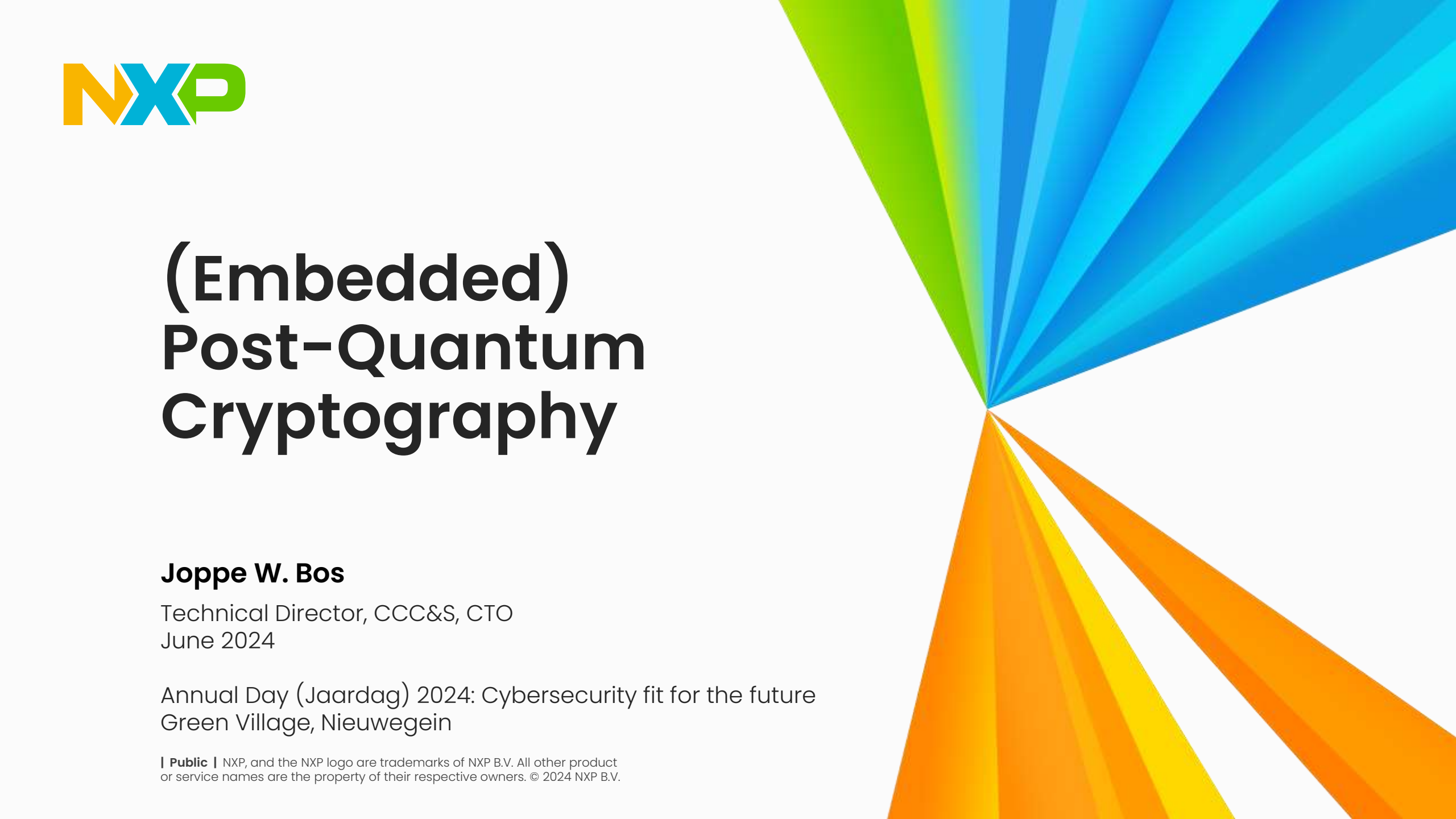


(Embedded) Post-Quantum Cryptography

Joppe W. Bos

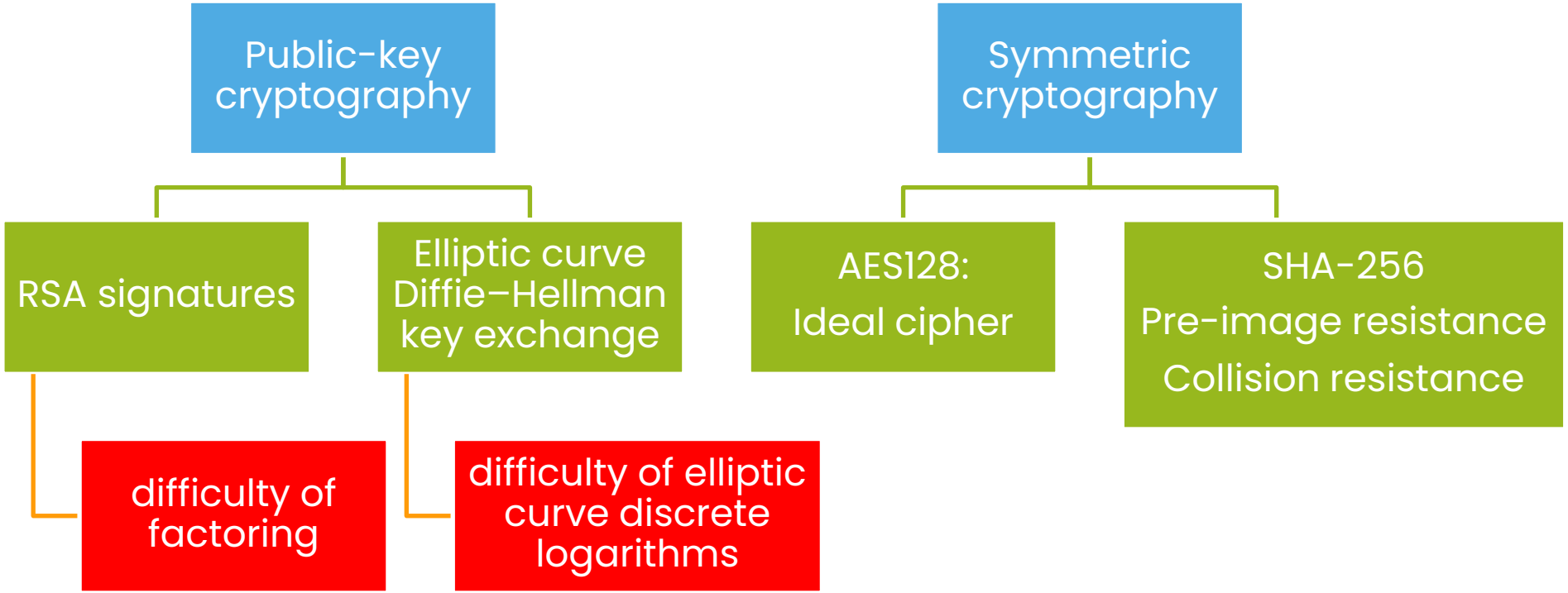
Technical Director, CCC&S, CTO
June 2024

Annual Day (Jaardag) 2024: Cybersecurity fit for the future
Green Village, Nieuwegein

Agenda

- Quantum Computing
- Post-Quantum Cryptography
- Standards
- Migration
- Awareness

Contemporary Cryptography
