Gevallenstudies Wiskundige Ingieurstechnieken

Joppe Bos

March 2025

Joppe W. Bos

Cryptographic Researcher and Technical Director at NXP Semiconductors

Secretary of the IACR (2017-2019, 2020-2022)

Editor of the Cryptology ePrint Archive (2019-today)

Editor-in-Chief of the IACR Communications in Cryptology

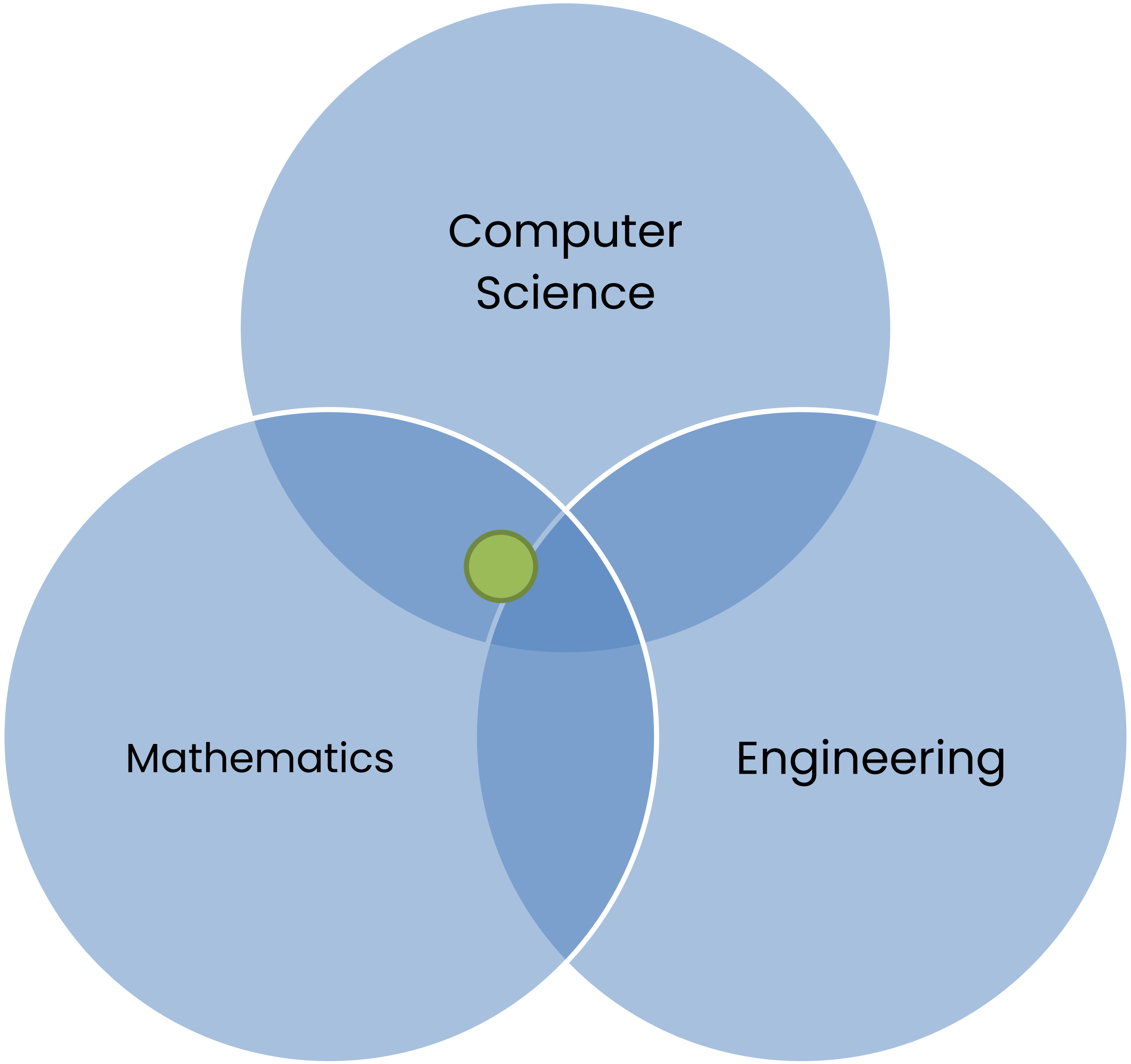
Leuven, Belgium

WHOAMI

- Cryptographic researcher + Technical Director
  - in the competence center crypto & security at NXP Semiconductors, Leuven
  - Lead the PQC team
  - Lead security + crypto funded projects & university relations
- Post-doc
  - Cryptography Research Group at Microsoft Research, Redmond, USA.
- PhD in Cryptology
  - EPFL, Lausanne, Switzerland
- Bachelor / Master in Computer Science
  - University of Amsterdam

Public Key Cryptography

- Computational number theory
- Number theoretic transform



Breaking ECC

112-bit ECDLP solved using 224 PlayStation 3 game consoles.

