



Build Resilience with Post-Quantum Cryptography

Joppe W. Bos

Cryptographer & Technical Director (CC C&S, CTO)
November 2024

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

IBM achieves an important milestone with new quantum computer in the cloud.

CHRIS LEE NEWS | 23 October 2019

Hello quantum world! Google publishes landmark quantum supremacy claim

The company says that its quantum computer is the first to perform a calculation that would be practically impossible for a classical machine.

Elizabeth Gibney

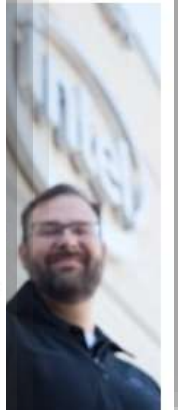


Intel Delivers 17-Qubit Superconducting Chip with Advanced Packaging to QuTech

Eagle's quantum performance progress

Last November, IBM Quantum announced Eagle, a 127-qubit quantum processor based on the transmon superconducting qubit architecture. The IBM Quantum team adapted advanced semiconductor signal delivery and packaging into a technology node to develop superconducting quantum processors.

quantum
new chip was
performance.



NXP, eleQtron and ParityQC Reveal their First Quantum Computing Demonstrator for the DLR Quantum Computing Initiative

May 30, 2024 2:00 PM CEST (UTC+2) by NXP Semiconductors Press Release

Quantum error correction below the surface code threshold

Google Quantum AI and Collaborators
(Dated: August 27, 2024)

SHARE





- NXP, eleQtron and ParityQC reveal their first quantum computing demonstrator for the DLR Quantum Computing Initiative.
- It was commissioned by the DLR Quantum Computing Initiative (DLR QCI) to expand the quantum expertise of its partners from research and industry

Security impact of quantum computers

“This document specifies the bare-minimum security requirements expected of System-on-Chips (SoC) across multiple markets.” [1]

Security Goals	
Cryptographic Identity	Rollback Protection
Security Lifecycle	Security By Isolation
Attestation	Secure Interfaces
Secure Boot	Binding
Secure Update	Trusted Services






Platform Security Requirements
1.0

Requirements: Cryptography

Asymmetric	Symmetric
RSA-3072	AES-128
ECC P-256	SHA-256



“All use of cryptography must use an algorithm that meets at least 128 bits of security.”

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

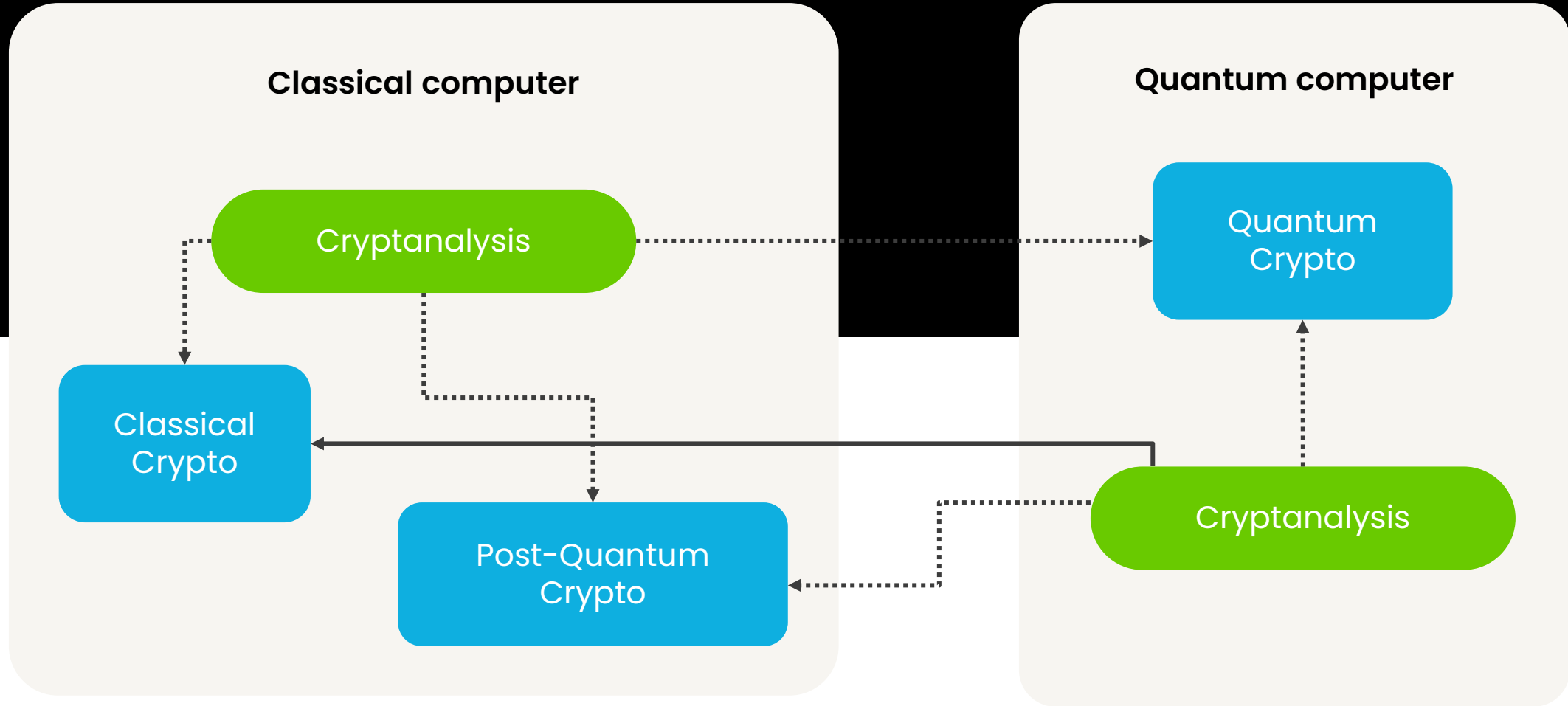


The integrity of blockchains

Could be retrospectively compromised – could include fraudulent manipulation of ledger and cryptocurrency transactions



Post-quantum versus quantum crypto





Post-Quantum Cryptography

Requirement 1

Run on
classical hardware

Requirement 2

Be secure against adversaries
armed with classical computers

Requirement 3 NEW

Be secure against adversaries
armed with quantum computers

Requirement 4

Be secure against Side-Channel Analysis (SCA)
and Fault Injection (FI) attacks

Is Post-Quantum Cryptography relevant for you?

