POST-QUANTUM CRYPTO: CHALLENGES FOR EMBEDDED APPLICATIONS

Joppe Bos

APRIL 2022

SECURE CONNECTIONS FOR A SMARTER WORLD

PUBLIC

POST-QUANTUM CRYPTO FOR EMBEDDED DEVICES?

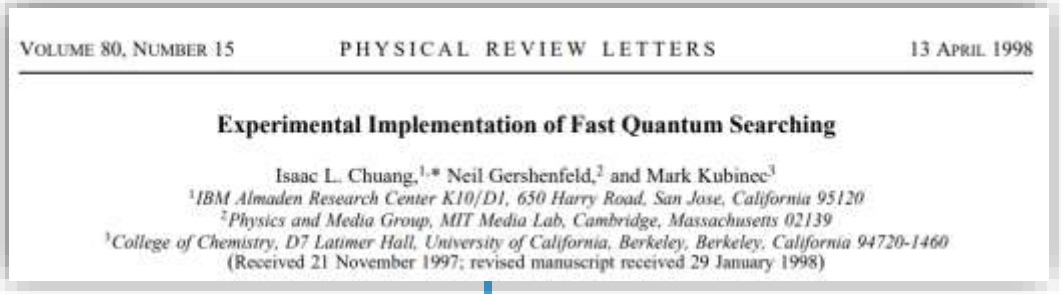
Outline

- Risk assessment: when to act?

<u>Embedded perspective</u>

- PQC performance
- High-assurance implementations

QUANTUM COMPUTERS - PROGRESS

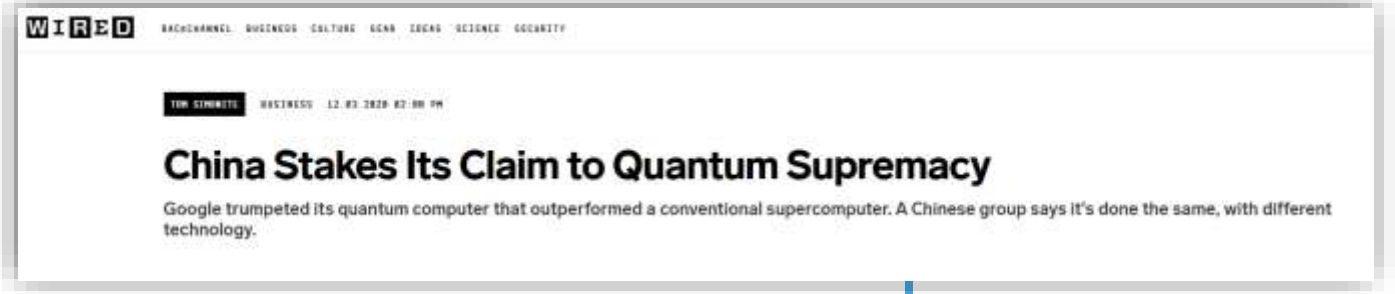


VOLUME 80, NUMBER 15 PHYSICAL REVIEW LETTERS 13 APRIL 1998

Experimental Implementation of Fast Quantum Searching

Isaac L. Chuang,[1,*] Neil Gershenfeld,[2] and Mark Kubinec[3]

[1]*IBM Almaden Research Center K10/D1, 650 Harry Road, San Jose, California 95120*
[2]*Physics and Media Group, MIT Media Lab, Cambridge, Massachusetts 02139*
[3]*College of Chemistry, D7 Latimer Hall, University of California, Berkeley, Berkeley, California 94720-1460*
(Received 21 November 1997; revised manuscript received 29 January 1998)



WIRED

TOM SIMONITE BUSINESS 12.03.2020 02:00 PM

China Stakes Its Claim to Quantum Supremacy

Google trumpeted its quantum computer that outperformed a conventional supercomputer. A Chinese group says it's done the same, with different technology.

1998:
2 qubit

2006: 1
2 qubit

2018:
72 qubit

2019:
Quantum
Supremacy
#1

2020: Quantum
Supremacy #2

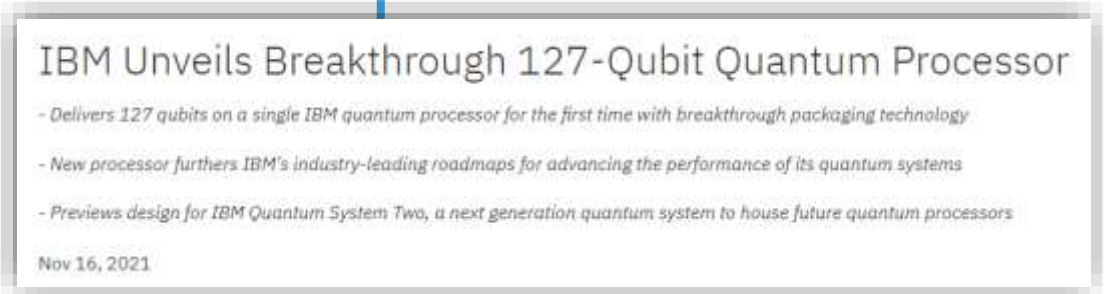
2021:
127 qubit

Google AI Blog

The latest from Google Research

Quantum Supremacy Using a Programmable Superconducting Processor

Wednesday, October 23, 2019



IBM Unveils Breakthrough 127-Qubit Quantum Processor

- *Delivers 127 qubits on a single IBM quantum processor for the first time with breakthrough packaging technology*
- *New processor furthers IBM's industry-leading roadmaps for advancing the performance of its quantum systems*
- *Previews design for IBM Quantum System Two, a next generation quantum system to house future quantum processors*

Nov 16, 2021

POST-QUANTUM CRYPTO STANDARDS ARE COMING

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

POST-QUANTUM CRYPTO STANDARDS TIMELINE

Fall 2016: Call for proposals

Nov. 2017: Deadline for submissions

Jan 2019: Round 2

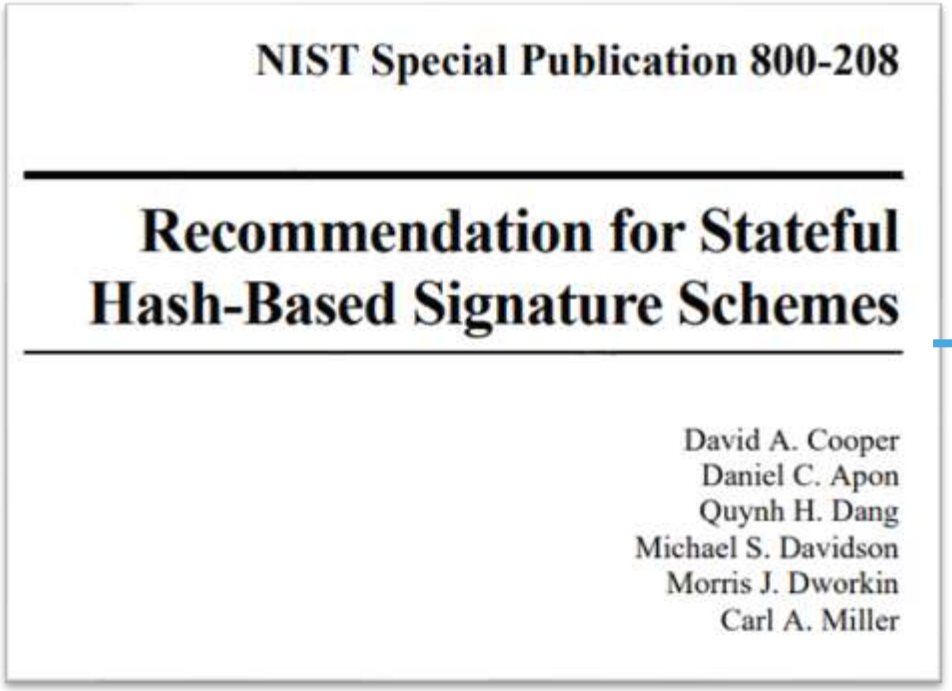
July 2020: Round 3

Oct. 2020: SP 800-208

March 2022: Winners

2024: NIST Standard is released

We are here


NIST Special Publication 800-208

Recommendation for Stateful Hash-Based Signature Schemes

David A. Cooper
Daniel C. Apon
Quynh H. Dang
Michael S. Davidson
Morris J. Dworkin
Carl A. Miller

Products need to support PQC standard

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 2021 to **12B units** in 2025

MOBILE

60B

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

COMMUNICATION INFRASTRUCTURE

40B

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

What is the impact on the billions of embedded devices?

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

TYPICAL EXAMPLES

Automotive

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

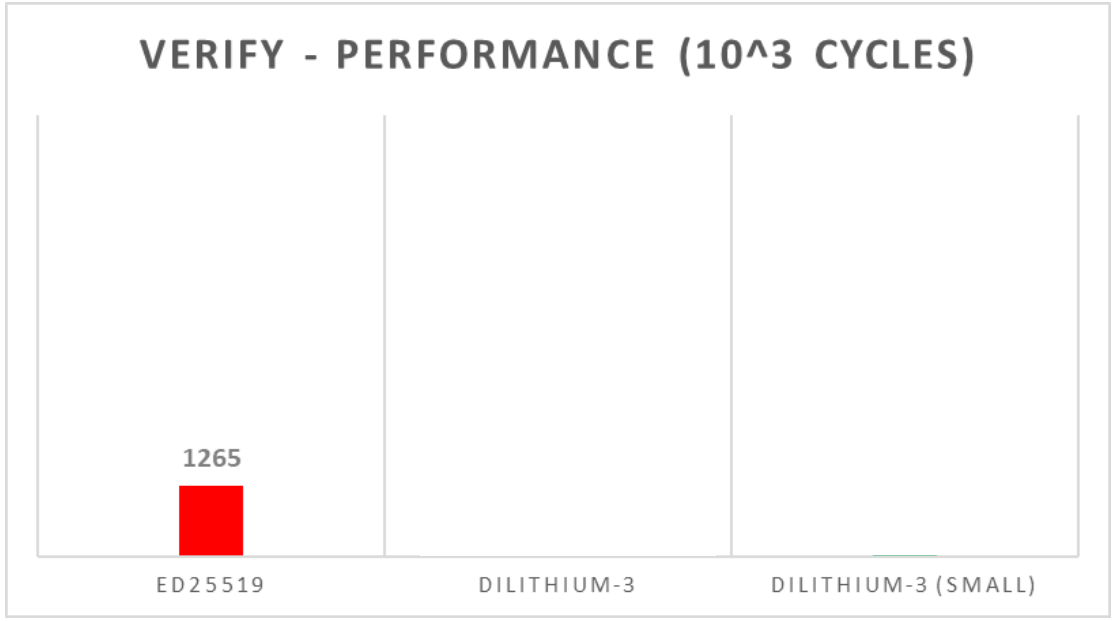
(Industrial) IoT

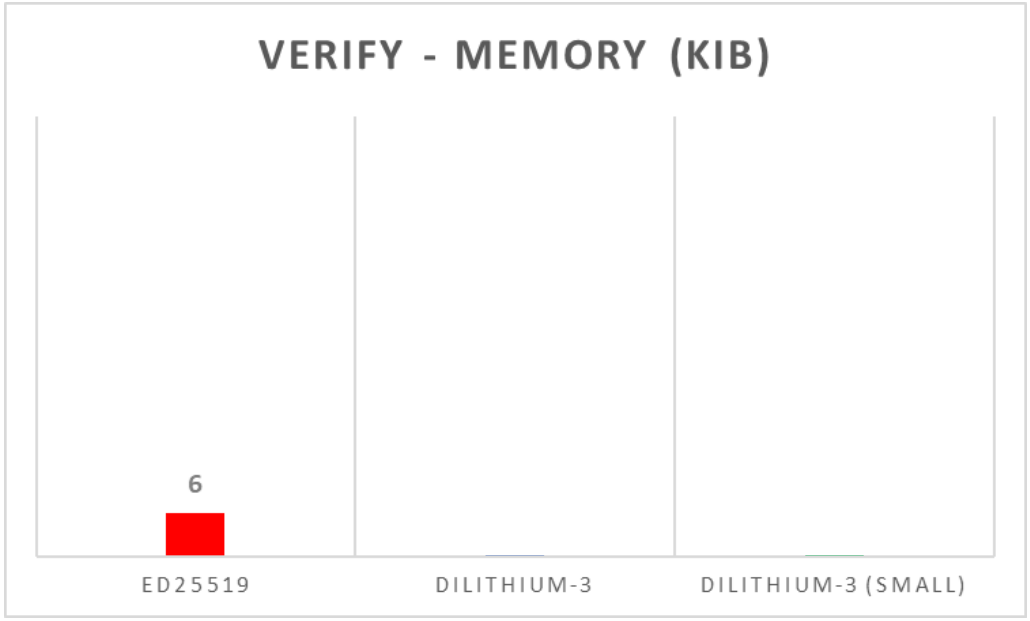
Devices sold now need to be able to support the new PQC standard in 2024: crypto agility

