Update on PQC: Standardization and Migration

Quantum Technology Workshop at CODE 2020

Leonie Bruckert, secunet AG

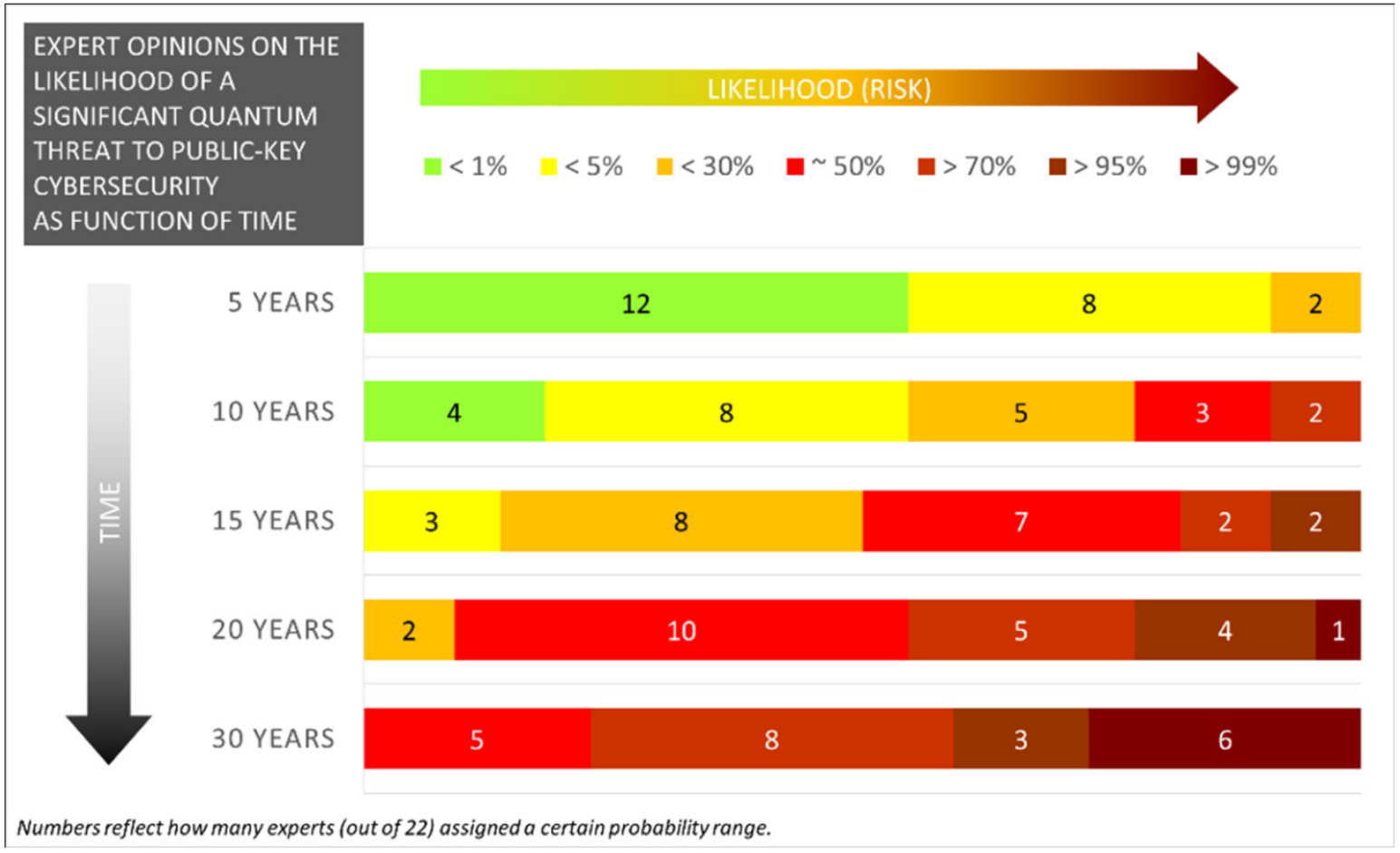
Agenda

01 Quantum Threat

02 Post-Quantum Cryptography and Standardization

03 Migration and Recommendations

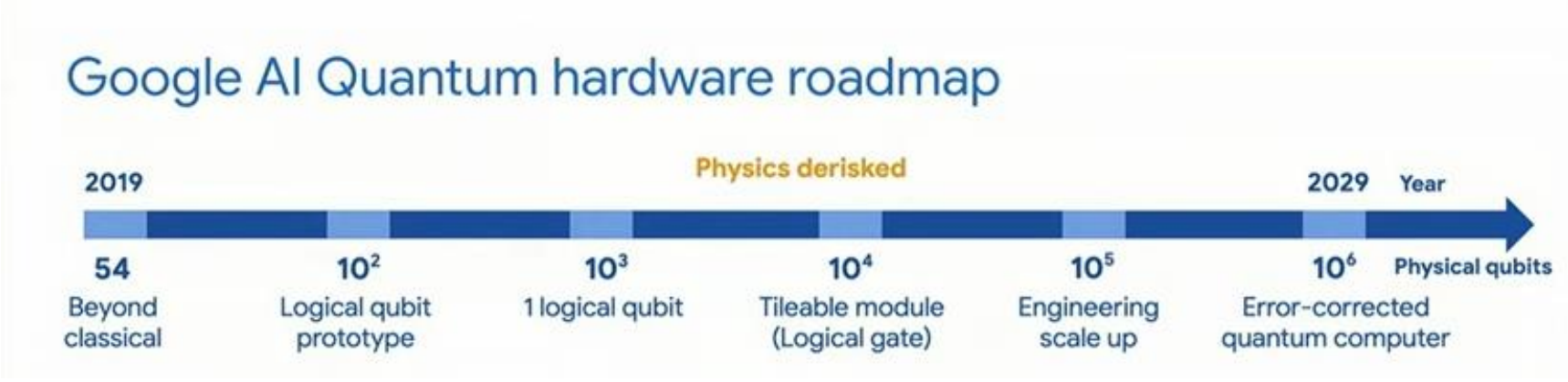
Quantum Threat (1)

