Embedded Post-Quantum Cryptography

Joppe W. Bos

Technical Director, CCC&S, CTO
April 2024

Inside Quantum Technology
The Hague

Agenda

PQC for Embedded: 2 main challenges

- High-secure implementations
- Fitting PQC on resource-constrained devices

PQC: Embedded Use-case

- Automotive

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

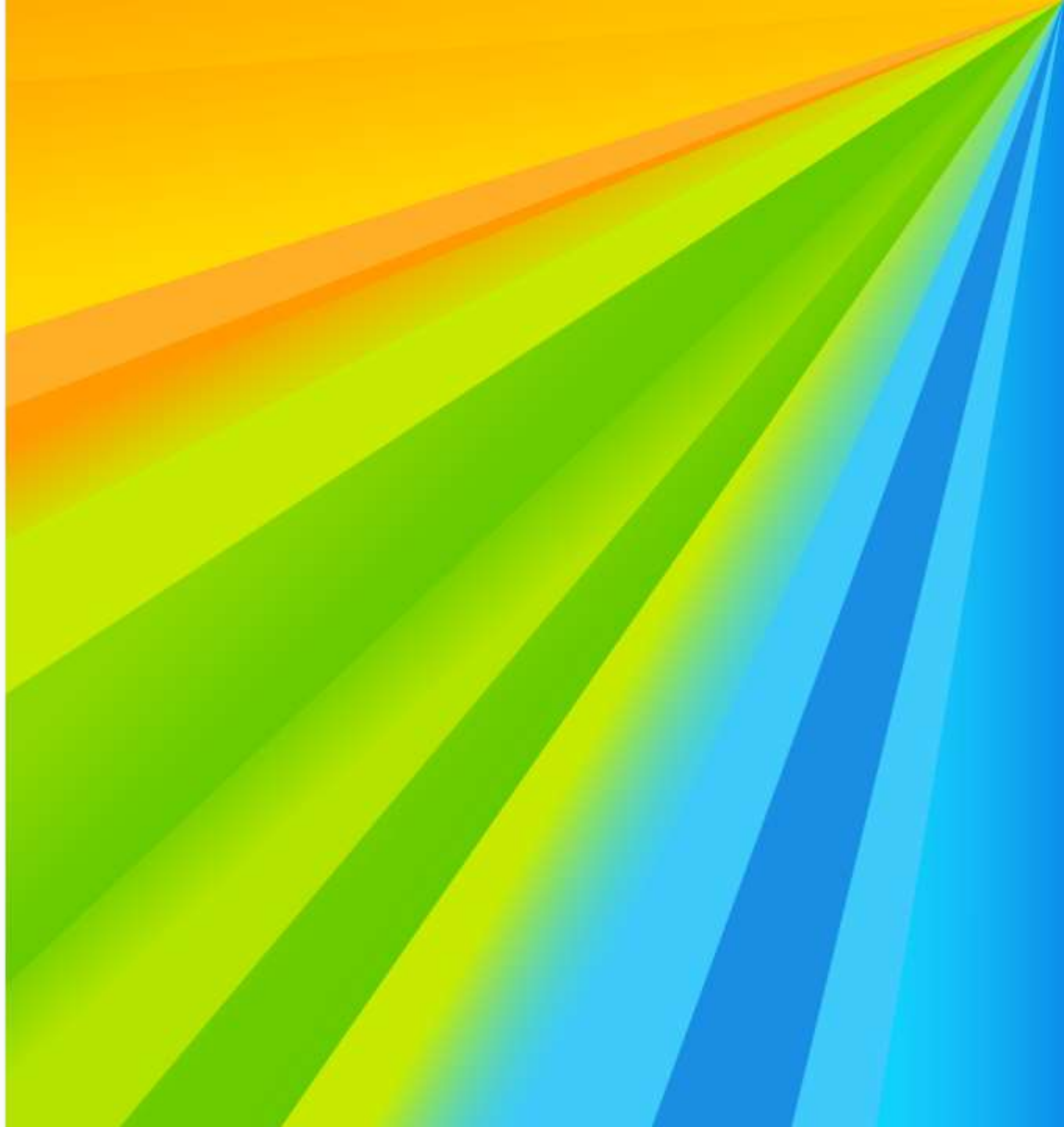
Firmware update mechanisms in vehicles
Could be circumvented and allow dangerous modifications