TLS-ECDHE-RSA-AES128-GCM-SHA256



QUANTUM CLOUD —

How IBM's new five-qubit universal quan computer works

IBM achie

CHRIS LEE - 5/4

Intel Delivers 17-Qubit Superconducting Chip with Advanced Packaging to QuTech

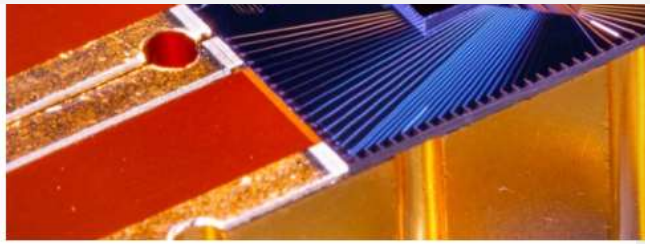
NEWS | 23 October 2019

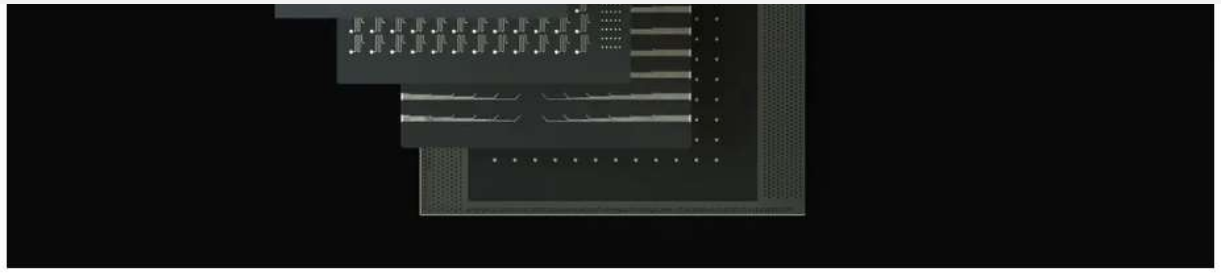
Hello quantum world! Goo Eagle's quantum performance

