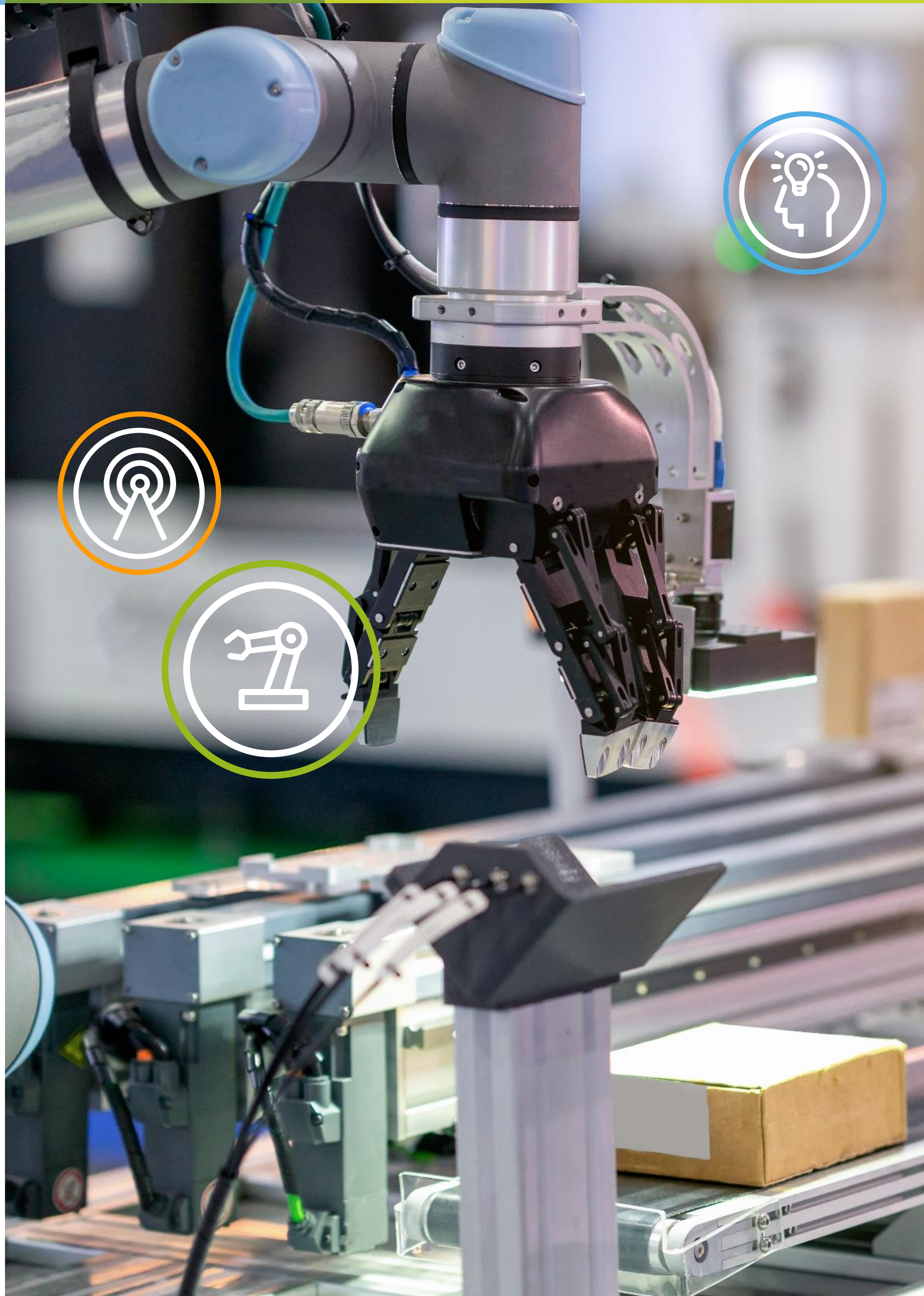
POST-QUANTUM CRYPTOGRAPHY: A NEW CYBERSECURITY ERA

Joppe Bos, Senior Principal Cryptographer
Competence Center Crypto & Security

NOREA QUANTUM-SEMINAR
NOVEMBER 2022

SECURE CONNECTIONS FOR A SMARTER WORLD



PUBLIC

SECURE CONNECTIONS FOR A SMARTER WORLD

OUR DIGITALLY ENHANCED WORLD IS EVOLVING TO ANTICIPATE AND AUTOMATE

NXP Semiconductors N.V. (NASDAQ: NXPI) is a global semiconductor company creating solutions that enable secure connections and infrastructure for a smarter world. NXP focuses on research, development and innovation in its target markets.

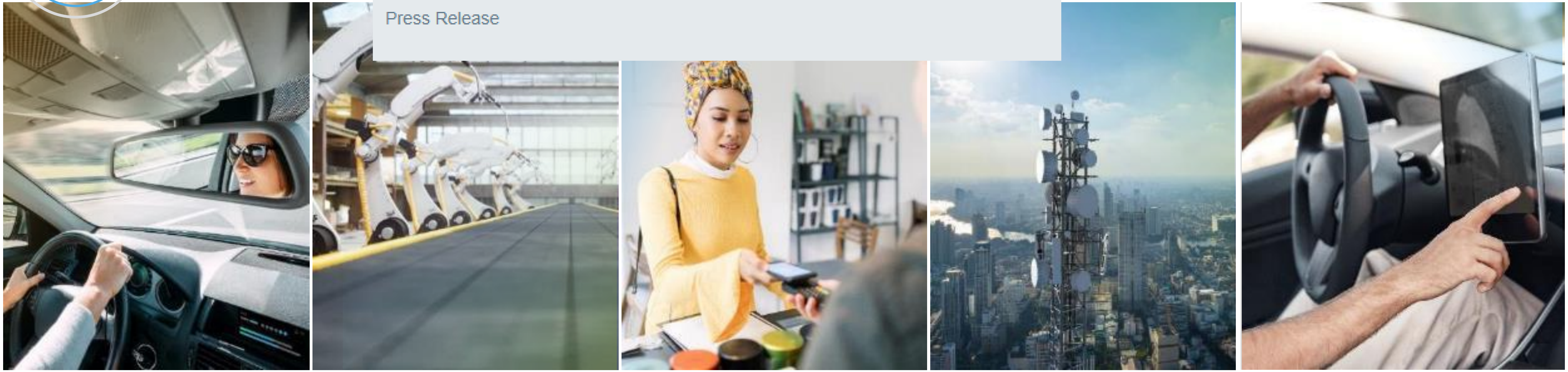
AUTOMOTIVE

NXP and German Aerospace Center DLR Collaborate on Quantum Computing Technologies in Germany

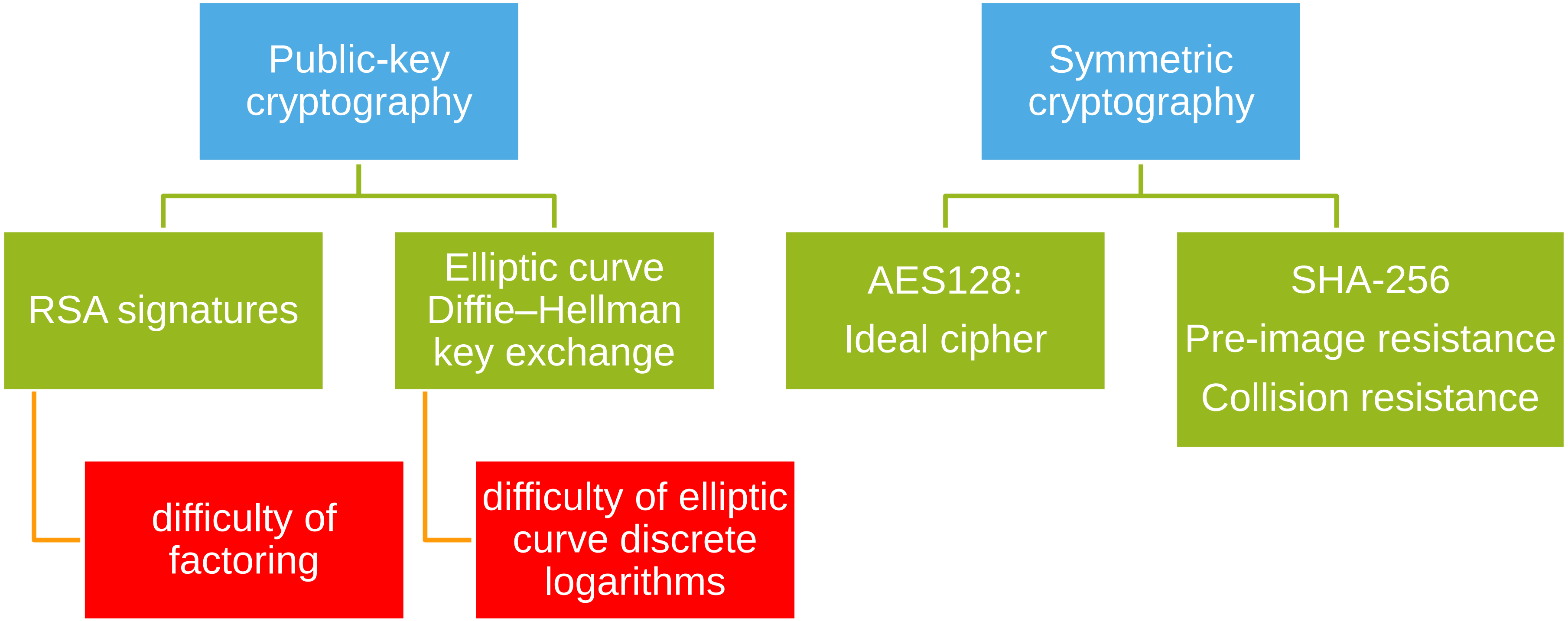
October 27, 2022 8:32 AM EDT (UTC-4) by NXP Semiconductors