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

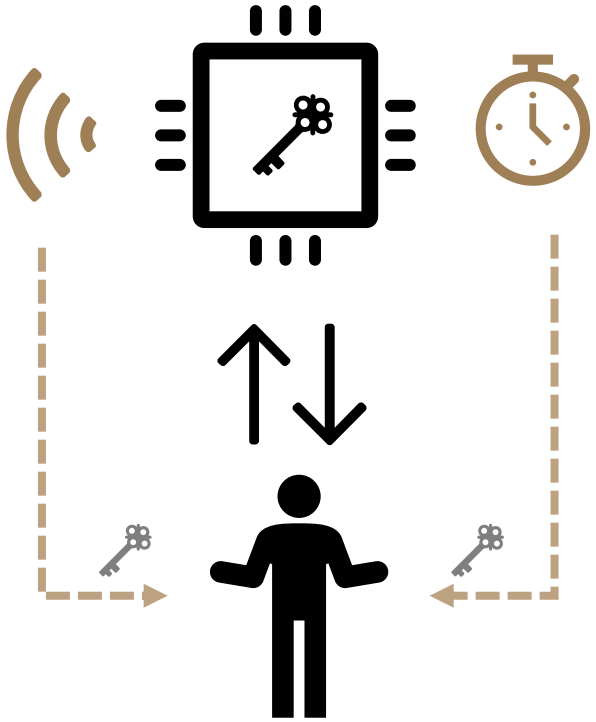
Audit trails and digitally signed documents associated with safety (auto certification and pharmaceutical authorizations)
Could be retrospectively modified

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

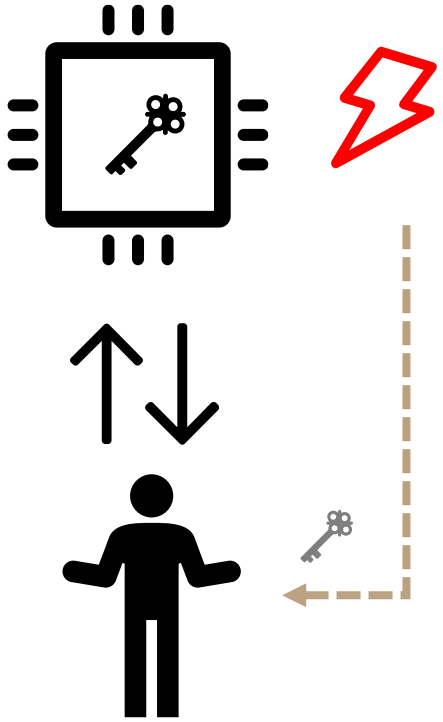
PQC & SCA



Embedded cryptography and implementation attacks



Side-Channel Attacks (SCA)



Fault Attacks (FA)

Challenges in the Embedded World

Attacks

Deep understanding in both academia and industry.

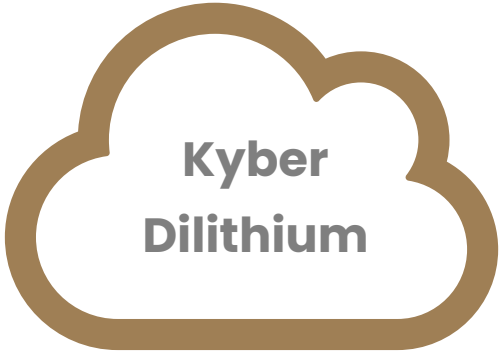
Current Cryptography

Countermeasures

Practically secure and certified implementations.

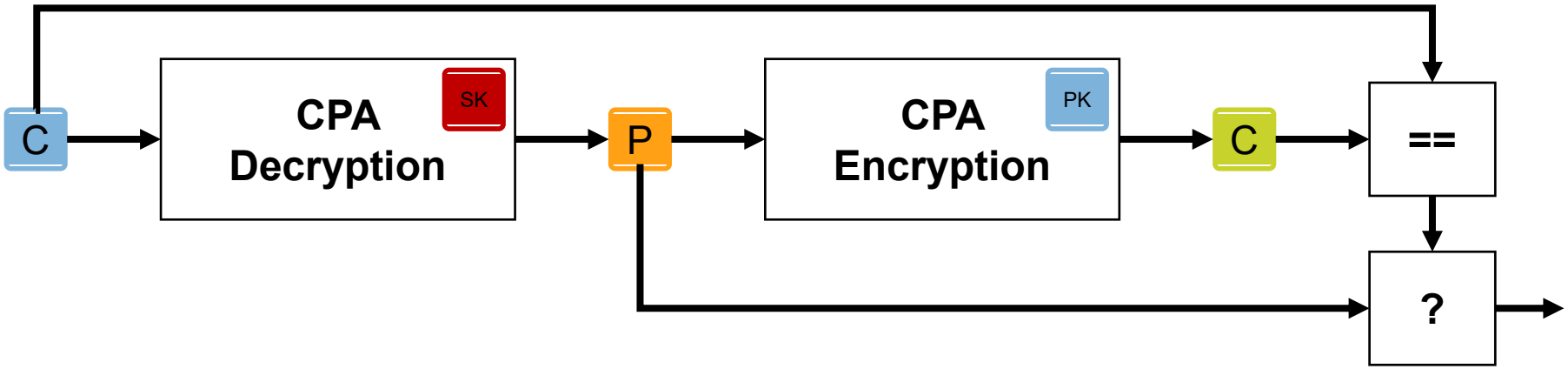
What does it mean to secure PQC implementations in "practice"?