NXP Corporate Overview

Together we accelerate the breakthroughs that advance our world

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

Automotive

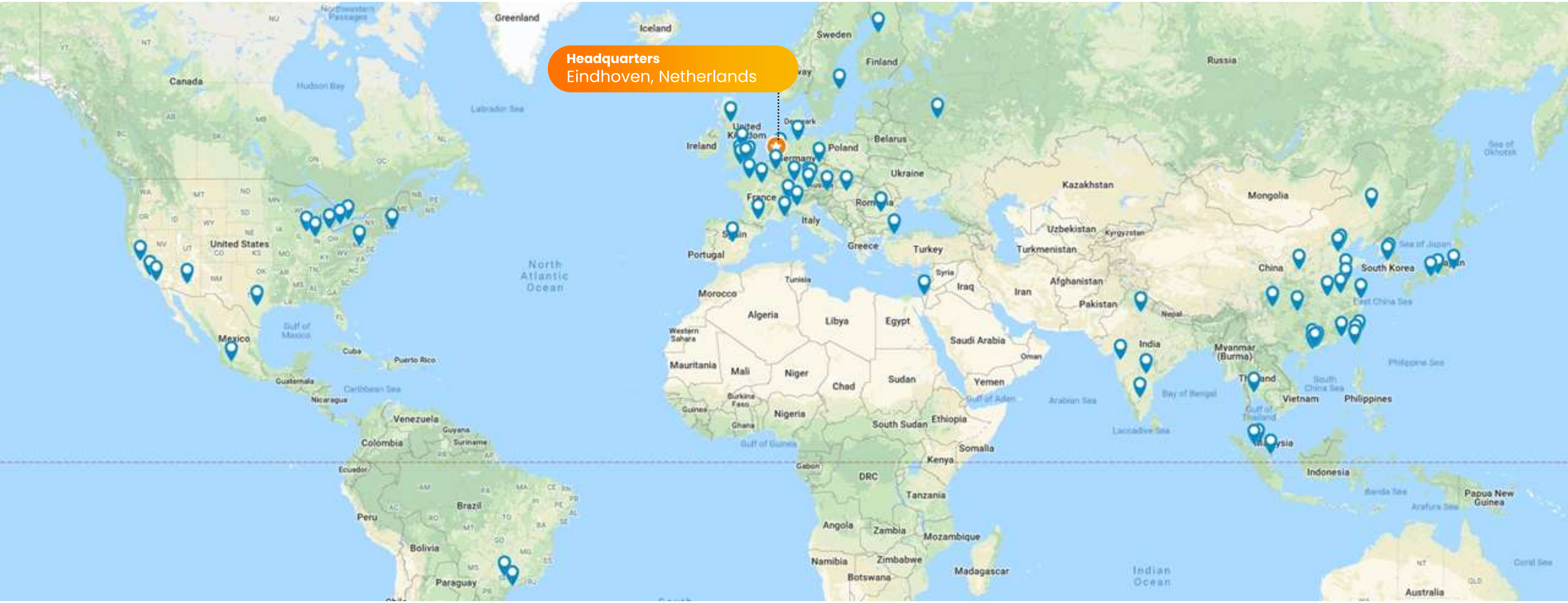
Industrial & IoT

Mobile

Communication Infrastructure

NXP locations

~34,200 team members with operations in more than **30 countries**



Automotive

market positions

Automotive

Technology Leadership

#1 Auto processors

#1 Auto applications processors

#1 Auto RF

#1 Auto DSPs

#1 Cross-domain processors

+

Applications Leadership

#1 Infotainment

#1 Car radio

#1 Secure car access

#1 In-vehicle networking

Sources: Strategy Analytics: Automotive Semiconductors Vendor Market Shares, April 2024, Strategy Analytics: Infotainment and Telematics Semiconductors Vendor Market Shares, April 2024, Gartner: Semiconductors Market Shares, April 2024, S&P: competitive landscaping tool, April 2024, IHS: automotive semiconductors market tracker, April 2024