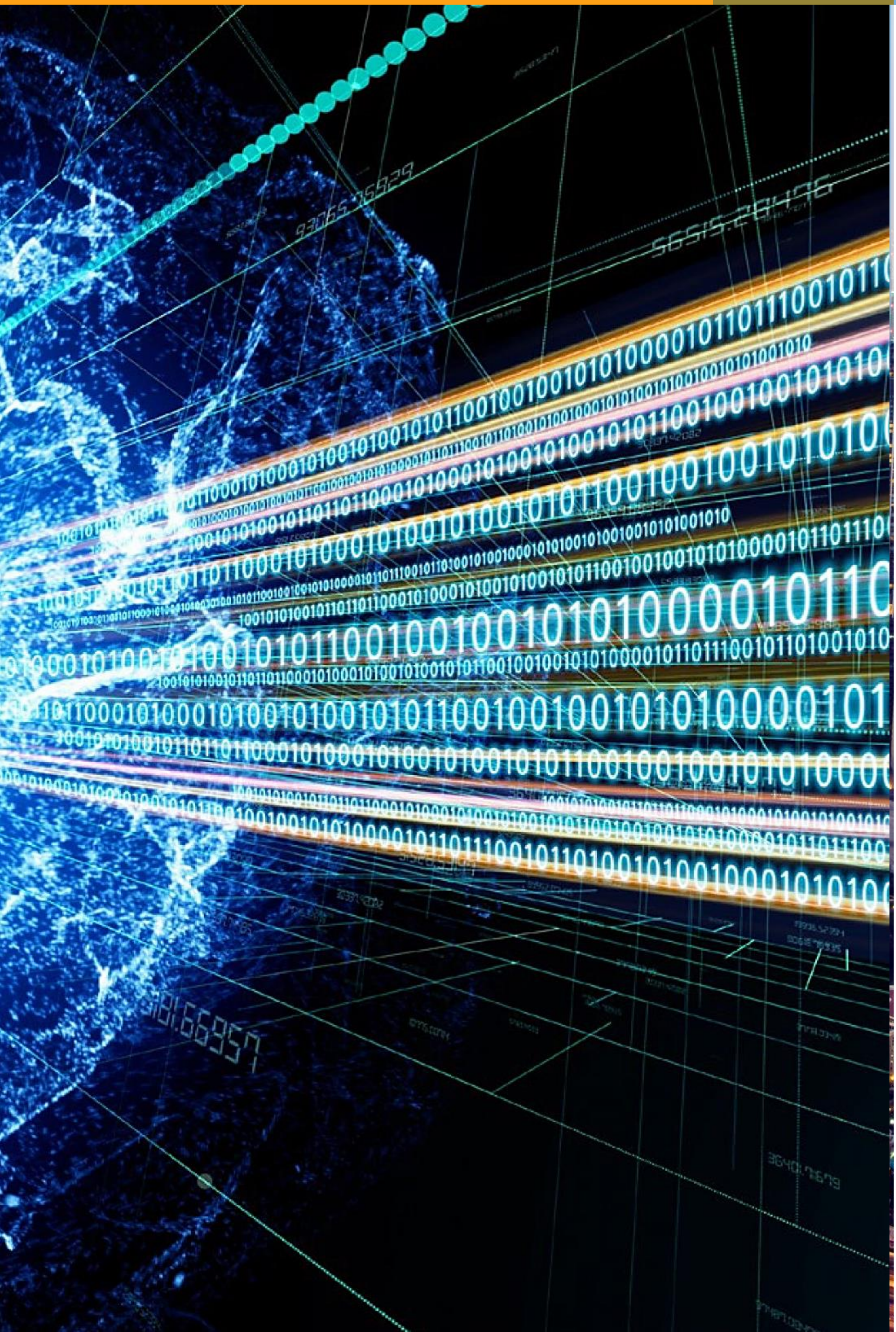
Press Release

COMMUNICATION INFRASTRUCTURE



CONTEMPORARY CRYPTOGRAPHY
TLS-ECDHE-RSA-AES128-GCM-SHA256





ADVANCES IN QUANTUM COMPUTING

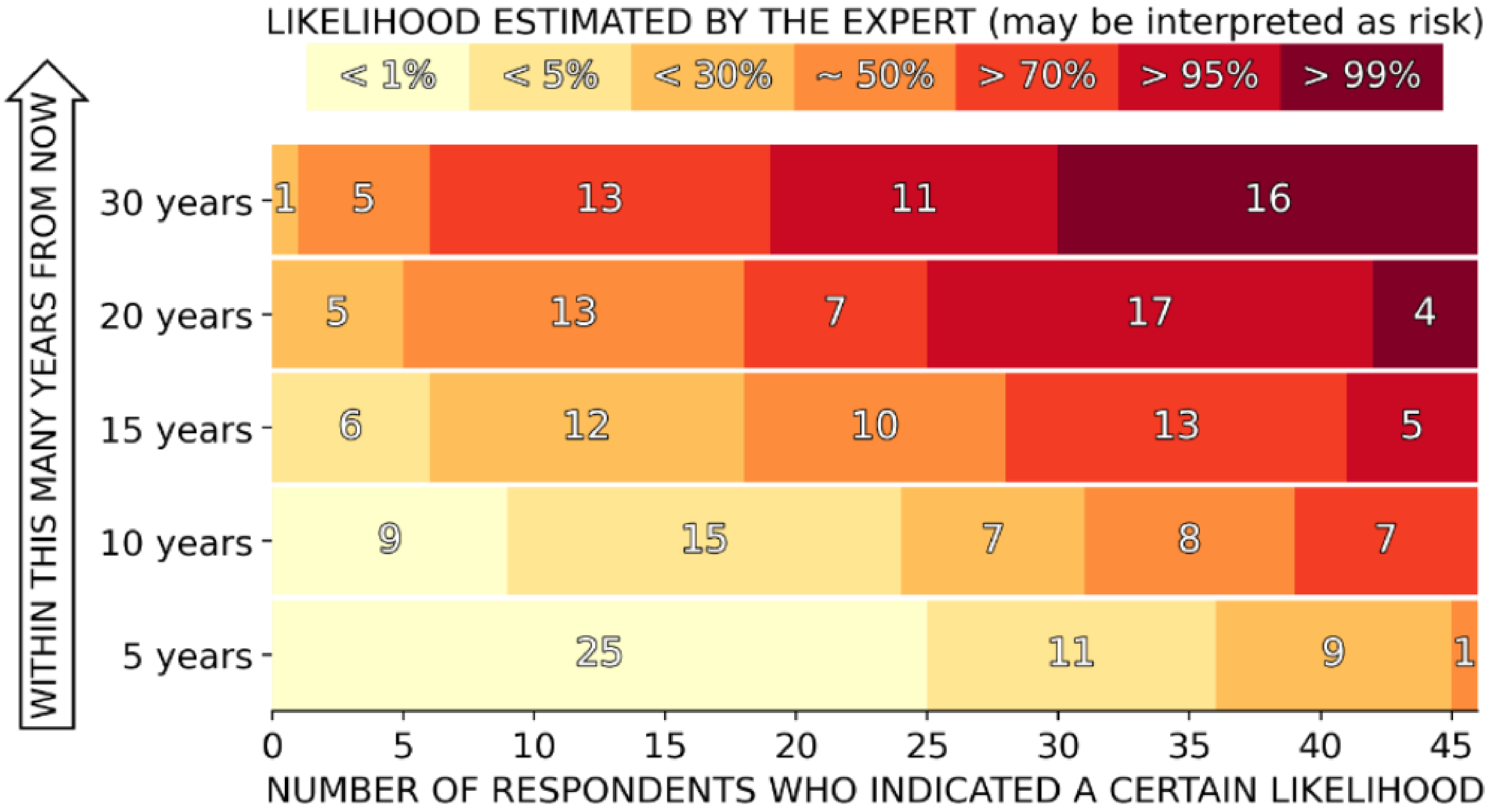
Quantum computers hold the promise of being able to take on certain problems exponentially faster compared to a normal computer

- Healthcare and pharmaceuticals
- Materials
- Sustainability solutions
- Financial trading
- Big data and many other complex problems and simulations

SO, WHEN IS IT GOING TO BE HERE ?

EXPERTS' ESTIMATES OF THE LIKELIHOOD OF A QUANTUM COMPUTER ABLE TO BREAK RSA-2048 IN 24 HOURS

The experts were asked to indicate their estimate for the likelihood of a quantum computer that is cryptographically relevant—in the specific sense of being able to break RSA-2048 quickly—for various time frames, from a short term of 5 years all the way to 30 years.



© https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/

CONTEMPORARY CRYPTOGRAPHY

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

“Double” the key sizes

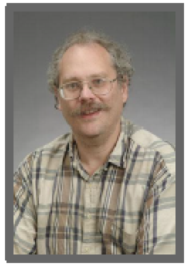
Public-key cryptography

RS … res

Di … an

difficulty of factoring

difficulty of elliptic curve discrete logarithms

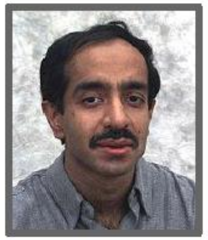


Shor’s algorithm (1994)

Symmetric cryptography

AES256:
Ideal cipher

SHA-384
Pre-image resistance
Collision resistance



Grover’s algorithm (1996)

Quantum Potential To destroy Security As We know it

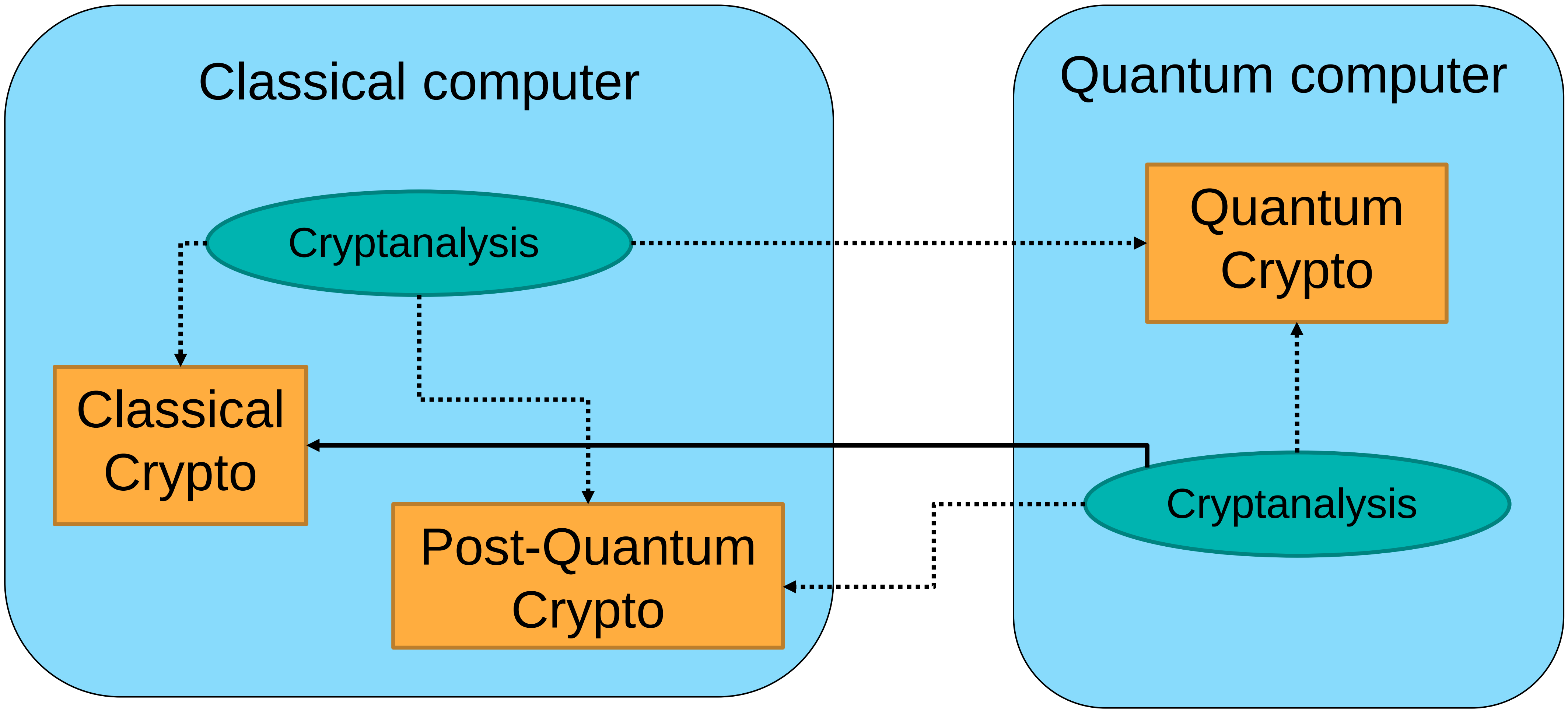
Confidential email messages, private documents, and financial transactions
Secure today but may be compromised in the future, even if recorded & encrypted

Firmware update mechanisms in vehicles
May 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


Classical computer
Cryptanalysis
Classical Crypto
Post-Quantum Crypto
Quantum computer
Quantum Crypto
Cryptanalysis

POST-QUANTUM CRYPTO STANDARDS ARE COMING

IT DOESN’T MATTER IF YOU BELIEVE IN QUANTUM COMPUTERS OR NOT

POST-QUANTUM CRYPTO STANDARDIZATION

2016
- Formal call for proposals

2017
- Deadline for submissions
- 69 candidates received

2019
- Second Round Candidates announced: 26 remaining candidates

2020
- Third Round Candidates announced: 7 Finalists and 8 Alternates

2022
- Announcement of Winners to be Standardized

2024
- Standards Available

2030
- Migration to new PQC public-key standards completed

AUTOMOTIVE

EGOVERNMENT

BANK CARDS

SMART MOBILITY (MIFARE) CARDS

TAGS & AUTHENTICATION

READERS

MOBILE

STANDARDS – NIST

CRYSTALS-Kyber
CRYSTALS-Dilithium
Winners

2024

Falcon
SPHINCS+
Secondary Winners

2025?

HQC
BIKE
Classic McEliece
SIKE
Round 4 Candidates

2028?

Proposals due '23
Digital Signature Competition

2030?

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

PQC Standard #2 (Digital Signatures)