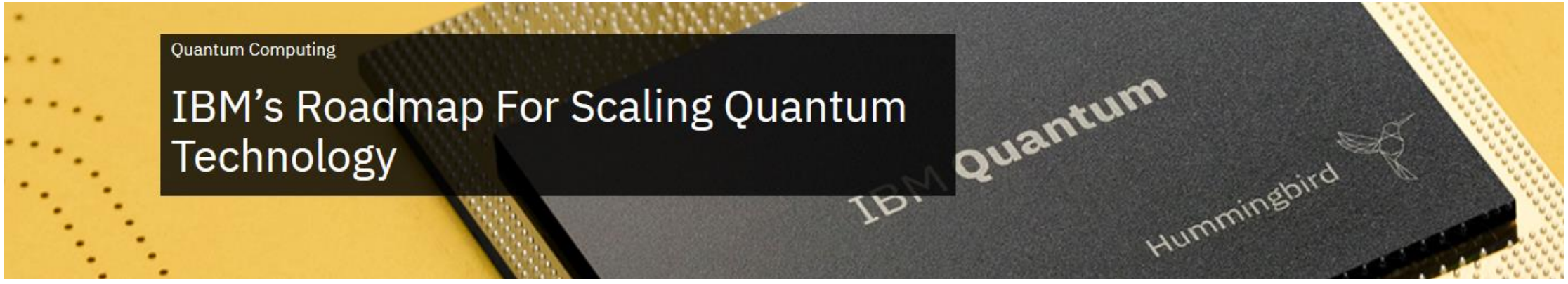


- Study from 10/2019
- More than 80 QC experts were asked for their estimation
- Only 22 experts sent a response

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

Quantum Threat (2)





[Reminder] Cryptographic Primitives

SYMMETRIC CRYPTOGRAPHY

Symmetric Ciphers e.g.