Edge processing –
a distributed intelligence pyramid

Millions

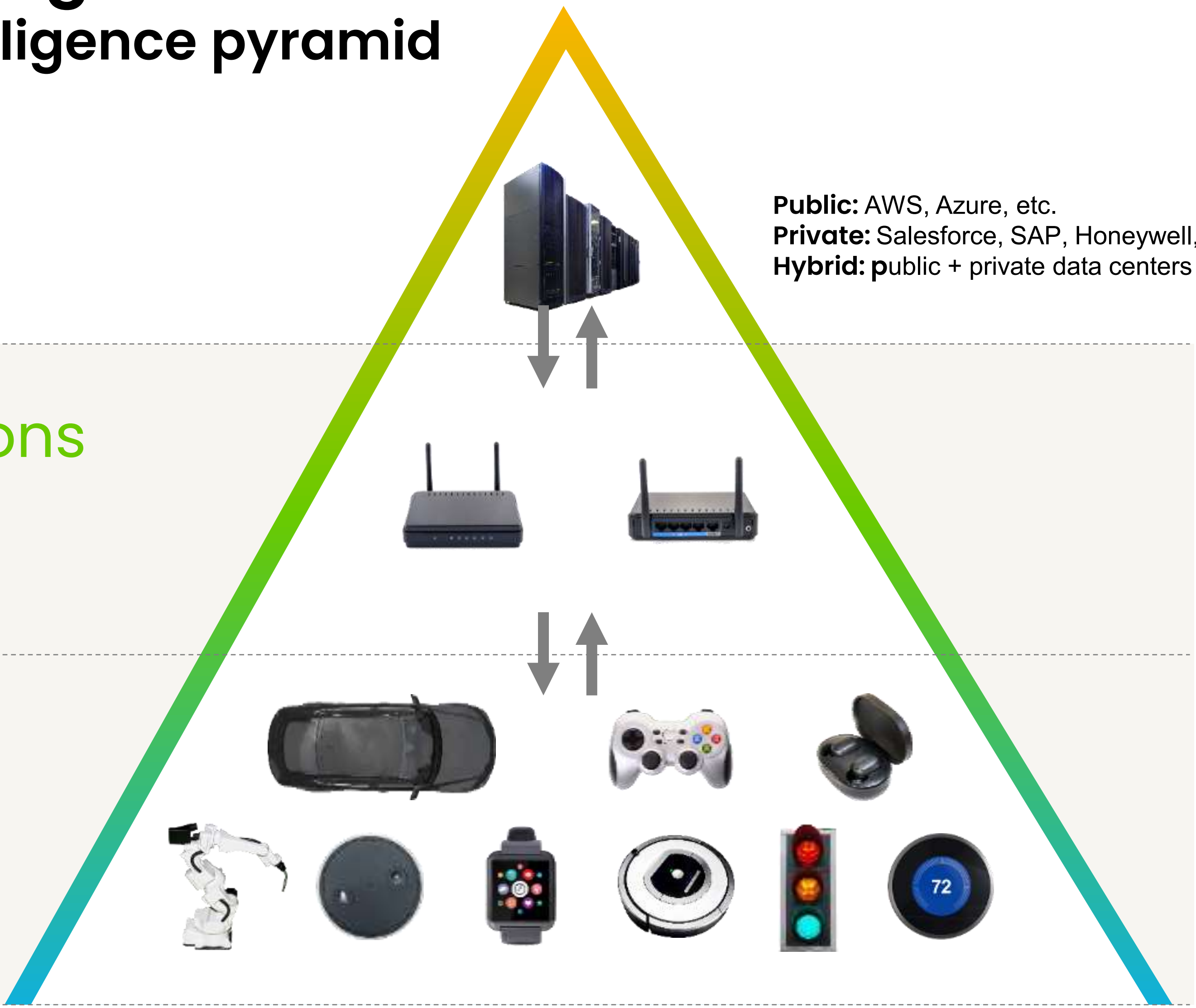
Cloud
Data centers

10's to 100's Millions

Network Edge
Network computing

Billions

Application Edge
IoT end points



Public: AWS, Azure, etc.
Private: Salesforce, SAP, Honeywell, etc.
Hybrid: public + private data centers