Development Roadmap

IBM Quantum

	2016–2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2033+
	Run quantum circuits on the IBM Quantum Platform	Release multi-dimensional roadmap publicly with initial aim focused on scaling	Enhancing quantum execution speed by 100x with Qiskit Runtime	Bring dynamic circuits to unlock more computations	Enhancing quantum execution speed by 5x with quantum serverless and Execution modes	Improving quantum circuit quality and speed to allow 5K gates with parametric circuits	Enhancing quantum execution speed and parallelization with partitioning and quantum modularity	Improving quantum circuit quality to allow 7.5K gates	Improving quantum circuit quality to allow 10K gates	Improving quantum circuit quality to allow 15K gates	Improving quantum circuit quality to allow 100M gates	Beyond 2033, quantum-centric supercomputers will include 1000's of logical qubits unlocking the full power of quantum computing
Data Scientist						Platform						
						Code assistant	Functions	Mapping Collection	Specific Libraries			General purpose QC libraries
Researchers					Middleware							
					Quantum Serverless	Transpiler Service	Resource Management	Circuit Knitting x P	Intelligent Orchestration			Circuit libraries
Quantum Physicist			Qiskit Runtime									
	IBM Quantum Experience		QASM3	Dynamic circuits	Execution Modes	Heron (5K)	Flamingo (5K)	Flamingo (7.5K)	Flamingo (10K)	Flamingo (15K)	Starling (100M)	Blue Jay (1B)
						Error Mitigation	Error Mitigation	Error Mitigation	Error Mitigation	Error Mitigation	Error correction	Error correction
						5k gates 133 qubits	5k gates 156 qubits	7.5k gates 156 qubits	10k gates 156 qubits	15k gates 156 qubits	100M gates 200 qubits	1B gates 2000 qubits
						Classical modular	Quantum modular	Quantum modular	Quantum modular	Quantum modular	Error corrected modularity	Error corrected modularity
						133x3 = 399 qubits	156x7 = 1092 qubits	156x7 = 1092 qubits	156x7 = 1092 qubits	156x7 = 1092 qubits		
	Early		Falcon		Eagle							
	Canary 5 qubits	Albatross 16 qubits	Penguin 20 qubits	Prototype 53 qubits								
			Benchmarking 27 qubits		Benchmarking 127 qubits							

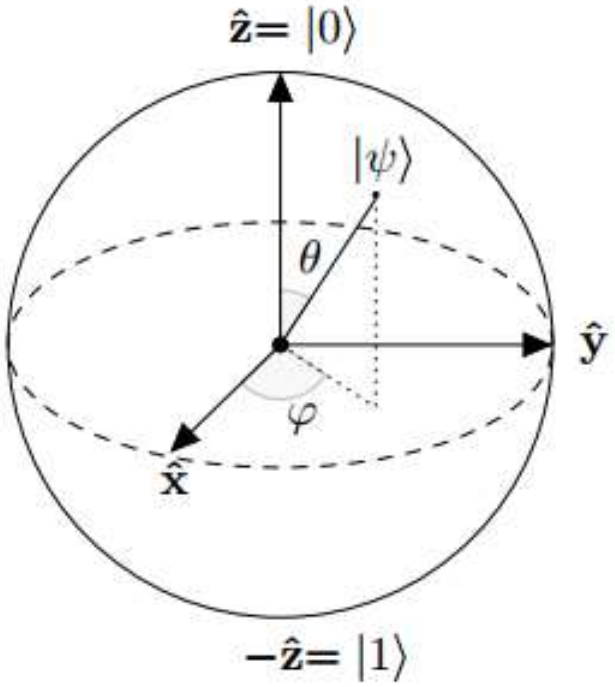




The Sycamore chip is composed of 54 qubits, each made of superconducting

Quantum Computing

Computer systems and algorithms based on principles of quantum mechanics
- Superposition
- Interference
- Entanglement



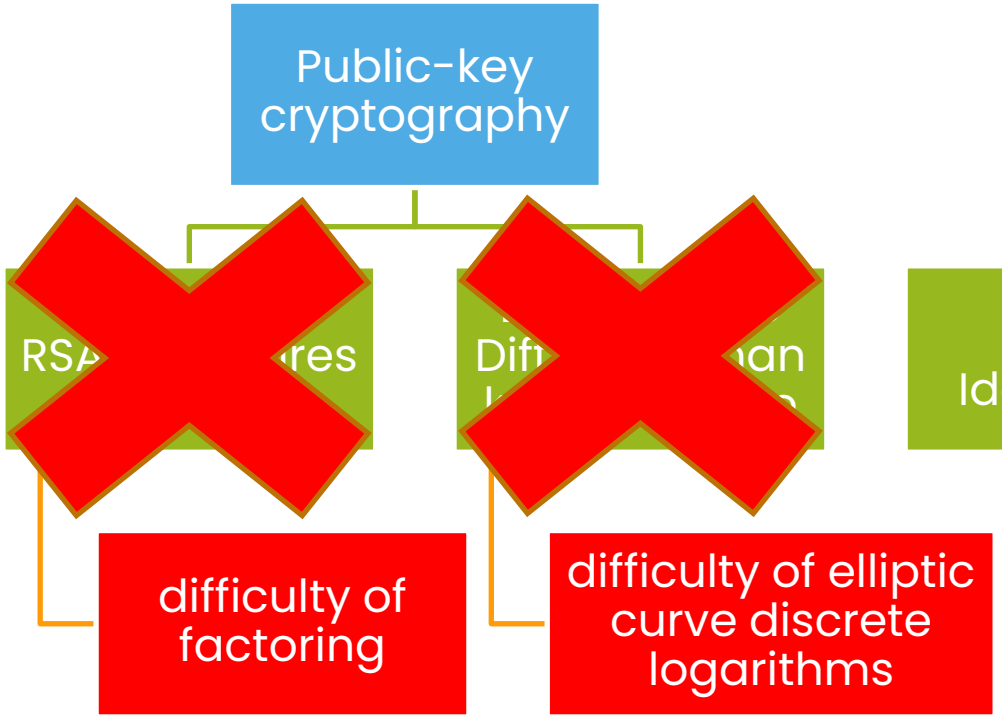
- A classical bit can only be in the state corresponding to 0 or the state corresponding to 1
- A qubit may be in a superposition of both states
  → when measured it is always 0 or 1

Shor's quantum algorithm (1994).
Polynomial-time algorithm to factor integers.
Impact. If we assume the availability of a large quantum computer, then one can break RSA instantly.