- AES

Hash Functions e.g.

- SHA-1
- SHA-2
- SHA-3

Message Authentication Code (MAC) e.g.

- HMAC
- CMAC

ASYMMETRIC CRYPTOGRAPHY

Asymmetric Encryption e.g.

- ElGamal
- ECIES

Digital Signatures e.g.

- RSA
- ECDSA

Key Exchange e.g.

- DH
- ECDH

Quantum Cryptanalysis

GROVER‘S ALGORITHM

Lov Grover, 1996

- Speeds up search in unstructured data base
  → key search

weakens symmetric ciphers and hash functions
e.g. AES, SHA2

» Increase key size and output length of hash functions

SHOR‘S ALGORITHM

Peter Shor, 1994

Solves efficiently

- The factoring problem
- The discrete logarithm problem

breaks conventional asymmetric cryptography
e.g. RSA, DH, ECC

» Develop new quantum-resistant algorithms

Quantum Resource Estimates

ECC		
[GM2019]	NIST P-224: 2042 logical qubits $\approx 4.91 \cdot 10^7$ physical qubits	NIST P-256: 2330 logical qubits $\approx 6.77 \cdot 10^7$ physical qubits
[HJN+2020]	NIST P-256: 2124 logical qubits	

RSA		
[GM2019]	RSA-2048: 4098 logical qubits $\approx 1.72 \cdot 10^8$ physical qubits	RSA-3072: 6146 logical qubits $\approx 6.41 \cdot 10^8$ physical qubits
[GE2019]	“How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits”	

» ECC is easier to break than RSA!

Classifying and Prioritizing Attack Scenarios

High priority

„low“ priority

„Store now, decrypt later“

- Intercept encrypted communication data and store it until large quantum computers are available

Malicious software updates

- Introduce malware via manipulated software updates with forged signatures

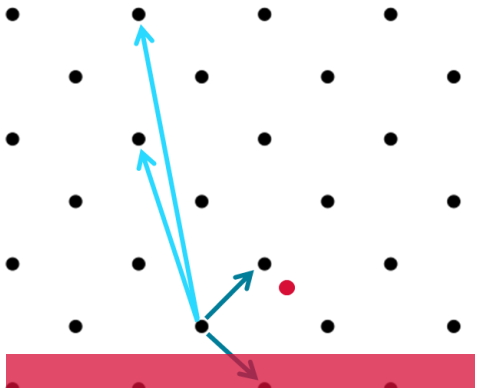
OFFLINE ATTACK

Man-in-the-middle

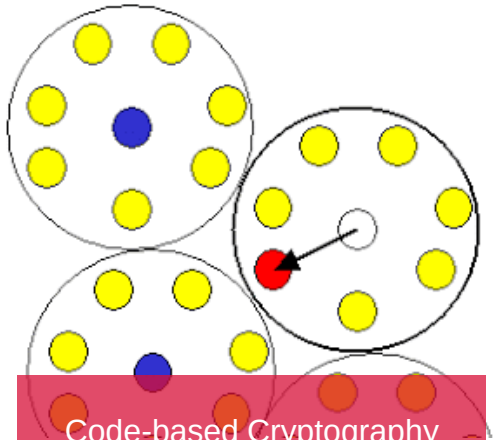
- Attack against short term authentication with forged signatures (e.g. establishment of an authenticated channel)

