Post-Quantum

Cryptography Conference

Post-Quantum Crypto: Challenges for Embedded Applications

Joppe Bos
Researcher at NXP Semiconductors

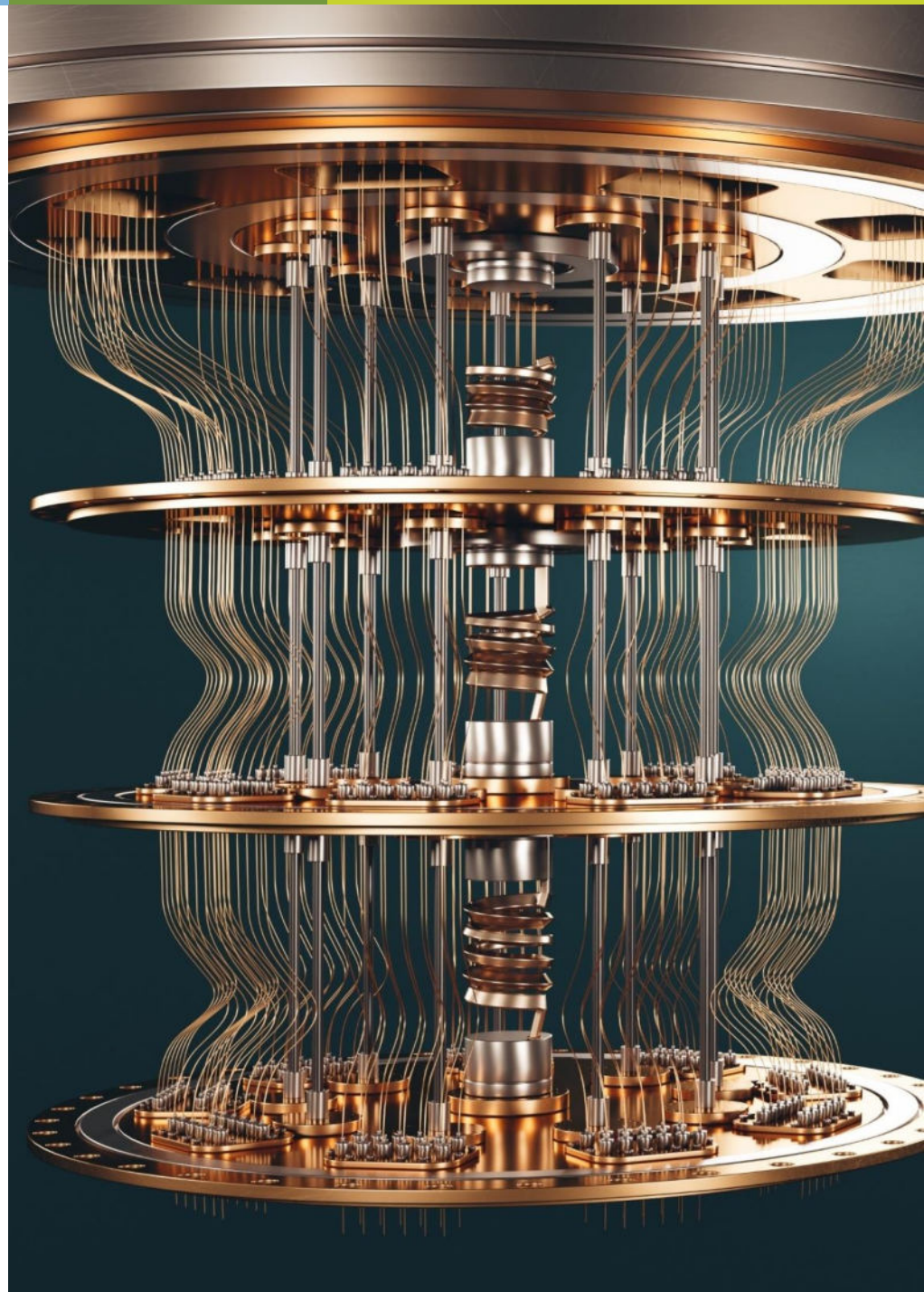
Post-Quantum Crypto: Challenges for Embedded Applications

Joppe W. Bos

contact: pqc@nxp.com

POST-QUANTUM CRYPTOGRAPHY CONFERENCE 2023
NOVEMBER 8, 2023 - AMSTERDAM

SECURE CONNECTIONS FOR A SMARTER WORLD



POST-QUANTUM CRYPTO FOR EMBEDDED DEVICES?

Outline

- Risk assessment: when to act?