Standards & Compliance

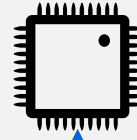


NIST



Crypto Agility

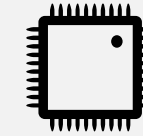
PQC RoT



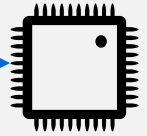
Secure Updates



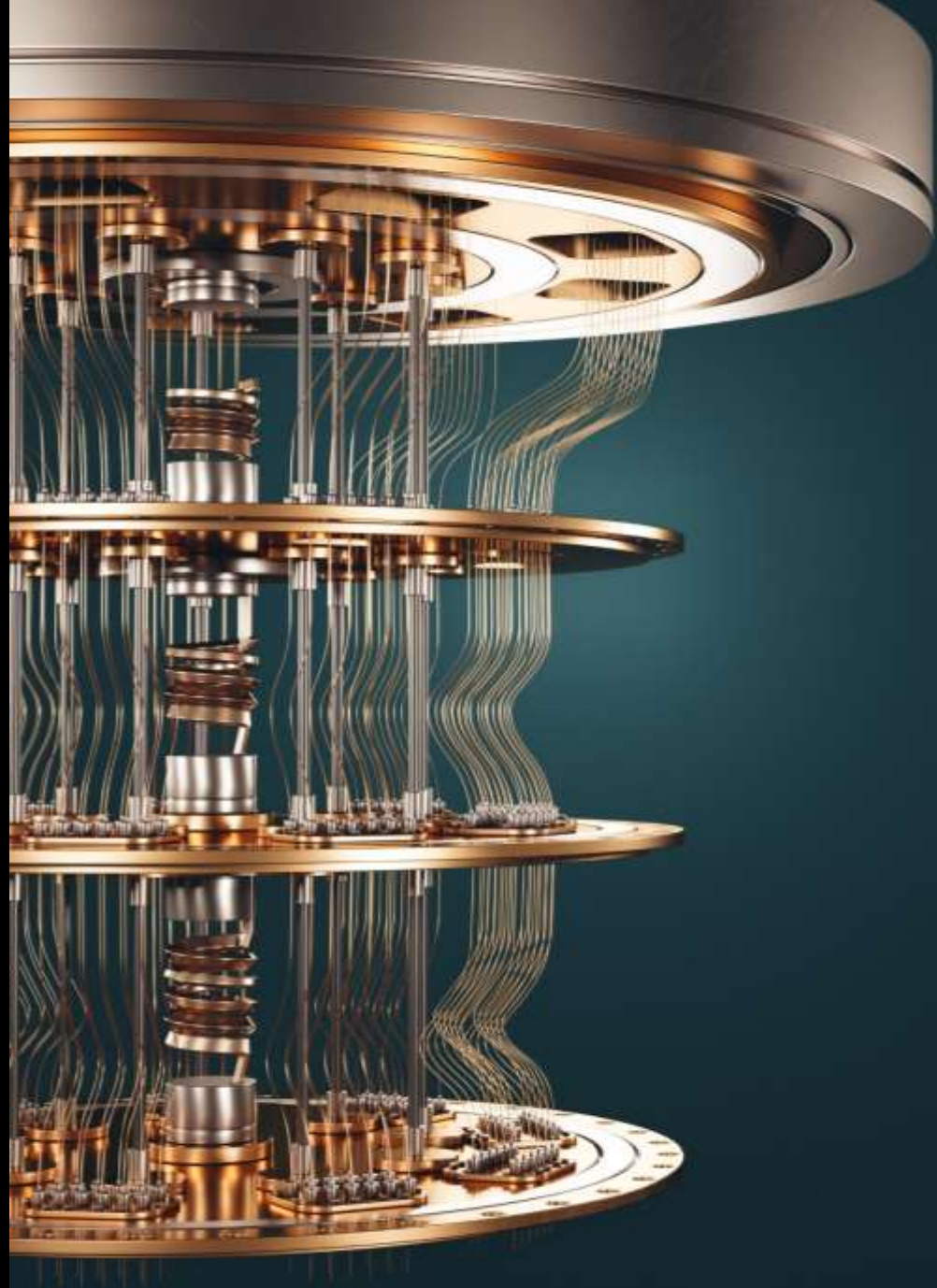
Store Now Decrypt Later



TLS 1.3



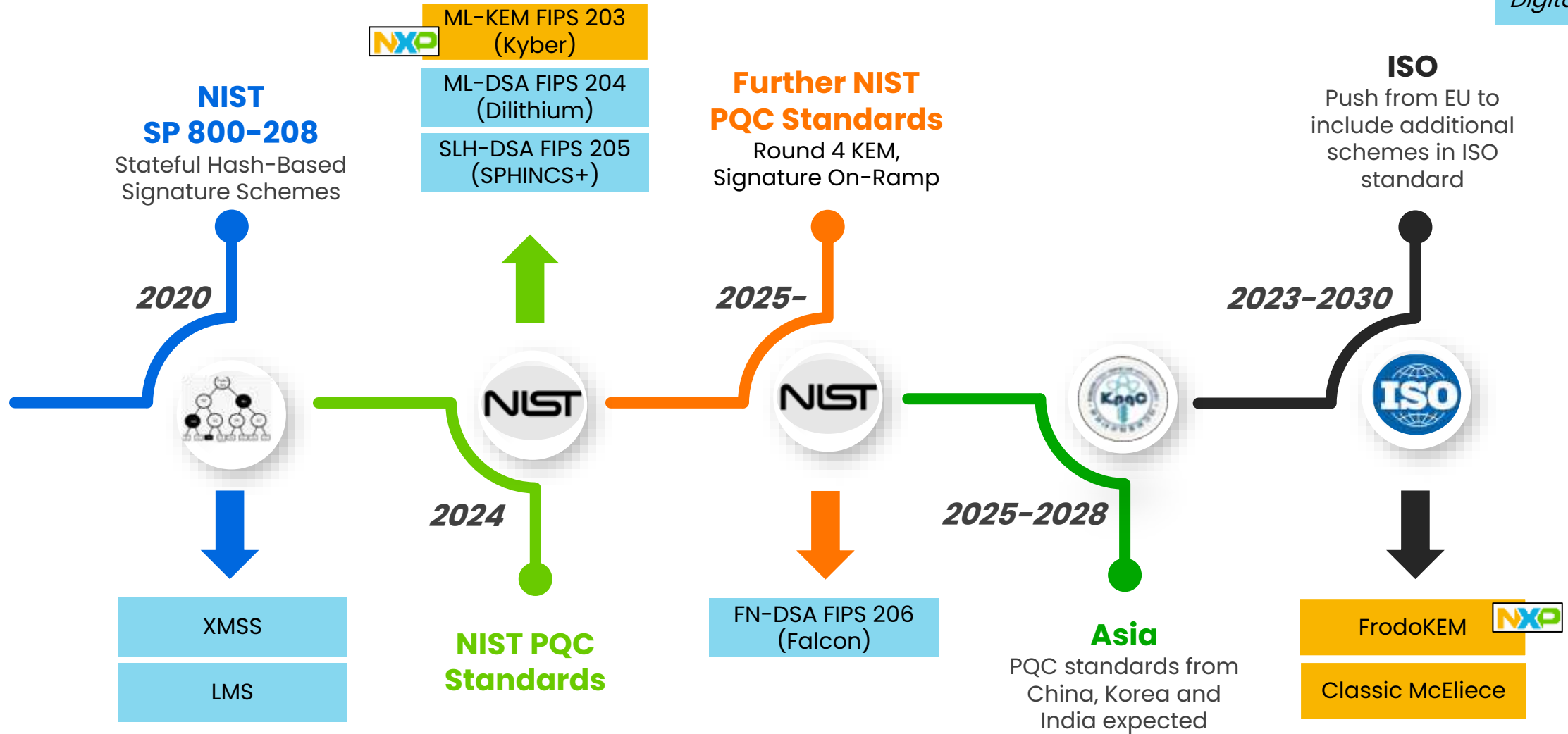
**Post-quantum
crypto standards
are coming
It doesn't matter if
you believe in
quantum
computers or not**



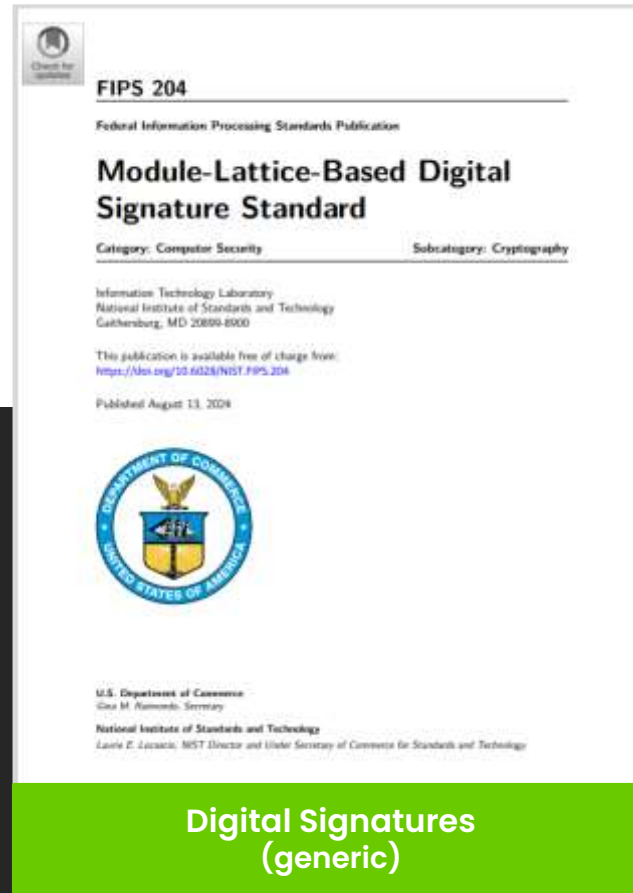
PQC Algorithm Standardization

Key Exchange

Digital Signature



New algorithms and standards



More ongoing and upcoming! FIPS 206, Round 4, On-Ramp, ISO, etc..

- [1] ML-KEM, <https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.203.pdf>
- [2] ML-DSA, <https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.204.pdf>
- [3] SLH-DSA, <https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.205.pdf>
- [4] LMS / XMSS, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-208.pdf>

PQC migration guidance



USA (NSA)

- [NSA recommendation](#) available
- Commercial National Security Algorithm Suite 2.0
- **Begin transitioning immediately**
- PQC FW signature supported **by 2025**
- PQC **transition complete by 2030** using SW update



Germany (BSI)