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

SIGNATURE VERIFICATION – ECC VERSUS PQC

Academic figures on ARM Cortex-M4





Typical crypto operation: signature verification

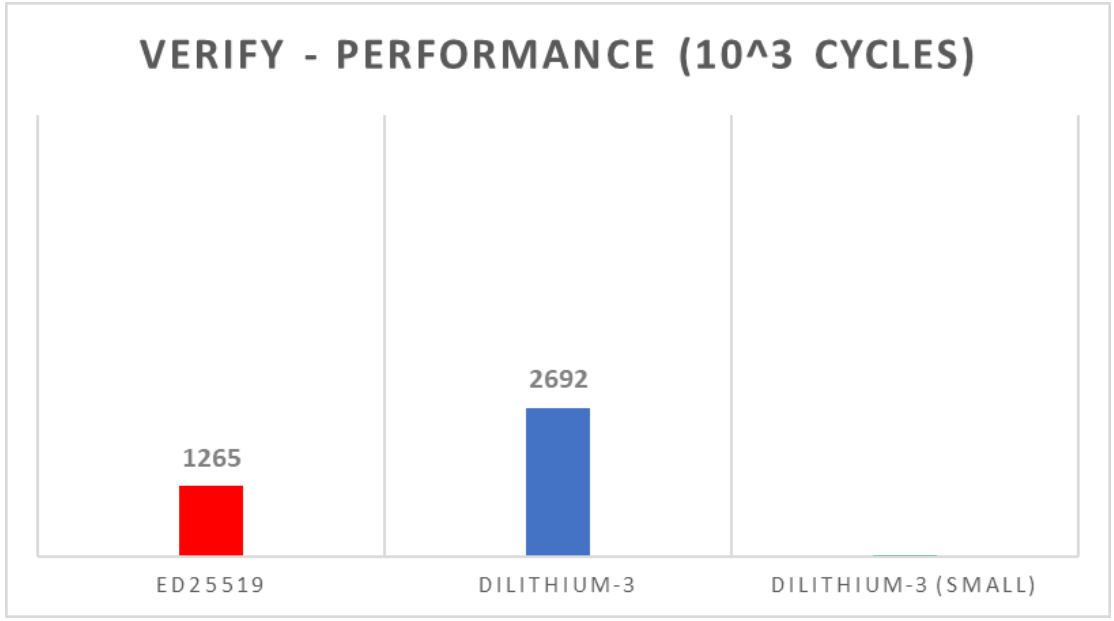
- Secure boot
- Secure (over-the-air) update

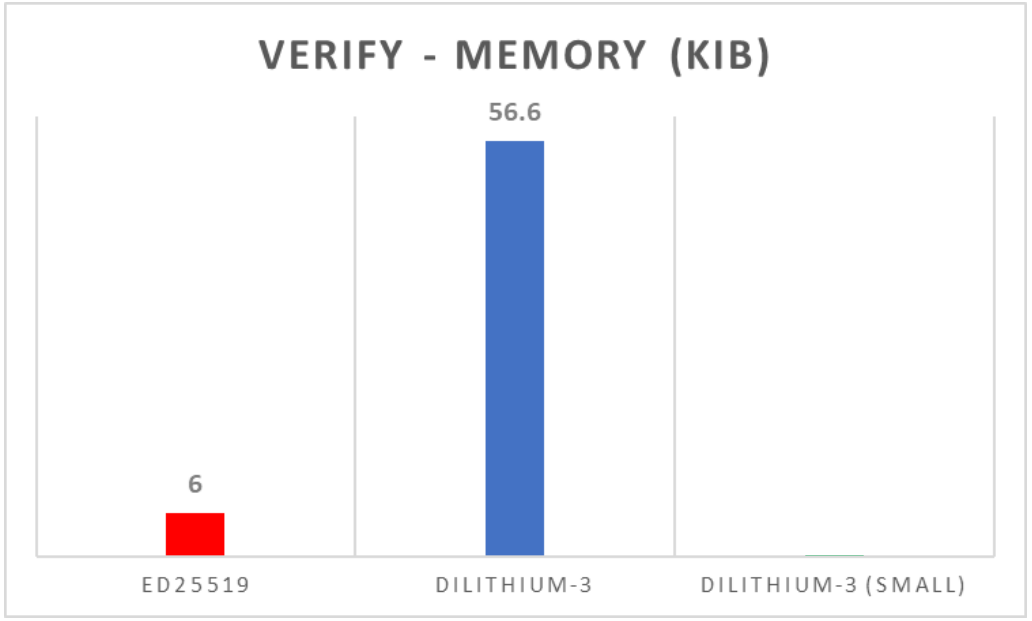
Size (bytes)	Ed25519	Dilithium-3
Private key	64	4000
Public key	32	1952
Signature	64	3293

- Ed25519 numbers from Fujii, Aranha. Curve25519 for the Cortex-M4 and beyond. In LatinCrypt 2017

SIGNATURE VERIFICATION – ECC VERSUS PQC

Academic figures on ARM Cortex-M4





Typical crypto operation: signature verification

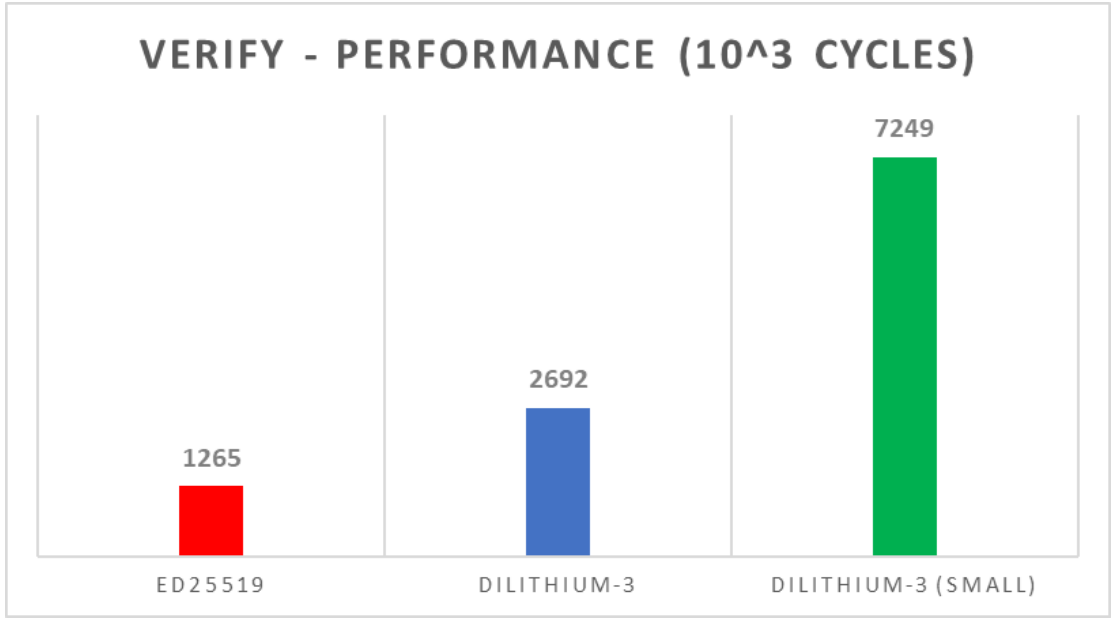
- Secure boot
- Secure (over-the-air) update

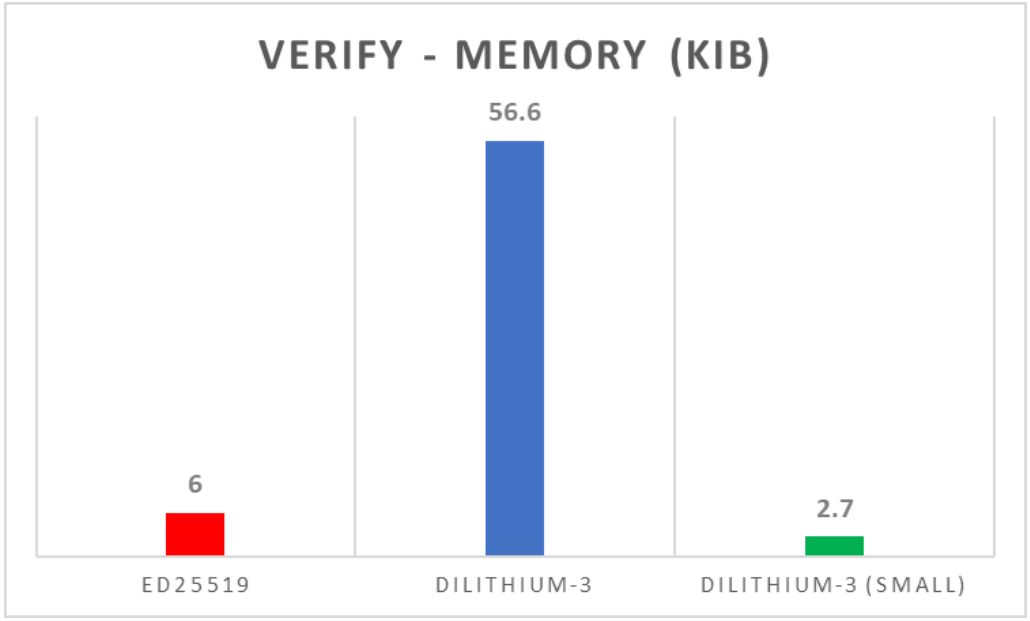
Size (bytes)	Ed25519	Dilithium-3
Private key	64	4000
Public key	32	1952
Signature	64	3293