<u>Embedded perspective</u>

- PQC performance
- High-assurance implementations

PQC STANDARDS – NIST

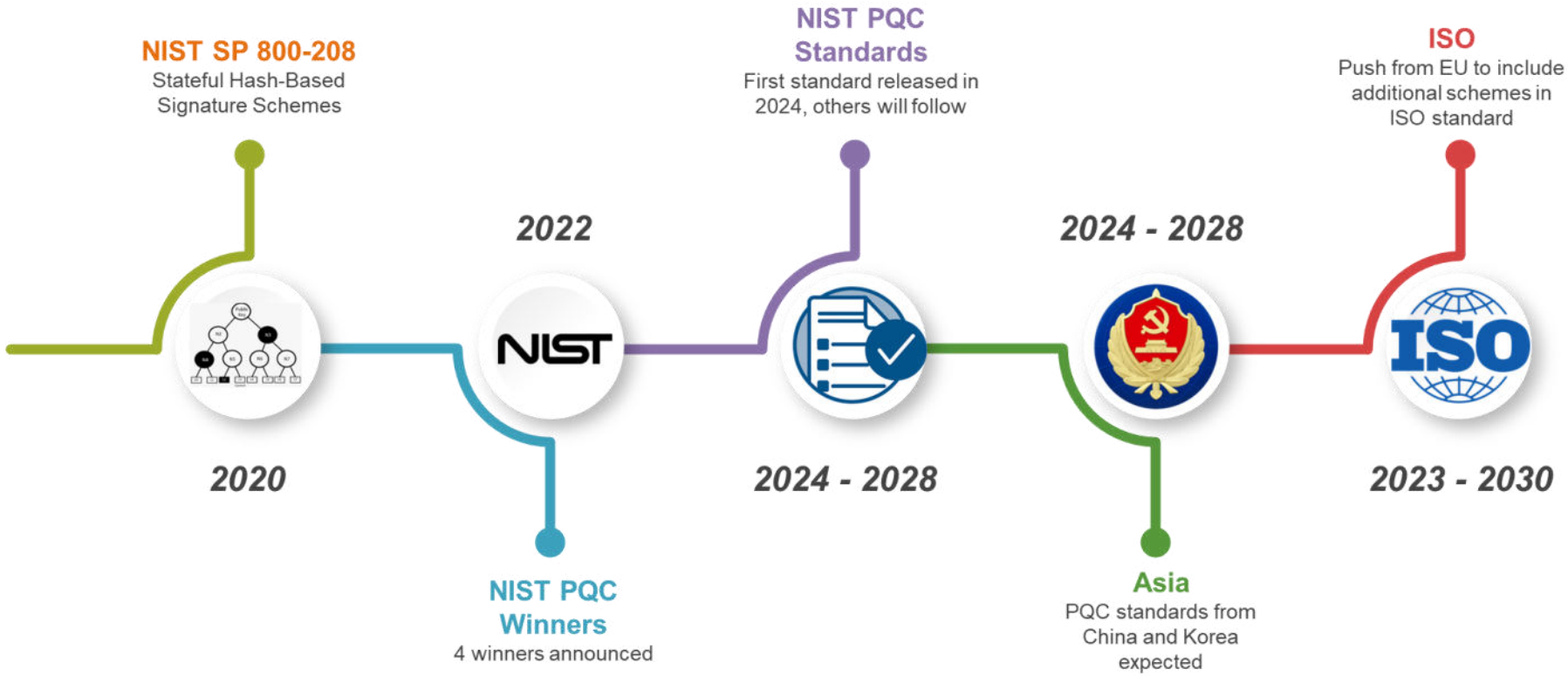
Winners	Secondary Winners	Round 4 Candidates	Digital Signature Competition
CRYSTALS-Kyber	Falcon	HQC	*Proposals June '23: 40 "complete & proper" submissions*
CRYSTALS-Dilithium	SPHINCS+	BIKE	
		Classic McEliece	
		SIKE	

2024 | 2025? | 2028? | 2030?

NIST *PQC Standard (Key Exchange + Digital Signatures)*

PQC Standard #2 (Digital Signatures)

Color key: Mathematical approach — Lattice | Hash | Code



National Standards

- **USA.** NIST announces standards release of 4 PQC schemes (‘24 – ’25). Additional standards to follow.
- **EU.** Push from EU for adding schemes to international standard. October ‘23: ISO to amend ISO/IEC 18033-2.
- **ASIA.** Selection of new schemes ongoing in both China/Korea.

Protocol Standards

- **IETF:** TLS, OpenPGP, hybrid keys, key serialization, encoding for signatures
- ISO/TC 68/SC 2/WG 11 (Encryption algorithms used in banking applications)
- ISO/IEC JTC1/SC 17/WG 4 (Cards and security devices for personal identification)

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

WHY DO WE WANT TO PROTECT KYBER / DILITHIUM?

NIST chooses **Kyber + Dilithium** as primary new PQC standards

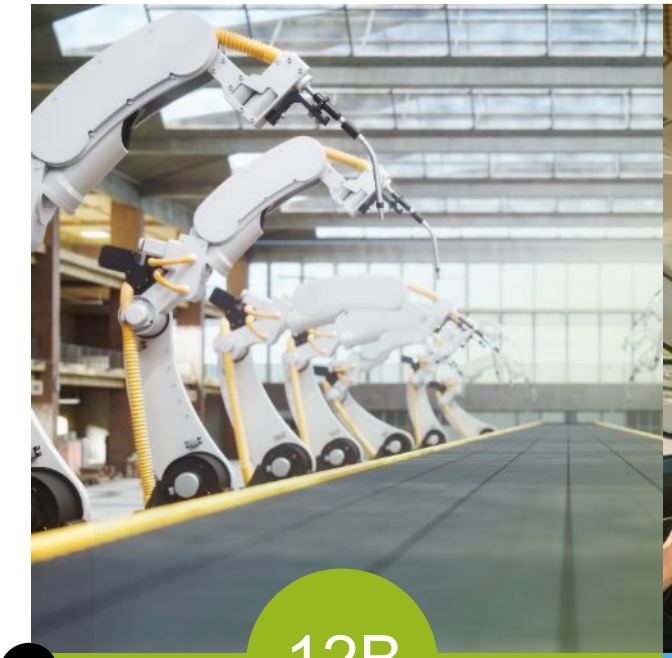
Transition

2022

2024

NIST publishes **standardization documents**.

INDUSTRIAL & IOT



12B

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

AUTOMOTIVE

70%

70% connected cars by 2025

RUNNING PQC ON EMBEDDED DEVICES

Key sizes

Performance

Memory usage

What about high security implementation?