Edge processing
served market

End-to-end solutions for Matter

A unified IP-based protocol to securely and robustly connect smart devices with each other, regardless of brand, and across smart home platforms

Bring interoperability in the Smart Home industry

Simplify development for “things”

Increase reliability for consumers

Ensure security and privacy

Led by global brands and 200+ companies

Classical Cryptography

Public-Key Cryptography

In **public-key** cryptography the theoretical foundation of the schemes used are problems which are **believed** to be hard

- Integer factorization problem (RSA)
- Discrete logarithm problem (DSA, ElGamal)

One of the main ingredients to these problems is a group

RSA → $(\mathbb{Z}/N\mathbb{Z})^{\times}$→ integers $[\,1, 2, \dots, N-1]$ which are co-prime to N

DSA/ElGamal → $\mathbb{F}_p^{\times} = (\mathbb{Z}/p\mathbb{Z})^{\times}$ → integers $[\,1, 2, \dots, p-1]$ where p is prime

Elliptic Curve Cryptography → $E/\mathbb{F}_p$ → point on $E(\mathbb{F}_p)$ where p is prime

<table>
<tr><td>Application</td><td colspan="3">Encryption Scheme, Signature Scheme, Identification Scheme, etc.</td></tr>
<tr><td>Cryptosystem</td><td colspan="2">DSA, ElGamal, Schnorr, etc.</td><td>RSA, Rabin, etc.</td></tr>
<tr><td>Computational Problem</td><td colspan="2">The Discrete Logarithm Problem in a Group of prime Order</td><td>The Factoring Problem</td></tr>
<tr><td>Algebraic Structure</td><td>The multiplicative group of integers modulo a prime</td><td>Elliptic Curve Group over a Finite Field</td><td>The set of integers modulo the product of two primes</td></tr>
</table>

Post-Quantum Cryptography

QUANTUM CLOUD —

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

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

CHRIS LEE

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

...uantum
...ew chip was
...rformance.

NEWS | 23 October 2019

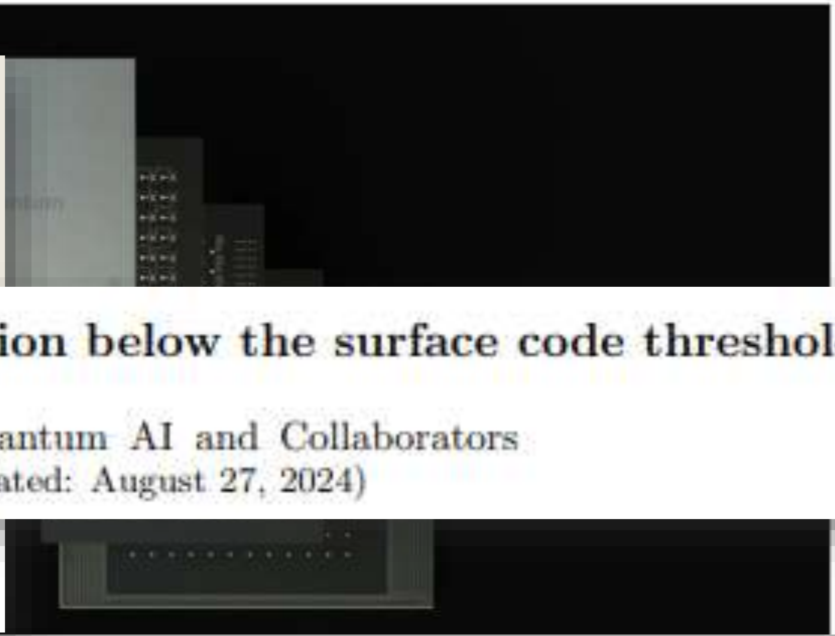
Hello quantum world! Google publishes landmark quantum supremacy claim

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

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.



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

SHARE

- NXP, eleQtron and ... quantum comput...
- It was commissioned by the DLR Quantum Computing Initiative (DLR QCI) to expand the quantum expertise of its partners from research and industry

Quantum error correction below the surface code threshold

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

Security impact of quantum computers

Requirements: Cryptography	
Asymmetric	Symmetric
RSA-3072	AES-128
ECC P-256	SHA-256
X	?