Active research area resulting in increasingly powerful attacks.



Early stage of academic research. Limited industrial results.

Fujisaki-Okamoto Transform



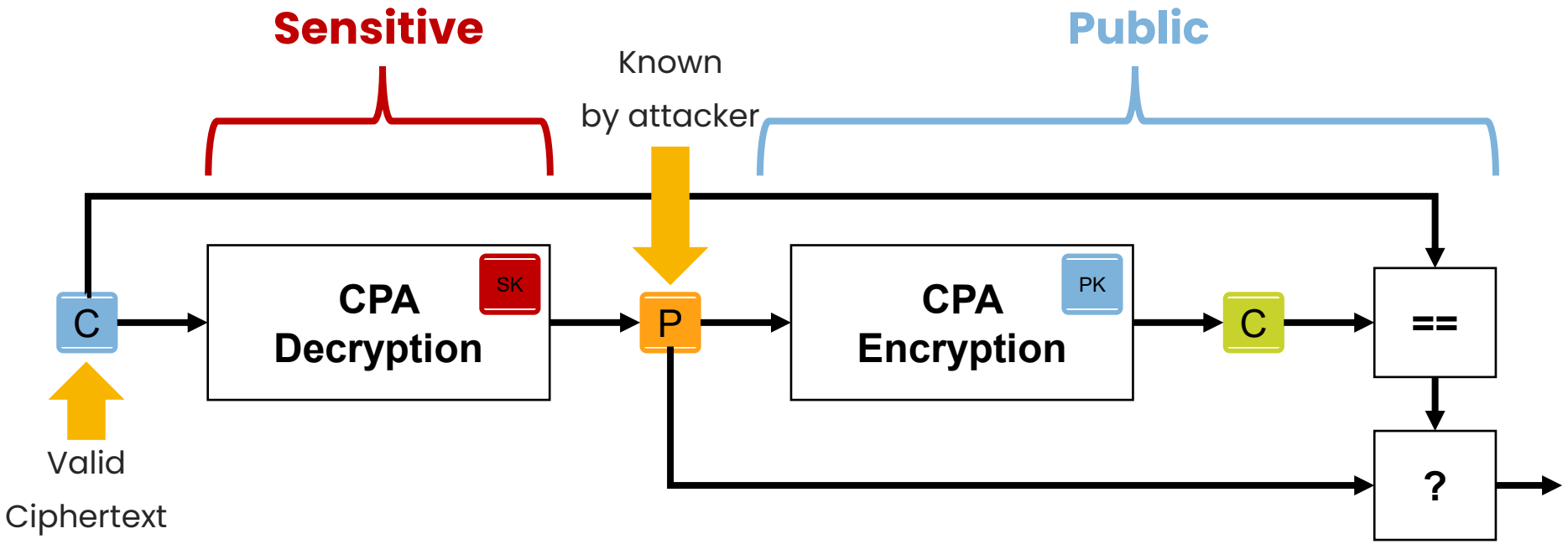
Transform a scheme which achieves IND-CPA ("chosen plaintext attack") security to reach IND-CCA ("indistinguishability against chosen-ciphertext attacks") security