PQC ON EMBEDDED DEVICES

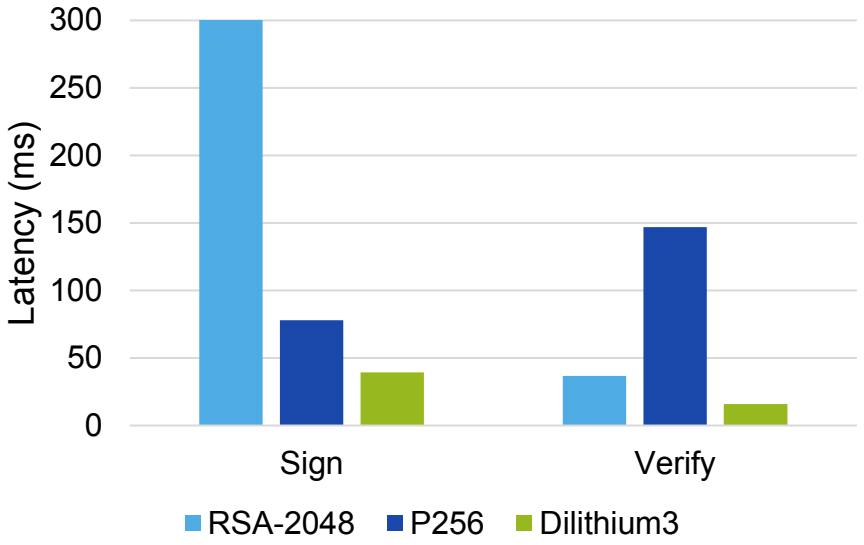
What is embedded?
- NIST has recommended Arm Cortex-M4

Pqm4: Post-quantum crypto library for the ARM Cortex-M4, STM32F4DISCOVERY
196 KiB of RAM and 1 MiB of Flash ROM

Low-power Edge computing: LPC800 Series
- 8 to 60 MHz Cortex-M0+ core
- $\{ 4, 8, 16 \}$ KiB of SRAM
- $\{ 16, 32 \}$ KiB Flash

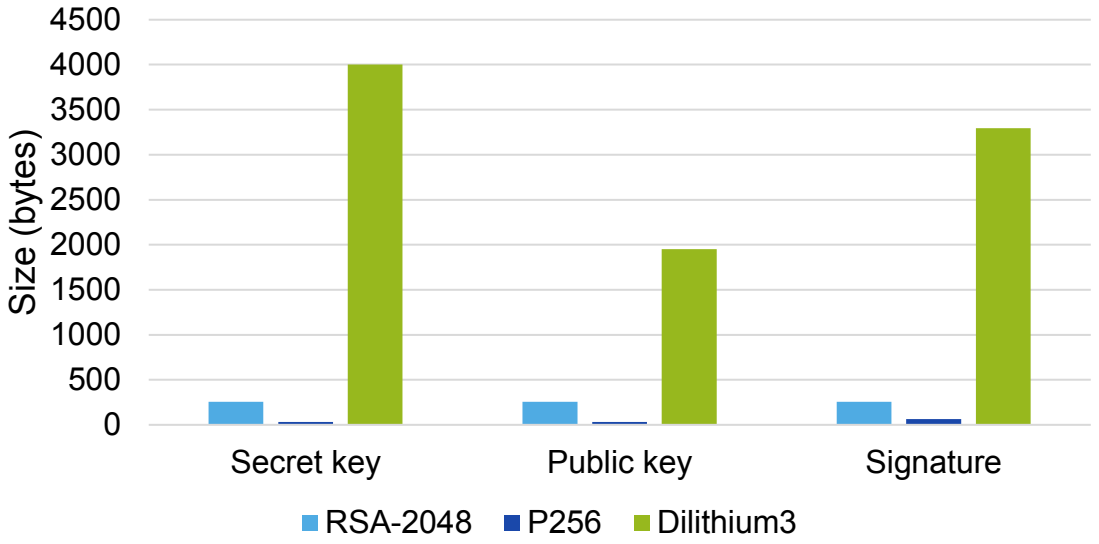
Variant			Dilithium-3	
			KiB	10^3 cc
C only	PQClean [1]	K	59.4	3,504
		S	77.7	12,987
		V	56.4	3,666
	New [2]	K	6.4	5,112
		S	6.5	36,303
		V	2.7	7,249

[1] M. J. Kannwischer, P. Schwabe, D. Stebila, and T. Wiggers: Improving Software Quality in Cryptography Standardization Projects. Security Standardization Research – EuroS&P Workshops. 2022.
[2] **J. W. Bos**, J. Renes and A. Sprenkels: Dilithium for Memory Constrained Devices. Africacrypt, LNCS, vol. 13503, Springer, 2022.



DILITHIUM IMPACT

- Measurements on Cortex-M4 from pqm4 framework
- Functional implementation only (not hardened)
- Large trade-offs between stack and efficiency
- **80 ~ 90 percent** of run-time in SHA-3



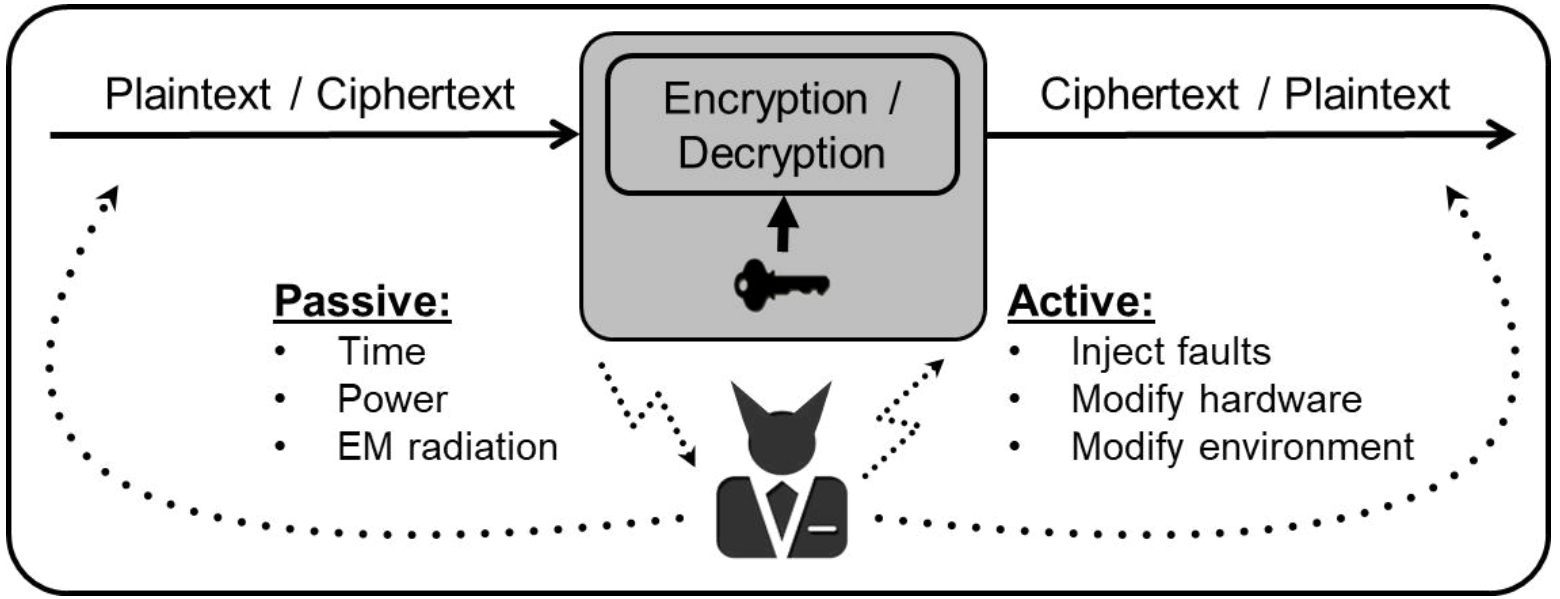
PQC SIGNATURE MIGRATION (EMBEDDED PERSPECTIVE)