"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

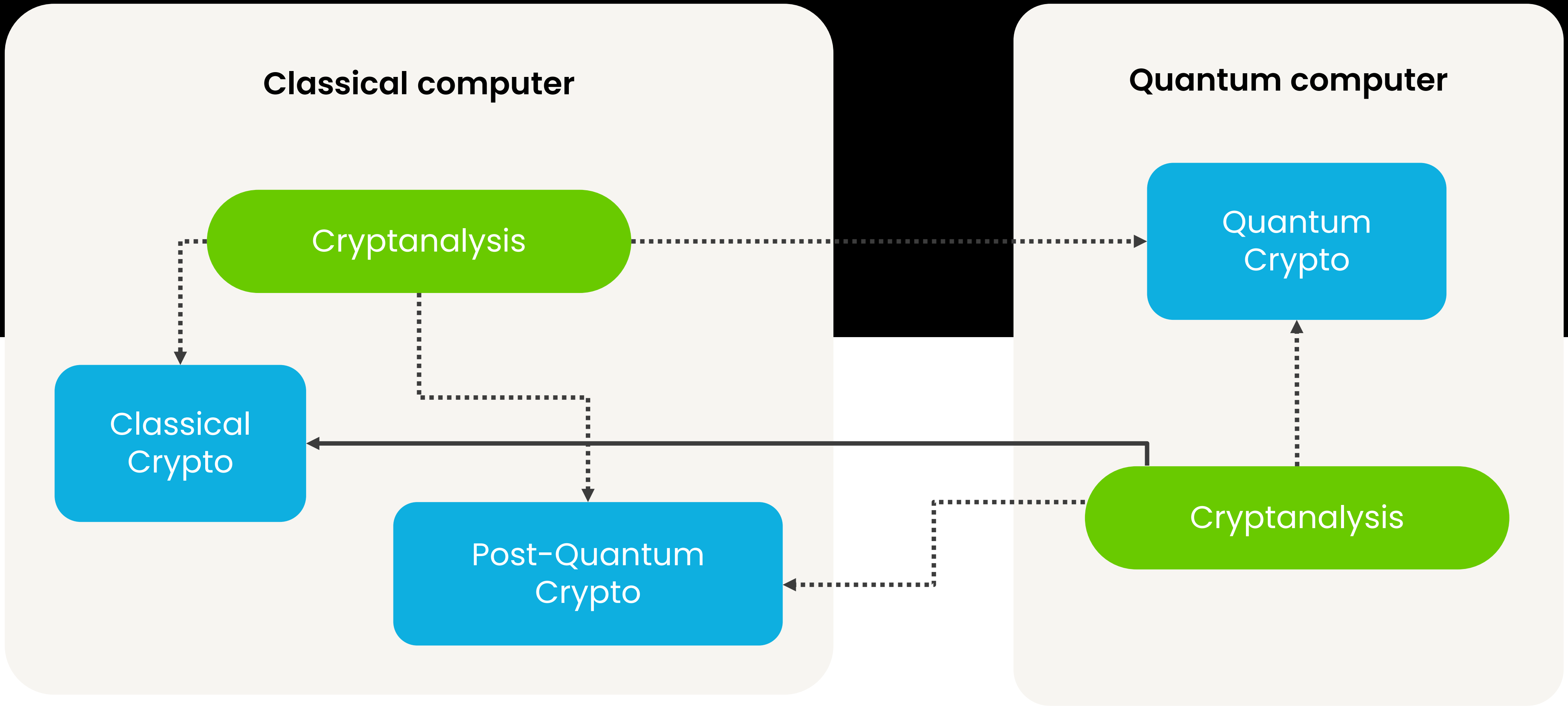
Firmware update mechanisms in vehicles
Could be circumvented and allow dangerous modifications