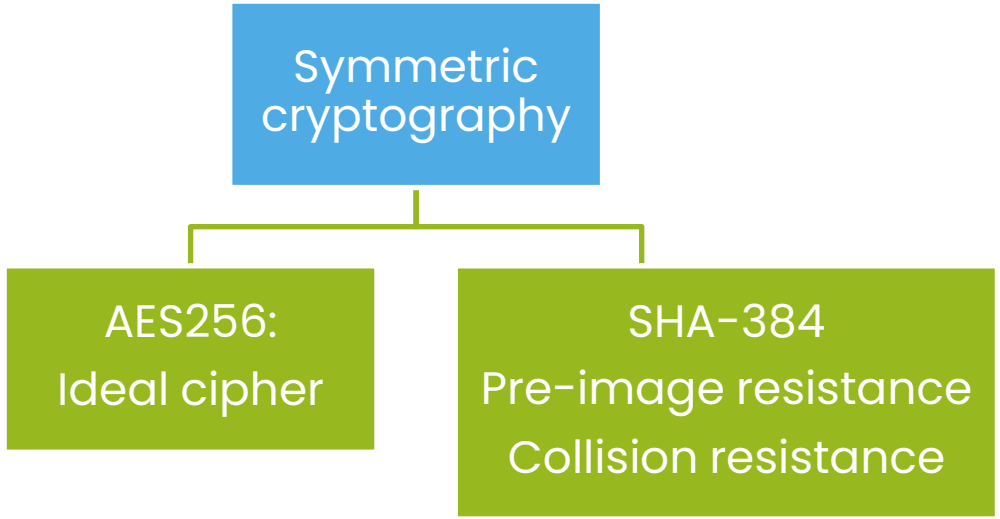
State-of-the-art.
IBM's 127-Qubit Quantum Processor
Break RSA-3072:
~10,000 qubits are needed