Algorithm (Level 3)	PQ Secure?	Standard?	Efficient Signing?	Stateful?	Efficient Verify?	Need hybrid?	PK (Bytes)	Sig (Bytes)
ECC	No	FIPS 186	Yes	No	Yes	N/A	32 B	64 B
Dilithium	Yes	PQC (2024)	Yes	No	Yes	Yes	1952 B	3293 B
Falcon (L5)	Yes	PQC (2024)	No	No	Yes	Yes	1793 B	1280 B
SPHINCS+	Yes	PQC (2024)	No	No	Yes	No	48 B	16224 B
LMS / XMSS	Yes	SP 800-208	Yes?	Yes	Yes	No	60 B	1744 B

FO-CALYPSE

SECURE CONNECTIONS
FOR A SMARTER WORLD

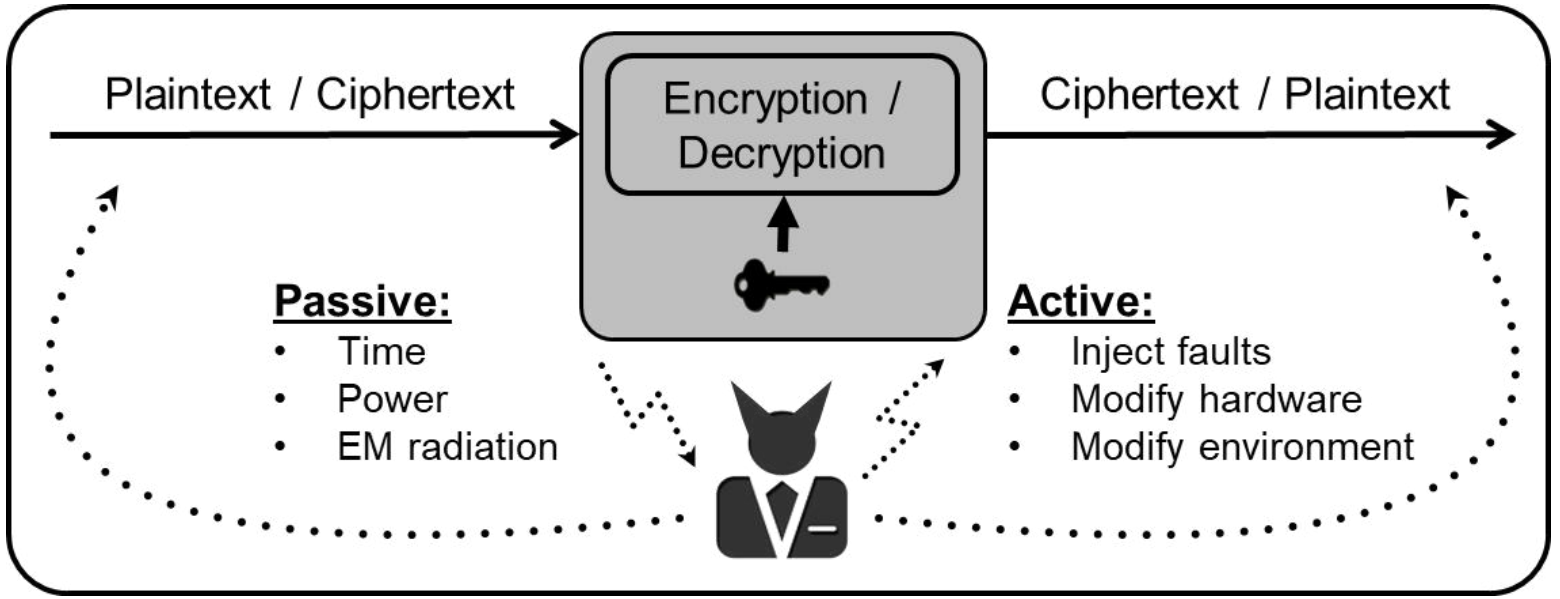
High-assurance implementations



Use meta-information to extract information about the key used in your target platform / product. Many powerful techniques:

fault injections, simple power analysis, differential power analysis, correlation power analysis, template attacks, higher-order correlation attacks, mutual information analysis, linear regression analysis, horizontal analysis, etc