ONLINE ATTACK

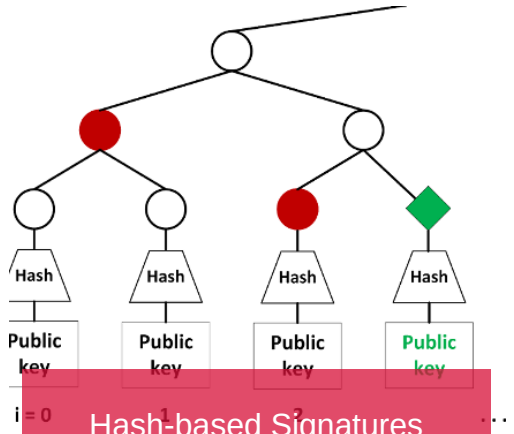
Post-Quantum Cryptography



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

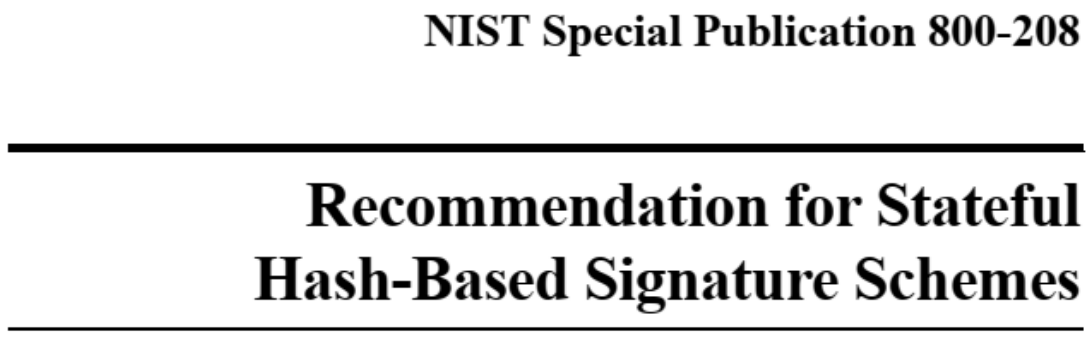
Hash-based Signatures

- Security is solely based on hash functions
- Building block: One-time Signatures (OTS)
  → A single signature per key pair!
- 1979, Ralph Merkle: binary hash trees
  → Limited number of signatures per key pair!
  → State management!
- Stateless hash-based signatures
  → Few-time Signatures (FTS)
  → Significantly larger signatures

» High confidence in security

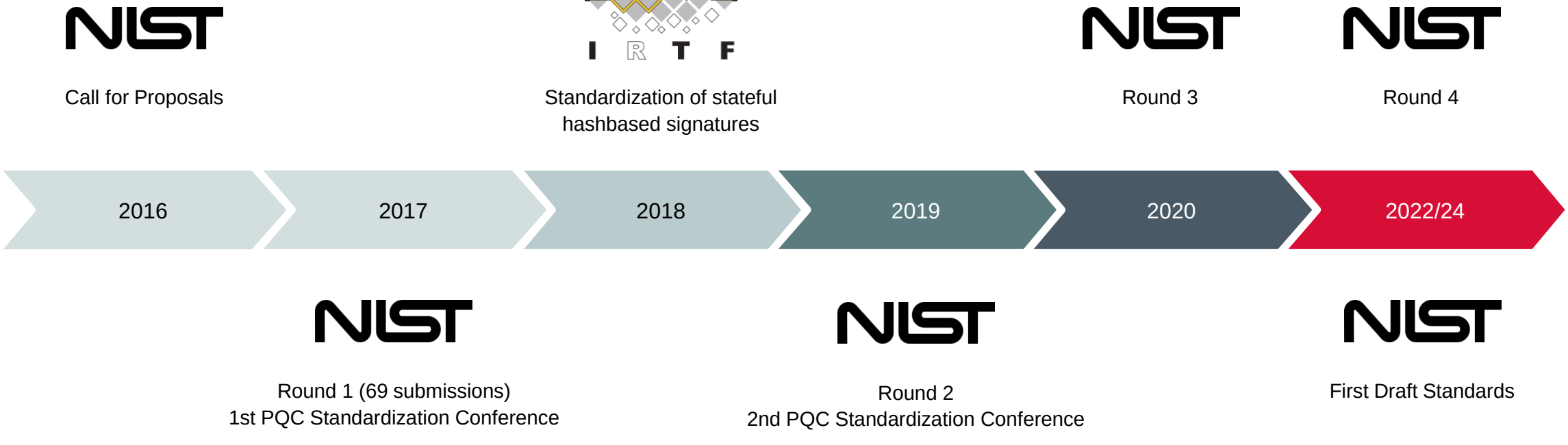
Two standardized stateful hash-based signature schemes