- 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**

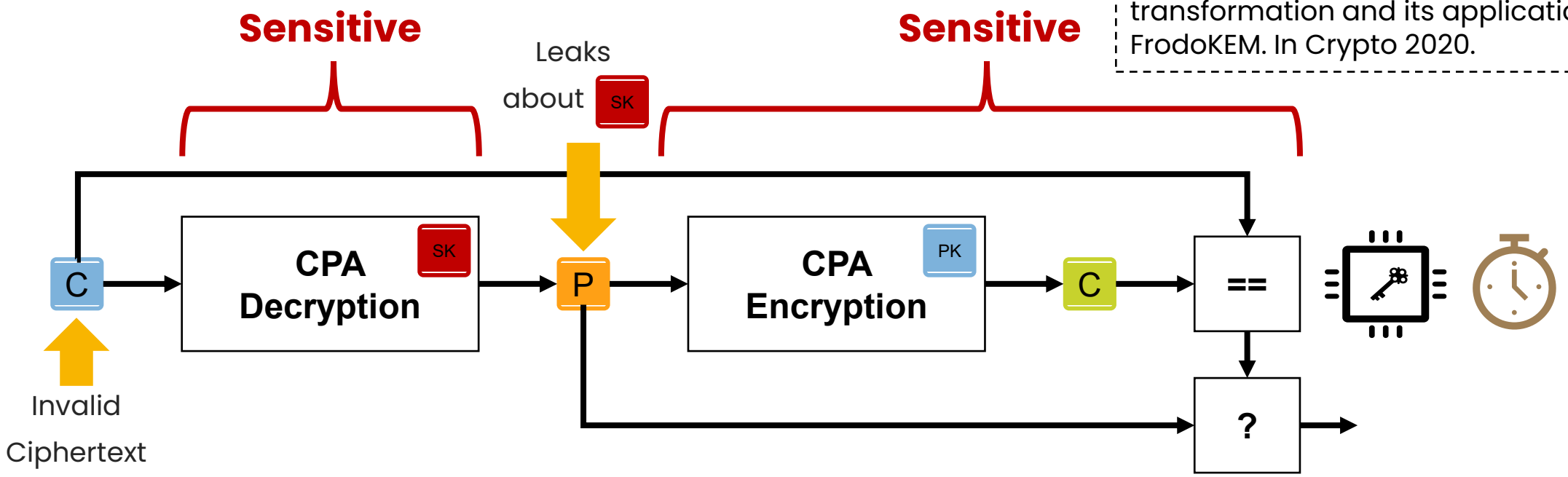


The SCA Problem of the FO-Transform

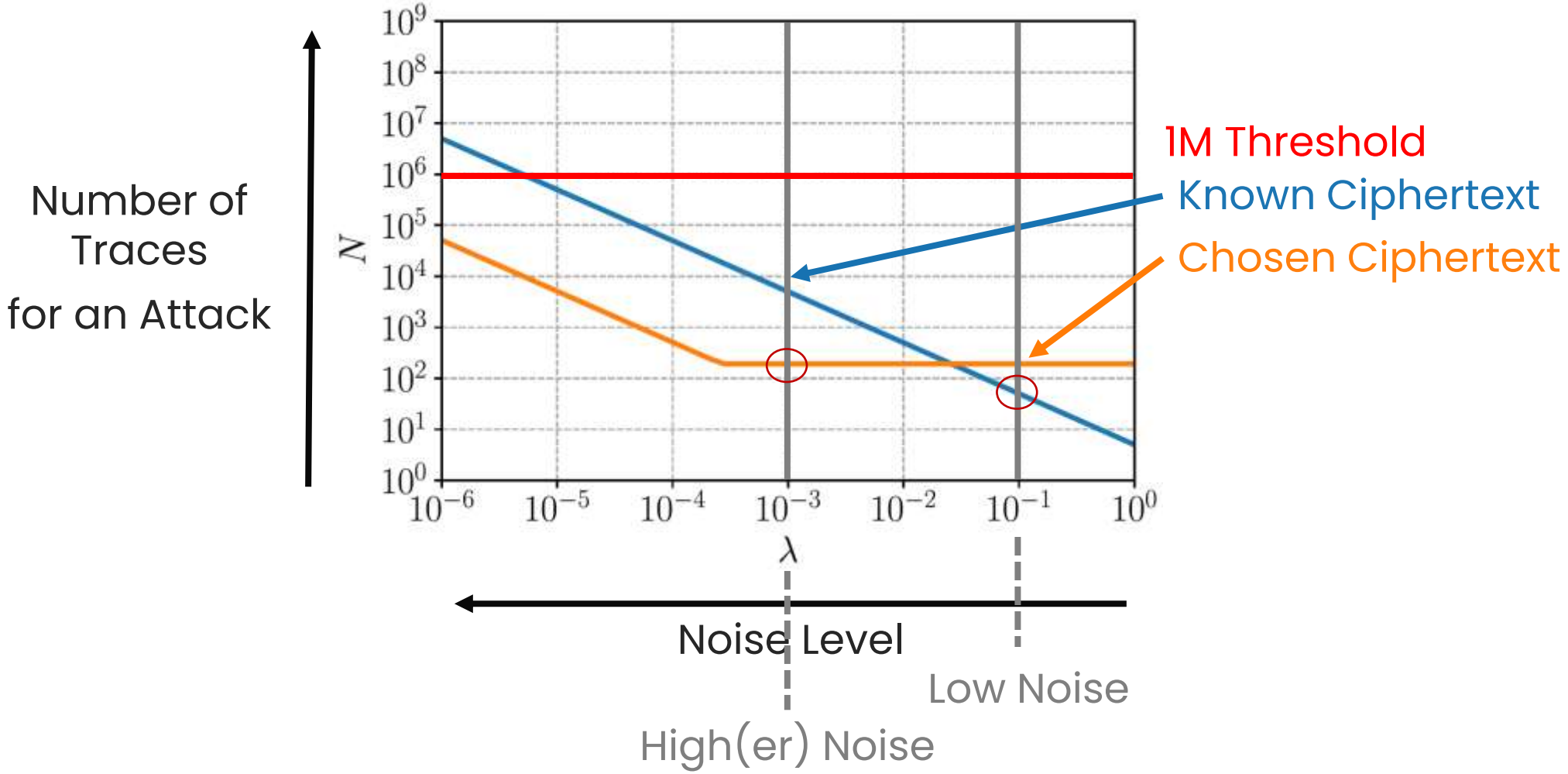
Attack 2: Chosen Ciphertext

- 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.



Case Study: Unprotected Kyber