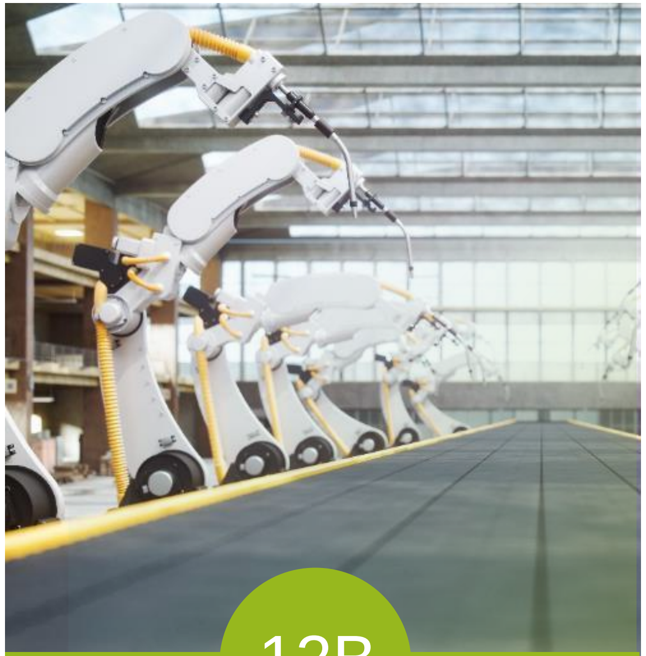
POST-QUANTUM CRYPTO IS ON THE HORIZON

AUTOMOTIVE

70%

70% connected cars by 2025

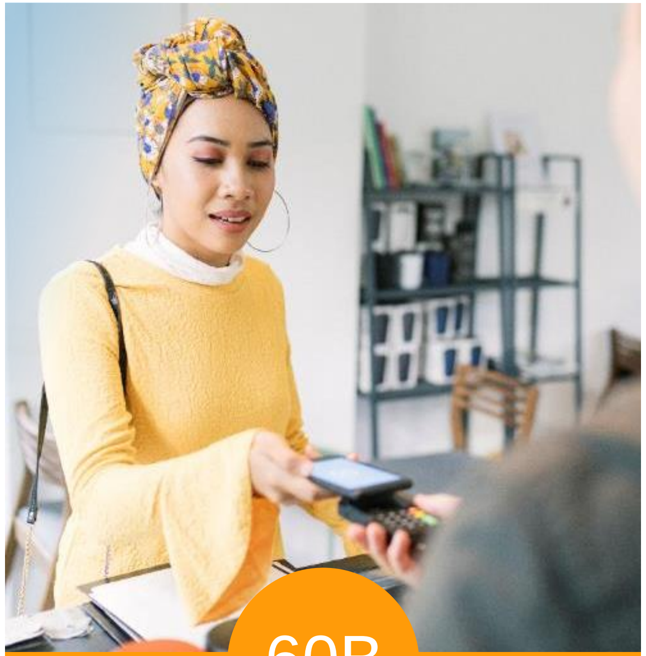
INDUSTRIAL & IOT



12B

IoT Edge & end nodes from 6B units in ‘21 to 12B units in ‘25

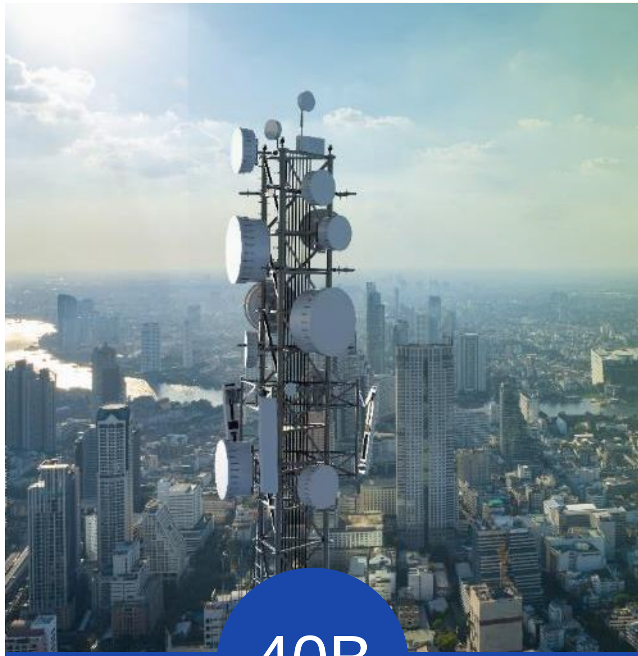
MOBILE



60B

Tagging 60B products per year by 2025

COMMUNICATION INFRASTRUCTURE



40B

Secure anchors & services for 40B processors

1. Source: NXP, Strategy Analytics, Evercore, Ericsson, IDTechex,

TYPICAL EXAMPLES

Automotive

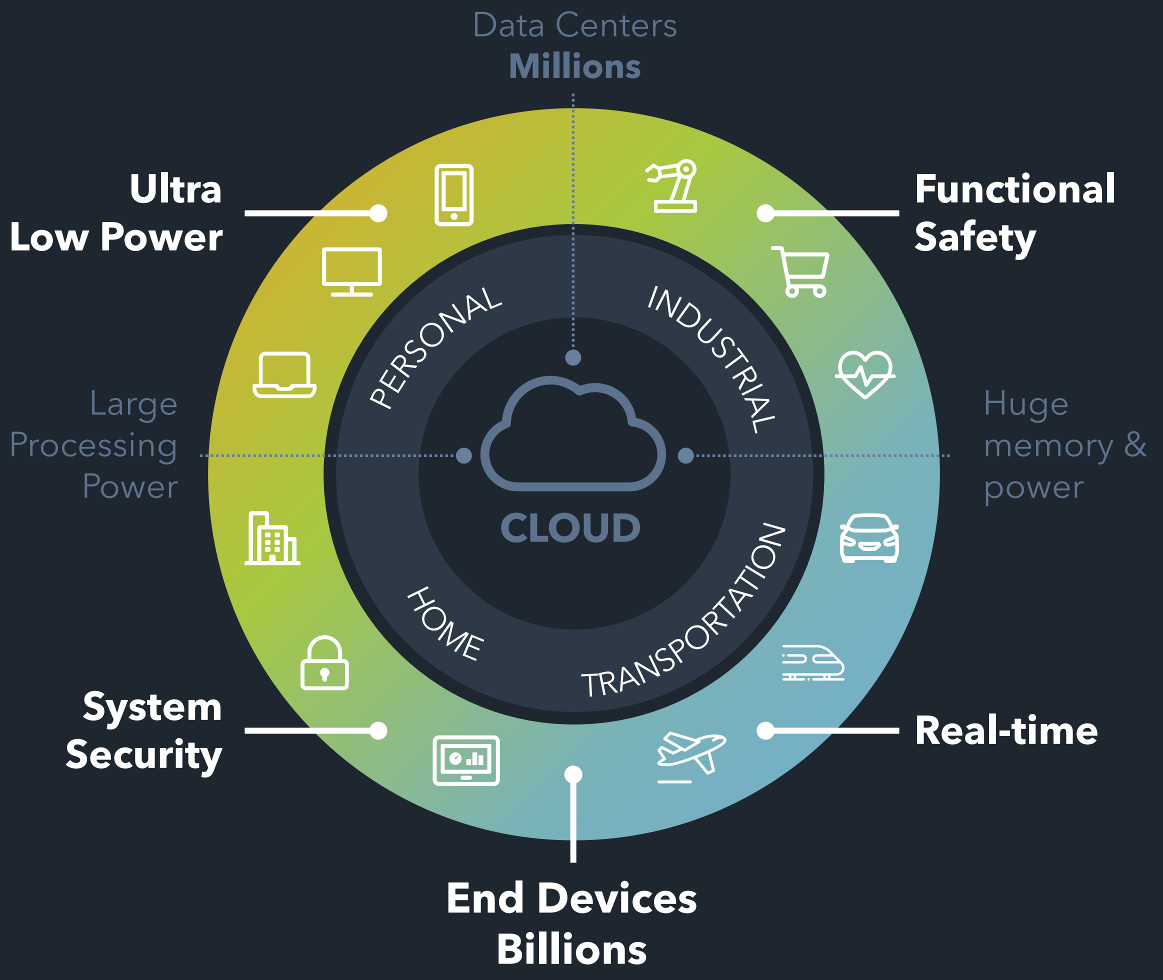
New platform designed <u>now</u> will likely enter the market after 2024 and remain in use for many years

(Industrial) IoT

Devices sold now need to be able to support the new PQC standard in 2024: crypto agility

Many embedded IoT platforms are resource constrained: 4-16 KiB memory

IMPACT PQC ON OUR ECO-SYSTEM



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

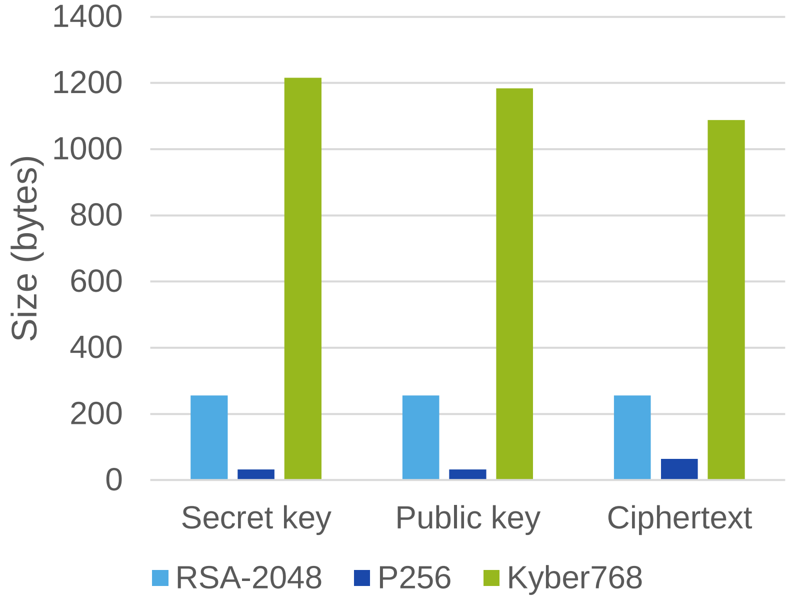
No Silver Bullet
If a crypto scheme was better, we would have standardized this already

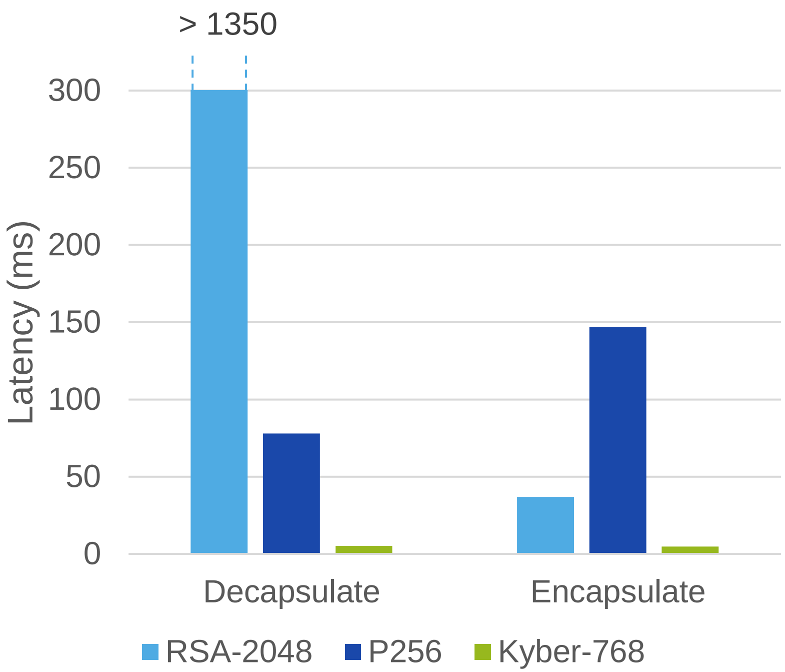
Cryptographic Keys
Orders of magnitude larger.
In the final: up to 1.3MB
Winners: up to 4.8KB
(ECC: 32 bytes, RSA: 384 bytes)

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

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



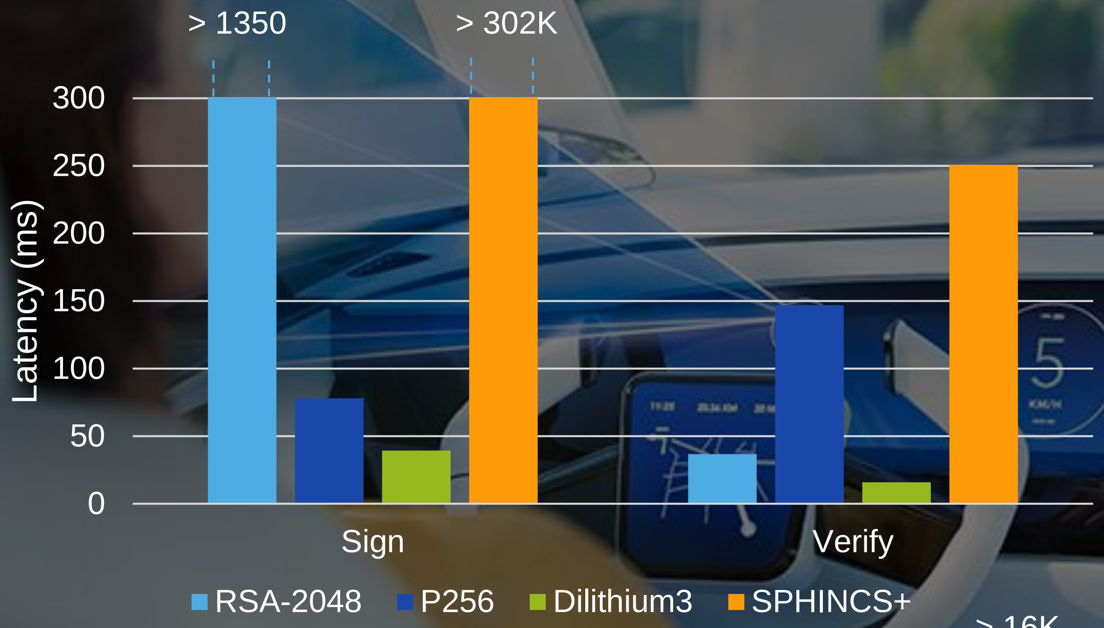


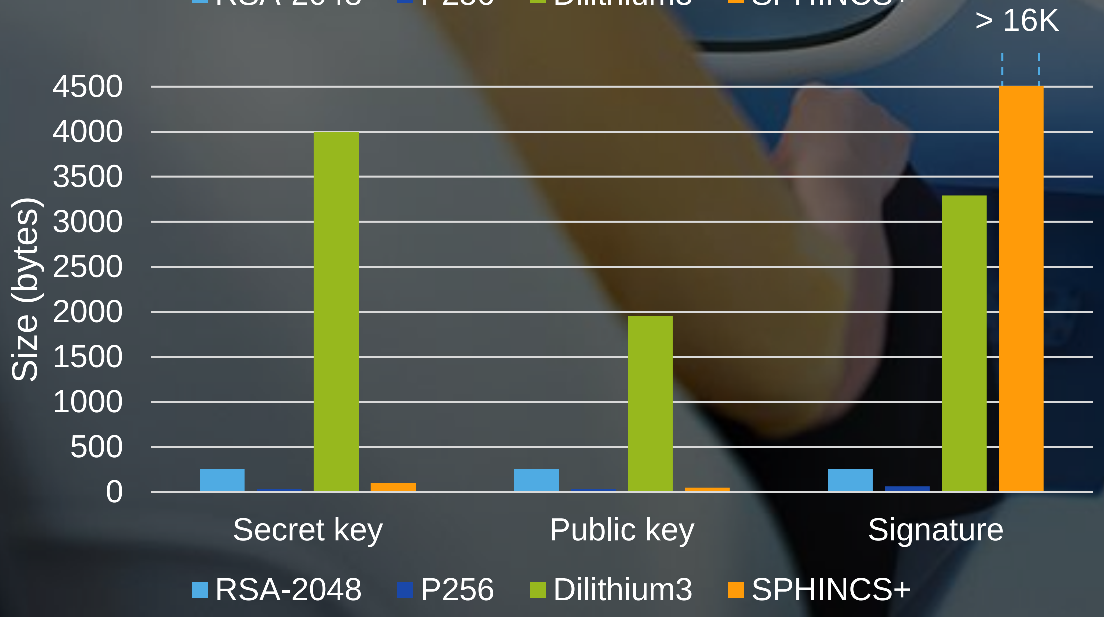
KEY-EXCHANGE IMPACT

Kyber **co-designed by NXP** with IBM, ARM and academic partners

- Measurements on Cortex-M4 @ 168MHz from pqm4 framework
- Functional implementation only (not hardened)
- **70 ~ 80 percent** of run-time in SHA-3