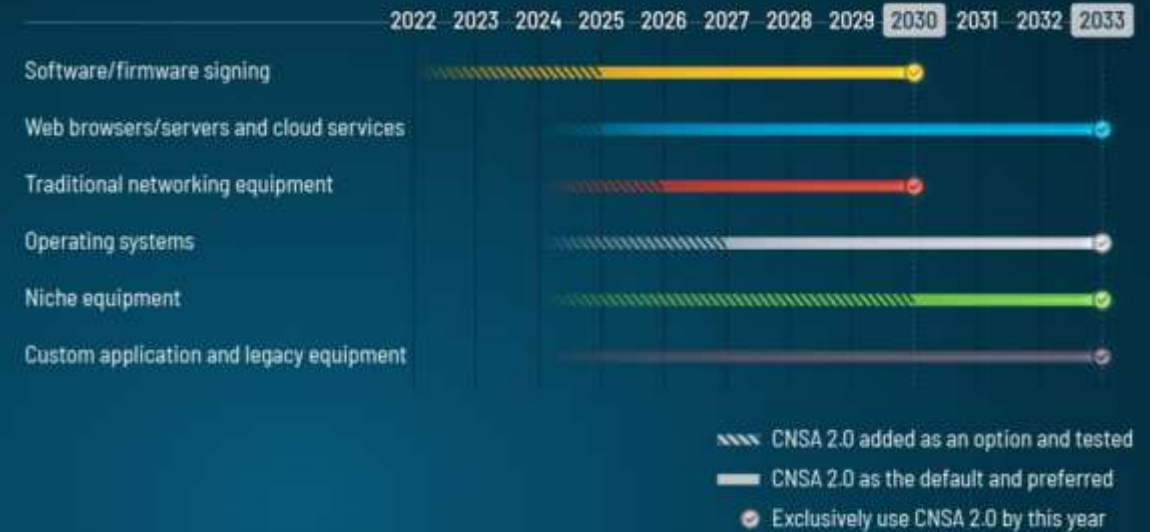
- [BSI first recommendation](#) (English)
- [BSI considerations](#) (German)
- Expectation is that beginning of 2030s, a relevant quantum computer is available to be a threat for high-secure applications
- “QKD is only suitable for specific use cases”



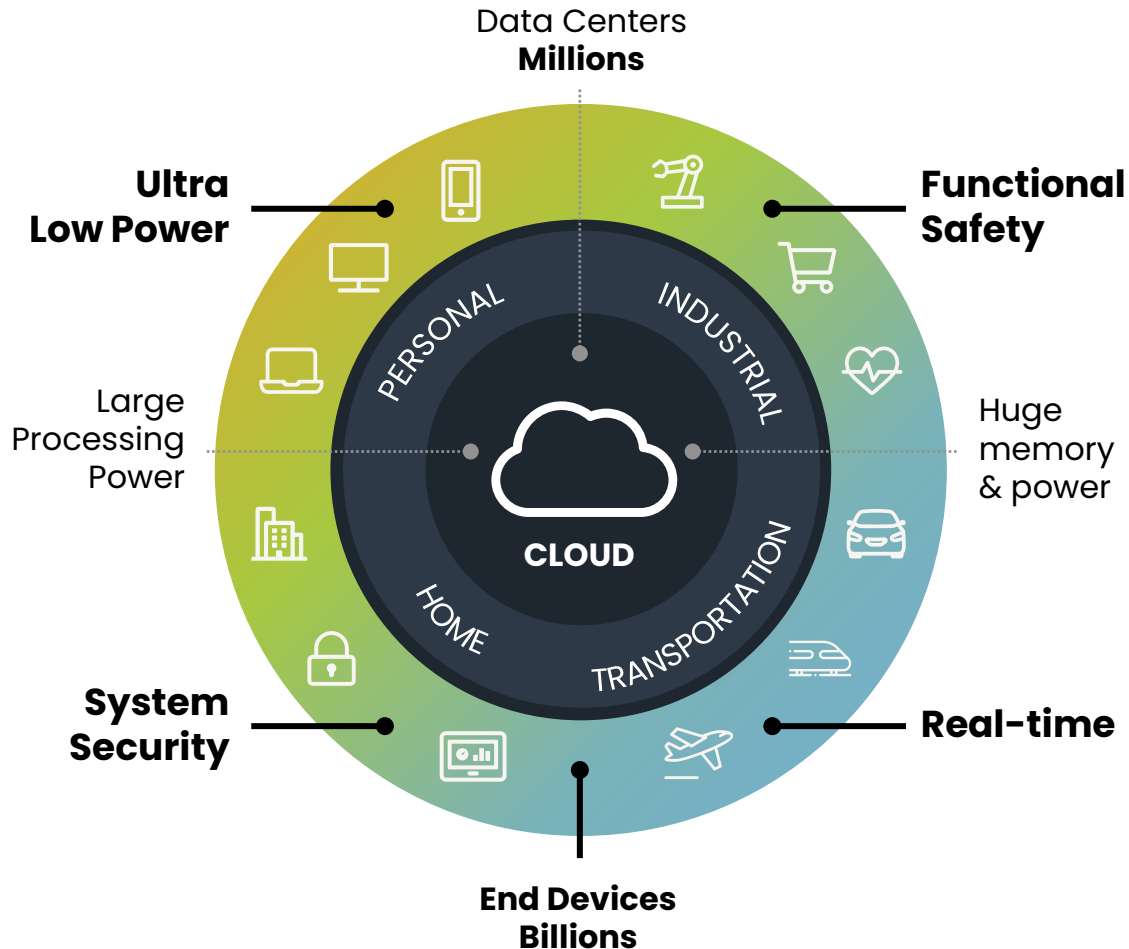
France (ANSSI)

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

CNSA 2.0 Timeline



Impact PQC on our 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

NXP has dedicated implementations reaching ~16KB of RAM

Bandwidth & Power

Larger signatures (up to 4.6KB)

→ more bandwidth required

→ increase in power usage

Technical aspects of new algorithms

See pqm4 open source project for benchmarks! [A]
Assuming Cortex-M4 @ 200 MHz software-only.
For LMS numbers taken from Campos et al. [B]

Algorithm	PQC	Encaps	Decaps	SK	PK	CT	Algorithm
EC-P384	No	"Fast"	"Fast"	48 B	48 B	96 B	EC-P384
FIPS 203 (ML-KEM)	Yes	4 ms	4 ms	2 400 B	1 184 B	1 088 B	FIPS 203 (ML-KEM)

Algorithm	PQC	Encaps	Decaps	SK	PK	CT	Algorithm
ECDSA-P384	No	"Fast"	"Fast"	48 B	48 B	96 B	ECDSA-P384
FIPS 204 (ML-DSA)	Yes	31 ms	12 ms	4 032 B	1 952 B	3 309 B	FIPS 204 (ML-DSA)
FIPS 205 (SLH-DSA)***	Yes	77 s	68 ms	96 B	48 B	16 224 B	FIPS 205 (SLH-DSA)***
SP 800-20 (LMS/XMSS)	Yes	** (Stateful) 19 s	13 ms	48 B	48 B	1 860 B	SP 800-208 (LMS/XMSS)

* NIST Level 3 parameter sets

** Significant reduction possible by increasing memory consumption for state

*** New parameter sets coming that will improve performance & signature size!

Typical embedded use cases for new algorithms

Many more ongoing and upcoming!

