How Quantum Computers threat security of PKIs and thus eIDs

@Open Identity Summit 2021

Holger Funke and Sebastian Vogt

secunet Security Networks AG

Overview of the talk

Identity is our most valuable asset and any future threat
such as quantum computing should be anticipated!

01 The Quantum Threat

02 When do we have to be prepared for this threat?

03 How can we prepare? – Example quantum-safe CSCA

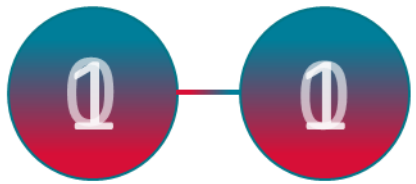
04 Summary

Quantum Computer

- Quantum Computers are based on law of quantum mechanics
  - Superpositions
  - Entanglement

  } kind of parallel computing → huge speedup
- Qubit is basic unit of quantum information
- Quantum computer are able to solve certain problems much faster
- Will not replace classical computers

Classical bits



Qubits

Quantum-Algorithm

Shor-Algorithm (1994)

- Efficient factorization of large integers (breaks security of RSA)
- Efficient calculation of discrete logarithm (breaks security of ECC)
- Runs in polynomial time
- Needs large-scale quantum computer

» New quantum-safe asymmetric algorithms needed (Post-Quantum-Cryptography)

Grover-Algorithm (1996)

- Fast searching in unsorted databases of size N in square root N iterations
- Needs large-scale quantum computer
- Halves the bit security of symmetric algorithms

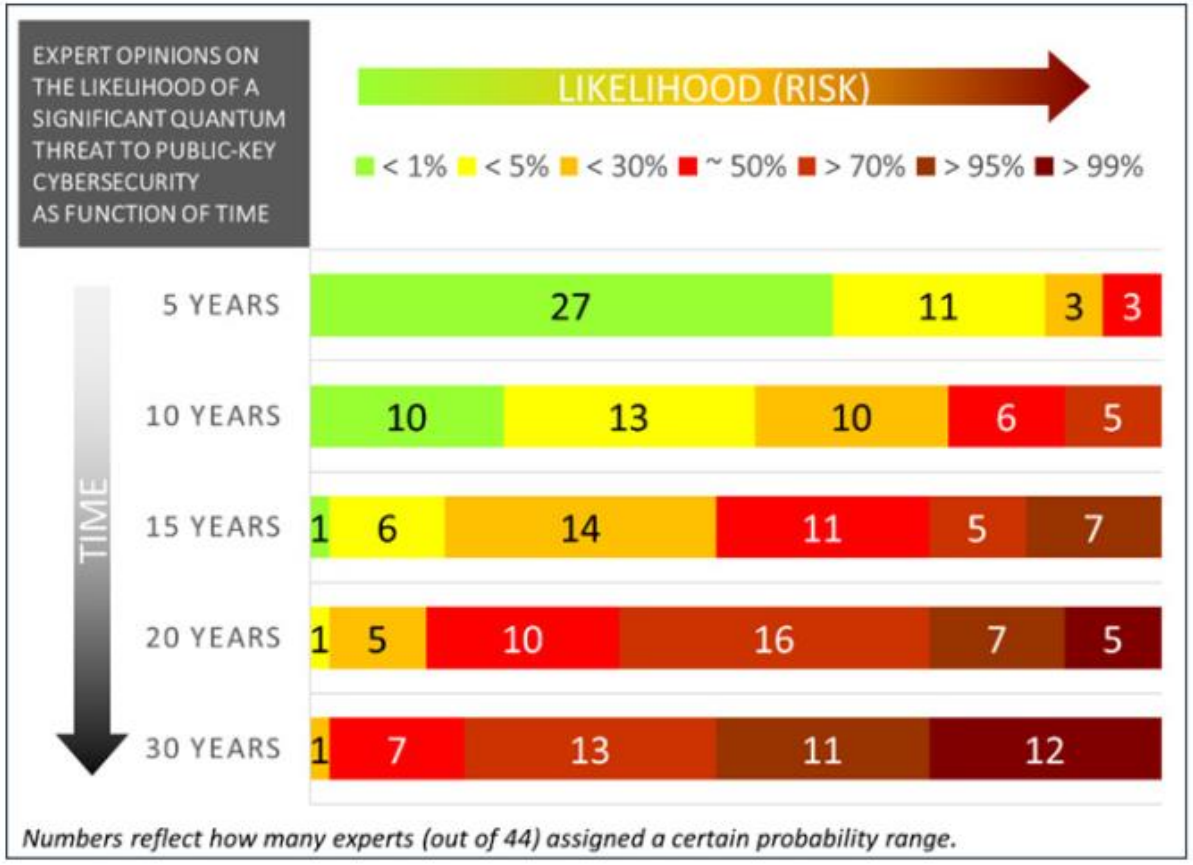
» Double size of symmetric keys resp. output length of Hash-Functions