- eXtended Merkle Signature Scheme (XMSS)
  RFC 8391, 2018
- Leigthon-Micali Signatures (LMS)
  RFC 8554, 2019

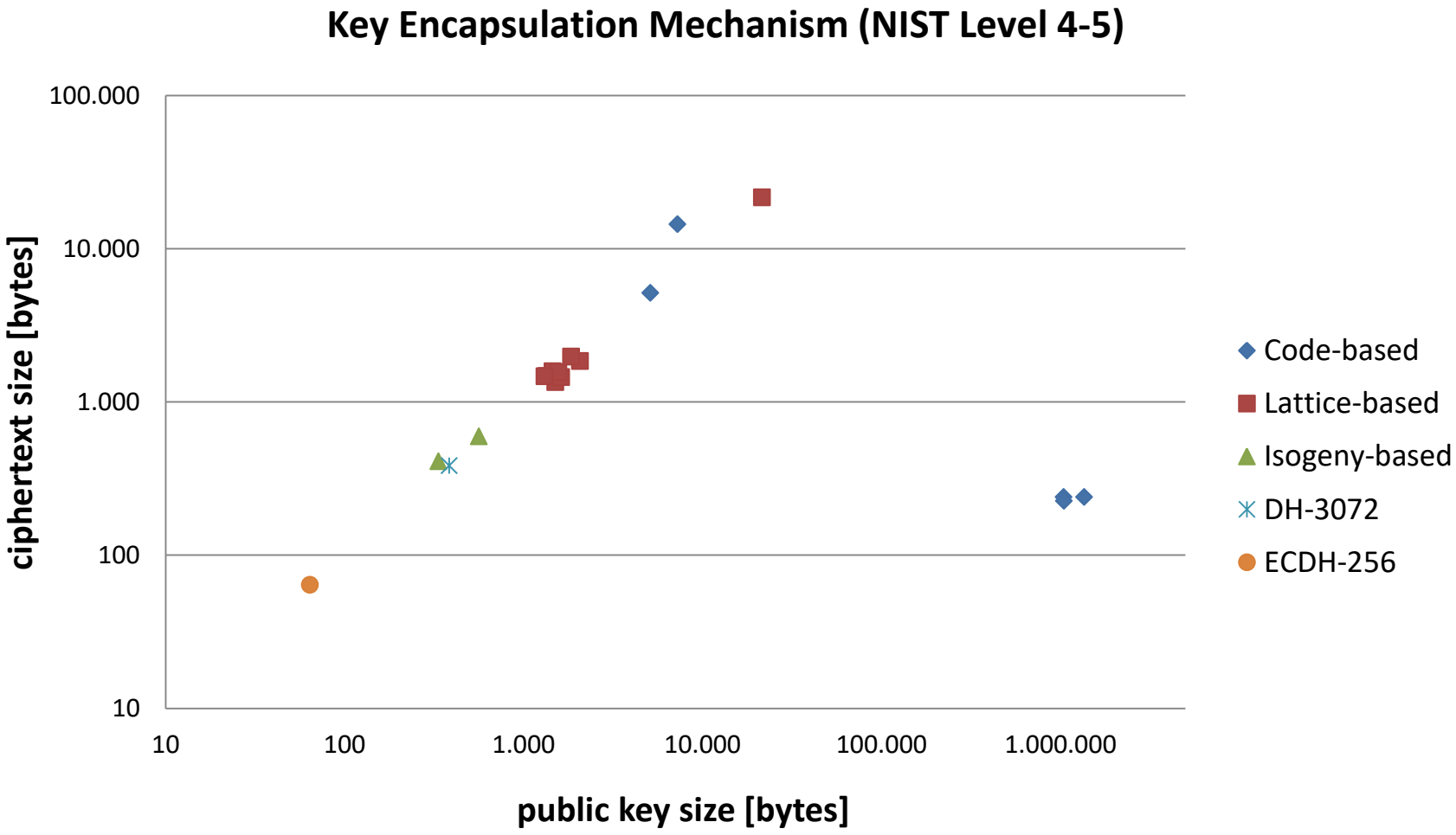

NIST Special Publication 800-208

Recommendation for Stateful
Hash-Based Signature Schemes

PQC Standardization - Timeline



NIST Standardization (1)