		FIPS 203	FIPS 204	FIPS 205 (Verify)	SP 800-208 (Verify)
Security Goals	Secure Boot	✓	✓	✓	✓
	Secure Update	✓	✓	✓	✓
	Secure Attestation	✗	✓	✗	✗
	Secure Debug / Test	✓	✓	✗	✗
	Certificates (PKI)	✗	✓	✓	✓**
	Runtime Crypto API	✓	✓	✓	✓
Protocols	TLS 1.3 (Hybrid)	✓	✓*	✗	✗
	IKEv2 (Hybrid)	✓	✓*	✗	✗
	GSMA eSIM	✓	✓	✗	✗
	GlobalPlatform: TEE/MCU	✓	✓	✓	✓

* Signatures for client authentication excluded from initial proposals, discussions ongoing

** Possible but the number of issued certificates should be carefully managed (e.g., Root CA)

Recommended use cases for new algorithms

FIPS 203 (ML-KEM)	NIST (std.)	NSA (CNSA 2.0)	BSI (TR-02102-1)	ANSSI
Key Establishment	✓	✓	✓	✓
Digital Signatures (Generic)	✗	✗	✗	✗
Firmware / Software Signing	✗	✗	✗	✗

FIPS 205 (SLH-DSA)	NIST (std.)	NSA (CNSA 2.0)	BSI (TR-02102-1)	ANSSI
Key Establishment	✗	✗	✗	✗
Digital Signatures (Generic)	✓	✗	✓	✓
Firmware / Software Signing	✓	✗	✓	✓

FIPS 204 (ML-DSA)	NIST (std.)	NSA (CNSA 2.0)	BSI (TR-02102-1)	ANSSI
Key Establishment	✗	✗	✗	✗
Digital Signatures (Generic)	✓	✓	✓	✓
Firmware / Software Signing	✓	✓	✓	✓

SP 800-208 (LMS / XMSS)	NIST (std.)	NSA (CNSA 2.0)	BSI (TR-02102-1)	ANSSI
Key Establishment	✗	✗	✗	✗
Digital Signatures (Generic)	✓	✗	✓	✓
Firmware / Software Signing	✓	✓	✓	✓

Only with carefully managed maximum number of issued signatures



What is the impact on the billions of embedded devices?



Automotive

70%

70% connected cars by 2025



Industrial & IoT

12B

IoT Edge & end nodes from **6B units** in 2021 to **12B units** in 2025



Mobile

60B

Tagging **60B products** per year by 2025



Communication Infrastructure

40B

Secure anchors & services for **40B processors**



Automotive



eGovernment



Bank cards



Smart mobility (MIFARE) cards



Tags & Authentication



Readers



Mobile

What is the impact of PQC on Industrial IoT?



From theory to practice: small-memory implementations

Do these implementations actually run on embedded systems?

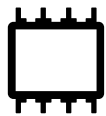
		pqm4	
		Runtime	RAM
Dilithium-2	Sign	19 ms	50 kB
	Verify	7 ms	11 kB
Dilithium-3	Sign	31 ms	69 kB
	Verify	12 ms	10 kB
Dilithium-5	Sign	42 ms	123 kB
	Verify	21 ms	12 kB

From theory to practice: small-memory implementations

Do these implementations actually run on embedded systems?

		pqm4	
		Runtime	RAM
Dilithium-2	Sign	19 ms	50 kB
	Verify	7 ms	11 kB
Dilithium-3	Sign	31 ms	69 kB
	Verify	12 ms	10 kB
Dilithium-5	Sign	42 ms	123 kB
	Verify	21 ms	12 kB

NXP PQC [A]		Slower	Smaller
Runtime	RAM	Runtime	RAM
61 ms	5 kB	3.2x	10.0x
16 ms	3 kB	2.3x	3.7x
119 ms	7 kB	3.8x	9.9x
29 ms	3 kB	2.4x	3.3x
168 ms	8 kB	4.0x	15.4x
50 ms	3 kB	2.4x	4.0x

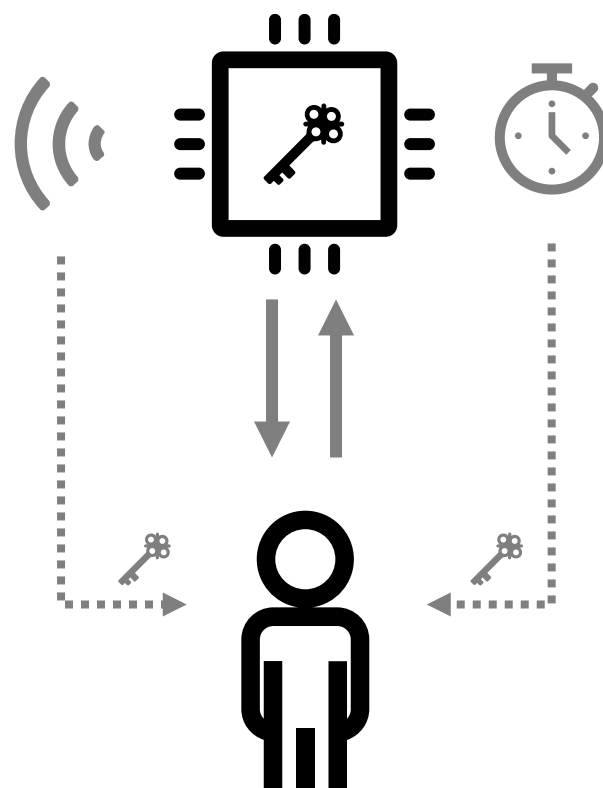


All Dilithium parameter sets will fit on a device with ~8KB memory.