Impacts on current Cryptography

Type	Algorithm	Classical bit security	Quantum bit security	Quantum attack
Asymmetric	RSA 2048	112	**0**	Shor´s Algorithm
	RSA 3072	128		
	ECC 256	128		
	ECC 521	256		
Symmetric	AES 128	128	**64**	Grover´s Algorithm
	AES 256	256	128	

When can we expect large-scale quantum computers?

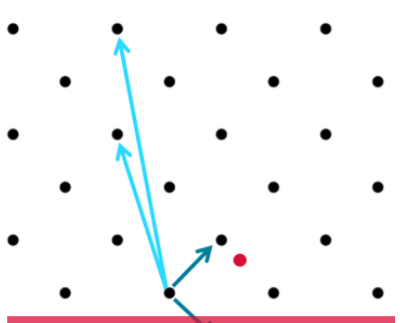
- Quantum threat timeline report 2020 of Global Risk Institute
- Optimistic interpretation:
  - Maybe not in next 10 years
  - >50 % likelihood in 15 years



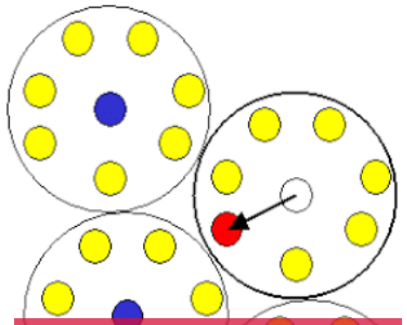
https://globalriskinstitute.org/publications/quantum-threat-timeline-report-2020/

Post-Quantum-Cryptography

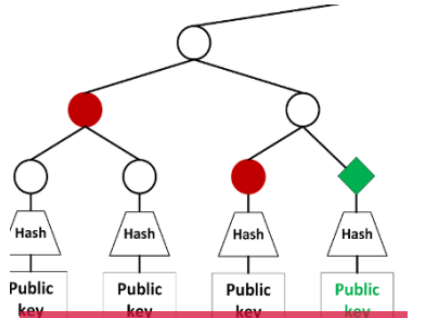
The security is based on hard mathematical problems that are assumed to be resistant against both classical and quantum attacks.