Contemporary cryptography
TLS-~~ECDHE-RSA~~-AES256-GCM-SHA384

"Double" the key sizes

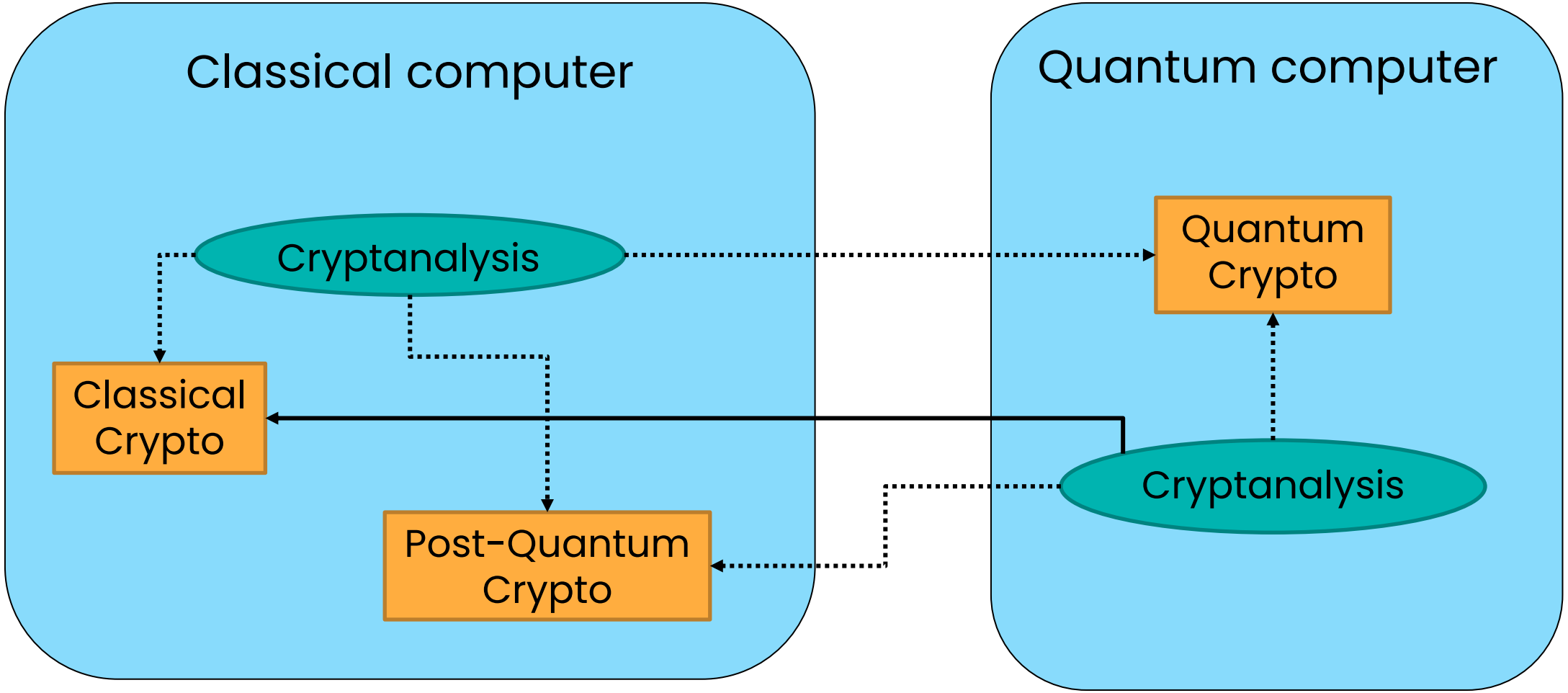


Shor's algorithm (1994)



Grover's algorithm (1996)

Post-quantum versus quantum crypto



Quantum Potential to Destroy Security as we know it

Confidential email messages, private documents, and financial transactions
Secure today but could be compromised in the future, even if encrypted

Firmware update mechanisms in vehicles
Could be circumvented and allow dangerous modifications

Critical industrial and public service infrastructure (for healthcare, utilities, and transportation using internet and virtual private networks)
Could become exposed – potentially destabilize cities

Audit trails and digitally signed documents associated with safety (auto certification and pharmaceutical authorizations)
Could be retrospectively modified

The integrity of blockchains
Could be retrospectively compromised - could include fraudulent manipulation of ledger and cryptocurrency transactions

PQC Migration Drivers

Standards

Prävention Detektion Reaktion

NIST

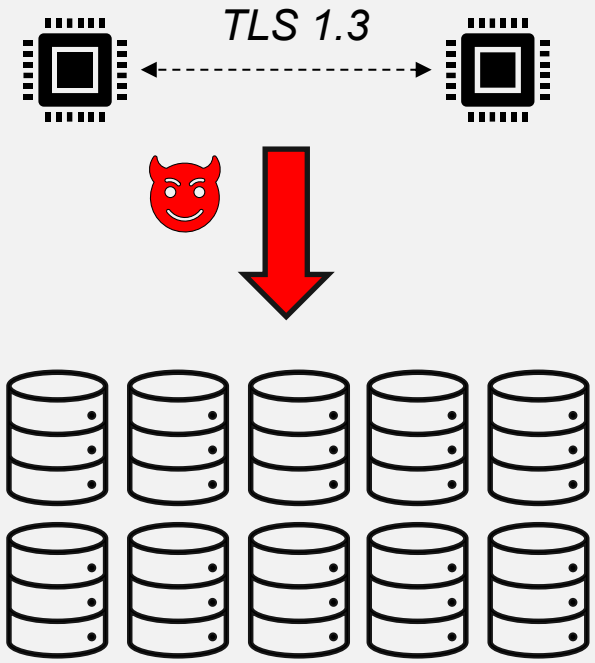
NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA

