERK, QR-UOV, RYDE, SDitH, SNOVA, SQIsign, and UOV.
- https://csrc.nist.gov/pubs/ir/8528/final

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, 2022

2 Min

PRESS RELEASE | Publication 11 April 2024

Commission publishes Recommendation on Post-Quantum Cryptography

Earlier this week, the Commission published a Recommendation on Post-Quantum Cryptography to encourage Member States to develop and implement a harmonised approach as the EU transitions to post-quantum cryptography. This will help to ensure that the EU's digital infrastructures and services are secure in the next digital era.

While quantum technologies will bring many economic and societal benefits, advances in quantum computing are expected to make it easier for malicious actors to access sensitive data, unless we advance our cryptography.

It is vital that communications remain protected in the future for the security of our citizens, societies, economies and the EU's digital single market. Post-Quantum Cryptography is one of the solutions to this future threat, as it is based on mathematical problems that are difficult even for quantum computers to solve. As a software-based solution, post-quantum cryptography is compatible with our existing infrastructures in several sectors, and so can be deployed relatively swiftly.

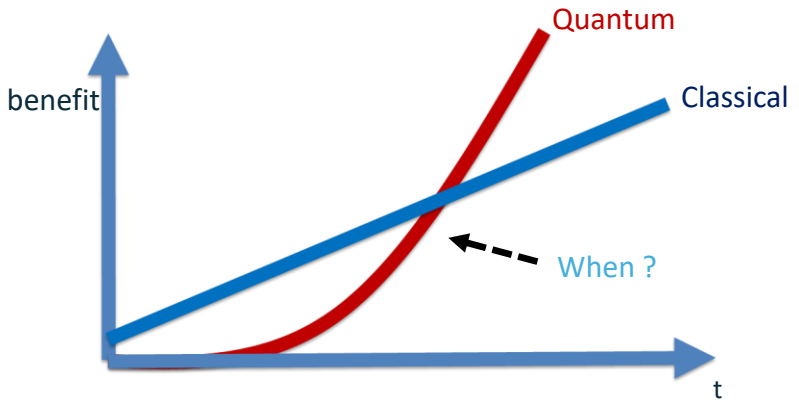
The Recommendation addresses the need for a coordinated approach to Europe's transition to a

iStock photo Getty images plus

Related topics

Cybersecurity

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 = 10, x = 5 and y = 5 means you need to start to prepare today!

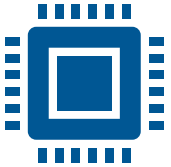
Thanks to Dr. Michele Mosca for the formula!

Hybrid PQC Self-Sovereign Identity stack

Hybrid PQC Self-Sovereign Identity Stack

Self-Sovereign Identity

Cross-border



Hybrid post quantum cryptography

Self-Sovereign Identities Stack

- Self-Sovereign Identities (SSI) allows users to control their identity
- Users have **digital credentials** (e.g. driver's license credentials, ePassports, University credentials)
- An SSI ecosystem requires a software stack
  1. Wallet
  2. Issuer
  3. Verifier
- We are supporting the open source solution walt.id

Post-quantum & hybrid cryptography

- Quantum computers threaten cryptography used in SSI
- **Post-quantum cryptography** (PQC) is resistant to quantum attacks
- In the short term:
  - PQC has just recently been standardized (Aug 13th)
  - PQC does not have a long track record
- **Hybrid cryptography** combines quantum-resistant and classical cryptography
  - In particular we are focused on a hybrid digital signature scheme that implements both ML-DSA (Dilithium) and ECDSA in parallel.

VTT, Finland and Ohio University, USA

Collaboration with Ohio University developing a transatlantic SSI stack

- SSI in the US and EU

- https://vcplayground.org/
  - Allows for testing implementations of a large variety of verifiable credentials
- OU partners have their own implementation of the SSI stack and we plan to be able to verify/issue credentials between our two systems

“Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the granting authority can be held responsible for them. Funded within the framework of the NGI Sargasso project under grant agreement No 101092887.”

NGI SARGASSO

Co-funded by the European Union

beyond

the obvious

Erik Hieta-aho
Erik.Hieta-aho@vtt.fi