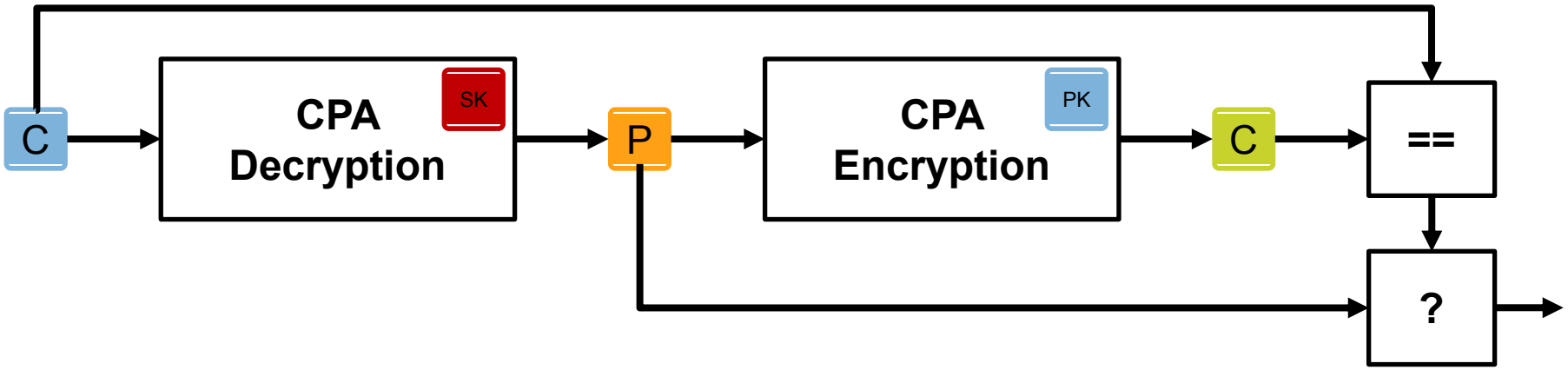
High-assurance implementations



It took many years to find secure and fast protections for RSA + ECC → still cat-and-mouse game

What about Post-Quantum Cryptography?

FUJISAKI OKAMOTO TRANSFORM



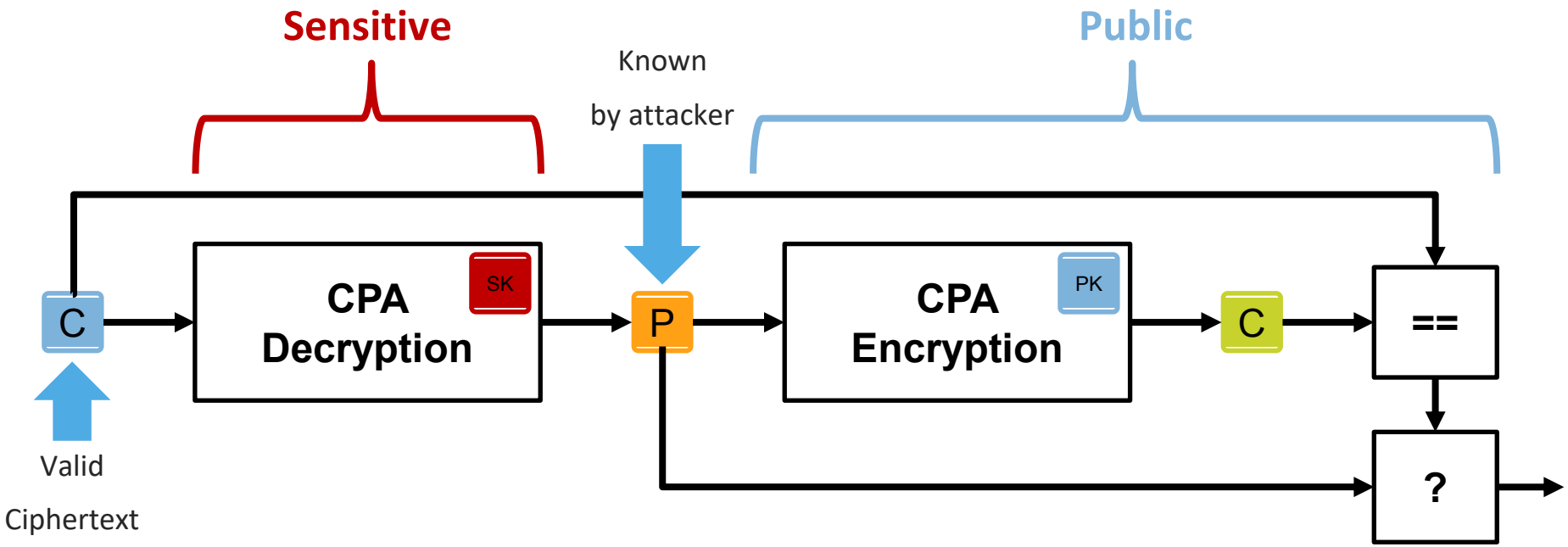
Transform a scheme which achieves IND-CPA (“chosen plaintext attack”) security
to reach IND-CCA (“indistinguishability against chosen-ciphertext attacks”) security