International Organization for Standardization ISO

ANSSI

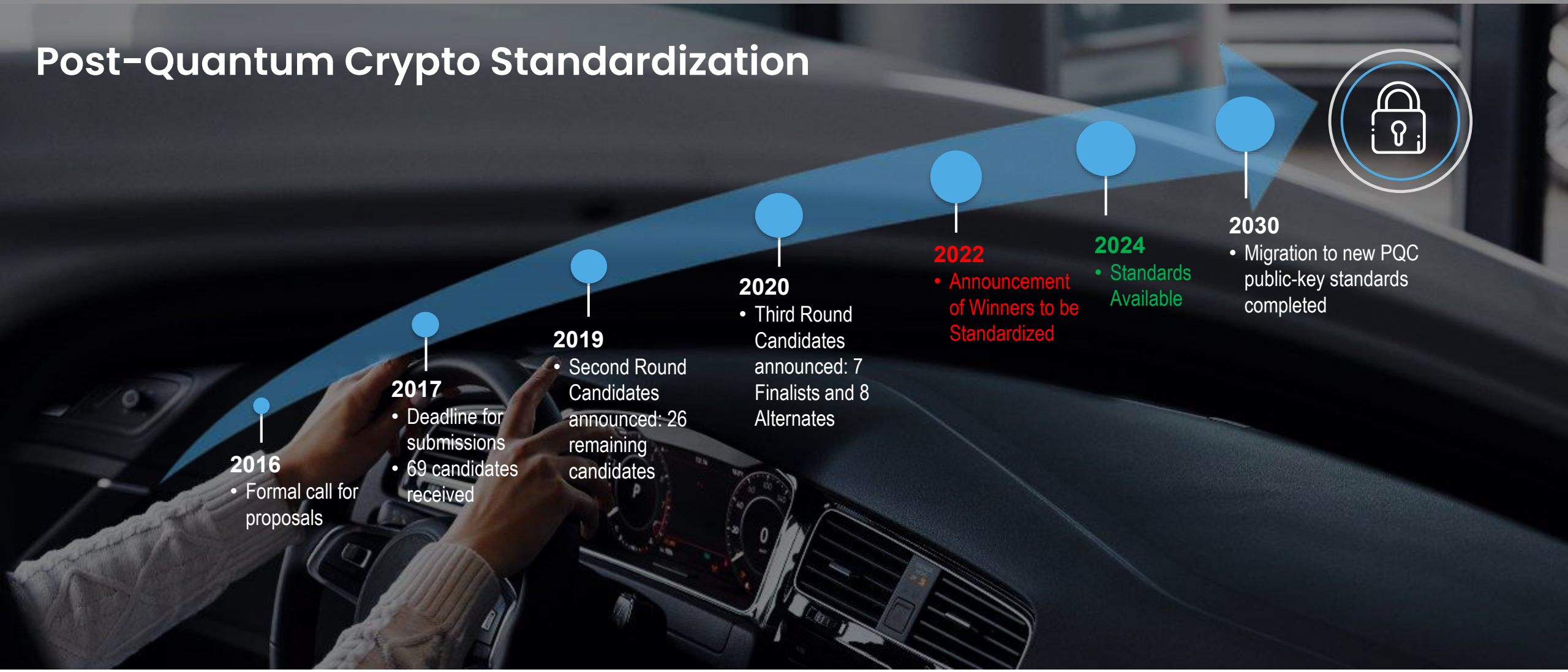
Crypto Agility

Store now decrypt later




Post-Quantum Crypto Standards Are Coming
It doesn’t matter if you believe in quantum computers or not

Post-Quantum Crypto Standardization

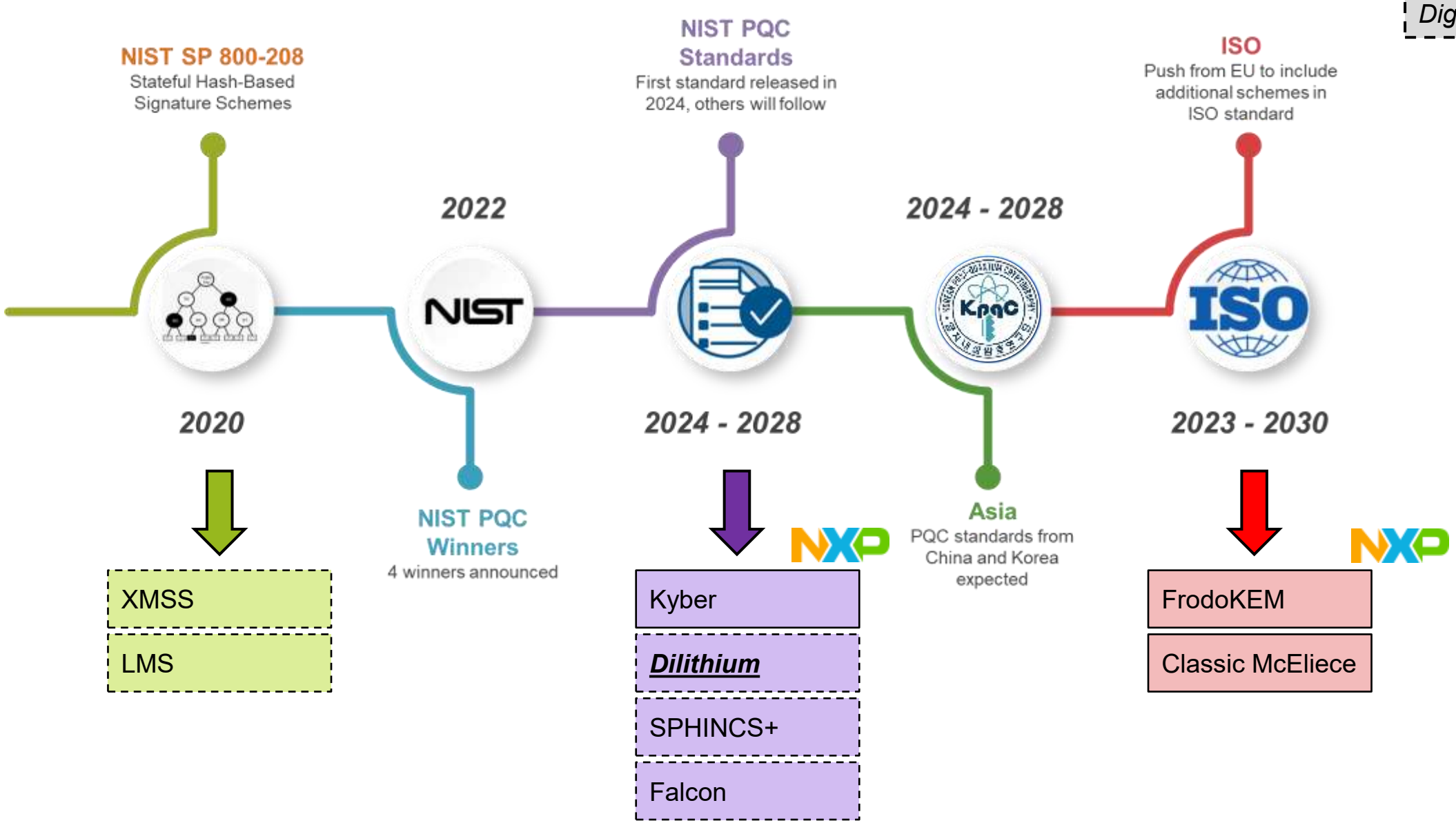


NIST
National Institute of Standards and Technology

Algorithm selection

Key Exchange

Digital signature



PQC Migration guidance by governments

USA (NIST/NSA)