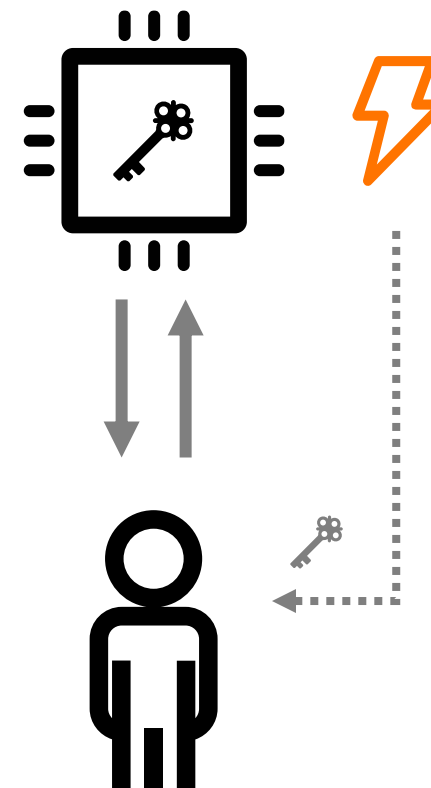


Price: factor 3 to 4 in performance HW accelerators

From theory to practice: Secure implementations

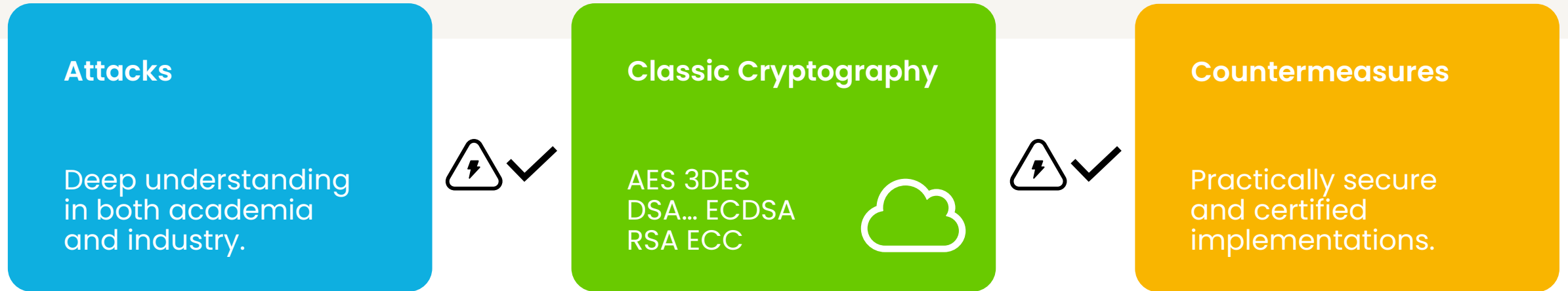


Side-Channel
Attacks (SCA)

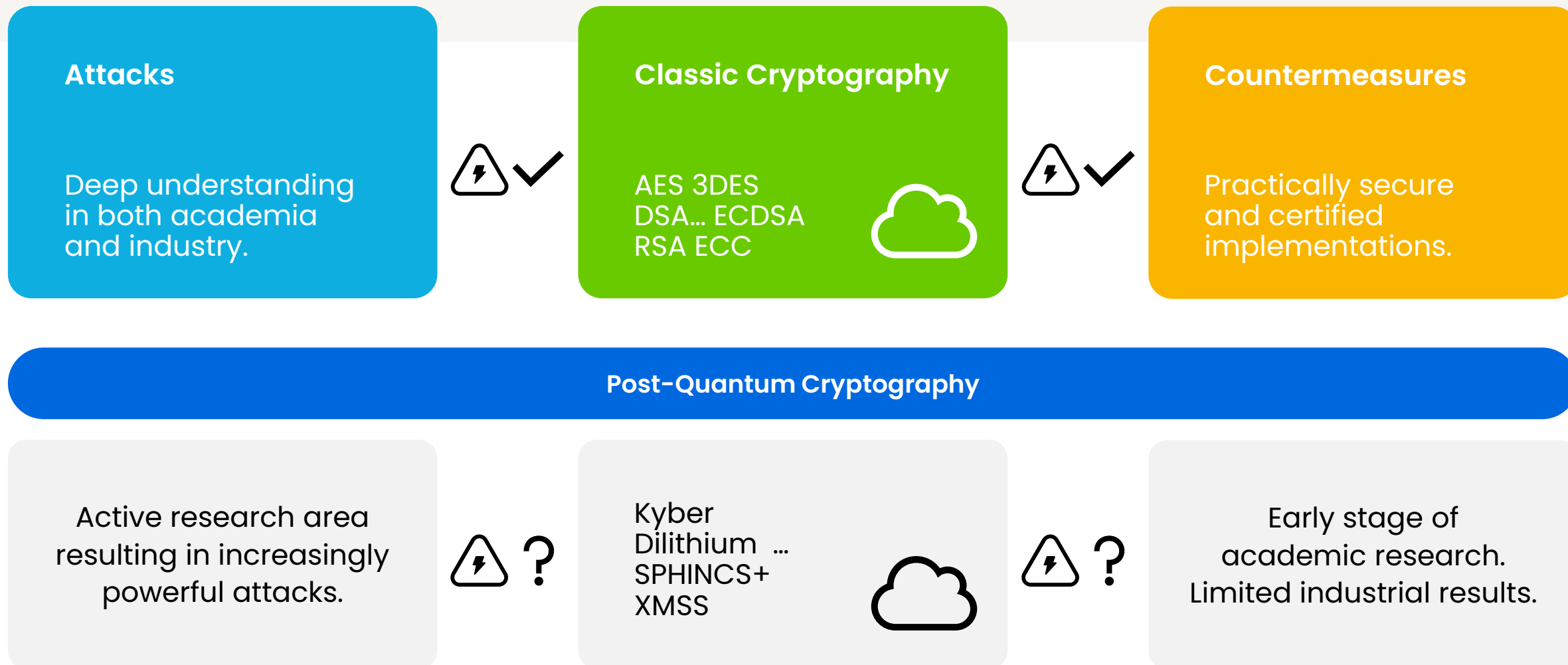


Fault
Injection (FI)