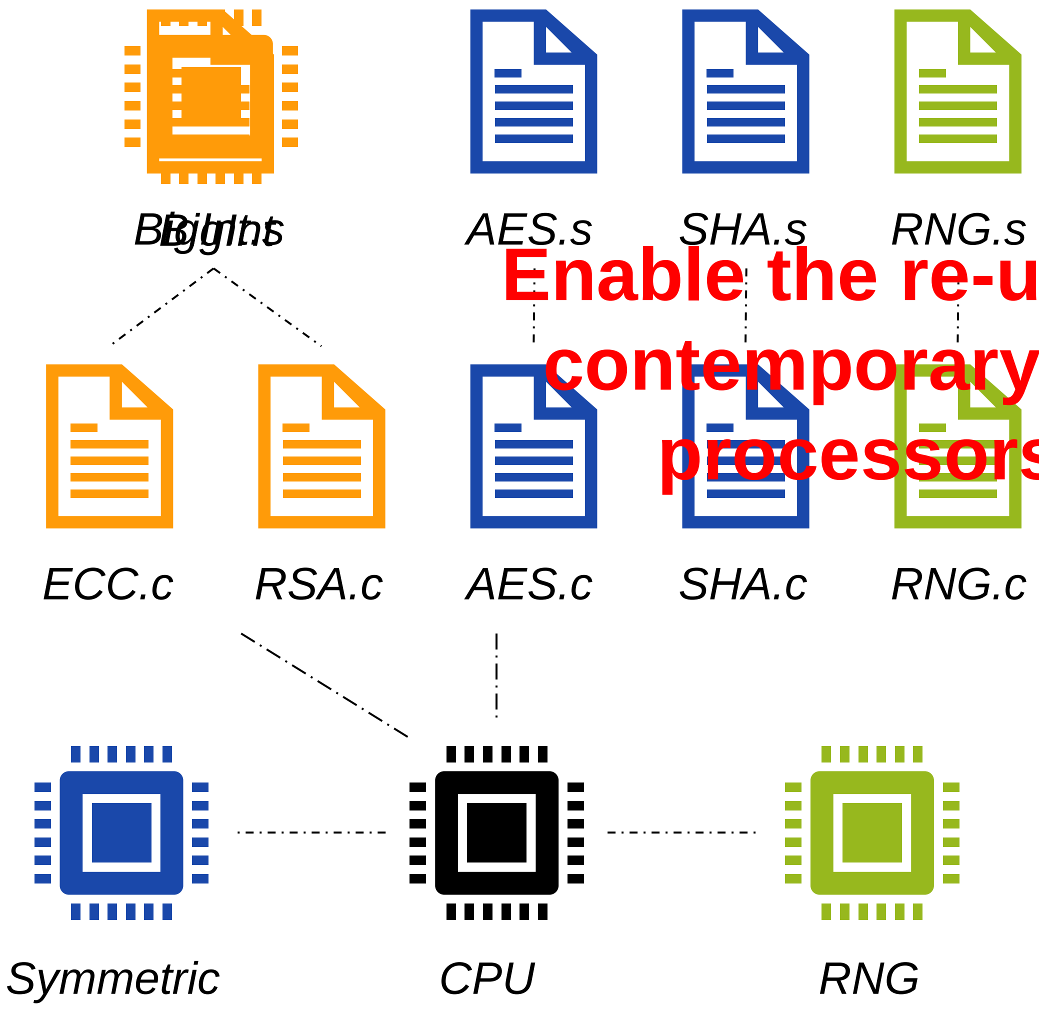
DIGITAL SIGNATURE IMPACT





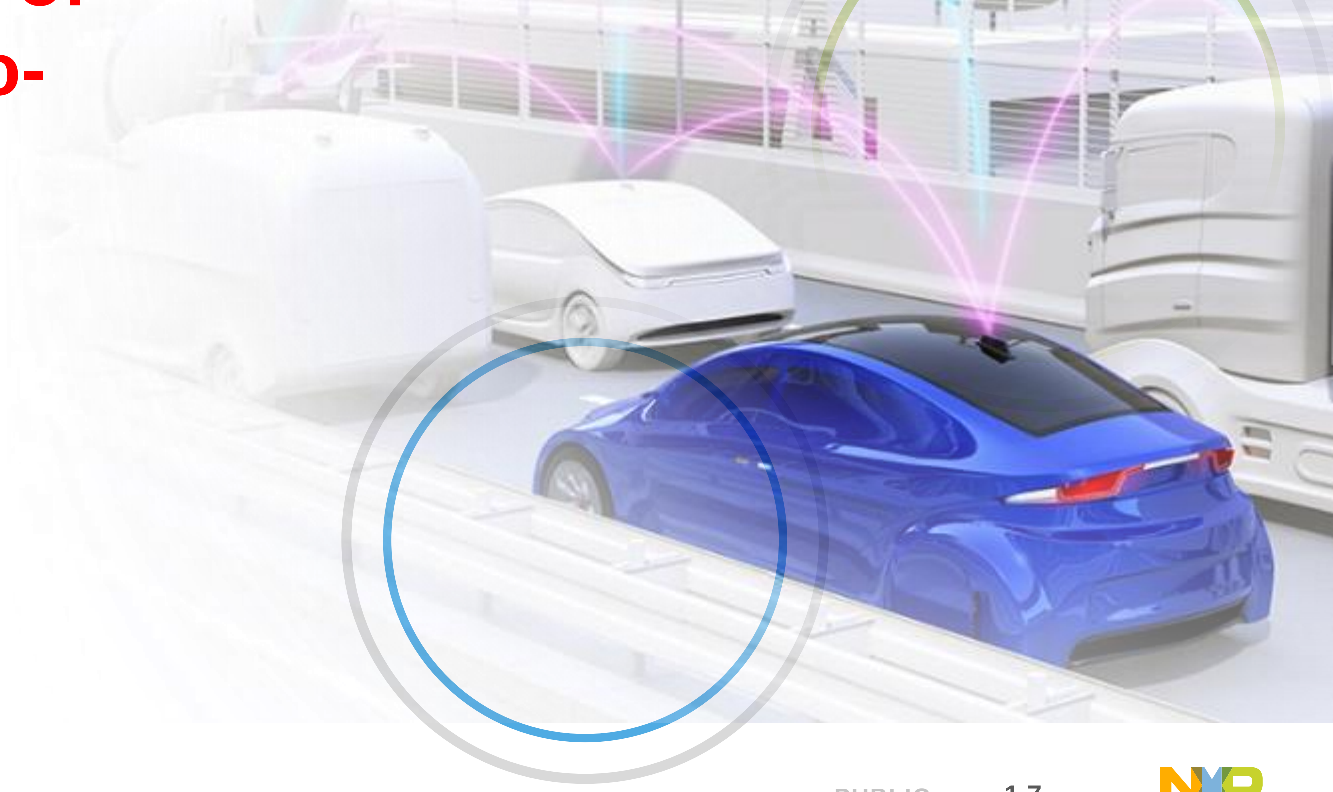
USE CASE STUDY IMPACT ASSESSMENT (SG32G AS AN EXAMPLE)

IMPLEMENTING CLASSICAL CRYPTOGRAPHY



Enable the re-use of contemporary co-processors

S32G2 automotive processor spec



Approach	Core	Structure	Size
RSA	Modular multiplication	$(\mathbb{Z}/n\mathbb{Z})^*$	n is 3072-bit
ECC	Elliptic curve scalar multiplication	$\mathrm{E}(\mathbb{F}_p)$	p is 256-bit
Lattice	Polynomial multiplication	$(\mathbb{Z}/q\mathbb{Z})[X]/(X^n+1)$	q is 16-bit n is 256

Co-pro present in current hardware

Can we use this?

Grundzüge einer arithmetischen Theorie der algebraischen Grössen.

(Von *L. Kronecker.*)

(Abdruck einer Festschrift zu Herrn *E. E. Kummers* Doctor-Jubiläum, 10. September 1881.)

Polynomial domain

$$f = 1 + 2x + 3x^2 + 4x^3$$

$$g = 5 + 6x + 7x^2 + 8x^3$$

$$\times$$

$$fg = 5 + 16x + 34x^2 + 60x^3 + 61x^4 + 52x^5 + 32x^6$$

Kronecker domain (with evaluation point 100)

$$f(100) = 4030201$$

$$g(100) = 8070605$$

$$\times$$

$$fg(100) = 32526160341605$$

ARITHMETIC CO-PROCESSORS

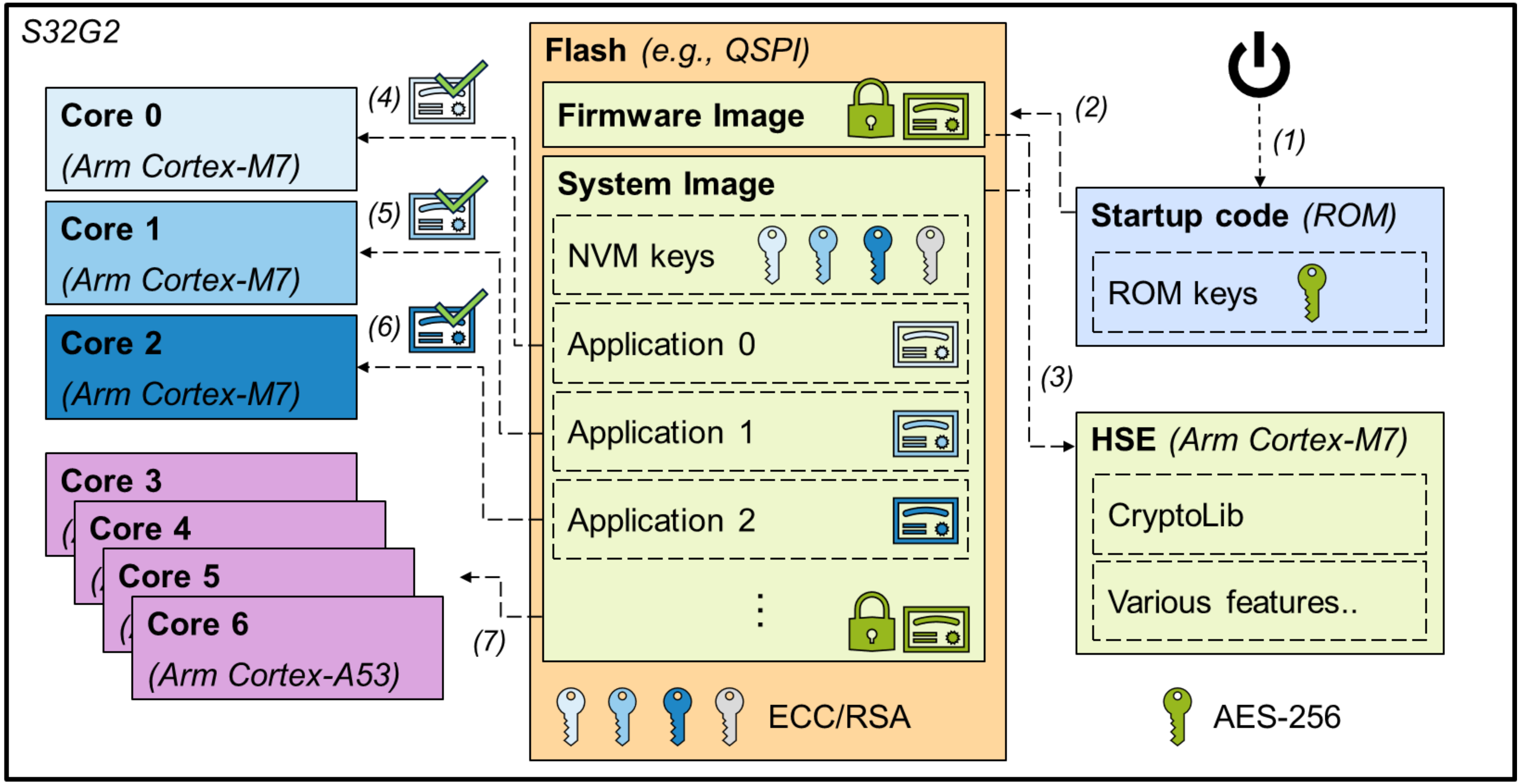
RE-USING EXISTING HARDWARE

ARITHMETIC CO-PROCESSORS	Dedicated secure hardware widely available to accelerate ECC and RSA
POST-QUANTUM CRYPTOGRAPHY	PQC work on completely different objects. Not straight-forward to re-use this hardware
KRONECKER+	Our new approach to run PQC on existing and deployed hardware. See: Bos, Renes, van Vredendaal; Post-Quantum Cryptography with Contemporary Co-Processors: Beyond Kronecker, Schönhage-Strassen & Nussbaumer; USENIX 2022