- NIST/NSA recommendation available
  - Commercial National Security Algorithm Suite 2.0
- PQC FW signature recommended for new products after 2025
- PQC transition complete by 2030 using SW update

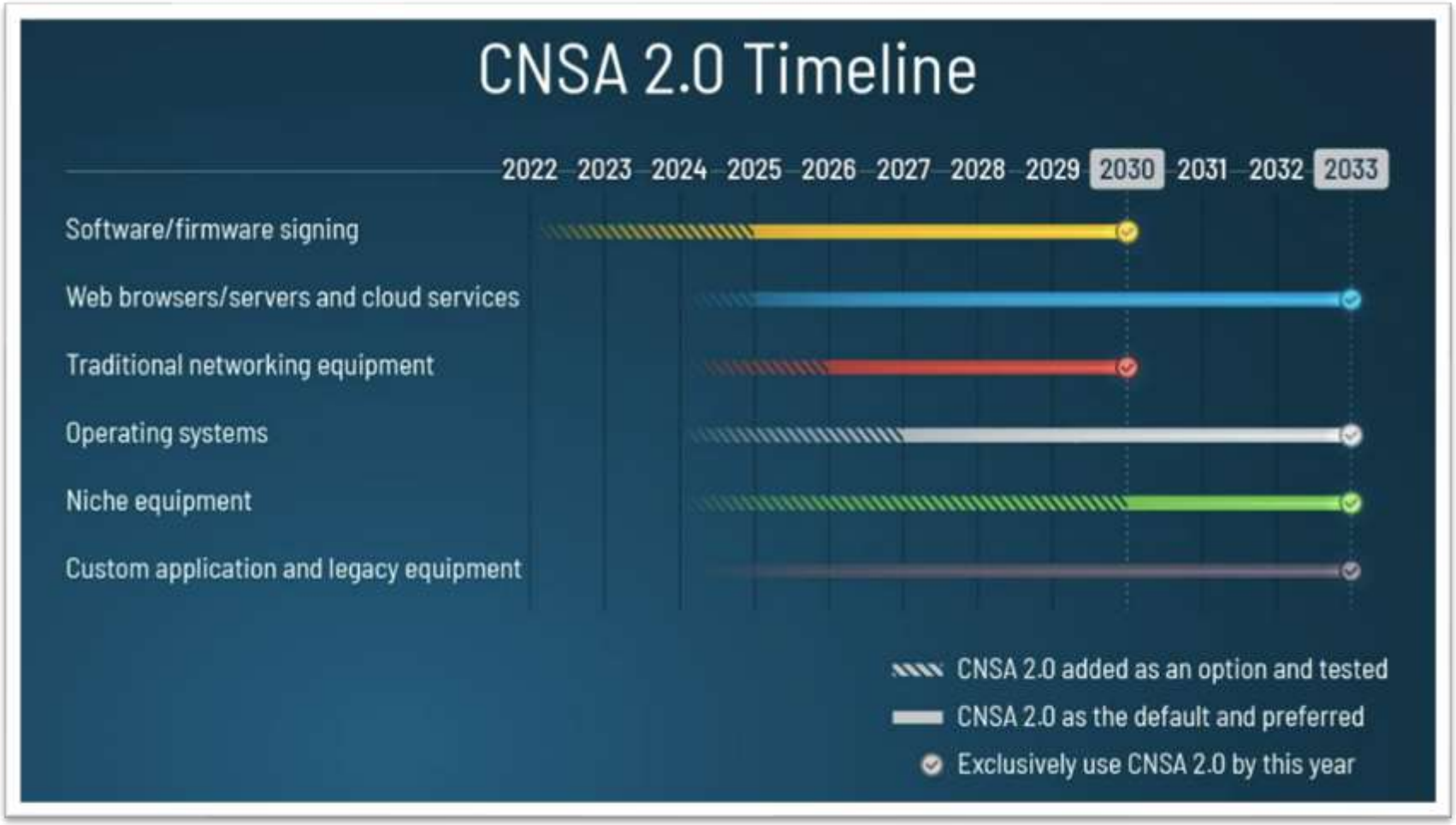
Germany (BSI)

- BSI first recommendation (English)
- BSI considerations (German)
- Expectation is that beginning of 2030s, a relevant quantum computer is available to be a threat for high-secure applications
- Quantum security: considers both PQC + QKD

France (ANSSI)