Case Study: Masked Kyber

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

Higher *d* = Higher security + Increased cost

For **low noise**:

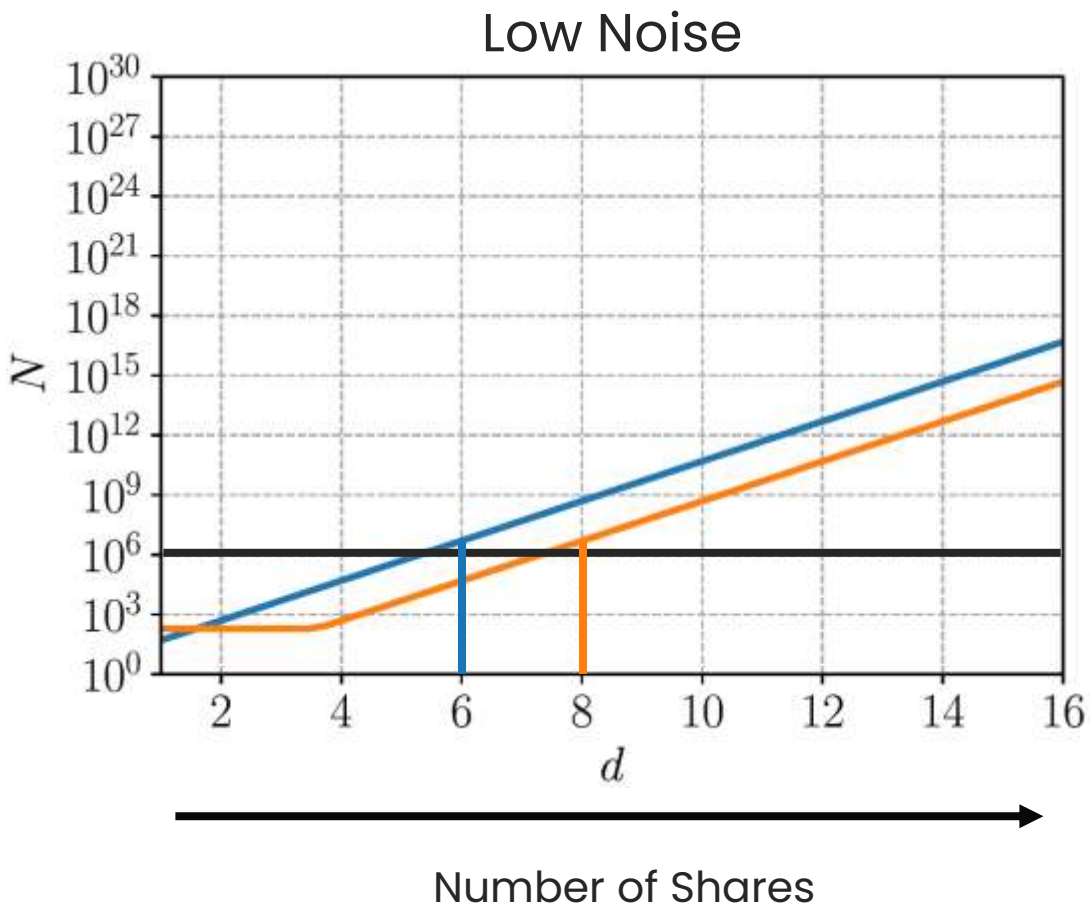
- Known ciphertext ➔ d = 6
- Chosen ciphertext ➔ d = 8

FO causes an increase of **2** security orders.