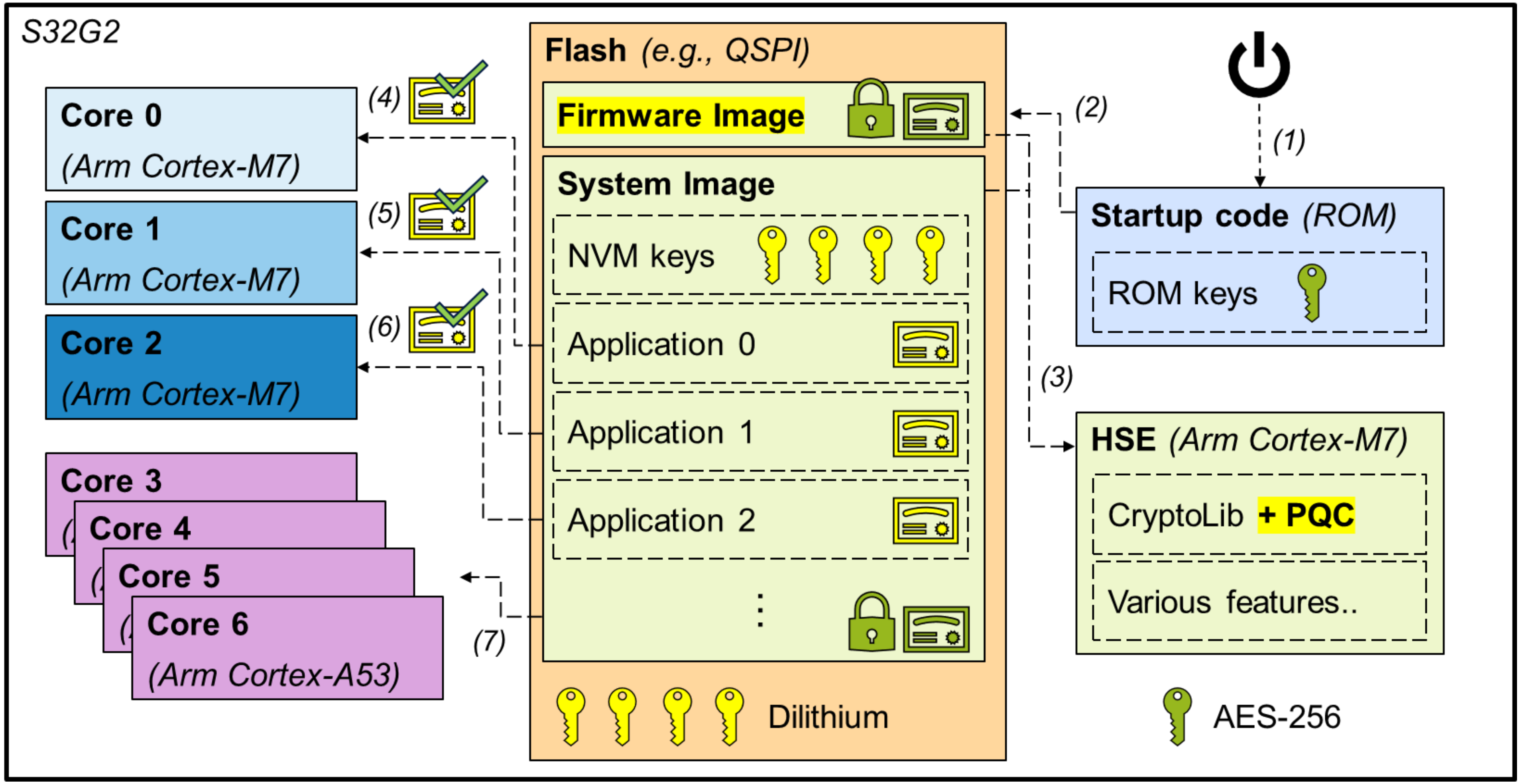
multiplications required

Multiplier width	512	256	128
Schoolbook	256	1024	4096
Kronecker+	16	32	64

PQC DEMO: HSE SECURE BOOT OVERVIEW



PQC DEMO: HSE SECURE BOOT OVERVIEW



S32G2 VEHICLE NETWORK PROCESSOR – A NEW TYPE OF AUTOMOTIVE PROCESSOR

OUR TARGET PLATFORM: S32G274A

3 Lockstep Arm® Cortex®-M7 Microcontrollers

4 Cluster Lockstep Cortex-A53 Microprocessors

8 MB of system RAM

POST-QUANTUM CRYPTO

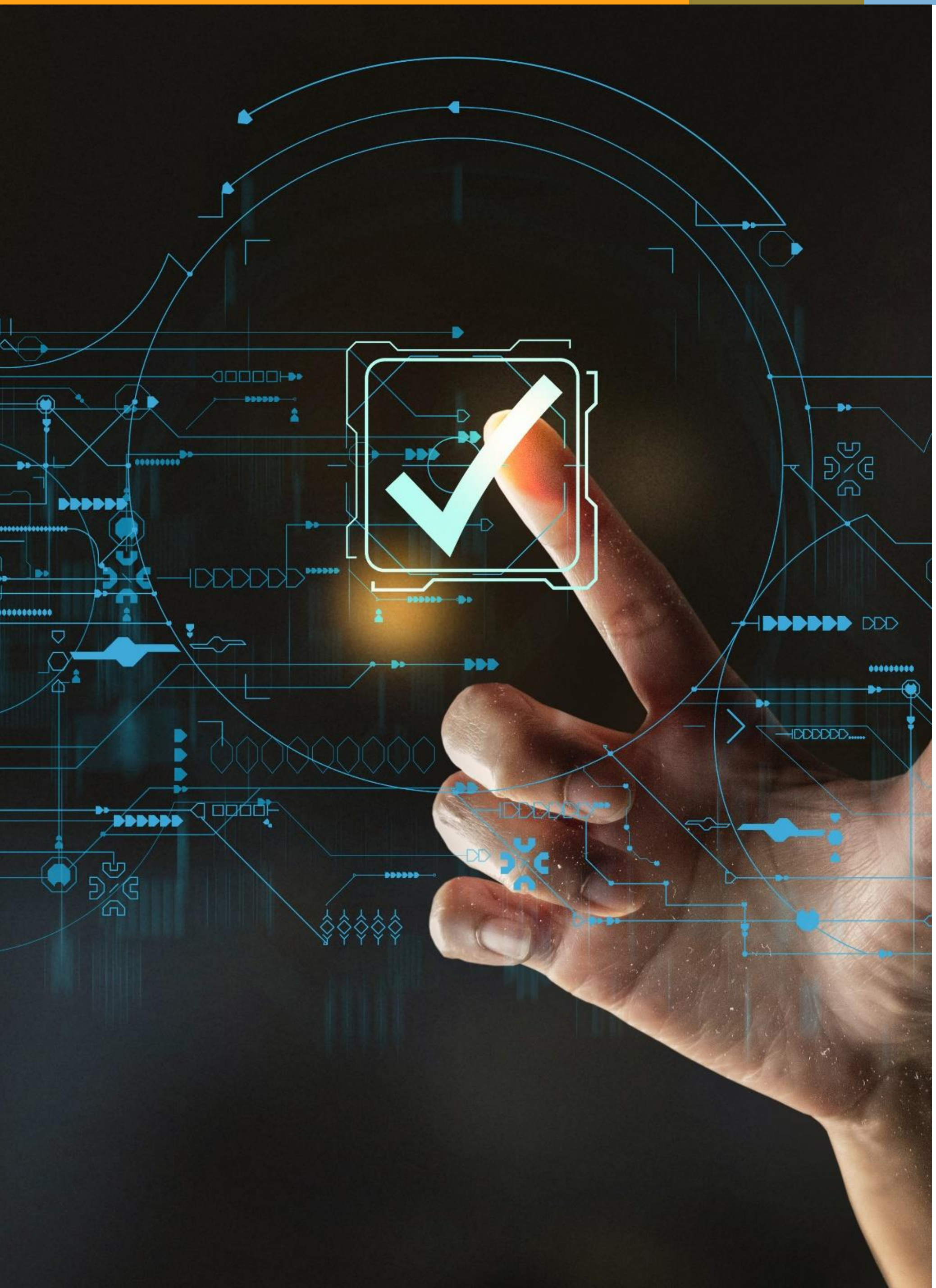
Can we enable PQC secure boot?

Integrate PQC secure signature verification

SAFE ASSURE™ by NXP

www.nxp.com/S32G2

EDGELOCK™ ASSURANCE by NXP



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**

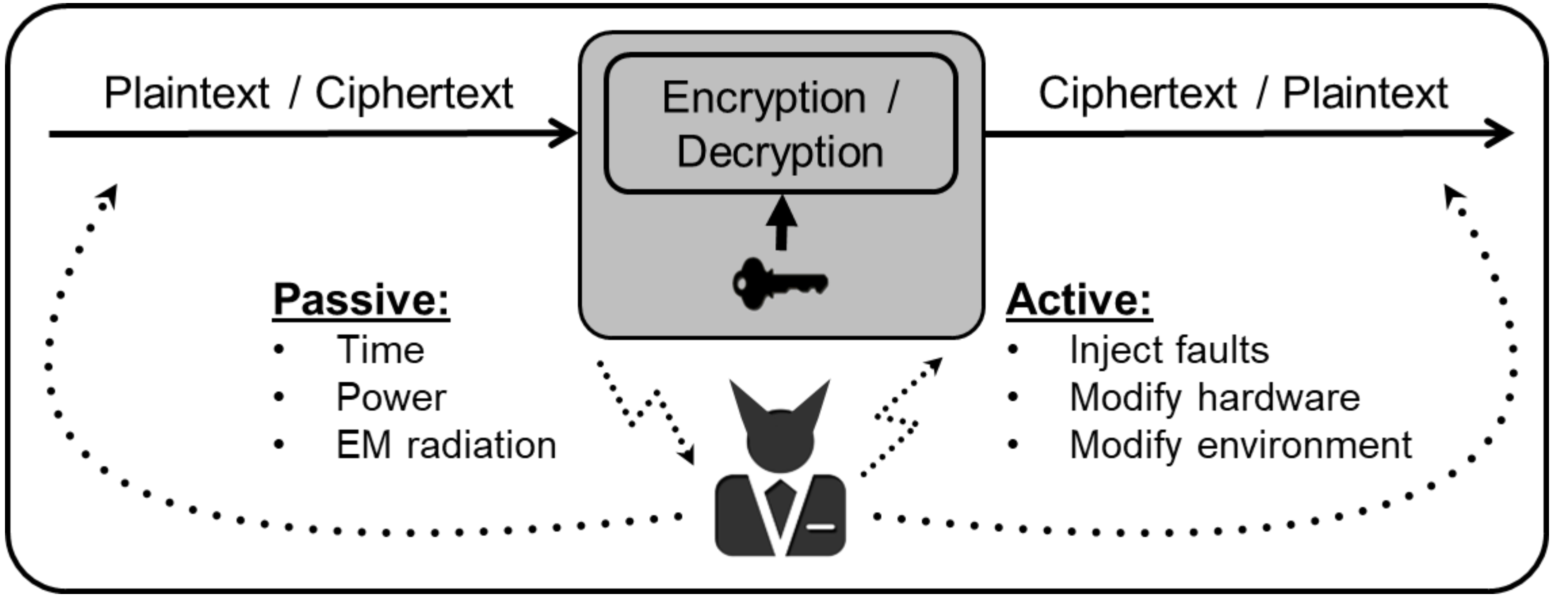
- Demonstrator only, further optimizations are possible (such as hardware accelerated SHA-3)
- Signature verification only required once for installation!
- During boot the signature verification can be replaced with a check of the Reference Proof of Authenticity

To appear:
J. W. Bos, B. Carlson, J. Renes, M. Rotaru, D. Sprenkels, G. P. Waters: Post-Quantum Secure Boot on Vehicle Network Processors. Embedded Security in Cars (escar) 2022

FO-CALYPSE

SECURE CONNECTIONS
FOR A SMARTER WORLD

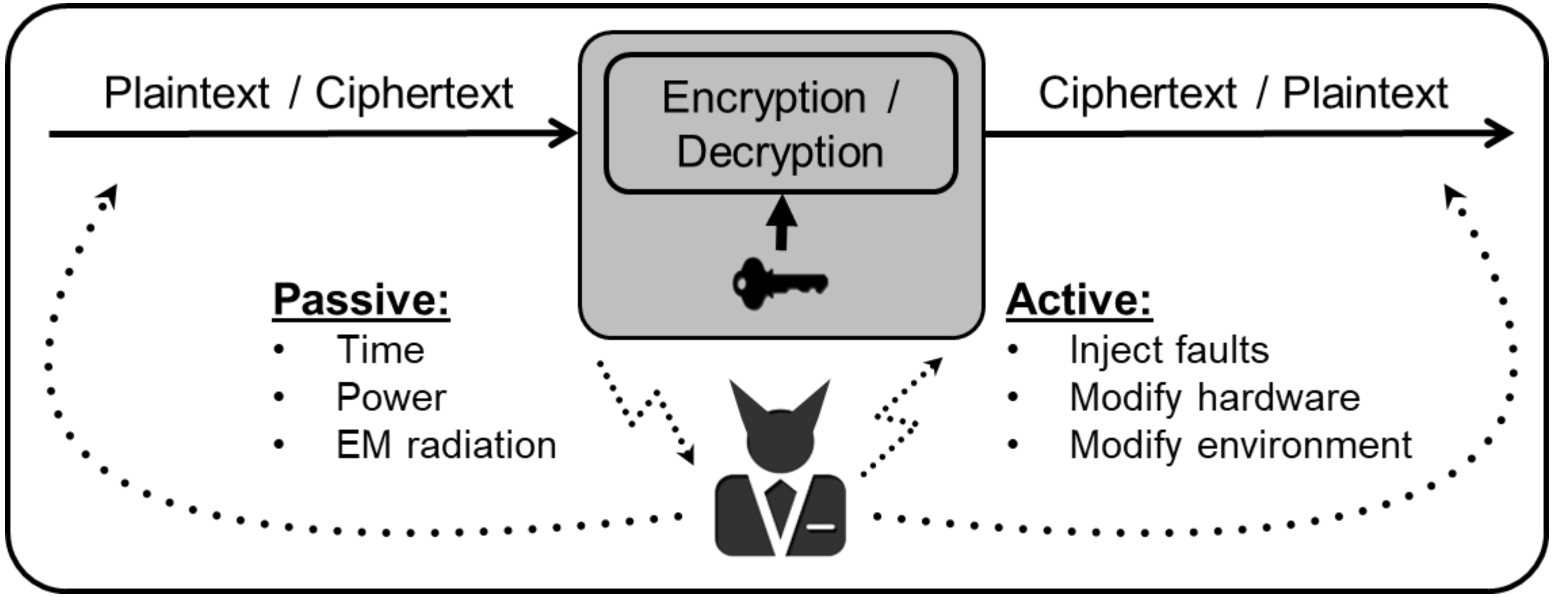
High-assurance implementations



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

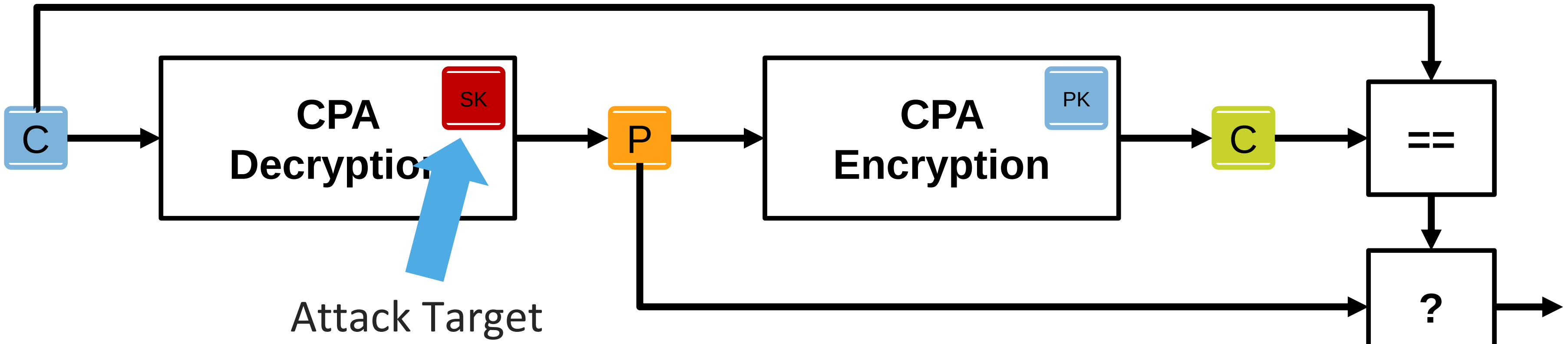
What about Post-Quantum Cryptography?