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



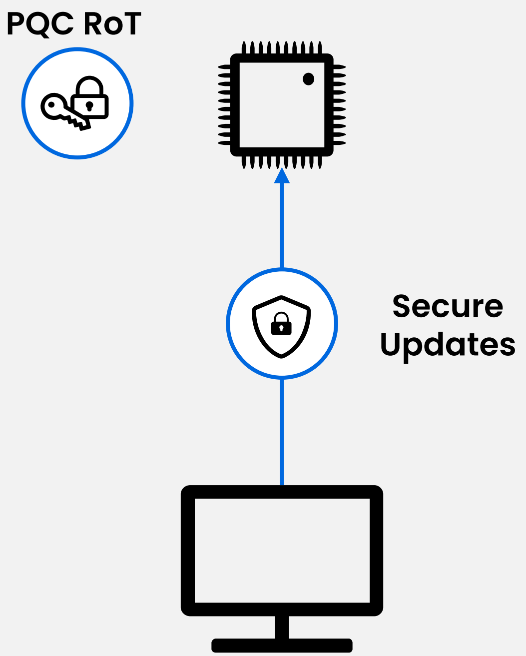
Post-Quantum Cryptography

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

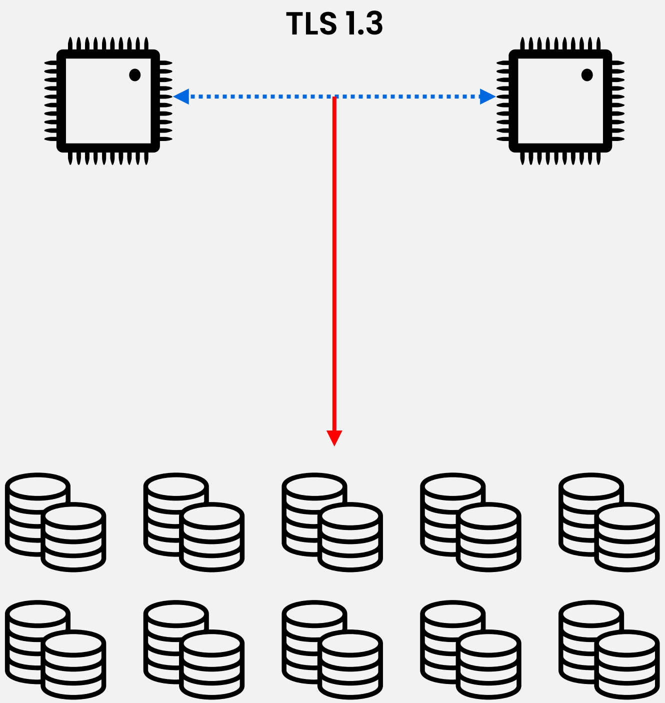
Is Post-Quantum Cryptography relevant for you?

Standards & Compliance

Crypto Agility



Store Now Decrypt Later



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

2020

NIST SP 800-208

Stateful Hash-Based Signature Schemes

- XMSS
- LMS

2024

NIST PQC Standards

- ML-KEM FIPS 203 (Kyber) — NXP
- ML-DSA FIPS 204 (Dilithium)
- SLH-DSA FIPS 205 (SPHINCS+)

2025-

Further NIST PQC Standards

Round 4 KEM, Signature On-Ramp

- FN-DSA FIPS 206 (Falcon)

2025-2028

Asia

PQC standards from China, Korea and India expected

2023-2030

ISO

Push from EU to include additional schemes in ISO standard

- FrodoKEM — NXP
- Classic McEliece

New algorithms and standards

FIPS 203

Federal Information Processing Standards Publication

Module-Lattice-Based
Key-Encapsulation Mechanism Standard

Category: Computer Security Subcategory: Cryptography

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.203

Published August 13, 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Key Exchange / Encapsulation

FIPS 204

Federal Information Processing Standards Publication

Module-Lattice-Based Digital
Signature Standard

Category: Computer Security Subcategory: Cryptography

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.204

Published August 13, 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Digital Signatures
(generic)