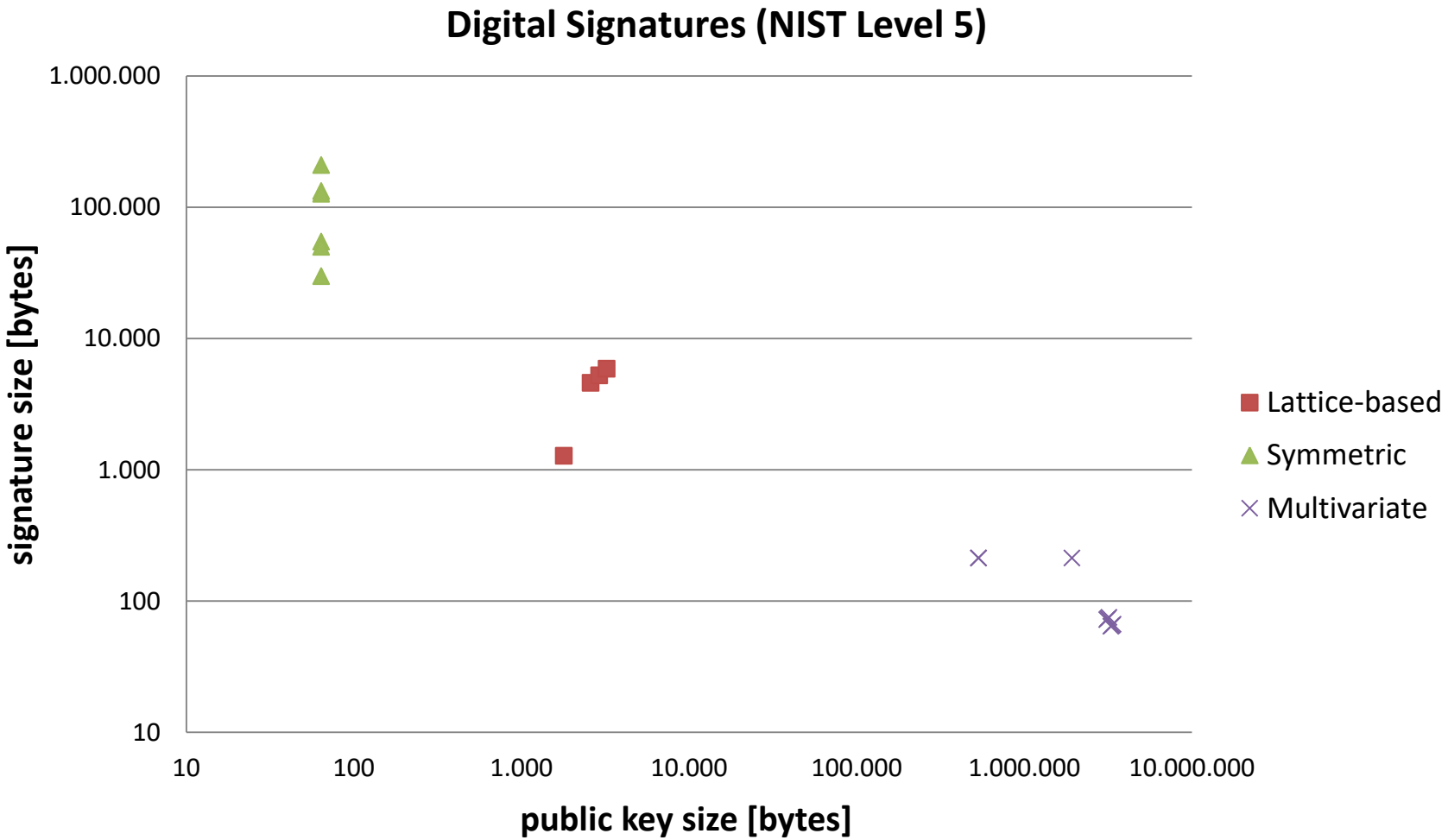
Finalists

Classic McEliece
CRYSTALS_KYBER
NTRU
SABER

Alternate Candidates

BIKE
FrodoKEM
HQC
NTRU Prime
SIKE

NIST Standardization (2)



Finalists

CRYSTALS_DILITHIUM
FALCON
Rainbow

Alternate Candidates

GeMSS
Picnic
SPHINCS+

Responding to Attack Scenarios

High priority

„low“ priority

„Store now, decrypt later“

→ Hybrid (classical + PQC) key exchange

Man-in-the-middle

→ PQC/Hybrid digital signatures

Malicious software updates

→ Stateful hash based signatures

OFFLINE ATTACK

ONLINE ATTACK

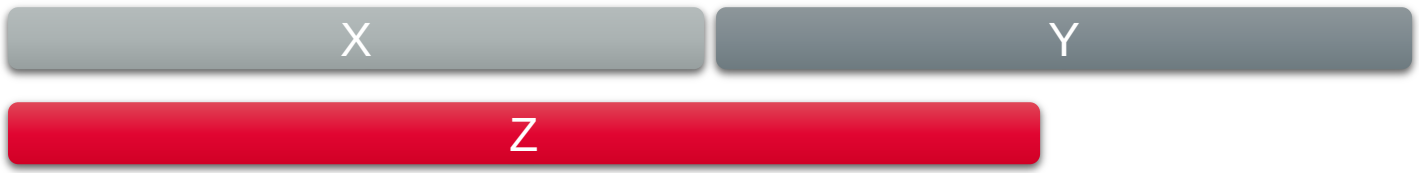
Migration to Post-Quantum Cryptography

X . . . How long should your data remain confidential?

Y . . . How long will it take to deploy PQC?

Z . . . How long will it take to build a cryptographic relevant quantum computer?