- Ed25519 numbers from Fujii, Aranha. Curve25519 for the Cortex-M4 and beyond. In LatinCrypt 2017
- Dilithium-3 numbers from Abdulrahman, Hwang, Kannwischer, Sprenkels: Faster Kyber and Dilithium on the Cortex-M4. Cryptology ePrint Archive, Report 2022/112

SIGNATURE VERIFICATION – ECC VERSUS PQC

Academic figures on ARM Cortex-M4





Typical crypto operation: signature verification

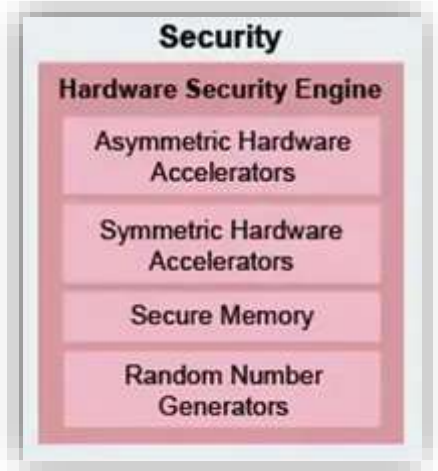
- Secure boot
- Secure (over-the-air) update

Size (bytes)	Ed25519	Dilithium-3
Private key	64	4000
Public key	32	1952
Signature	64	3293

- Ed25519 numbers from Fujii, Aranha. Curve25519 for the Cortex-M4 and beyond. In LatinCrypt 2017
- Dilithium-3 numbers from Abdulrahman, Hwang, Kannwischer, Sprenkels: Faster Kyber and Dilithium on the Cortex-M4. Cryptology ePrint Archive, Report 2022/112
- **Bos**, Renes, Sprenkels: Dilithium for Memory Constrained Devices. Cryptology ePrint Archive, Report 2022/323

IMPLEMENTING CLASSICAL CRYPTOGRAPHY

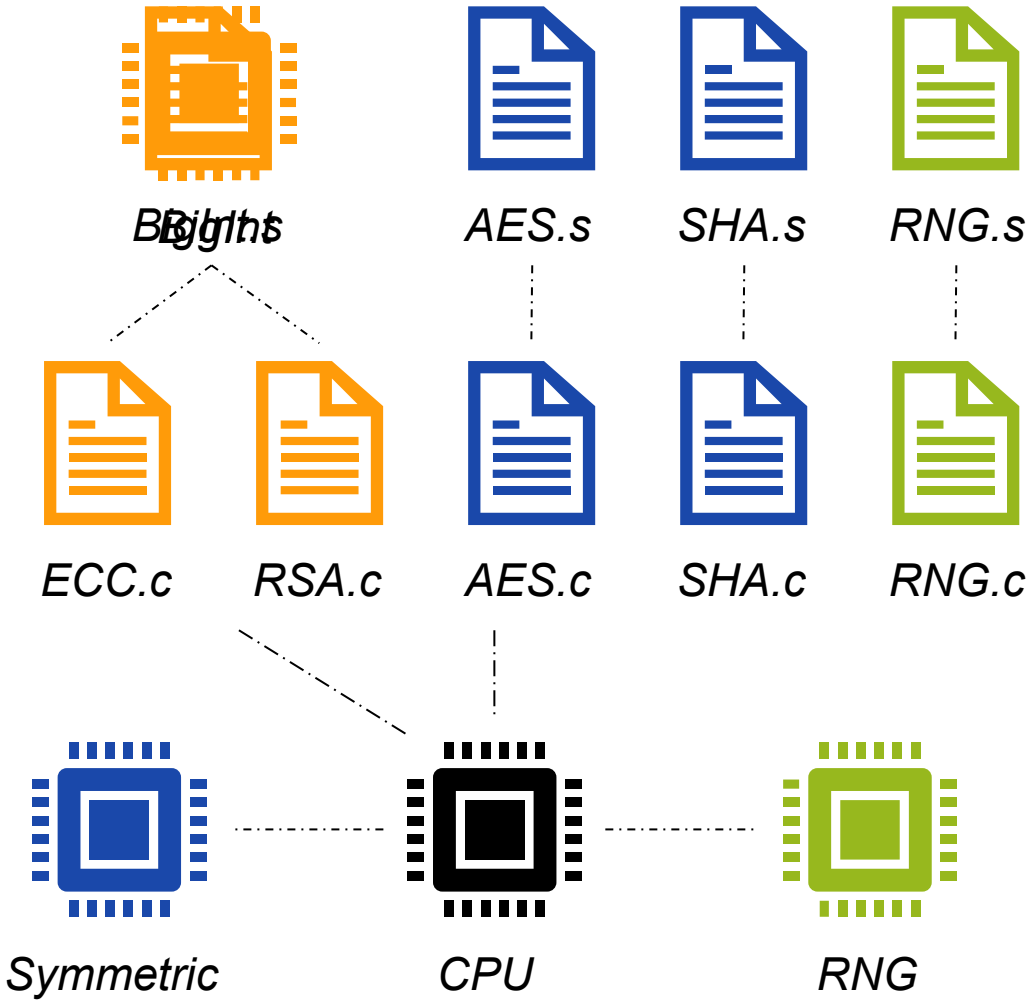
NIST
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER
PUBLICATIONS
FIPS 186-5 (Draft)
Digital Signature Standard (DSS)



S32G2 automotive processor spec

Internet Engineering Task Force (IETF) — K. Moriarty, Ed.
Request for Comments: 8017 — EMC Corporation
Obsoletes: 3447 — B. Kaliski
Category: Informational — Verisign
ISSN: 2070-1721 — J. Jonsson
Subset AB
A. Rusch
RSA
November 2016

PKCS #1: RSA Cryptography Specifications Version 2.2



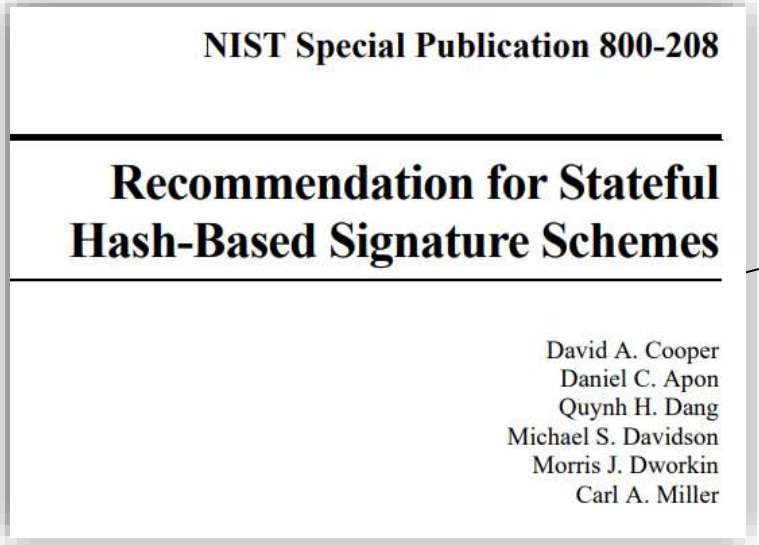
1. https://www.nxp.com/products/processors-and-microcontrollers/arm-processors/s32g-vehicle-network-processors:S32G-PROCESSORS

IMPLEMENTING POST-QUANTUM CRYPTOGRAPHY

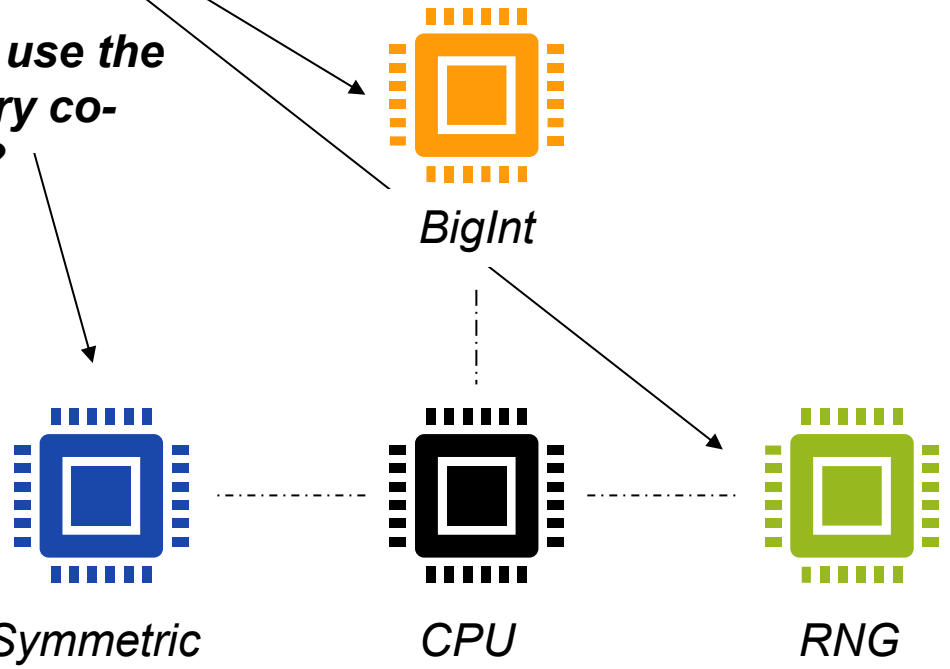
- For the lattice KEMs, the main decision will be **Kyber/NTRU/Saber**
- Similarly for lattice signatures, the main decision will be **Dilithium/Falcon**

-- Dustin Moody (NIST R3 Status Update)

How can we use the contemporary co-processors?



XMSS
LMS



REUSING EXISTING COPROCESSORS

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

Lattice cryptography uses 16-bit coefficients, how to use our bignum coprocessors?

Proposal from [A] for 128-bit coprocessors

Pack multiple 16-bit coefficients in large 128-bit register

Ensure sufficient “space” is reserved to avoid overflow

[A] Albrecht, Hanser, Hoeller, Pöppelmann, Virdia, Wallner: Implementing RLWE-based schemes using an RSA co-processor. TCHES 2019

KRONECKER SUBSTITUTION: POLYNOMIAL MULTIPLICATION WITH INTEGER MULTIPLIERS

Polynomial domain

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

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

$$\times$$

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

Grundzüge einer arithmetischen Theorie der algebraischen Grössen.

(Von *L. Kronecker.*)

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

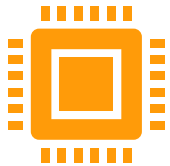
Kronecker domain (with evaluation point 100)

$$f(100) = 4030201$$

$$g(100) = 8070605$$

$$\times$$

$$fg(100) = 32526160341605$$



REUSING EXISTING COPROCESSORS

Lattice	**Polynomial multiplication**	$(\mathbb{Z}/q\mathbb{Z})[X]/(X^n+1)$	q **is 16-bit** n **is 256**

Can we do better?

- Exploit ring properties: Combine Schönhage-Strassen with Kronecker
- Use the roots of unity modulo $X^n + 1$ to construct fast **symbolic** NTTs (as in Nussbaumer)

*Harvey. Faster polynomial multiplication via multipoint Kronecker substitution. J. Sym. Comp. 2009.
New: **Bos**, Renes and Vredendaal: Polynomial Multiplication with Contemporary Co-Processors: Beyond Kronecker, Schönhage-Strassen & Nussbaumer. USENIX Security Symposium, 2022.