THE SCA PROBLEM OF THE FO-TRANSFORM

The Fujisaki-Okamoto (FO) transformation (or slight variants) underlies the IND-CCA security of many KEMs, e.g.:

Crystals-Kyber	NTRU-prime	BIKE	SIKE
Saber	Frodo-KEM	HQC	

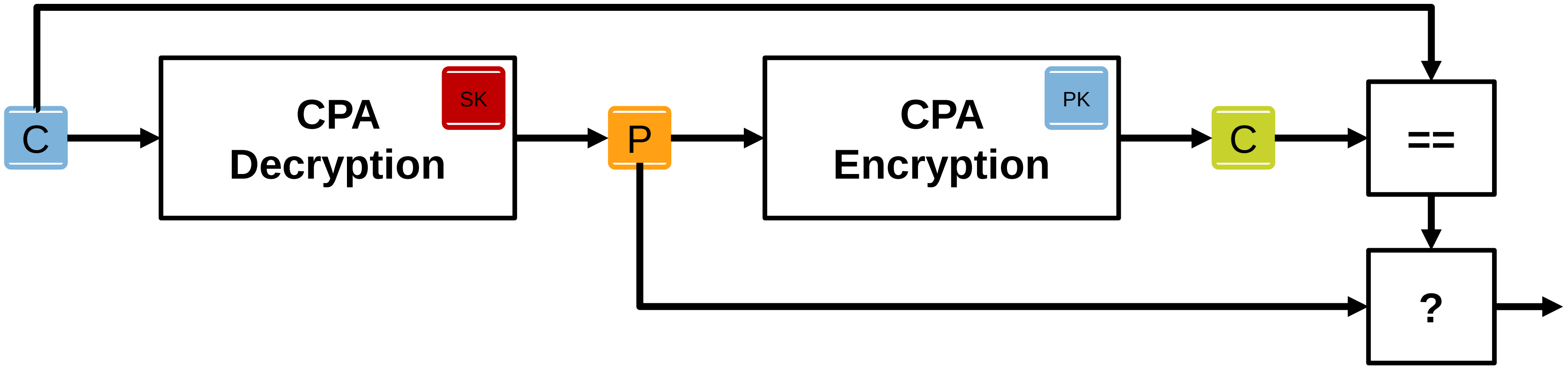
Exemplary Decapsulation:



THE SCA PROBLEM OF THE FO-TRANSFORM

Attack 1: Chosen Plaintext

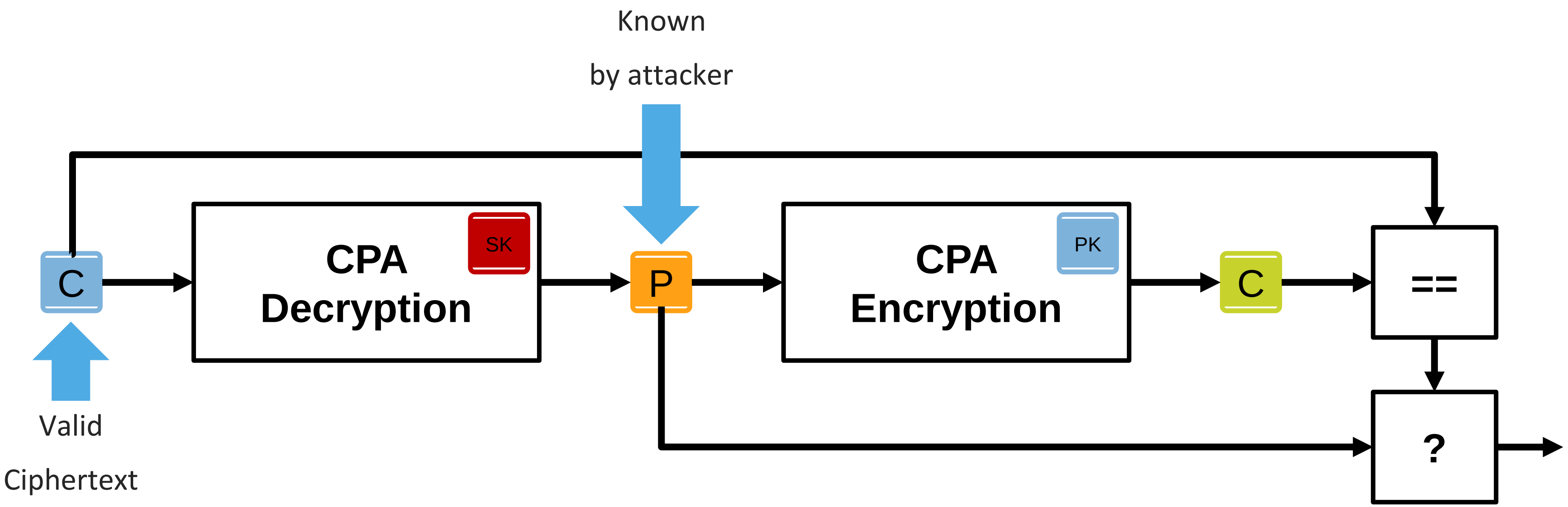
- Attacker inputs only valid ciphertexts



THE SCA PROBLEM OF THE FO-TRANSFORM

Attack 1: Chosen Plaintext

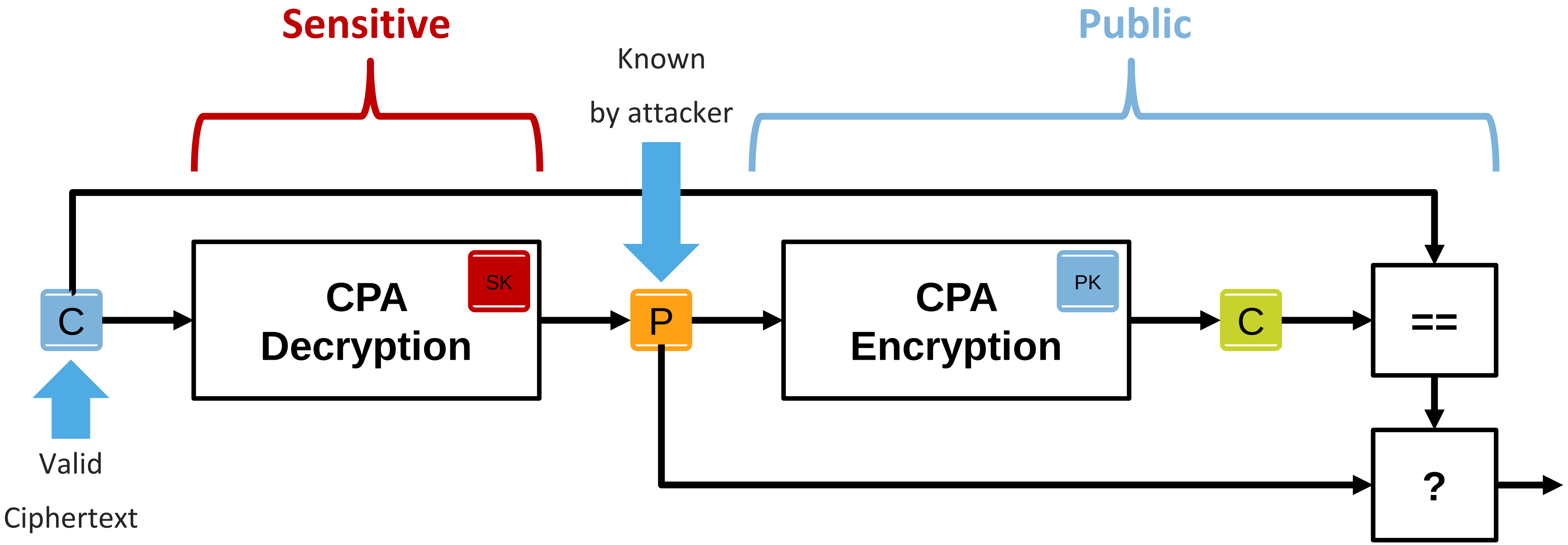
- Attacker inputs only valid ciphertexts



THE SCA PROBLEM OF THE FO-TRANSFORM

Attack 1: Chosen Plaintext

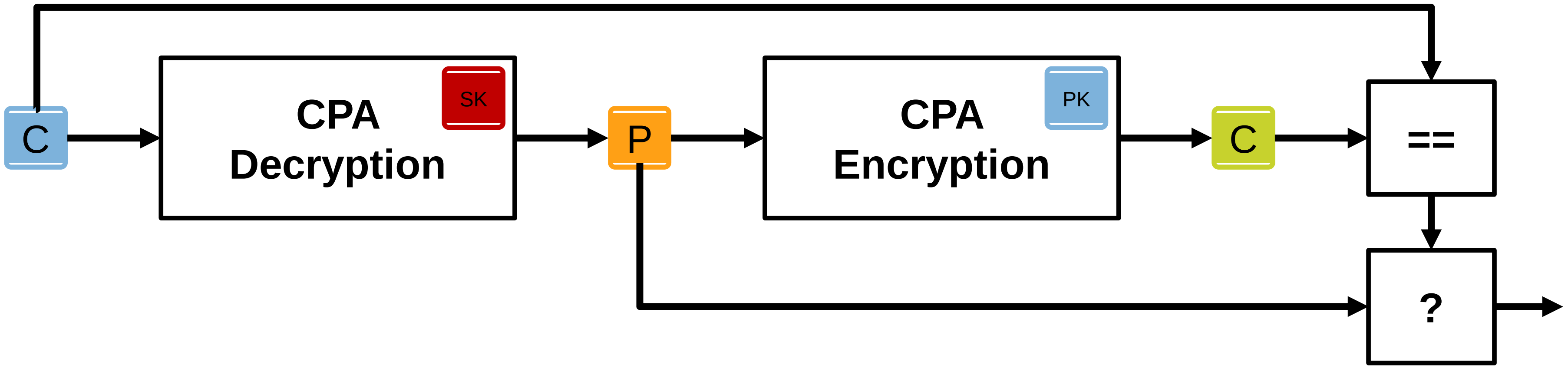
- Attacker inputs only valid ciphertexts
- Attack focuses on **CPA Decryption**, everything after (and including) P is public
- Only need to protect **CPA Decryption**



THE SCA PROBLEM OF THE FO-TRANSFORM

Attack 2: Chosen Ciphertext

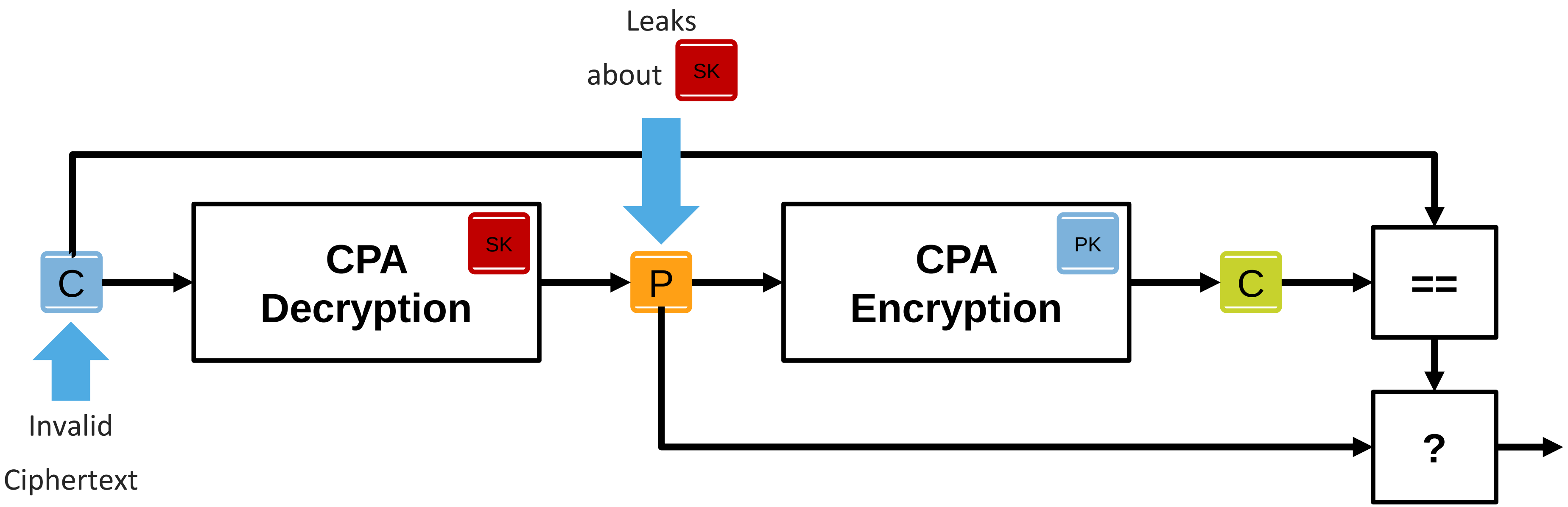
- Attacker inputs specially-crafted invalid ciphertexts



THE SCA PROBLEM OF THE FO-TRANSFORM

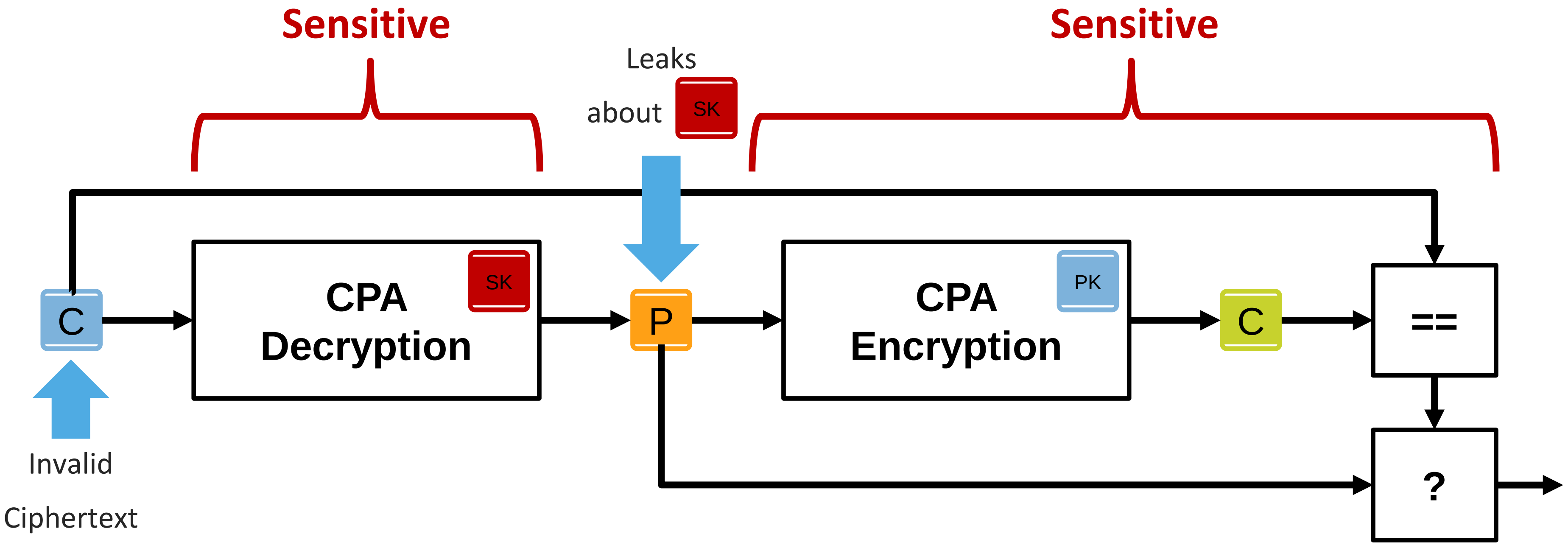
Attack 2: Chosen Ciphertext

- Attacker inputs specially-crafted invalid ciphertexts



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



THE SCA PROBLEM OF THE FO-TRANSFORM

Why is it bad?