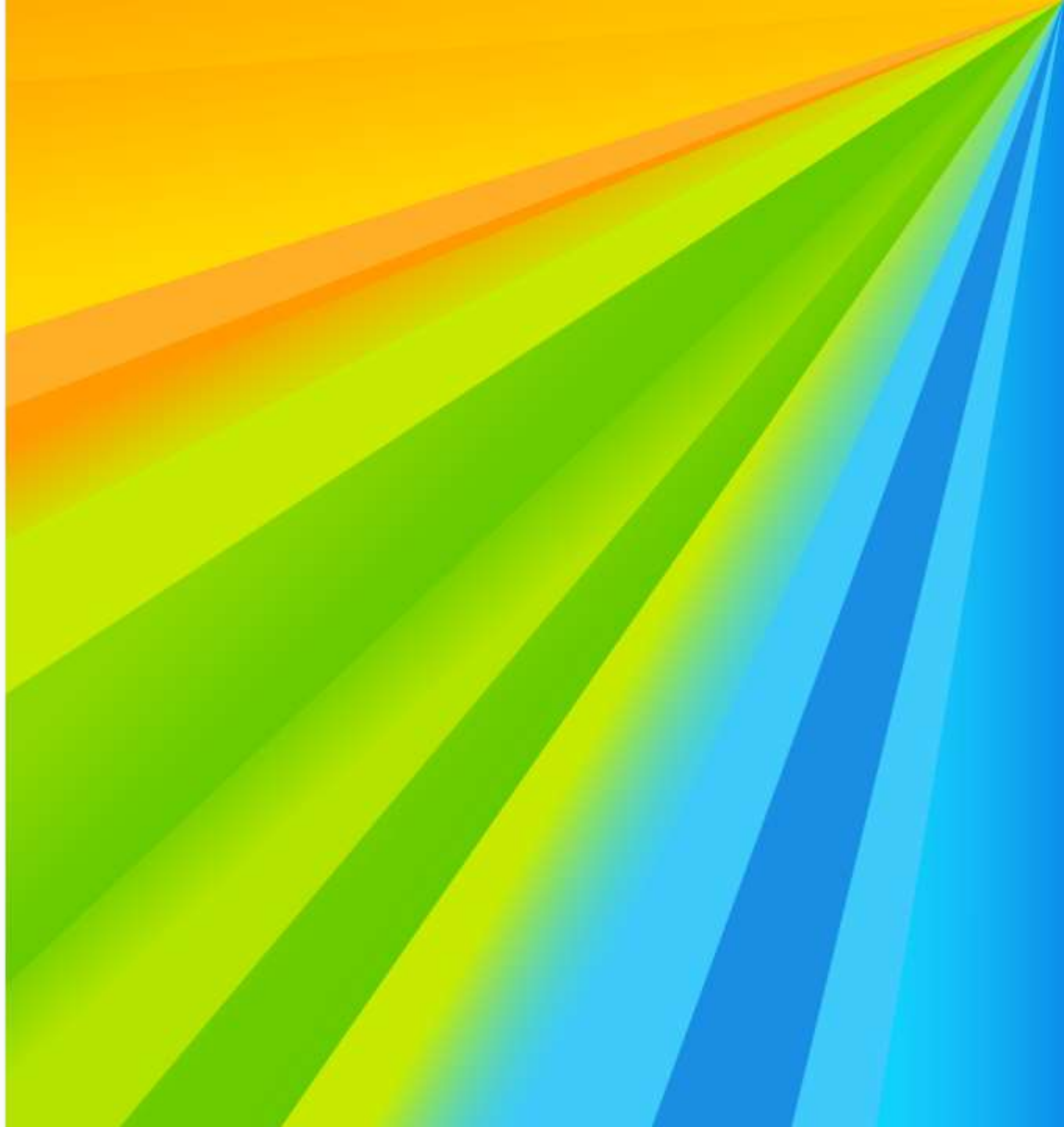
For **high(er) noise**:

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

FO causes an increase of **1** security order.



PQC + Memory Requirements



A smarter world starts with NXP

We design purpose-built, rigorously tested technologies that enable devices to sense, think, connect and act intelligently to improve people's daily lives.

Automotive

Industrial & IoT

Mobile

Smart Home

Smart City

Communication Infrastructure

INDUSTRIAL

- Fit-for-purpose Scalable Processors
- Functional Safety & Security
- Industrial Connectivity & Control
- Machine Learning & Vision
- Comprehensive Software

PQC ON EMBEDDED DEVICES

What is embedded?

- NIST has recommended a focus on the 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

The fastest implementations in pqm4 require ≈ 49, ≈ 80 and ≈ 116 KiB memory for Dilithium-{2,3,5}.