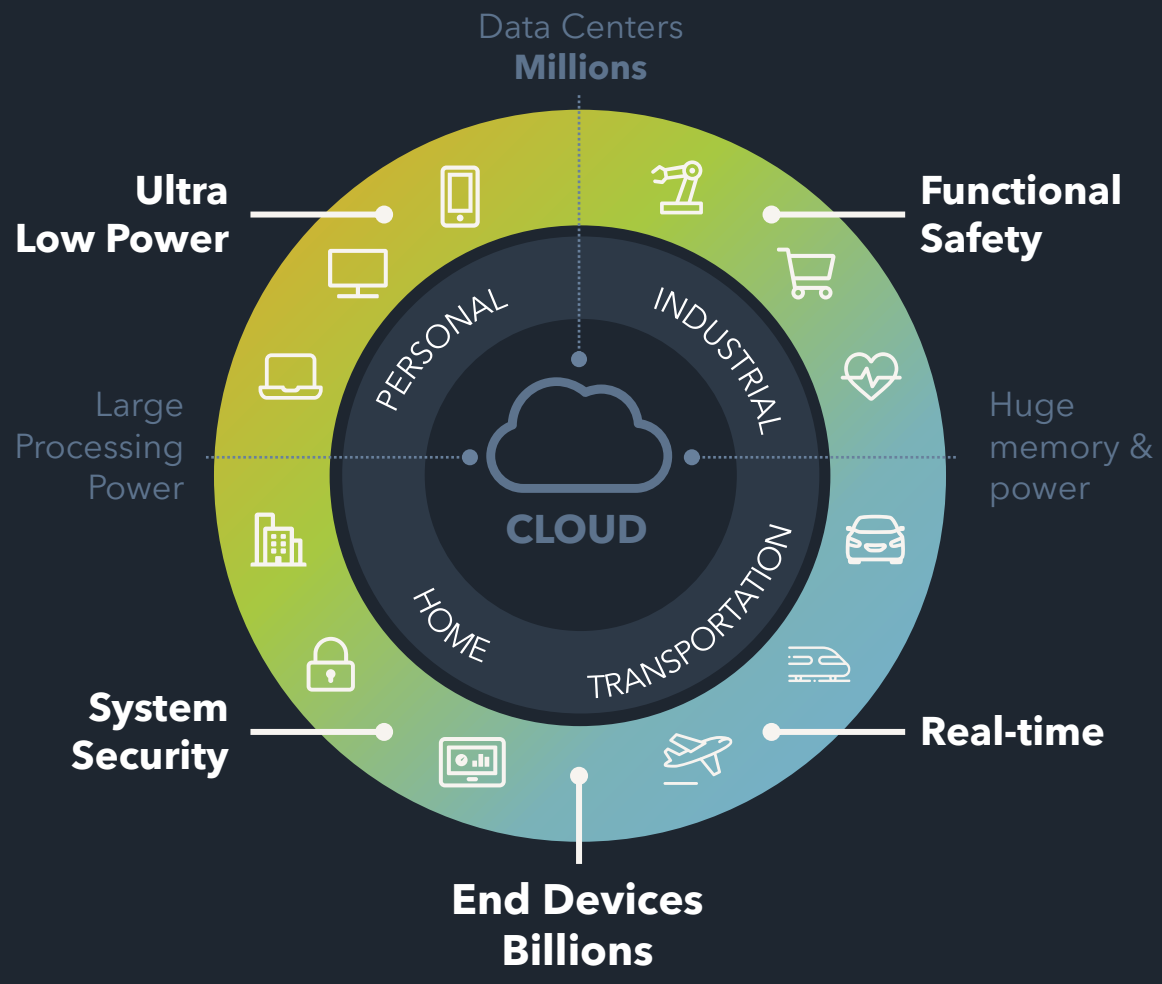
- PQC for security products “as soon as possible” when long-lasting (until 2030) protection is required
- Others to migrate to classic-PQC hybrid in 2025 – 2030
- Switch to PQC-only expected by 2030

PQC Migration: USA



Commercial National Security Algorithm Suite 2.0, Sept 2022

Impact of PQC on embedded eco-system



Data collection, processing and decisions at the edge
Devices securely connected to the cloud

No Silver Bullet
If a crypto scheme was better, we would have standardized this already

Cryptographic Keys
Orders of magnitude larger.
In the final: up to 1.3MB
Winners: up to 4.8KB
(ECC: 32 bytes, RSA: 384 bytes)

Performance
Varies: some faster some significantly slower.
SHA-3 is a dominating component (~80%)

Memory
Orders of magnitude more: up 100KB memory of RAM when executing

Bandwidth & Power
Larger signatures (up to 4.6KB) → more bandwidth required → increase in power usage

Conclusions

- Standardized PQC will be everywhere in the very near future
- Migration to PQC is a difficult & hot topic, particularly in embedded environments
- Many practical challenges
  - Memory
  - Available hardware (co-processors)
  - Efficient side-channel countermeasures

For some scenarios with more powerful end devices:

✓ Large key sizes no issue, marginal increase in stack usage

- SHA-3 performance crucial, hardware acceleration important
- Little impact on OTA time for updates

✓ Transition to PQC practical right now

Get in touch

Joppe W. Bos
joppe.bos@nxp.com

nxp.com