Lattice-based Cryptography



Code-based Cryptography



Hash-based Signatures

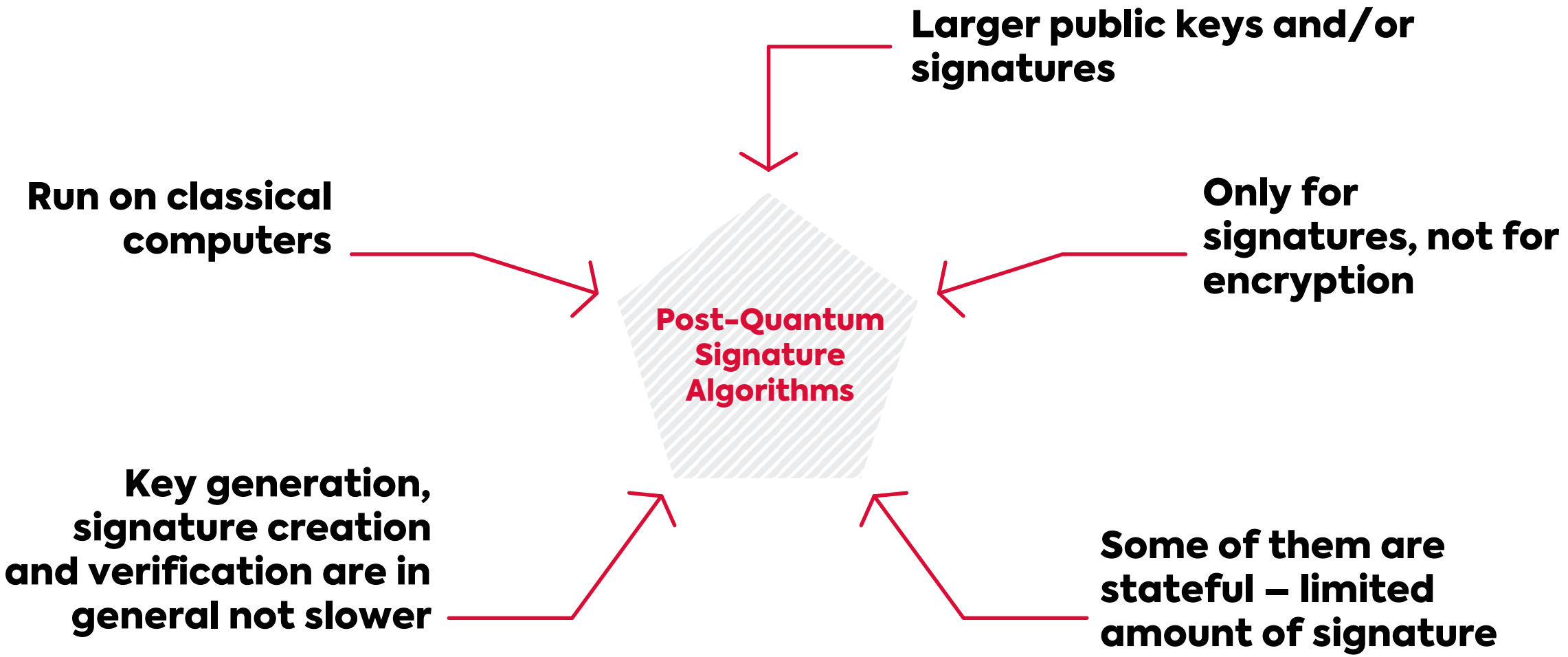
$$\sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(1)} \cdot x_i \cdot x_j + \sum_{i=1}^{n} p_i^{(1)} \cdot x_i + p_0^{(1)} = 0$$
$$\sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(2)} \cdot x_i \cdot x_j + \sum_{i=1}^{n} p_i^{(2)} \cdot x_i + p_0^{(2)} = 0$$
$$\vdots$$
$$\sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(m)} \cdot x_i \cdot x_j + \sum_{i=1}^{n} p_i^{(m)} \cdot x_i + p_0^{(m)} = 0$$

Multivariate Cryptography

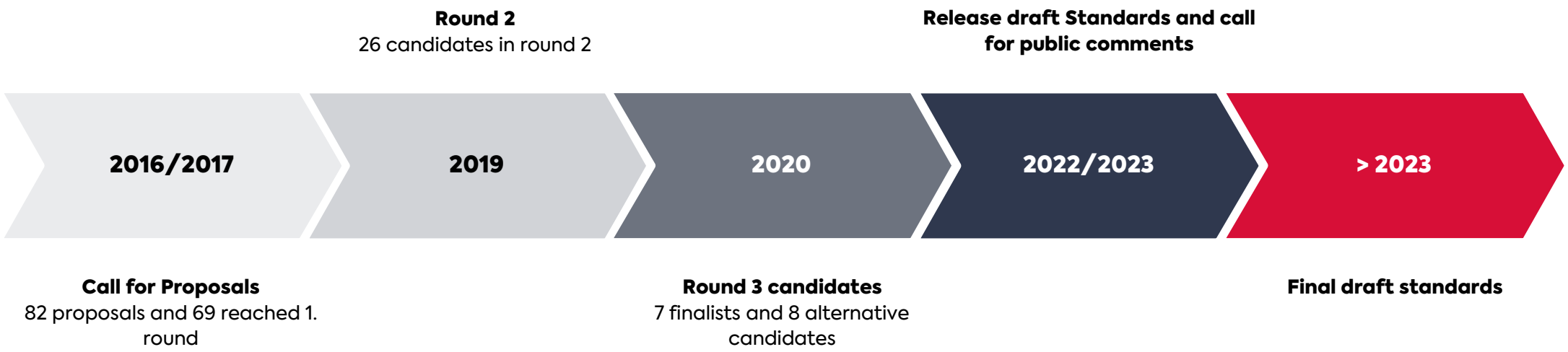
$$\begin{array}{ccc} E & \xrightarrow{\phi_A} & E/\langle A\rangle \\ \downarrow{\scriptstyle \phi_B} & & \downarrow{\scriptstyle \phi'_B} \\ E/\langle B\rangle & \xrightarrow{\phi'_A} & E/\langle A,B\rangle \end{array}$$

