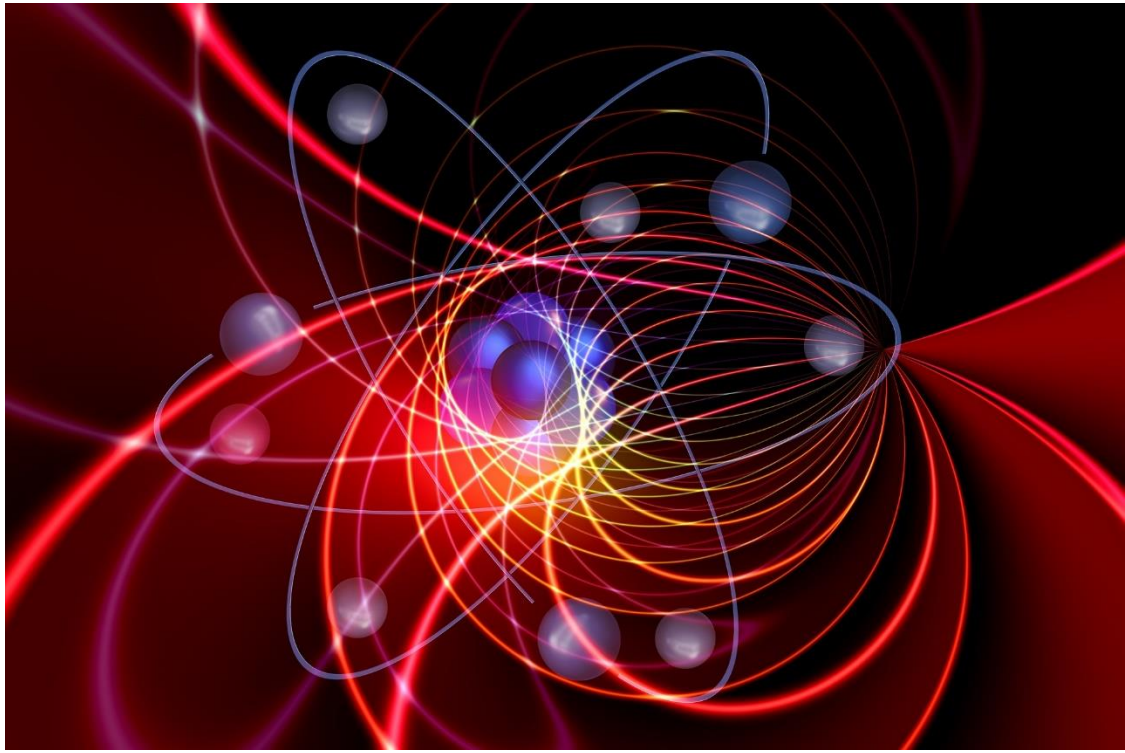
Post-Quantum Cryptography

Kimmo Halunen

Quantum computing vs cryptography

- Both encryption (through key exchange) and authentication (digital signatures) are in danger from quantum computers
- Currently quantum computers have some dozens of qubits and can not yet solve cryptographic problems
- To be effective in solving cryptography, quantum computers need qubits in the order of millions (based on current state of the art)
- When will we have such quantum computers?



NIST Standardisation

- In cryptography NIST has arranged several competitions for new standards
- In PQC they have a similar approach
- Earlier only one winner (AES, SHA-3), but now for PQC probably several algorithms will be standardisesd and for different uses
  - Encryption and signatures are considered separately

Current status

- Finalists have been announced in July
- These have been grouped into two pools: finalists and alternative candidates
- Alternative candidates are considered in case there are new, major issues found in finalists and may be standardised later
- More research on these is needed

*Comparing with RSA**

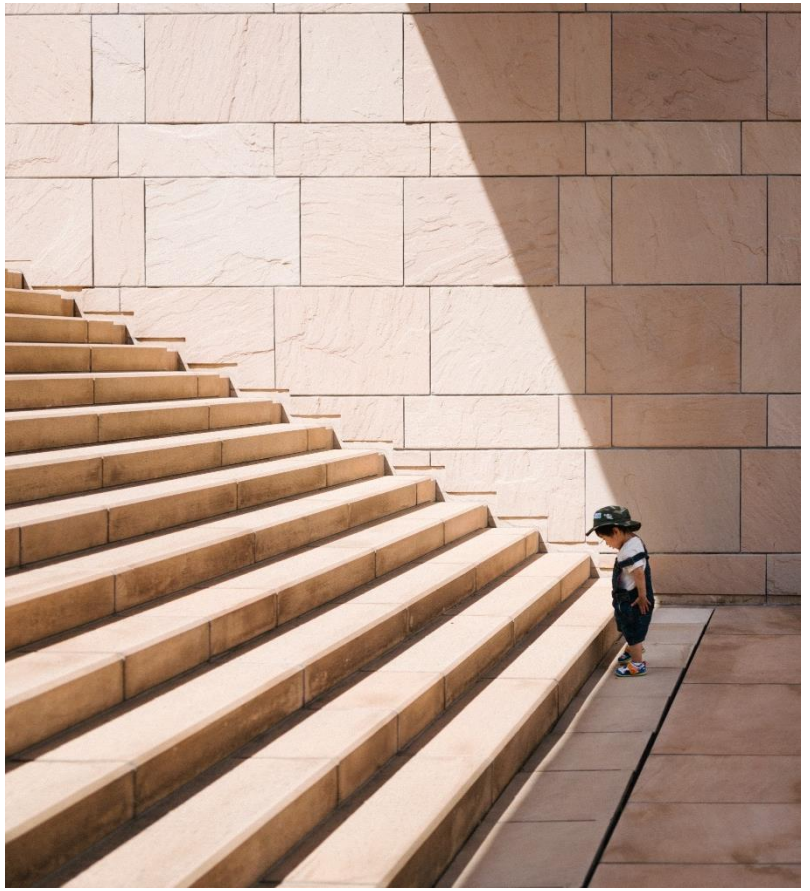
scheme	sk size	pk size	sig size	pk + sig
dilithium2	7.3	3.1	5.3	8.4
falcon512dyn	3.3	2.3	1.7	4.1
gemss128	37.8	1087.0	0.1	1087.1
picnic2l1fs	0.1	0.1	32.0	32.1
rainbow1a	261.0	396.1	0.2	396.3
sphincsf128	0.2	0.1	44.2	44.3

- SK size matters for implementations
- All applications care about sig size
- Most care about PK
- Cert chains care about PK+sig

*Sizes in terms of 3K RSA key and signature sizes

Next steps

- Standard will be ready in 2024
- At the moment very conservative evaluation
  - Only systems that have been scrutinised for a relatively long period of time are conidered
- Implementing these in different systems will be a huge challenge for the latter half of 2020s



beyond the obvious

Kimmo Halunen

@khalunen