- 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**

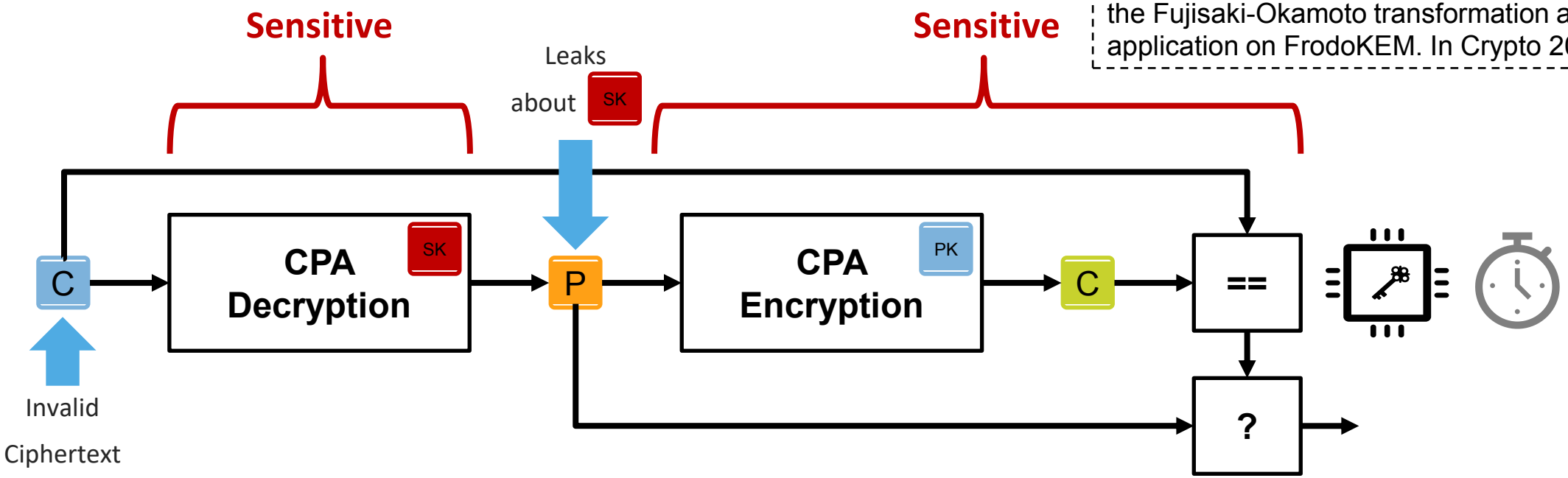


THE SCA PROBLEM OF THE FO-TRANSFORM

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

Guo, Johansson, Nilsson. A key-recovery timing attack on post-quantum primitives using the Fujisaki-Okamoto transformation and its application on FrodoKEM. In Crypto 2020.



THE SCA PROBLEM OF THE FO-TRANSFORM

Why is it bad?

- ☑ Millions of Points of Interest (PoI)
- ☑ Easy to build templates

Masked Kyber is broken with only 15k traces.

Curse of Re-encryption: A Generic Power/EM Analysis on Post-Quantum KEMs

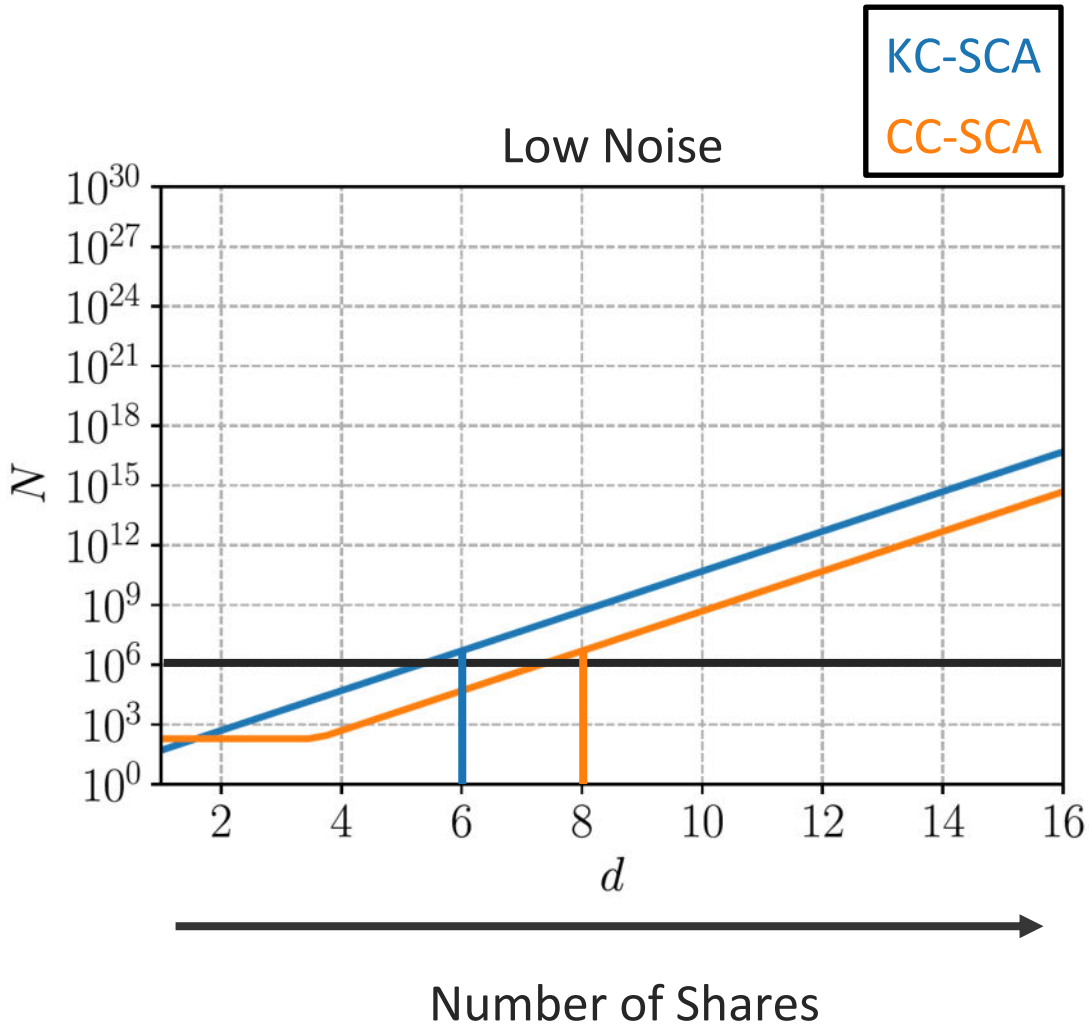
Rei Ueno[1,2,3], Keita Xagawa[4], Yutaro Tanaka[1,2], Akira Ito[1,2], Junko Takahashi[4] and Naofumi Homma[1,2]

CASE STUDY: MASKED KYBER

Split variables into *d* **shares**.

Higher *d* = Higher security + Increased cost

Pre-Quantum: Certified industrial solutions **d = 2-3**



CASE STUDY: MASKED KYBER

Split variables into *d* **shares**.