Kronecker	1 x 8192-bit multiplication	4096 x 128-bit multiplications
Harvey*	2 x 4096-bit multiplication	2048 x 128-bit multiplications
Harvey* / New	4 x 2048-bit multiplication	1024 x 128-bit multiplications
New	8 x 1024-bit multiplication	512 x 128-bit multiplications
New	16 x 512-bit multiplication	256 x 128-bit multiplications

RUNNING PQC ON EMBEDDED DEVICES

Key sizes

- Many current embedded devices struggle with RSA-3072 keys
  → PQC is order of magnitude larger

Performance

- Not always as bad as people think.
  → Dilithium verification (secure boot, update) “only” 1x – 3x slower
- Notable disadvantages: variable signing time in Dilithium: probability run-time twice as slow than average is 14 percent
- Possibility to re-use existing hardware to accelerate lattice-based crypto

Memory usage

- Many schemes use a lot of stack by default (50 – 100 KiB).
  → Dedicated techniques needed

RUNNING PQC ON EMBEDDED DEVICES

Key sizes

- Many current embedded devices struggle with RSA-3072 keys
  → PQC is order of magnitude larger

Performance

- Not always as bad as people think.
  → Dilithium verification (secure boot, update) “only” 1x – 3x slower
- Notable disadvantages: variable signing time in Dilithium: probability run-time twice as slow than average is 14 percent
- Possibility to re-use existing hardware to accelerate lattice-based crypto

Memory usage

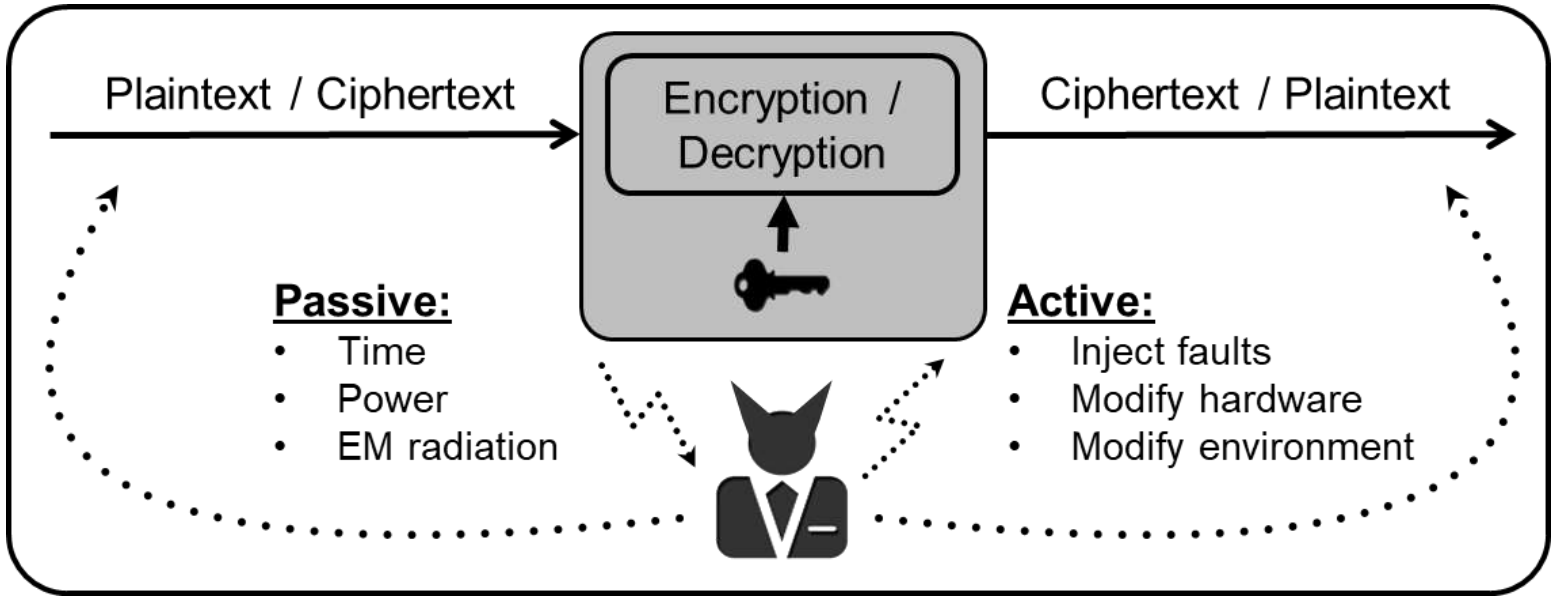
- Many schemes use a lot of stack by default (50 – 100 KiB).
  → Dedicated techniques needed

What about high security implementation?

FO-CALYPSE

SECURE CONNECTIONS
FOR A SMARTER WORLD

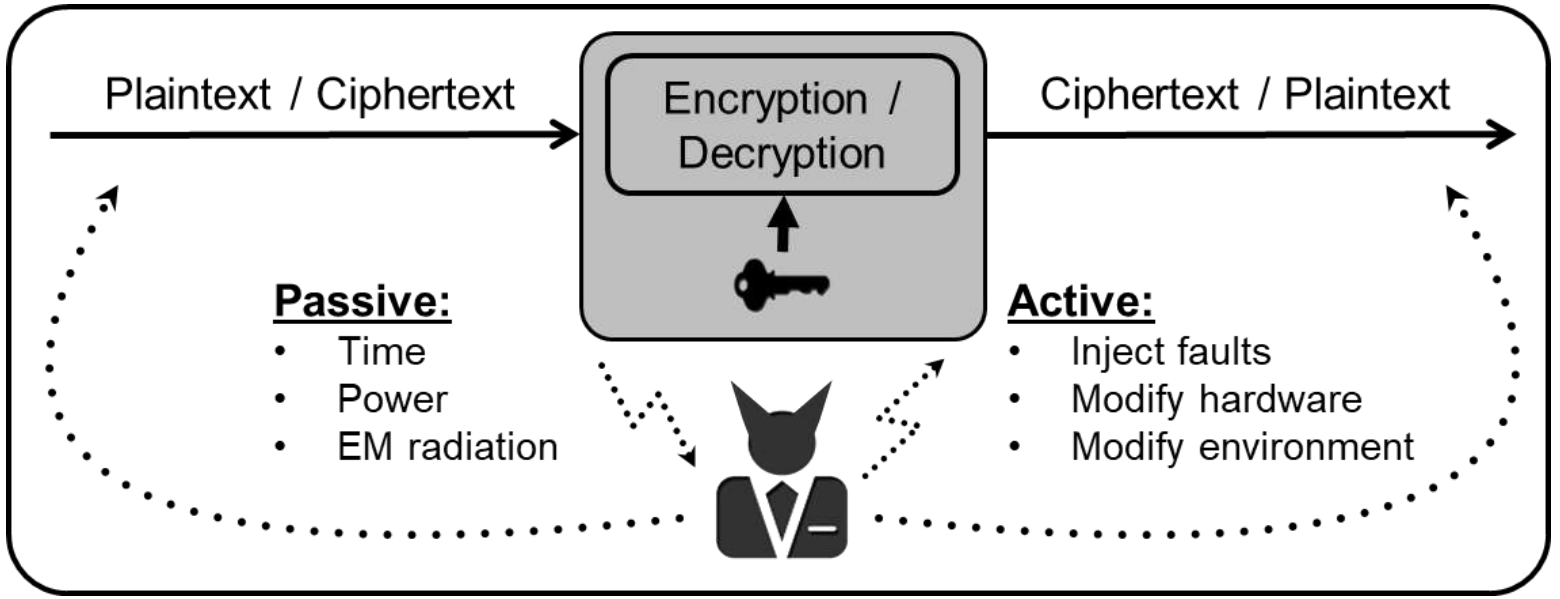
High-assurance implementations



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

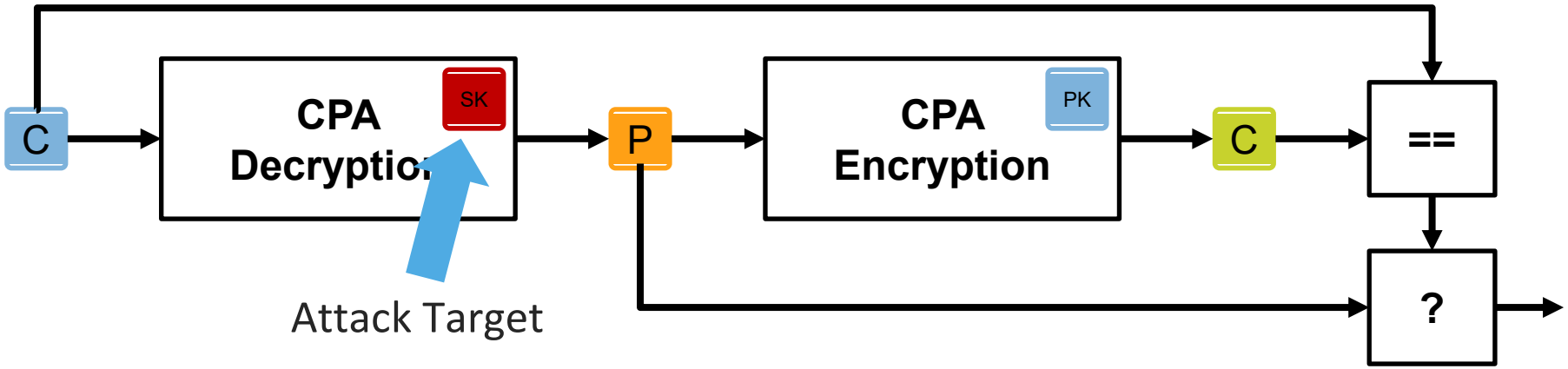
What about Post-Quantum Cryptography?