Small implementations

Measurements on a Cortex-M4

		NXP PQC	PQClean	Smaller
Dilithium-2	Sign	5.0	50.7	10.1x
	Verify	2.7	35.4	13.1x
Dilithium-3	Sign	6.5	77.7	12.0x
	Verify	2.7	56.4	20.9x
Dilithium-5	Sign	8.1	☹	∞
	Verify	2.7	☹	∞

Numbers are in KB

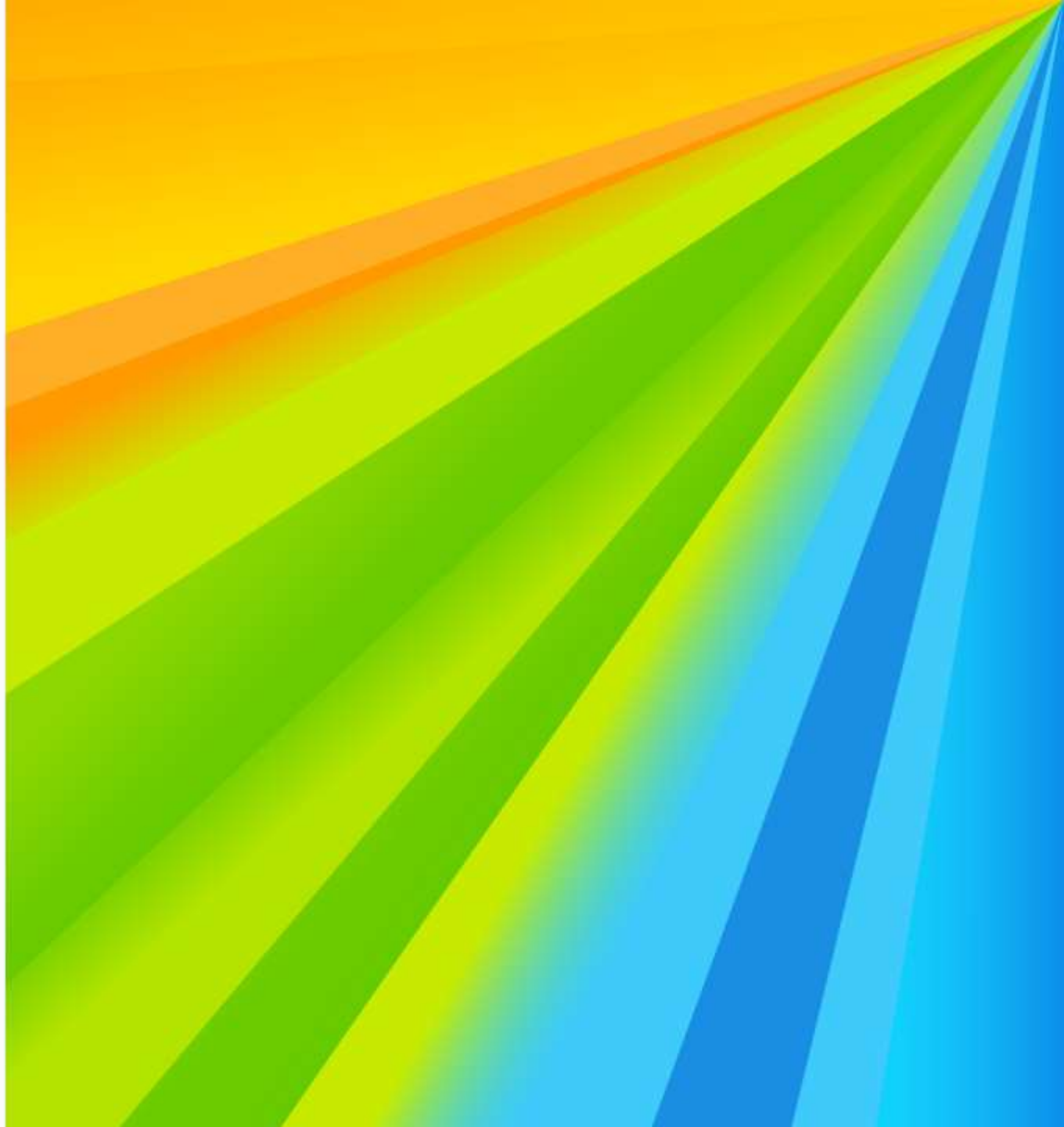
NXP PQC	PQClean	Slower
18,470	8,034	2.3x
4,036	2,223	1.8x
36,303	12,987	2.8x
7,249	3,666	2.0x
44,332	☹	∞
7,249	☹	∞

Numbers are in 10^3 cycles

- ✓ All Dilithium parameter sets will fit on a device with 16KB memory
- ✓ Price: factor 2 to 3 in performance → HW accelerators

PQCLEAN: Kannwischer, M. J., Schwabe, P., Stebila, D., & Wiggers, T., 2022. Improving software quality in cryptography standardization projects. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. https://github.com/PQClean/PQClean
NXP PQC: Bos, J.W., Renes, J. and Sprenkels, A., 2022. Dilithium for memory constrained devices. In *International Conference on Cryptology in Africa* (pp. 217-235).