Higher *d* = Higher security + Increased cost

Pre-Quantum: Certified industrial solutions **d = 2-3**

For **low noise**:

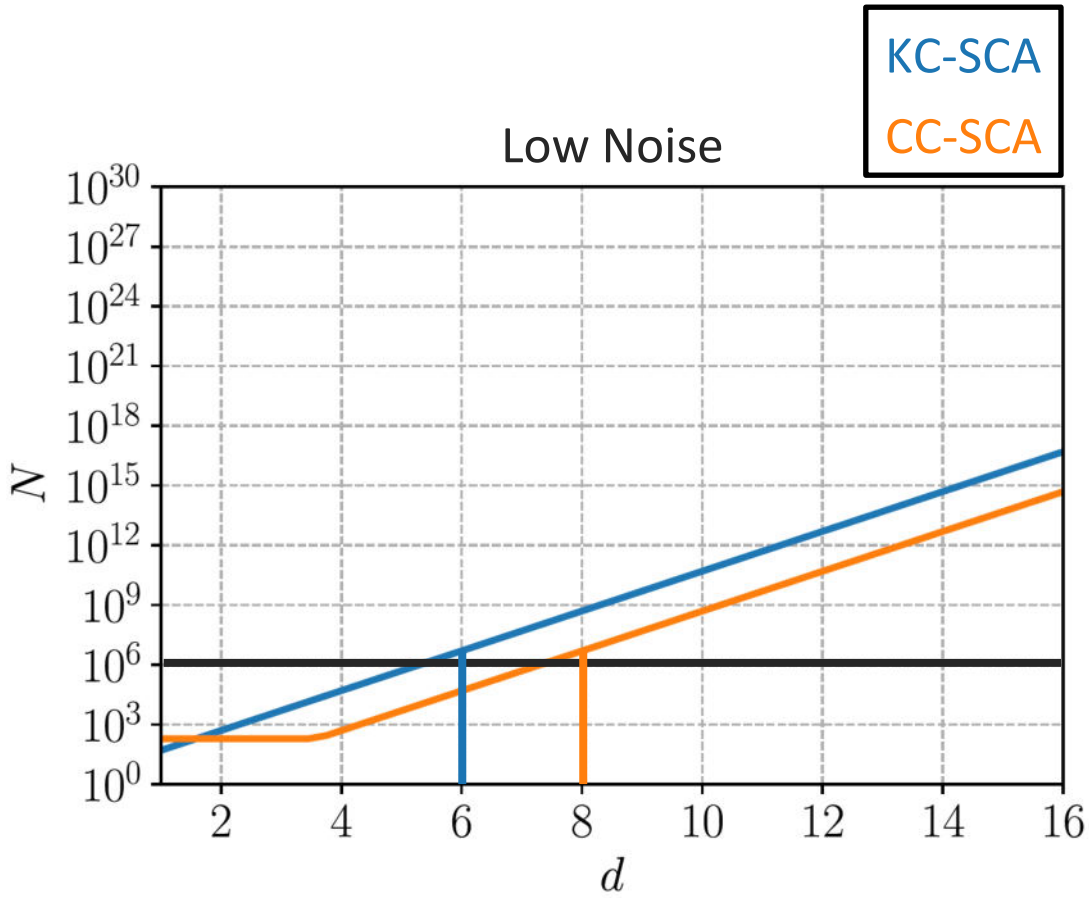
- Known ciphertext ➔ d = 6
- Chosen ciphertext ➔ d = 8

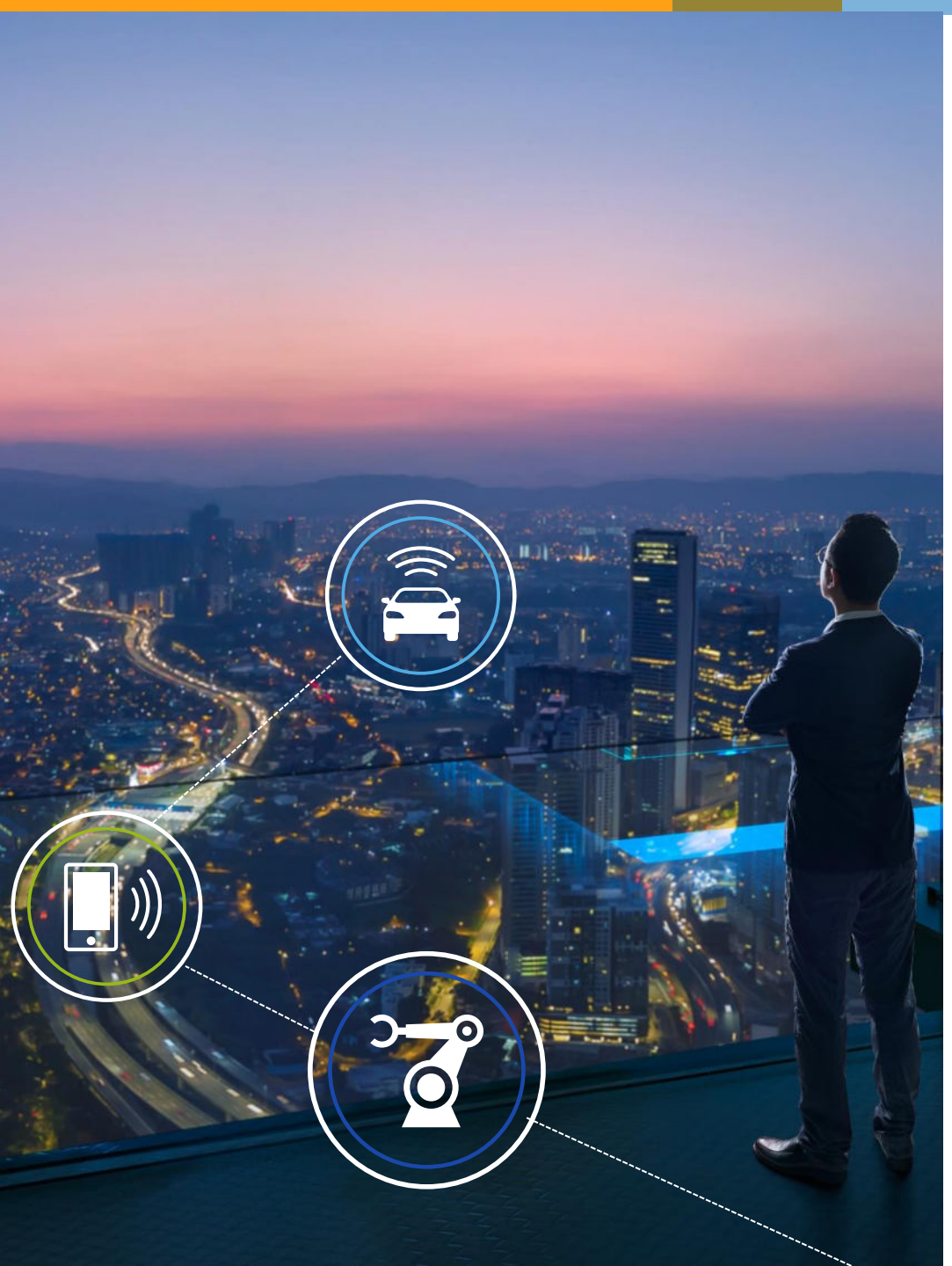
FO leakage causes an increase of **2** shares.