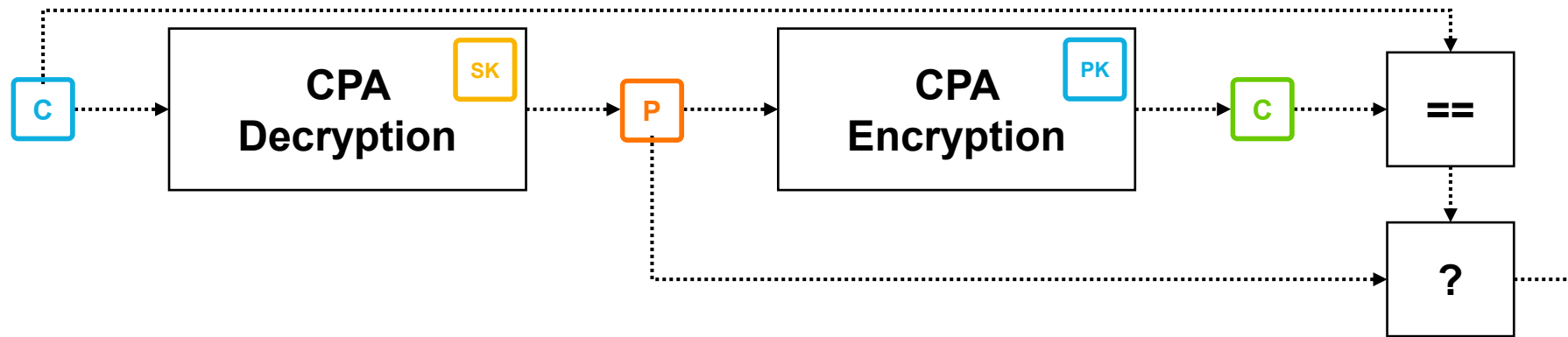
Embedded cryptography and implementation attacks



Embedded cryptography and implementation attacks



Fujisaki Okamoto transform



Transform a scheme which achieves **IND-CPA**
("chosen plaintext attack") security to reach **IND-CCA**
("indistinguishability against chosen-ciphertext attacks") security

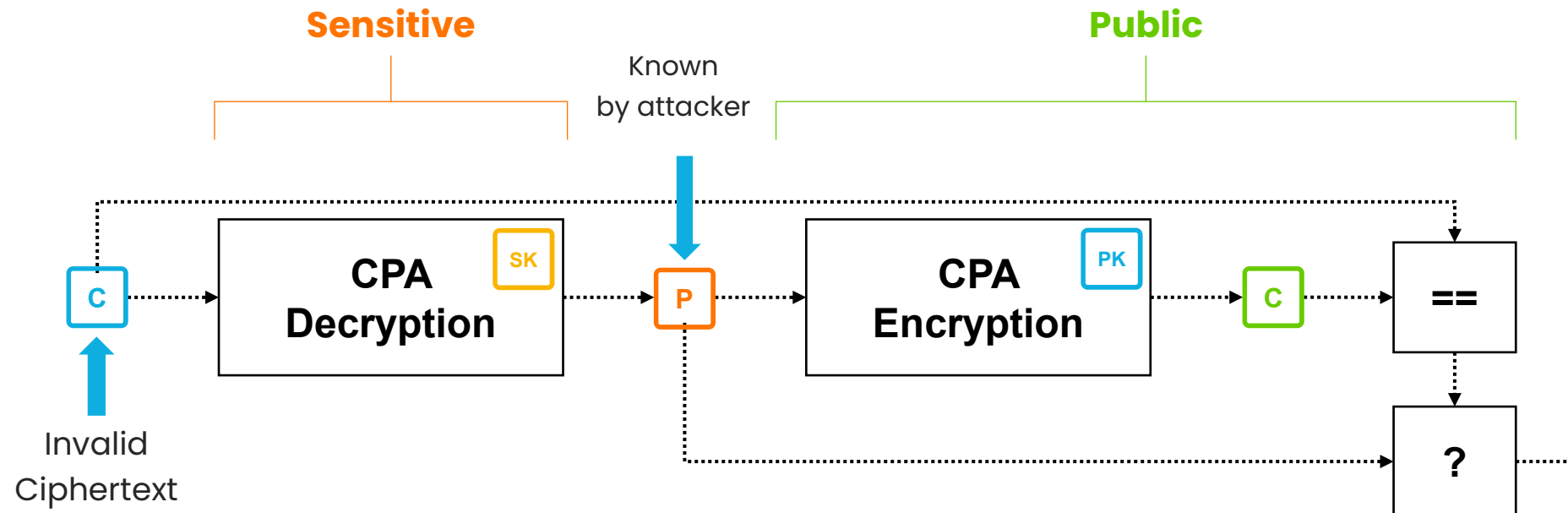
Fujisaki, E. and Okamoto
T., Secure integration of
asymmetric and symmetric
encryption schemes, CRYPTO
1999 and JoC 2013

The SCA Problem of the FO-Transform



Attack 1: Chosen Plaintext

- Attacker inputs only valid ciphertexts
- Attack focuses on **CPA Decryption**, everything after (and including) **P** is public
- Only need to protect **CPA Decryption**

