TeleTrusT-EBCA "PKI-Workshop" 2020

Berlin, 01.10.2020

"Adoption of quantum-safe crypto in PKI"

Dieter Bong, Utimaco

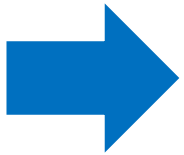

Quantum Computing will decimate the security infrastructure of the digital economy
Dr. Michele Mosca
Founder of the Institute for Quantum Computing, University of Waterloo

Quantum-safe cryptography

utimaco®

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

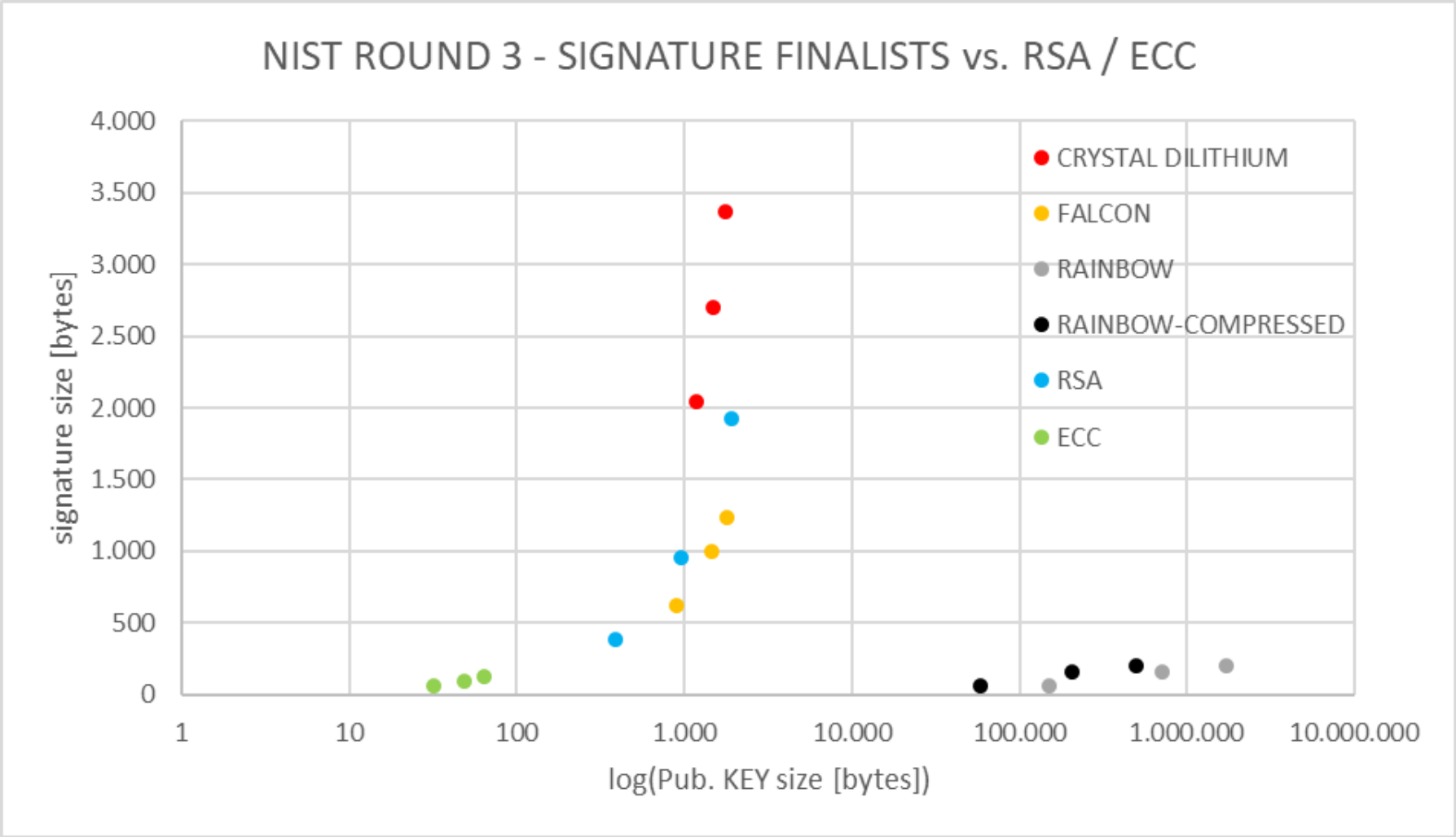
Type	Algorithm	Key Strength Classic (bits)	Key Strength Quantum (bits)	Quantum Attack
Asymmetric	RSA 2048	112	0	Shor's Algorithm
	RSA 3072	128		
	ECC 256	128		
	ECC 521	256		
Symmetric	AES 128	128	64	Grover's Algorithm
	AES 256	256	128	



NIST PQC Round 3 finalists

- Digital Signature
  - CRYSTALS-DILITHIUM
  - FALCON
  - Rainbow
- Public-key Encryption and Key-establishment
  - Classic McEliece
  - CRYSTALS-KYBER
  - NTRU
  - SABER

NIST ROUND 3 - SIGNATURE FINALISTS vs. RSA / ECC



Adoption of quantum-safe crypto in PKI

- What‘s the impact on certificate size ?
  - Communication overhead
- Is this performant (enough) ?
  - Key generation
  - Signature generation / verification
- And when do we go live ?