- [x] Millions of Points of Interest (PoI)

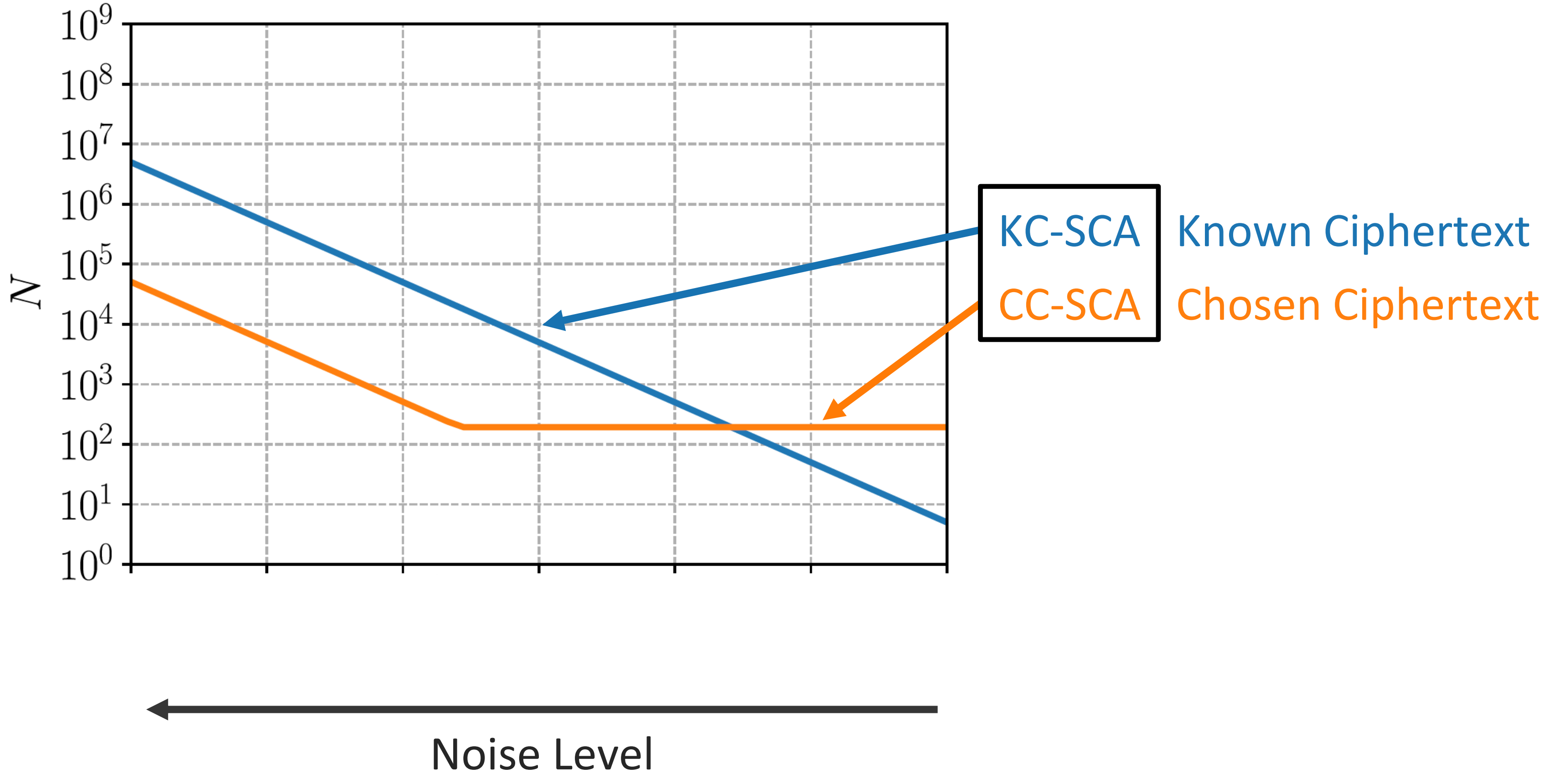
Most recently at TCHES-2022:

Masked Kyber / Saber is broken with only 15k traces.

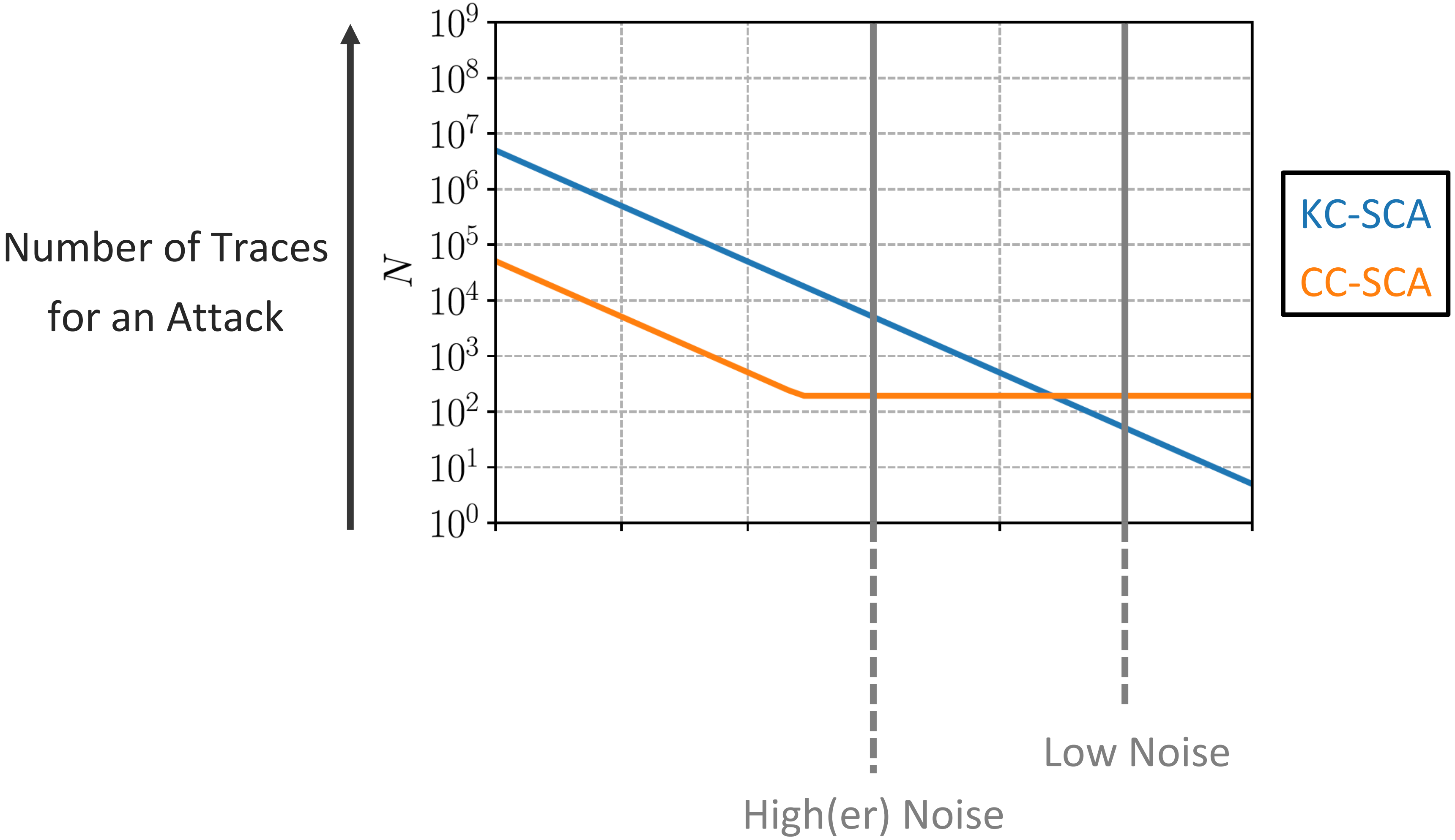
Curse of Re-encryption: A Generic Power/EM Analysis on Post-Quantum KEMs

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

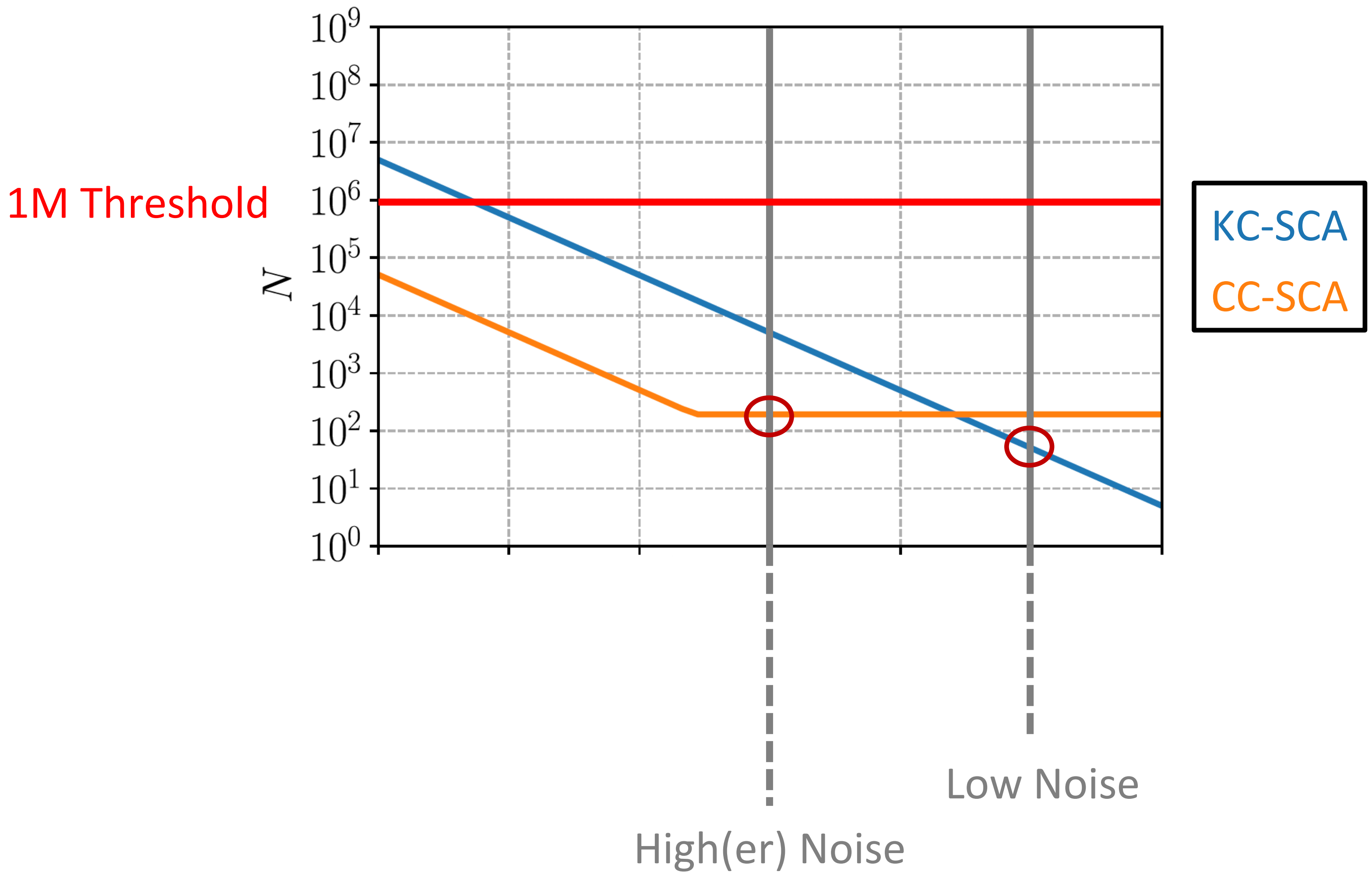
CASE STUDY: UNPROTECTED KYBER



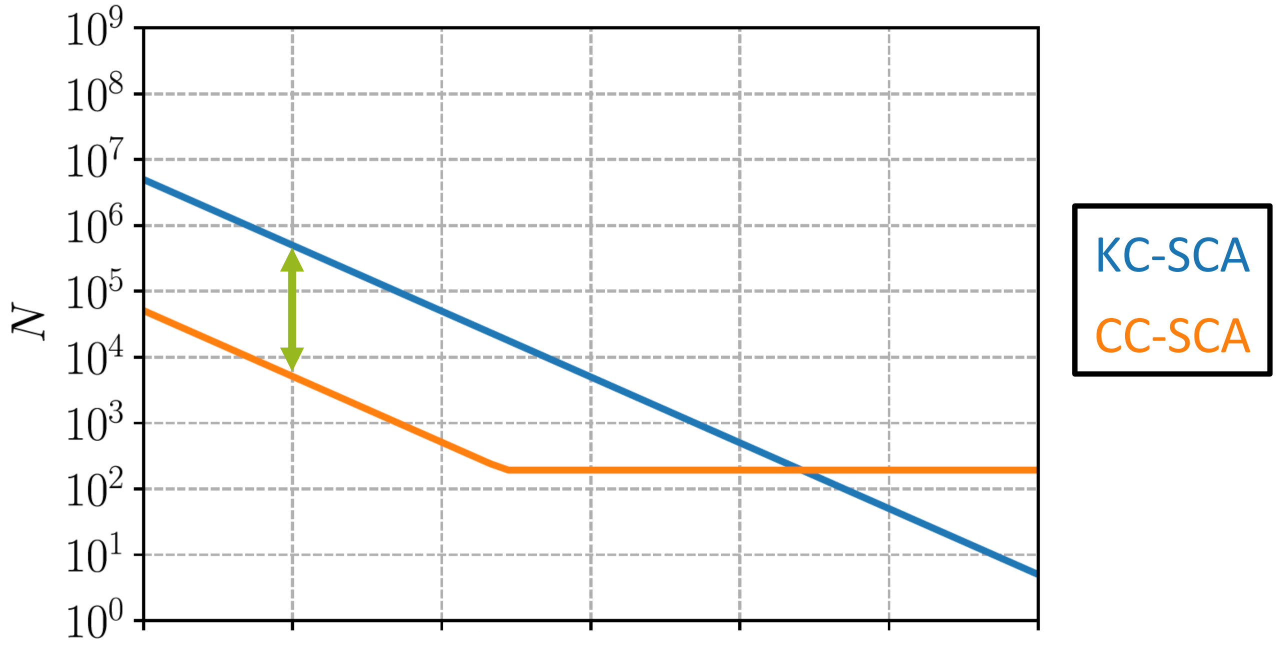
CASE STUDY: UNPROTECTED KYBER



CASE STUDY: UNPROTECTED KYBER



CASE STUDY: UNPROTECTED KYBER



- Unprotected Kyber is (unsurprisingly) not sufficient for both noise levels
- There is a gap of roughly **x100** between the attacks for high(er) noise