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	

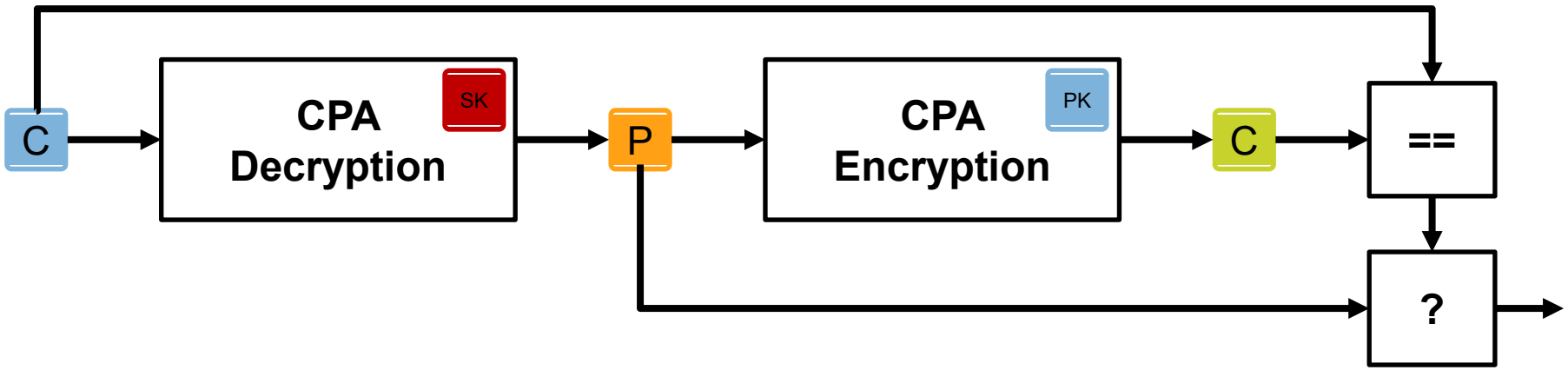
Exemplary Decapsulation:



THE SCA PROBLEM OF THE FO-TRANSFORM

Attack 1: Chosen Plaintext

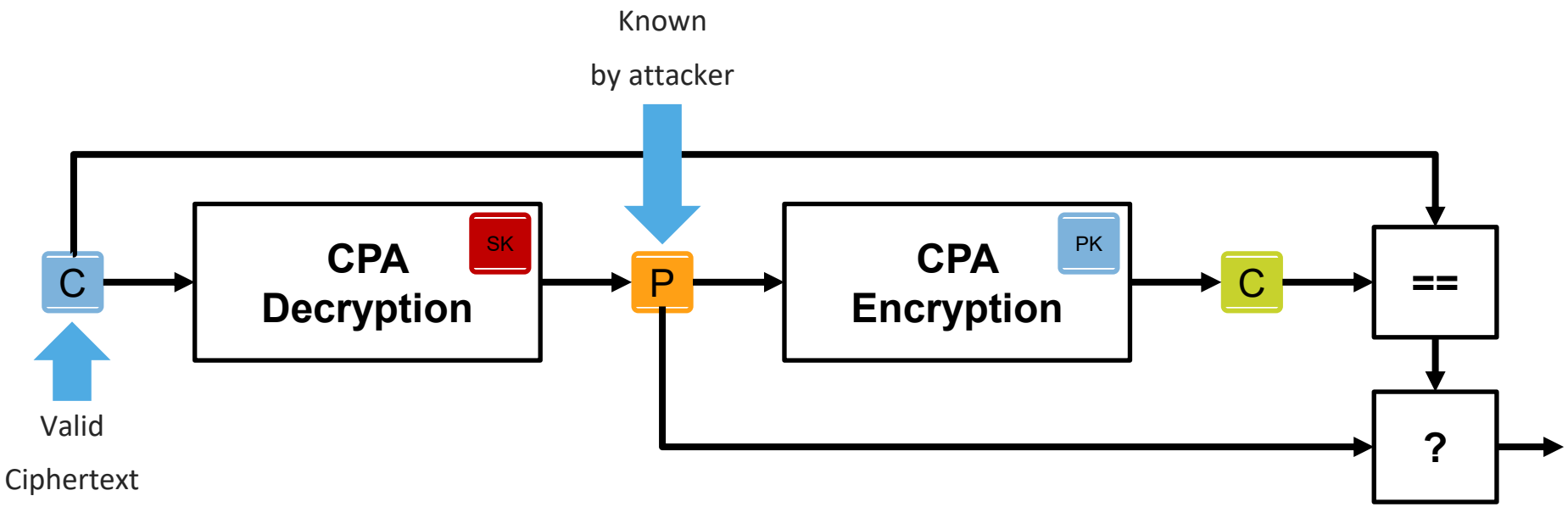
- Attacker inputs only valid ciphertexts



THE SCA PROBLEM OF THE FO-TRANSFORM

Attack 1: Chosen Plaintext

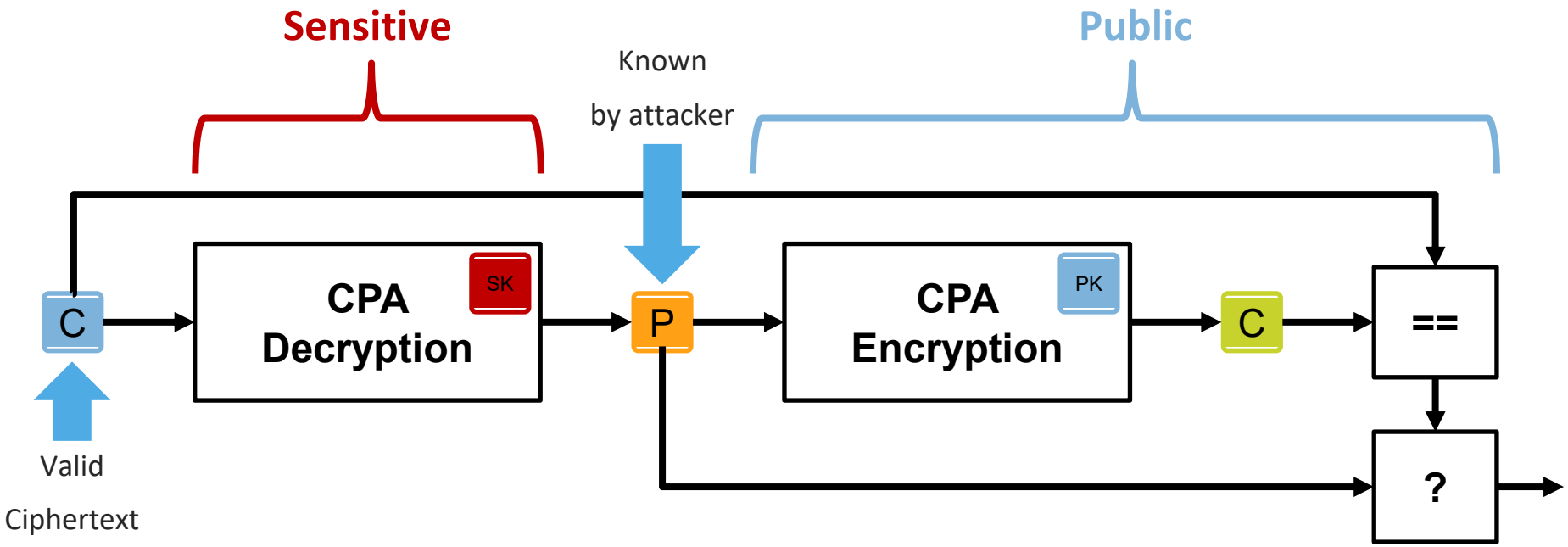
- Attacker inputs only valid ciphertexts



THE SCA PROBLEM OF THE FO-TRANSFORM

Attack 1: Chosen Plaintext

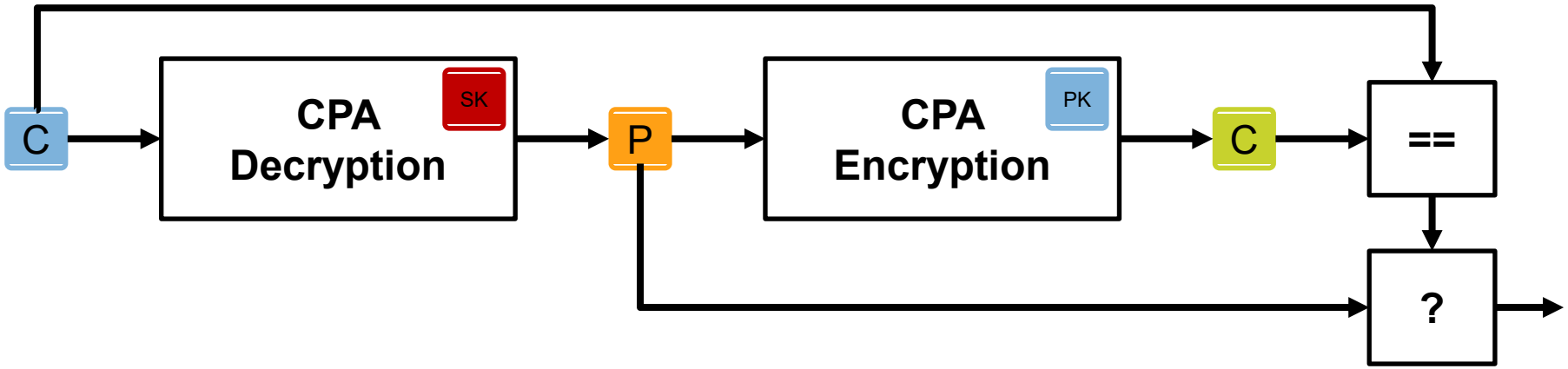
- Attacker inputs only valid ciphertexts
- Attack focuses on **CPA Decryption**, everything after (and including) P is public
- Only need to protect **CPA Decryption**



THE SCA PROBLEM OF THE FO-TRANSFORM

Attack 2: Chosen Ciphertext

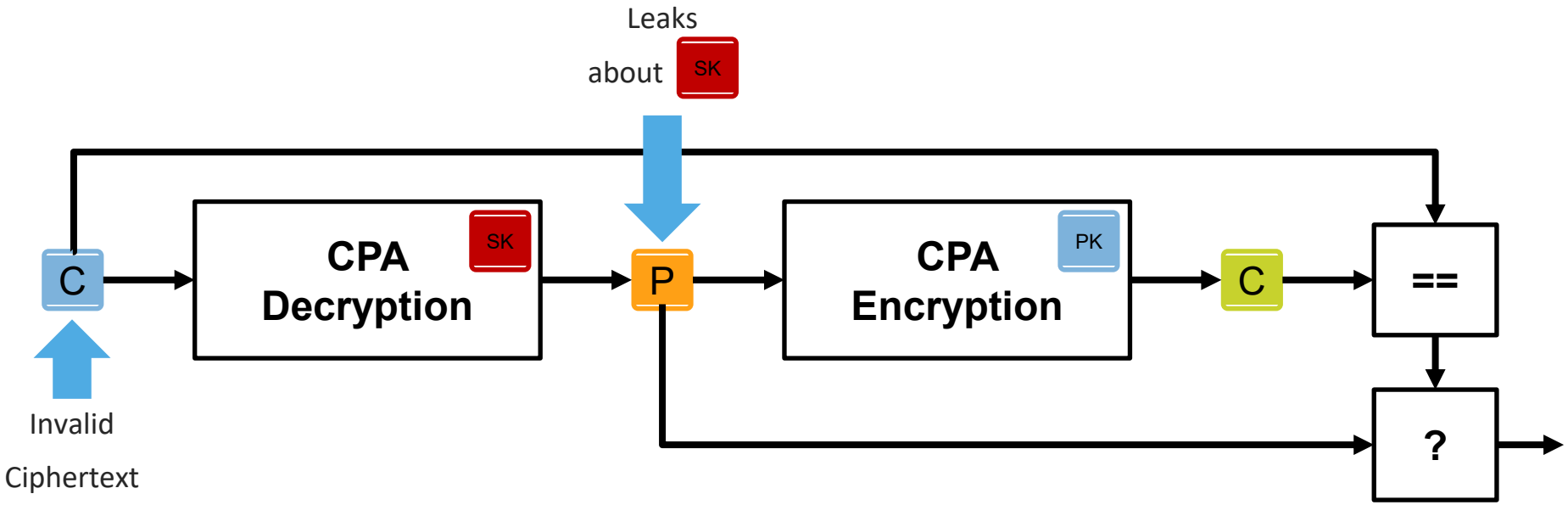
- Attacker inputs specially-crafted invalid ciphertexts