PQC Embedded Use Cases



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

Enable PQC secure boot

Secure Over-the-Air (OTA) updates

Secure vehicle and driver data

SAFE ASSURE™ by NXP

www.nxp.com/S32G2

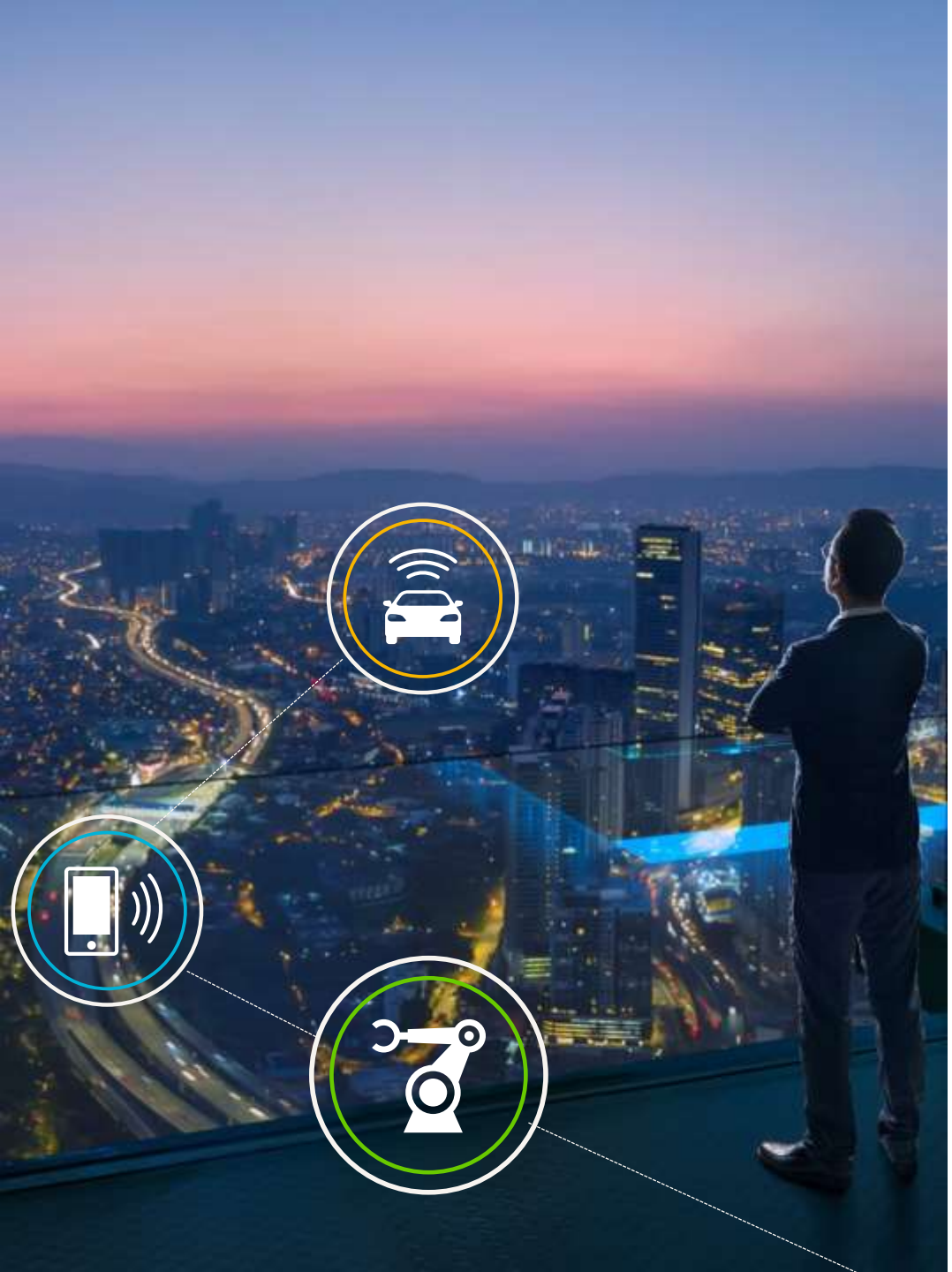
EDGELOCK™ ASSURANCE by NXP

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

Bos, Carlson, Renes, Rotaru, Sprenkels, Waters: Post-Quantum Secure Boot on Vehicle Network Processors. Embedded Security in Cars. Escar 2022



Conclusions

- 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 edge-devices**:

✓ Large key sizes no issue

- SHA-3 performance crucial, hardware acceleration important

✓ Transition to PQC practical right now

Get in touch

Joppe W. Bos
Joppe.Bos@nxp.com

nxp.com