Isogeny-based Cryptography

Post-Quantum Signature Algorithms



NIST-Process Post-Quantum-Cryptography



PQ Signature Algorithms for PKI

Stateful hash-based

- XMSS (RFC 8391) and LMS (RFC 8554)
- Evaluated and standardised
- Stateful: Only one signature for each state
- Limited amount of possible signature per private key (around one thousand or one million)

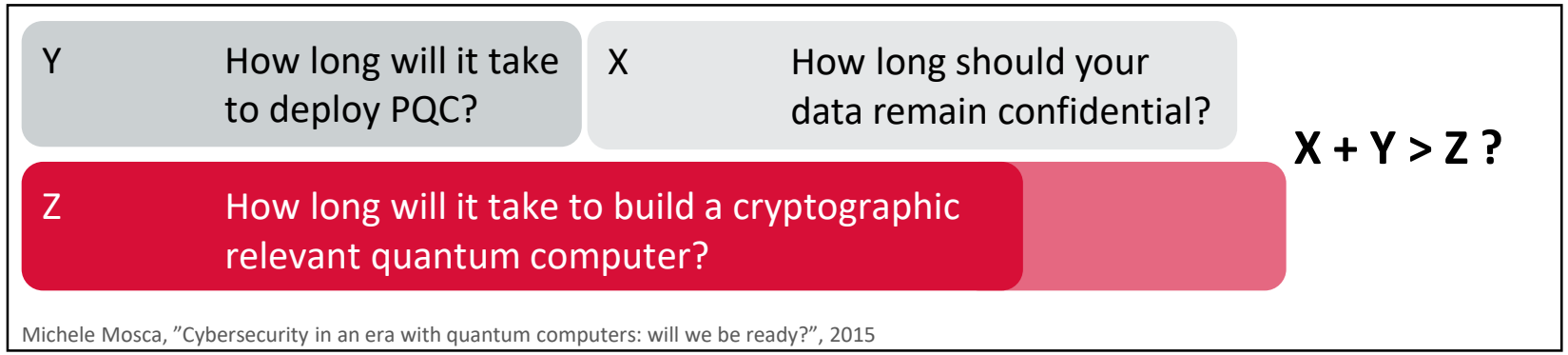
» Can be used right now, but not suitable for all use-cases

NIST process

- Dilithium or Falcon (both lattice based) are the most promising once
- Third finalist Rainbow not suitable for PKI
- Alternative candidate SPHINC+ might be suitable as well
- At first hybrid approach might be needed

» We need to wait until NIST process is over, but should already test usage of lattice based schemes in our applications/protocols today

Use case CSCA



Use case CSCA

- X is 13 years
- Z might be 15 years (optimistic assumption)
- Y could be 4-5 years, but should not be larger than 2 years (based on X and Z)

» X + Y > Z

Use case CSCA

- Can we use stateful hash-based signature algorithms?
  - CSCA and Document Signers are used in a controlled environment
  - Limited amount of signatures needed for each CSCA (at least parameter set with one million signatures should be feasible)
- No need for hybrid certificates if stateful hash-based signature algorithms are used

- ICAO should evaluate whether stateful hash-based signature algorithms are suitable and update ICAO Doc 9303
- Fast migration of CSCAs is needed

Summary

The threat

- Large-scale quantum computers will be able to break currently used asymmetric cryptography.
- Data which shall be secure for more than 10 or 15 years (like eIDs) needs to be issued quantum-safe soon.

(Possible) solution (for CSCA)

- Stateful hash-based signature algorithms should be suitable for CSCA PKI.
- Evaluate whether stateful hash-based signature algorithms are suitable for other use-cases as well.
- As soon as standardisation of post-quantum algorithms (e.g. Dilithium or Falcon) is done, we should immediately be ready to use them.


secunet