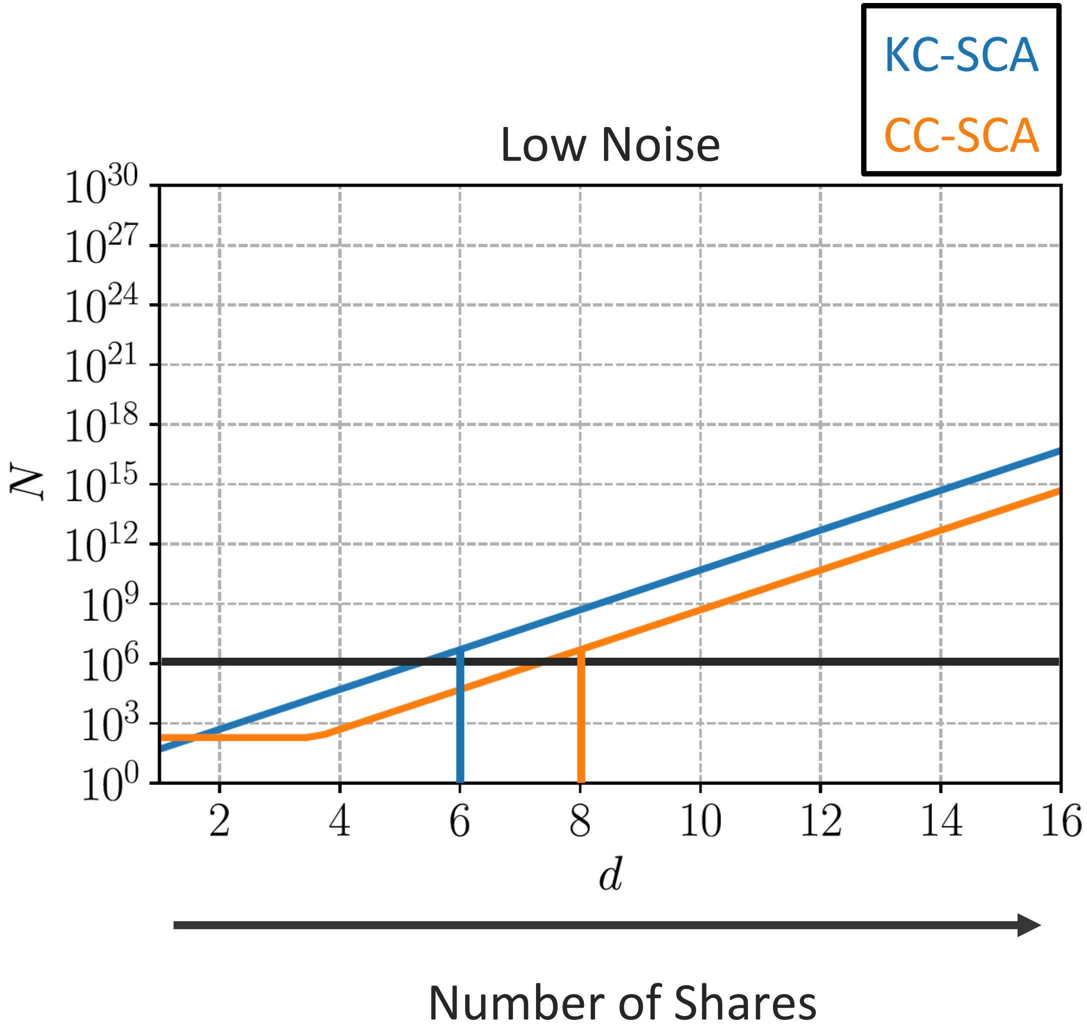
Can this be overcome through masking?

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**:

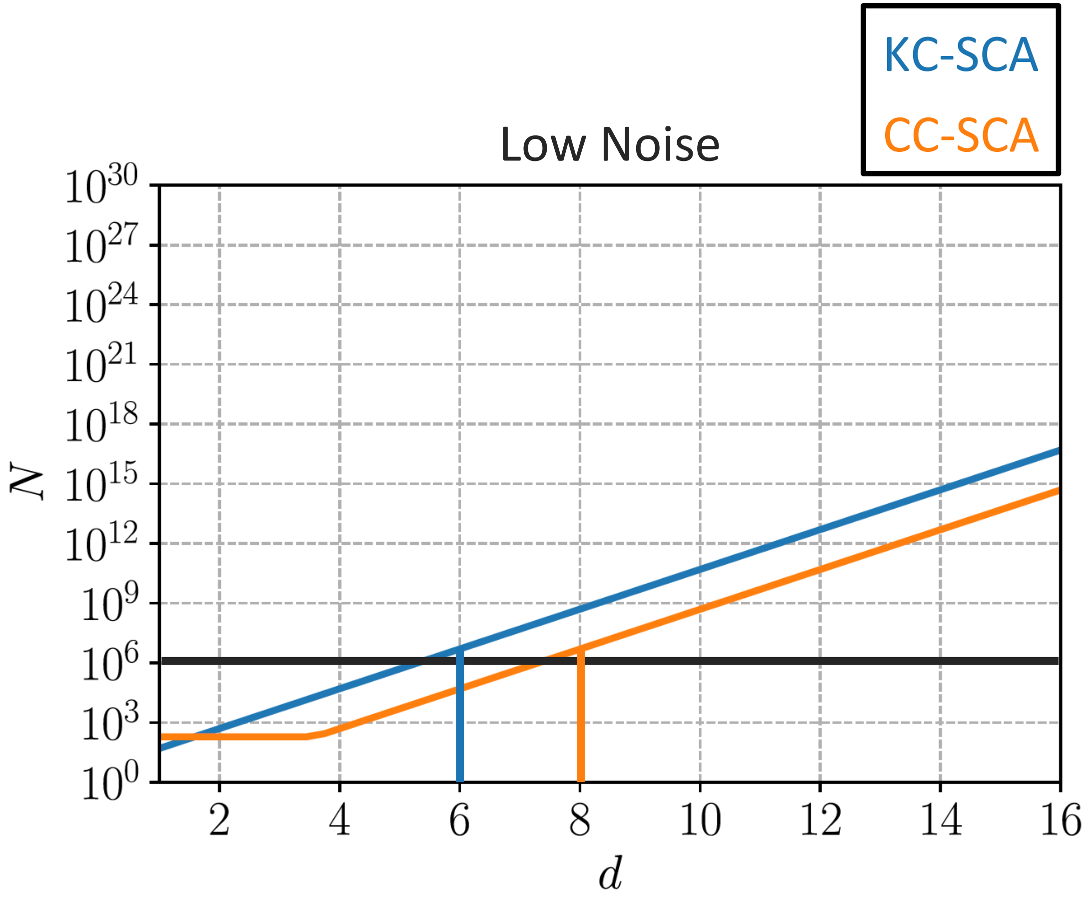
- Known ciphertext ➔ d = 6
- Chosen ciphertext ➔ d = 8

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.



Higher-Order Masking

Case Study: Higher-order masked Kyber (M4) from [BGR+21]
(with adapted A2B)

Overhead compared to unprotected (d=1):

d=2	d=3	d=4	d=5	d=6	d=7
3.5x	64x	110x	197x	293x	397x

[BGR+21] Bos et al.: Masking Kyber, TCHES-2021

SURVIVAL STRATEGIES

Higher-Order Masking

Case Study: Higher-order masked Kyber (M4) from [BGR+21]
(with adapted A2B)

Overhead compared to unprotected (d=1):

d=2	d=3	d=4	d=5	d=6	d=7
3.5x	64x	110x	197x	293x	397x

18x

High(er)

SURVIVAL STRATEGIES

Higher-Order Masking

Case Study: Higher-order masked Kyber (M4) from [BGR+21]
(with adapted A2B)

Overhead compared to unprotected (d=1):

d=2	d=3	d=4	d=5	d=6	d=7
3.5x	64x	110x	197x	293x	397x

18x

High(er)

?

N/A*

Low

* For this specific implementation + board.

Requires further stack usage optimization.

Leakage caused by the FO significantly increases deployment costs of affected KEMs

SURVIVAL STRATEGIES

Alternative Solution: Encrypt-then-Sign KEM

Replace FO check by **signature verification** for some use cases

- Uses less shares because no FO leakage
- Verification only with public values (no SCA protection)

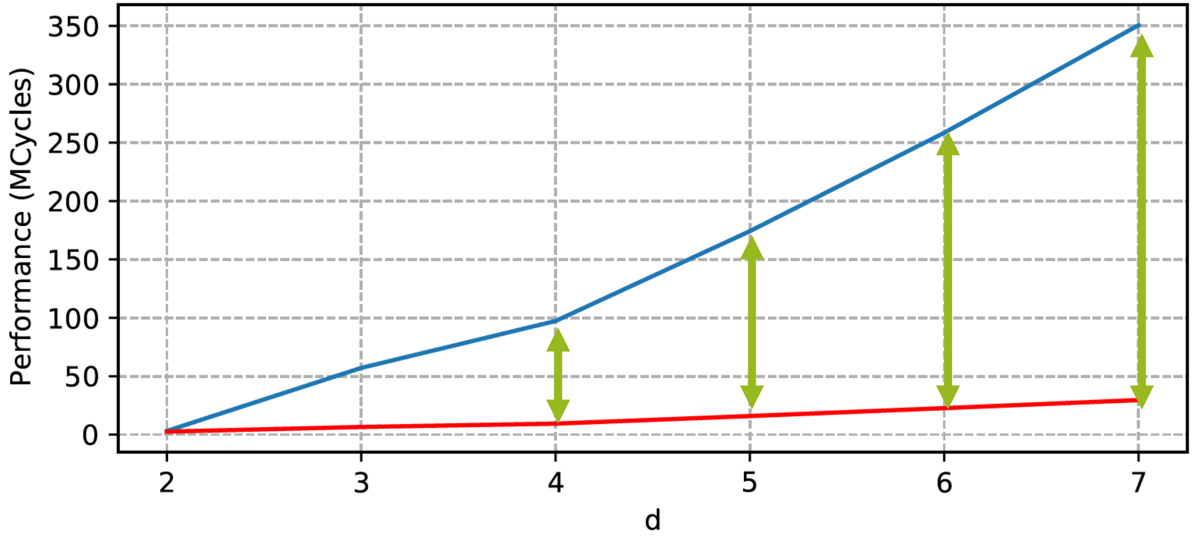
SURVIVAL STRATEGIES

Alternative Solution: Encrypt-then-Sign KEM

Replace FO check by **signature verification** for some use cases

- Uses less shares because no FO leakage
- Verification only with public values (no SCA protection)

Example: Kyber + Dilithium



Speed-Up

~**10x**

CONCLUSIONS

Irrelevant if the quantum threat is real or not
New PQC-Standard are coming!
→ Post-quantum crypto is already being requested

For embedded platforms challenges in terms of

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

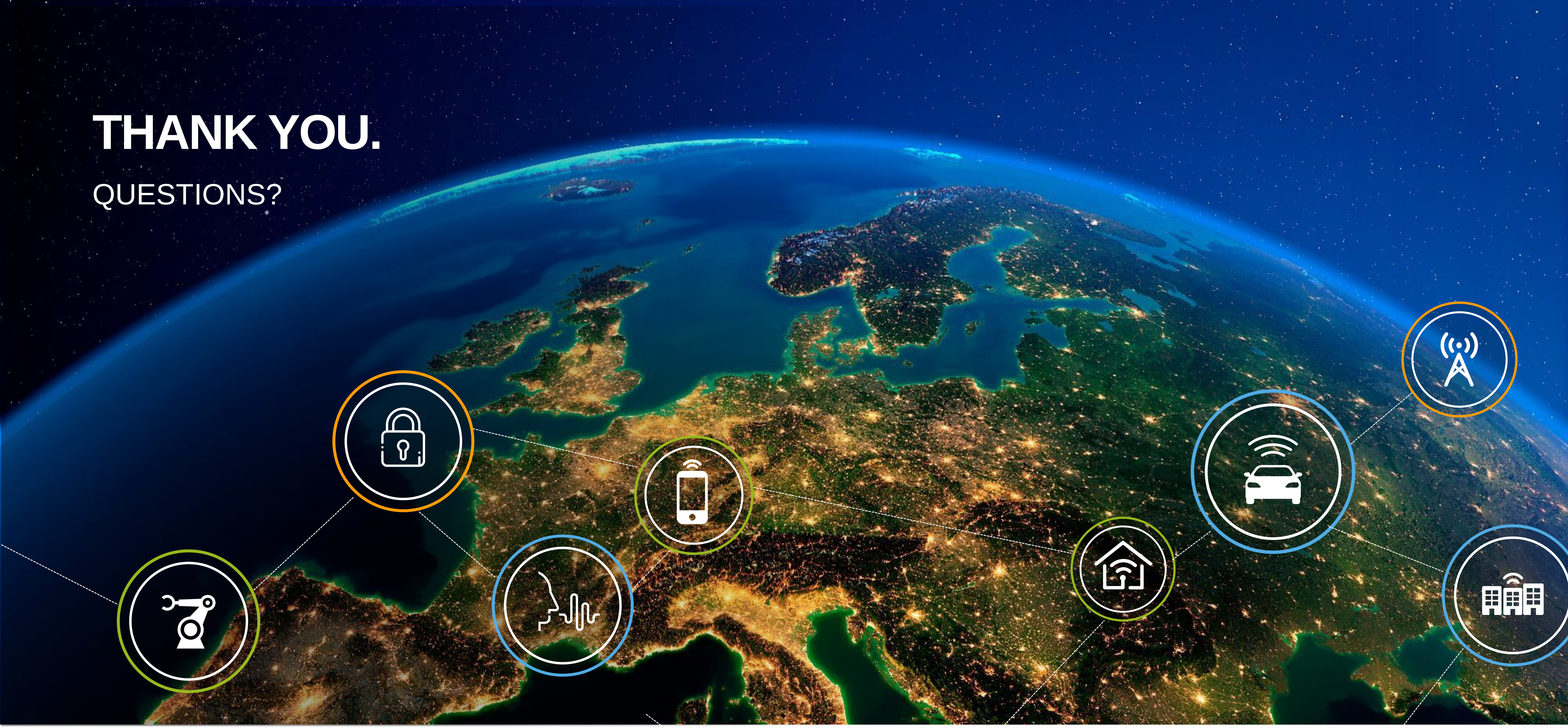
✓ **Think about migration paths now**

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

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

THANK YOU.

QUESTIONS?



SECURE CONNECTIONS
FOR A SMARTER WORLD

SECURE CONNECTIONS
FOR A SMARTER WORLD