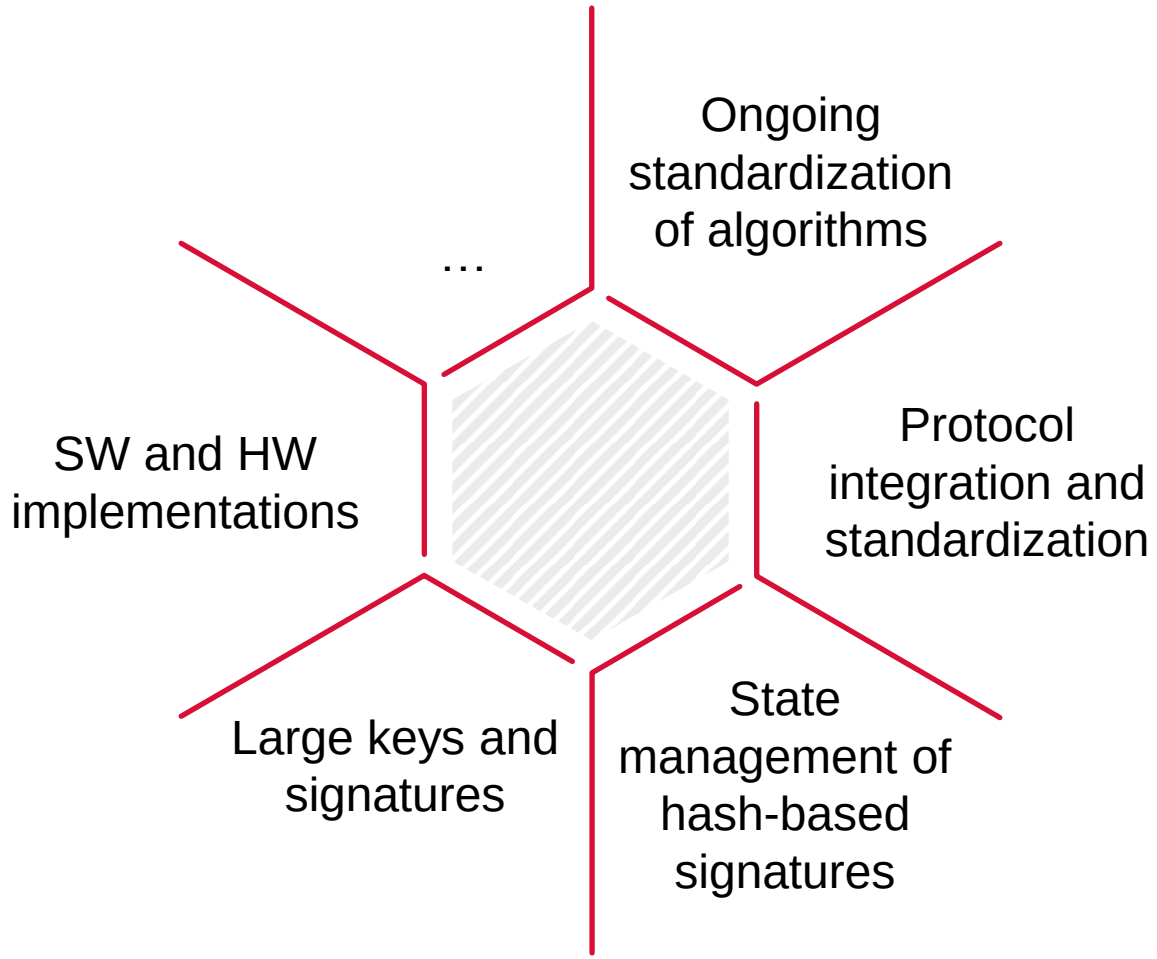
X + Y > Z ?



In addition, consider that data encrypted today can be (and actually is) intercepted, stored and decrypted later!

Michele Mosca in ”Cybersecurity in an era with quantum computers: will we be ready?” 2015

Migration Challenges



Further Standardization Activities

- draft-ietf-ipsecme-ikev2-intermediate-05
- draft-ietf-ipsecme-ikev2-multiple-ke-01
- draft-campagna-tls-bike-sike-hybrid-05
- draft-ietf-tls-hybrid-design-01
- draft-hoffman-c2pq-07

- ITU-T X.509 / ISO/IEC 9594-8

- Quantum-safe Algorithmic Framework
- Limits to Quantum Computing applied to symmetric key sizes
- Quantum-safe Threat Assessment
- Case Studies and Deployment Scenarios
- Quantum-Safe Key Exchanges
- Quantum-safe Virtual Private Networks
- Quantum-safe Identity-based Encryption
- Migration Strategies and Recommendations to Quantum-safe Schemes

Conclusion

- Deploy PQC as early as possible
  - Priority on key exchange and software updates
  - Use hybride mode = classical cryptography + PQC
- Develop migration strategies
- Adapt cryptographic protocols to PQC
  - standardization
  - cryptoagility
- Secure implementations in hardware and software

Act now!

Bundesamt
für Sicherheit in der
Informationstechnik

Migration zu
Post-Quanten-Kryptografie

Handlungsempfehlungen des BSI

Thank you for your attention!
Any Questions?

Leonie Bruckert

Beratung Defence

secunet Security Networks AG

leonie.bruckert@secunet.com