For **high(er) noise**:

- Known ciphertext ➔ d = 2
- Chosen ciphertext ➔ d = 3

FO leakage causes an increase of **1** share.





CONCLUSIONS

Irrelevant if the quantum threat is real or not
New PQC-Standard are coming!
→ Post-quantum crypto is already being requested by customers in all areas including Industrial, IoT and Automotive!

For embedded platforms challenges in terms of

- Performance, memory and key-sizes
- How to efficiently achieve protection against sophisticated side-channel attacks?

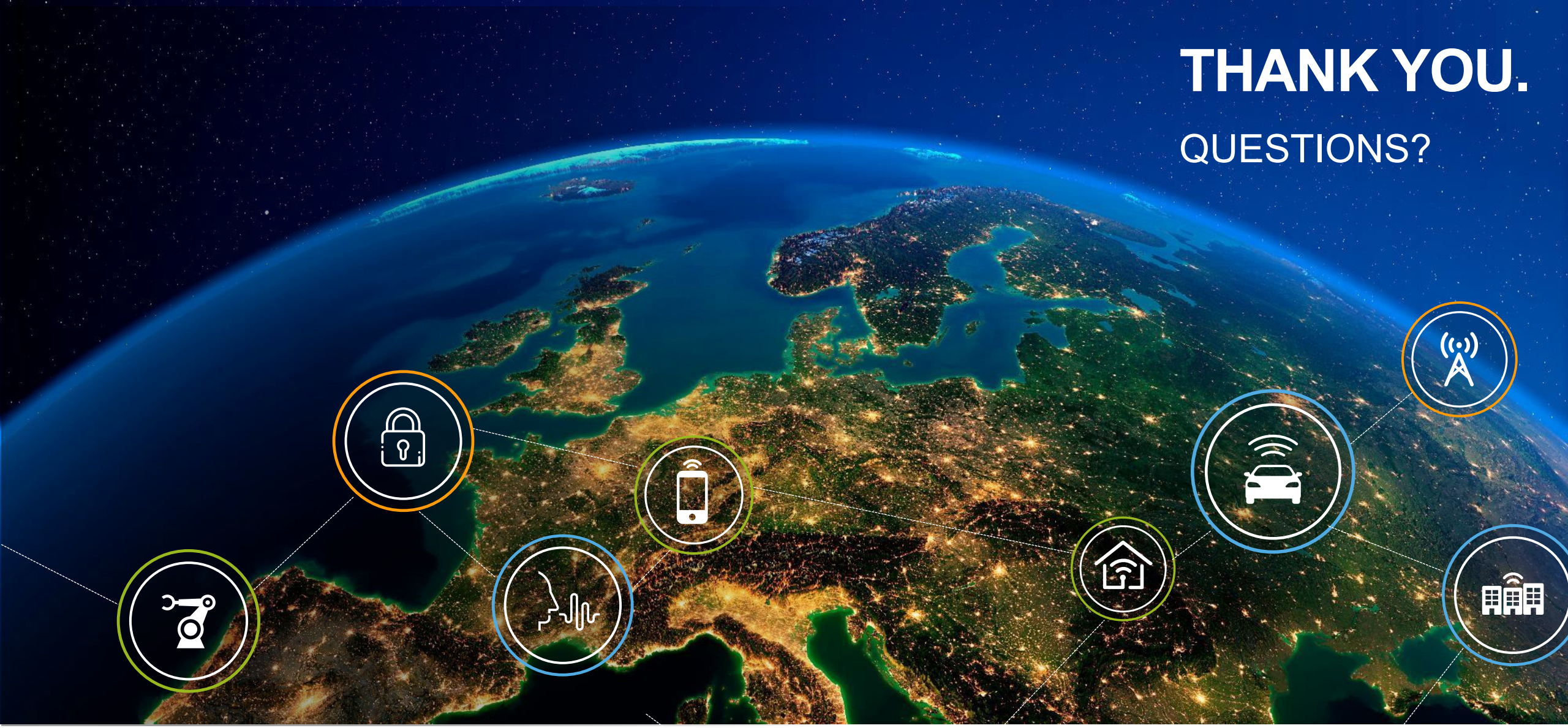
✓ **Think about migration paths now**

✓ **Exciting times to work on crypto & security solutions!**

CONTACT: PQC@NXP.COM | NXP.COM/PQC

THANK YOU.

QUESTIONS?



SECURE CONNECTIONS
FOR A SMARTER WORLD

CONTACT: PQC@NXP.COM | NXP.COM/PQC

Post-Quantum Cryptography Conference

PKI Consortium

ENTRUST

HID

PQ SHIELD

Fortanix

KEYFACTOR

NOREG

QRL

THALES

d-trust.

amsterdam convention bureau

ascertia

亞洲誠信 TRUSTAsia