THE SCA PROBLEM OF THE FO-TRANSFORM

Attack 2: Chosen Ciphertext

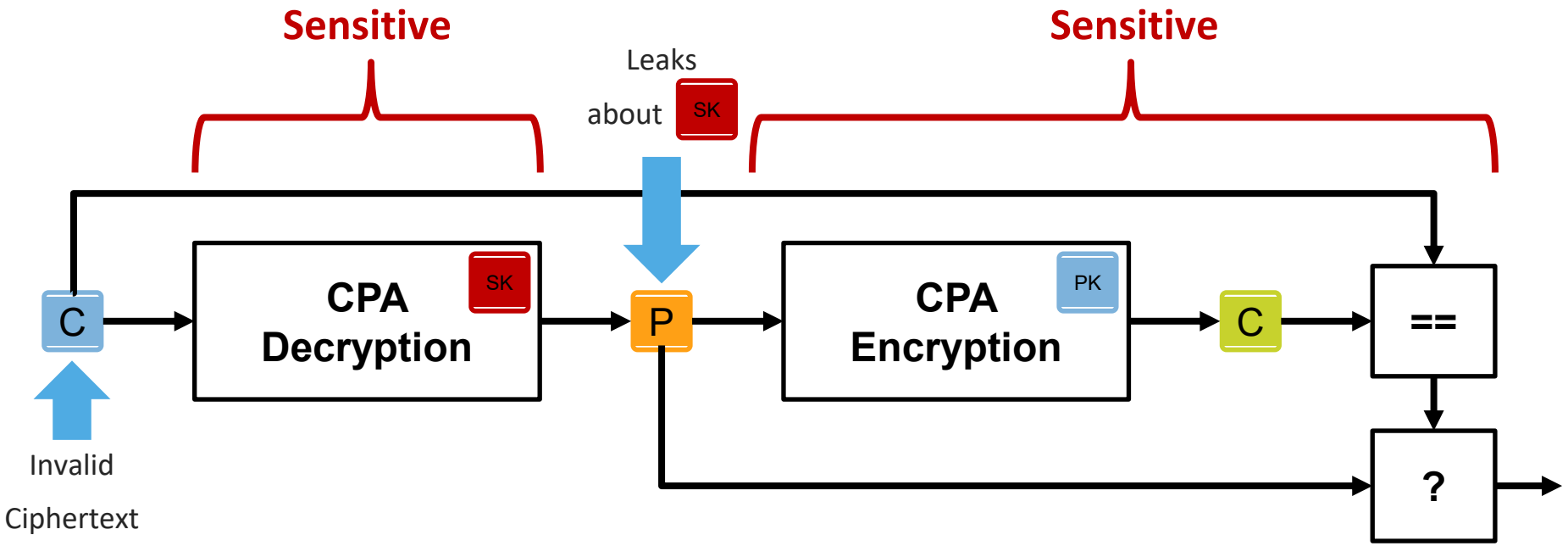
- Attacker inputs specially-crafted invalid ciphertexts



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



THE SCA PROBLEM OF THE FO-TRANSFORM

Why is it bad?

☑ Millions of Points of Interest (PoI)

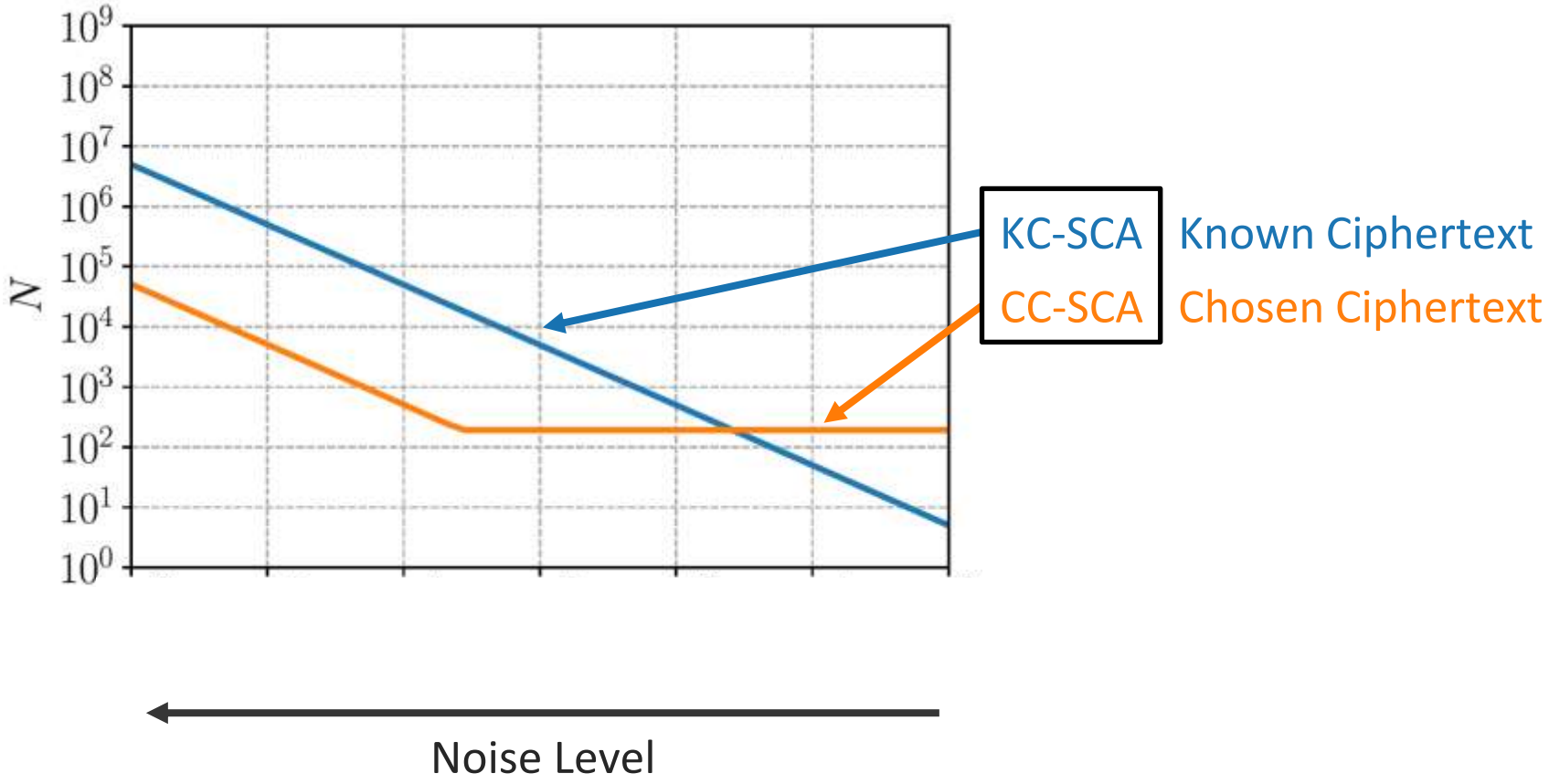
Most recently at TCHES-2022:

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

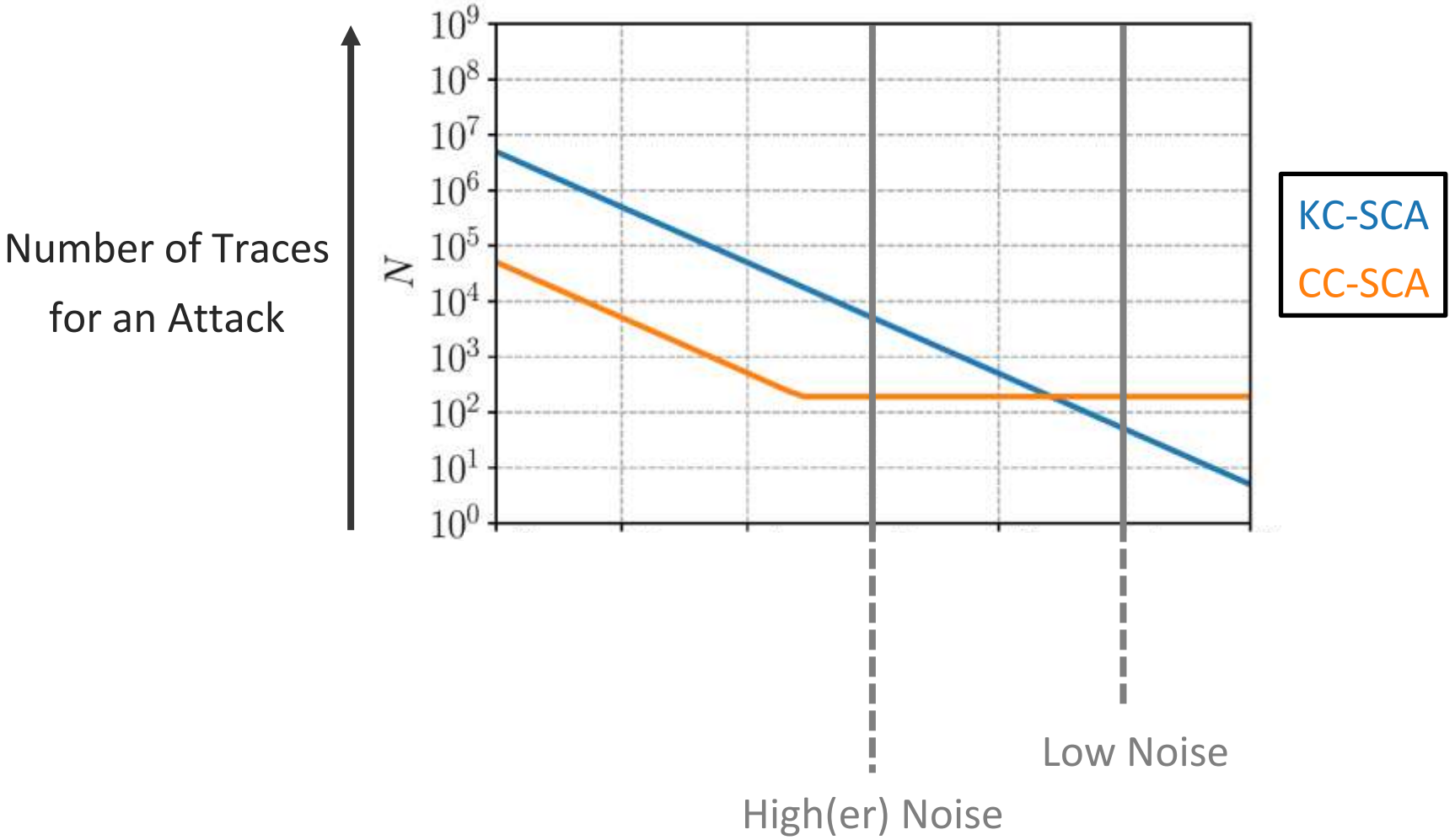
Curse of Re-encryption: A Generic Power/EM Analysis on Post-Quantum KEMs