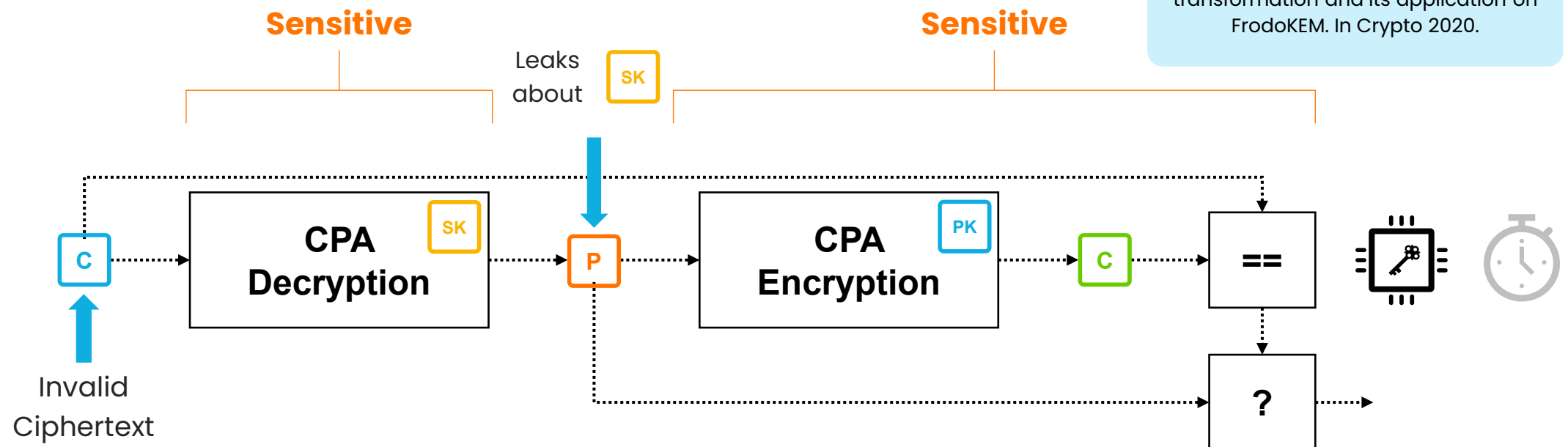


The SCA Problem of the FO-Transform



Attack 2: Chosen Ciphertext

- Attacker inputs specially-crafted invalid ciphertexts
- Attack focuses on **CPA Decryption** + everything after (and including) **P** is potentially sensitive
- Potentially all (or most) modules need to be hardened



From Theory to practice: Secure implementations (NXP PQC Team)

Only with carefully managed maximum number of issued signatures

First completely masked implementation of Kyber / FIPS 203 !

Year	Venue	FIPS 203	FIPS 204	Title
2021	TCHES			Masking Kyber: First- and Higher-Order Implementations
2021	RWC			Post-Quantum Crypto: The Embedded Challenge
2022	TCHES			Post-Quantum Authenticated Encryption against Chosen-Ciphertext SCA
2022	RWC			Surviving the FO-calypse: Securing PQC Implementations in Practice
2023	TCHES			From MLWE to RLWE: A Differential Fault Attack on Randomized & Deterministic Dilithium
2023	TCHES			Protecting Dilithium Against Leakage Revisited Sensitivity Analysis
2024	RWC			Lessons Learning from Protecting CRYSTALS-Dilithium
2024	TCHES			Exploiting Small-Norm Polynomial Multiplication with Physical Attacks
2024	RWC			Challenges of Migration to PQ Secure Embedded Systems

Completely masked implementation of Dilithium / FIPS 204 !

Hybrid migration

Transition Period



ECC / RSA benefit from decades of cryptanalysis including logical / physical attacks



Can combine security of both in a hybrid mode

Hybrid Signed Container

Image



ECC Sig.



ML-DSA Sig.



“ NIST will **accommodate** the use of a hybrid key-establishment mode and dual signatures in FIPS 140 validation when suitably combined with a NIST-approved scheme ”



“ the BSI does not recommend using post-quantum cryptography alone, but **only “hybrid”** ”



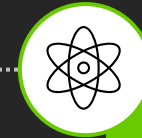
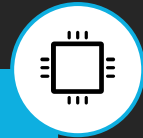
“ the role of hybridation in the cryptographic security is crucial and will be **mandatory** for phases 1 and 2.

public key cryptography [...] would strongly benefit from the introduction of new alternative algorithms. ”

NXP S32G2 vehicle network processor with PQC integration

Our target platform: S32G274A

- 3 Lockstep Arm® Cortex®-M7 Microcontrollers
- 4 Cluster Lockstep Cortex-A53 Microprocessors
- 8 MB of System RAM
- Network Accelerators (LLCE/PFE)
- **Hardware Security Engine (HSE)**
- ASIL D Functional Safety Support



Post-Quantum Crypto

- Integrate PQC secure signature verification
- Protection against Fault Attacks
- Enable PQC secure boot
- Secure Over-the-Air (OTA) updates
- Secure vehicle and driver data

www.nxp.com/s32g2



Benchmarks for authentication of FW signature on the S32G2

Alg.	Size		Performance (ms)			
			1 KB		128 KB	
	PK	Sig.	Inst.	Boot	Inst.	Boot
RSA 4K	512	512	2.6	0.0	2.7	0.2
ECDSA-p256	64	64	6.2	0.0	6.4	0.2
Dilithium-3	1952	3293	16.7	0.0	16.9	0.2



Demonstrator only, further optimizations are possible (such as hardware accelerated SHA-3)



Signature verification only required once for installation!



During boot the signature verification can be replaced with a check of the Reference Proof of Authenticity



Conclusions



ML-KEM, ML-DSA ready for adoption in general-purpose cryptolibs



SP 800-208 & SLH-DSA ready for adoption in software / firmware signing



Migration recommended by governments (NSA, BSI, ANSSI, many others!)

- Harvest-now Decrypt-later
- Software / Firmware Signing
- + More use cases in a phased / hybrid migration!



NXP has been working to resolving practical challenges for 8+ years!

- Algorithm design (ML-KEM)
- Low-memory implementations
- Protection against Side-Channel Analysis (SCA) and Fault Injection (FI)
- Hardware acceleration (SHA-3)





Get in touch

Joppe W. Bos

joppe.bos@nxp.com

[nxp.com](https://www.nxp.com)