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

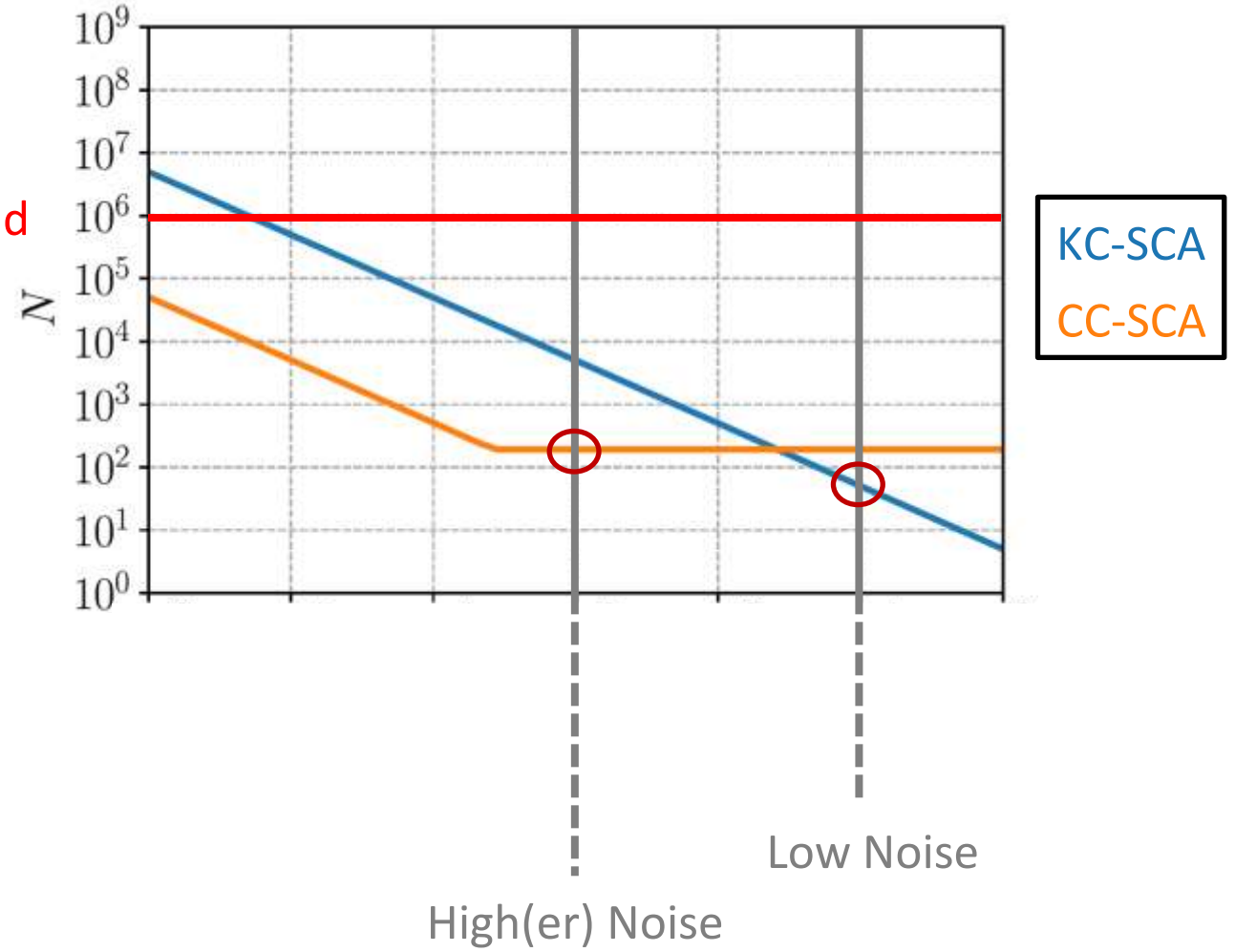
CASE STUDY: UNPROTECTED KYBER



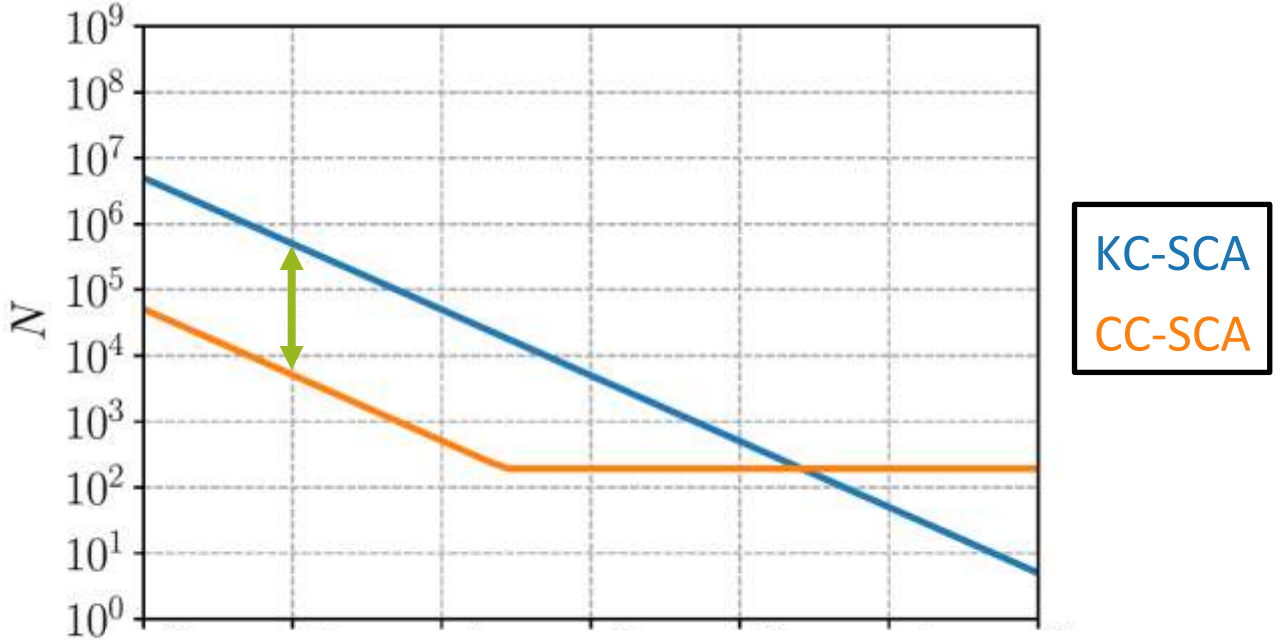
CASE STUDY: UNPROTECTED KYBER



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

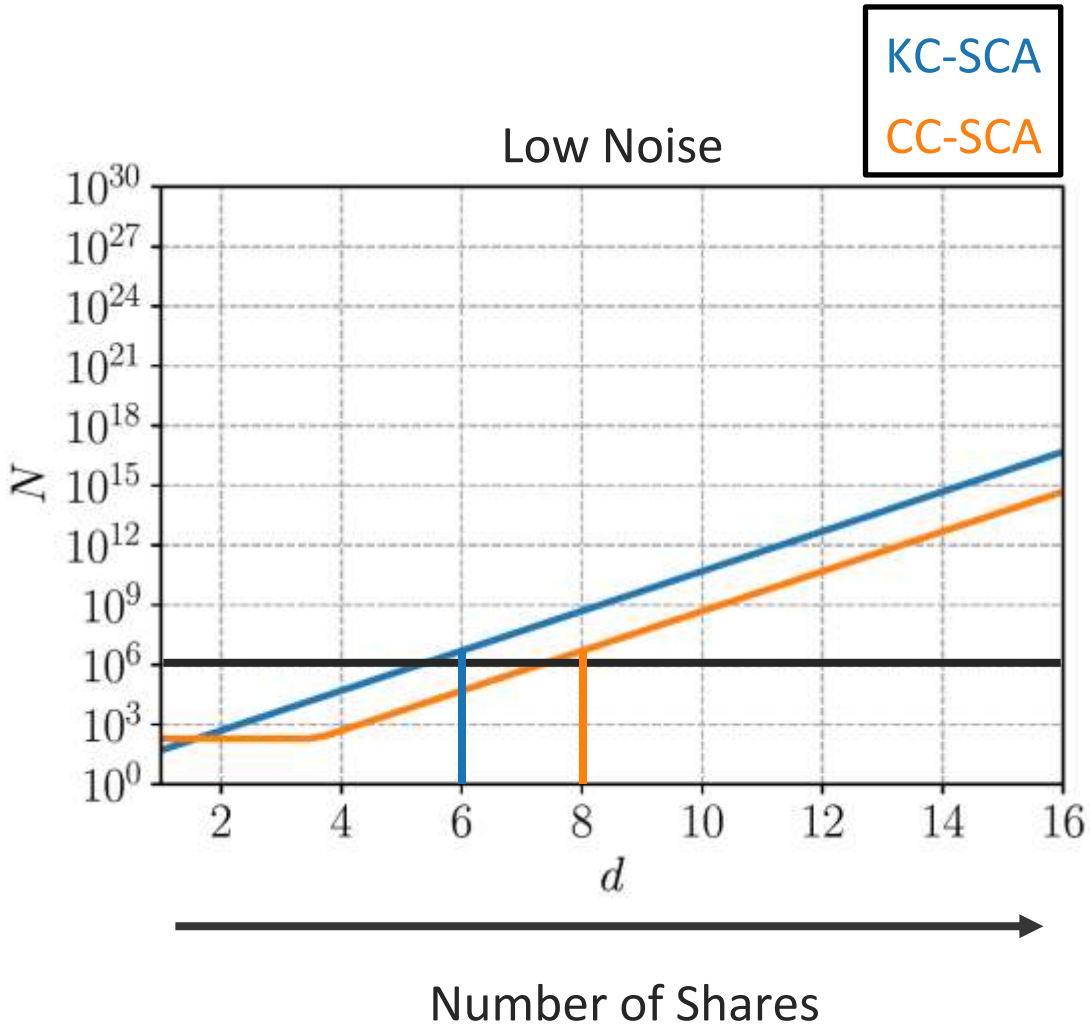
Can this be overcome through masking?

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**:

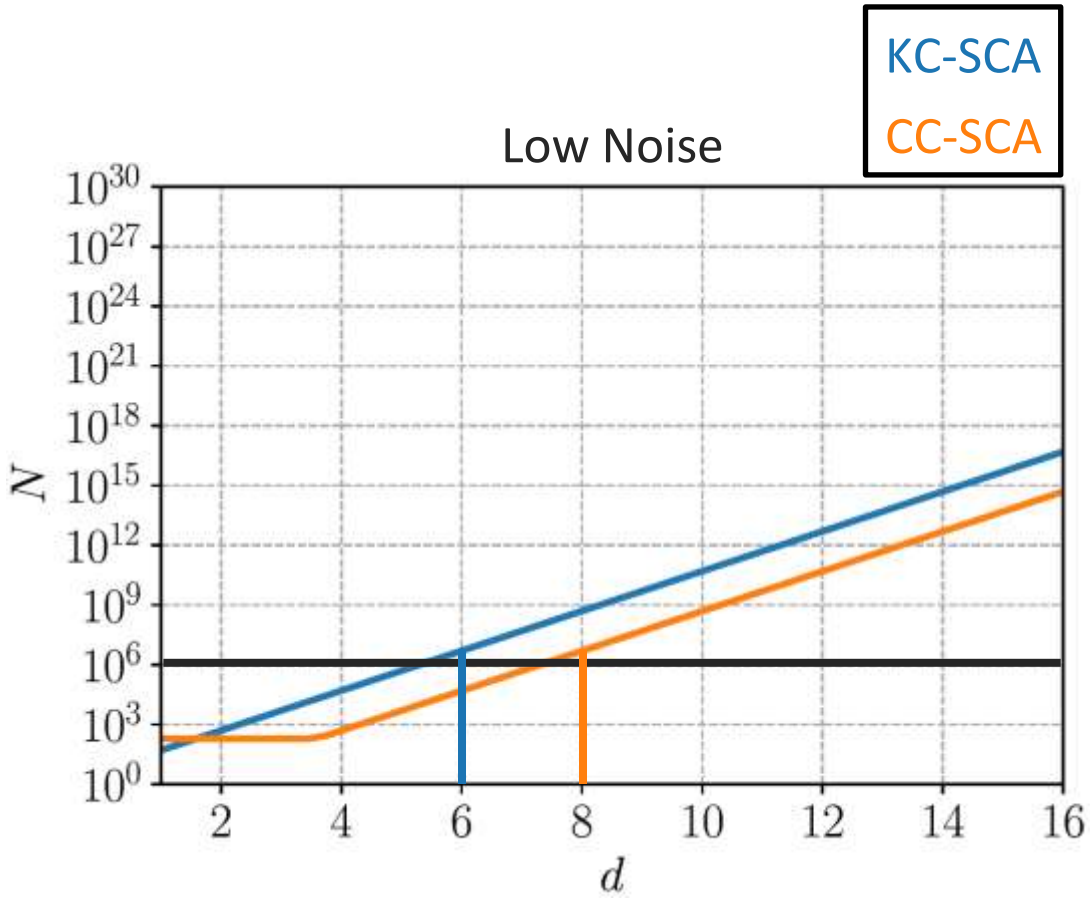
- Known ciphertext ➔ d = 6
- Chosen ciphertext ➔ d = 8

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.



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

[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)

[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	N/A*
3.5x	64x	110x	197x	293x	397x	Low

18x → High(er)

? → Low

* For this specific implementation + board.

Requires further stack usage optimization.

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

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

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)

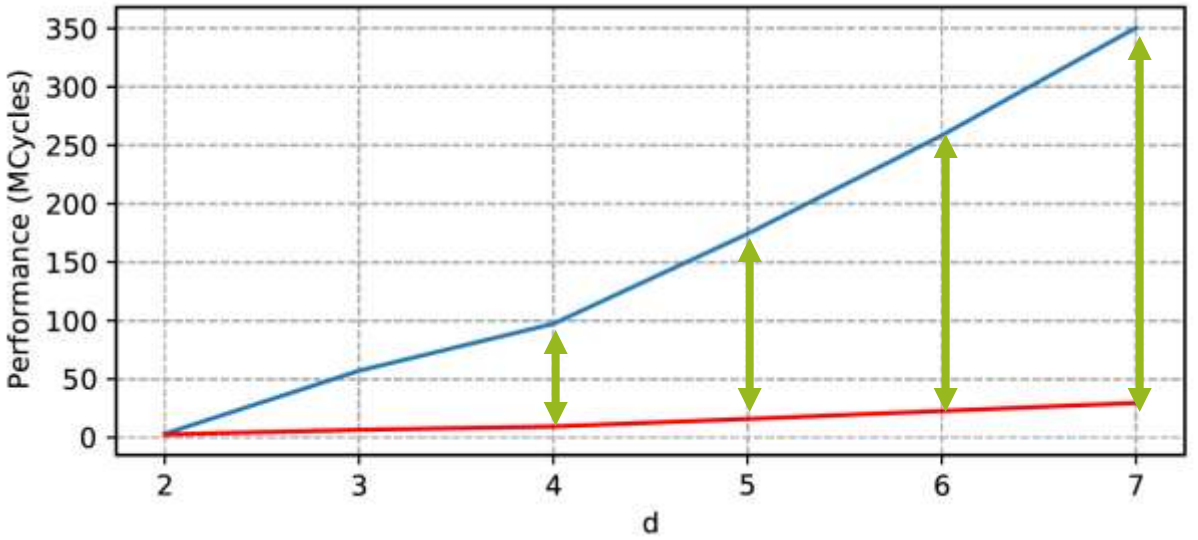
SURVIVAL STRATEGIES

Alternative Solution: Encrypt-then-Sign KEM

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

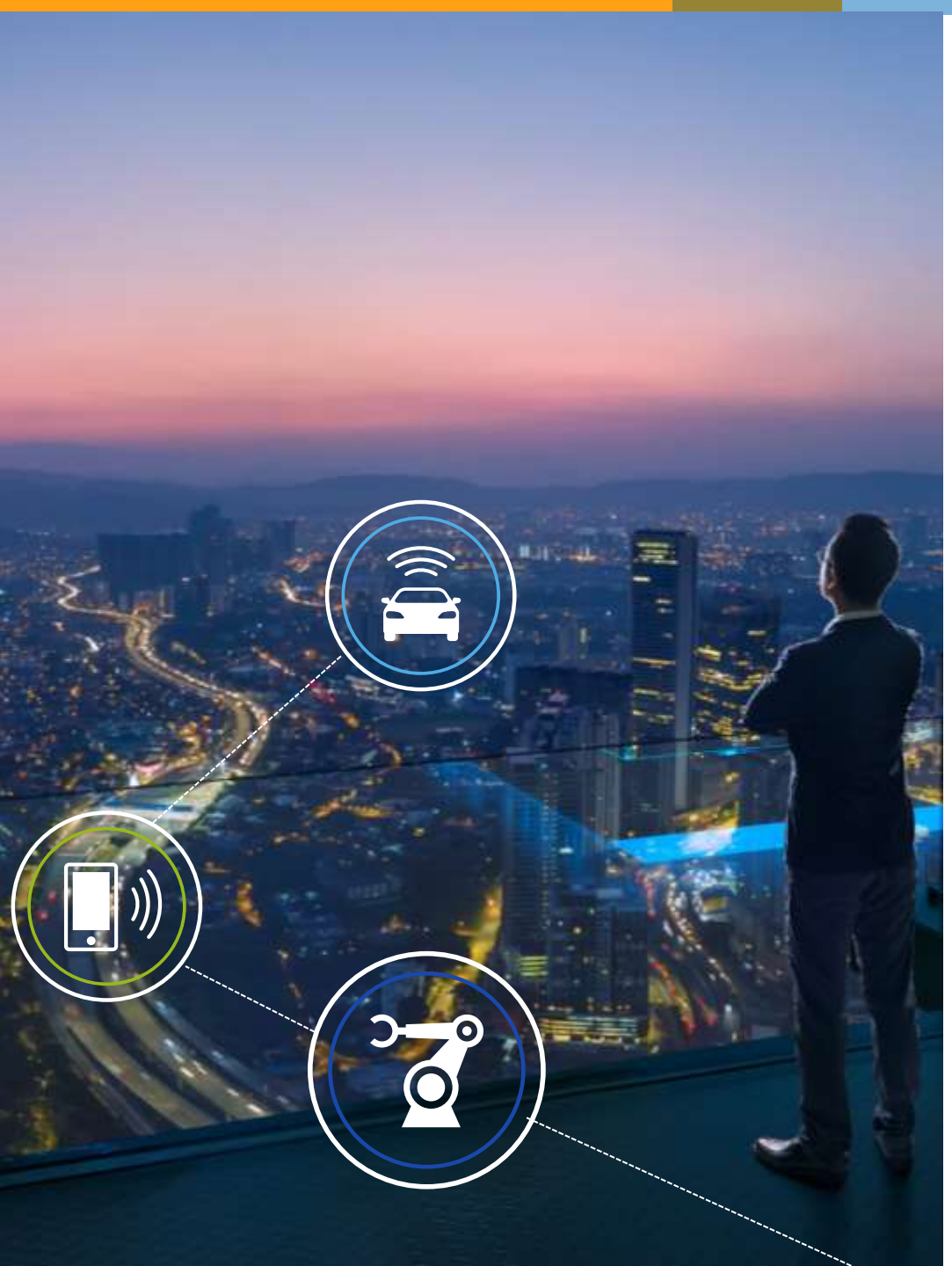
- Uses less shares because no FO leakage
- Verification only with public values (no SCA protection)

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?

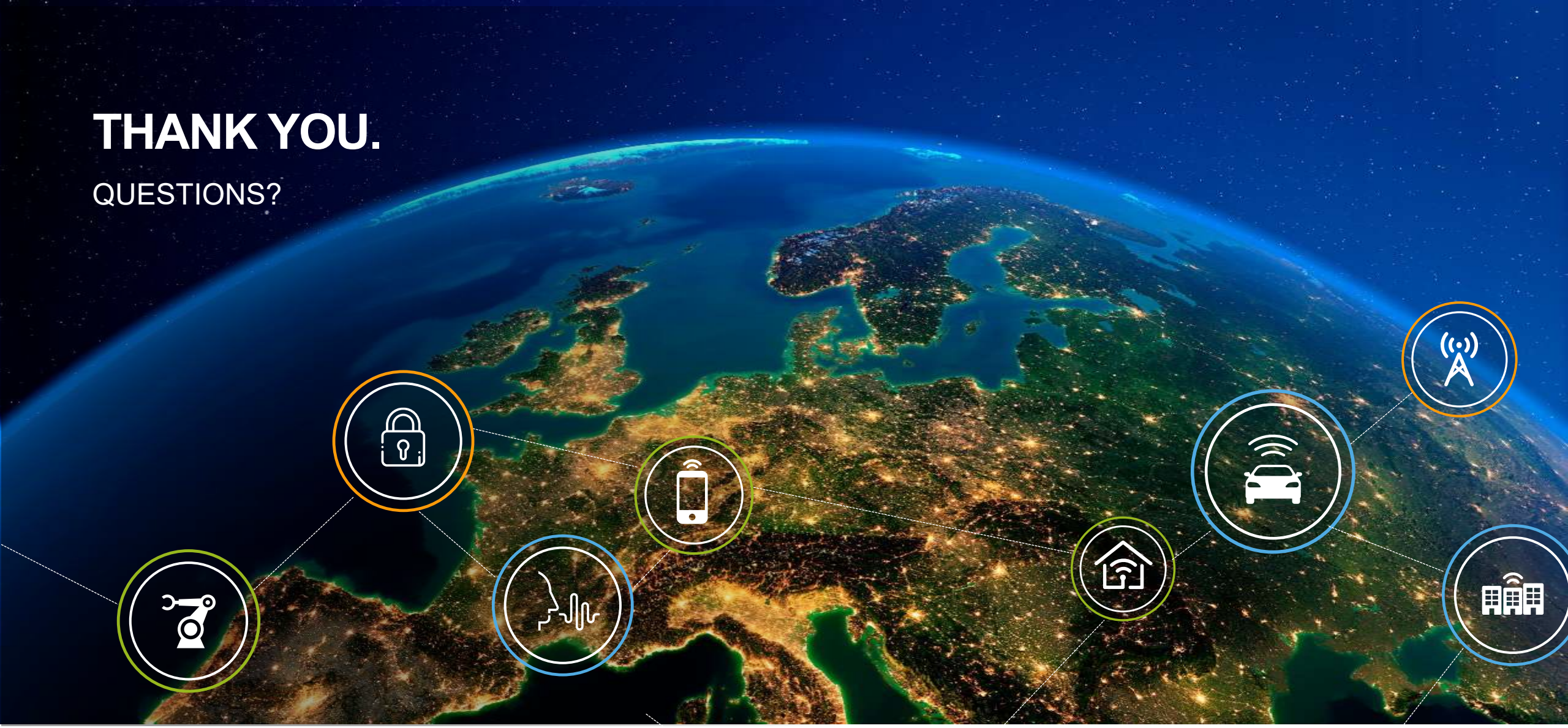
✓ **Think about migration paths now**

✓ **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