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

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-208

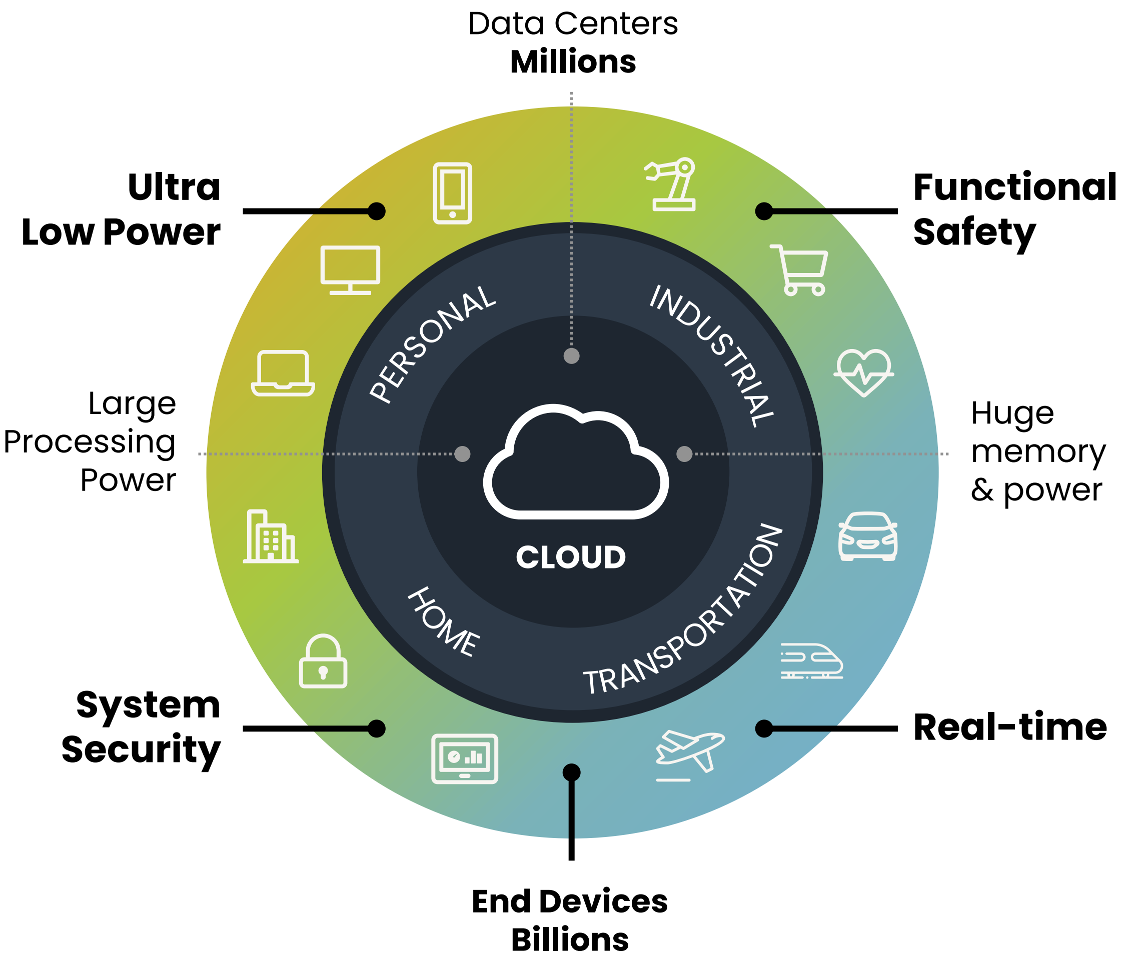
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Digital Signatures
(software / firmware signing)

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

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!*

[A] pqm4; pqm4/benchmarks.md at master · mupq/pqm4 · GitHub
[B] Campos, Kohlstadt, Reith, Stöttinger; https://eprint.iacr.org/2020/470.pdf

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**

Cryptographic Suite for Algebraic Lattices (CRYSTALS)

The Cryptographic Suite for Algebraic Lattices (CRYSTALS) encompasses

- **Kyber**, a Key Encapsulation Mechanism (KEM) -> referred to in FIPS 203 as **ML-KEM**
- **Dilithium**, for Digital Signatures -> referred to in FIPS 204 as **ML-DSA**

Theory: same building blocks

- Module Learning with Errors
- Number-Theoretic Transformations

Many new techniques to deal with!

Kyber uses the 'Fujisaki-Okamoto Transform' to get strong security

Dilithium uses 'Rejection Sampling' as a core component for producing signatures

Solving systems of linear equations

secret

$$\underset{\mathbb{Z}_{13}^{7\times 4}}{\begin{pmatrix} 4 & 1 & 11 & 10 \\ 5 & 5 & 9 & 5 \\ 3 & 9 & 0 & 10 \\ 1 & 3 & 3 & 2 \\ 12 & 7 & 3 & 4 \\ 6 & 5 & 11 & 4 \\ 3 & 3 & 5 & 0 \end{pmatrix}} \times \underset{\mathbb{Z}_{13}^{4\times 1}}{\begin{pmatrix} \, \\ \, \\ \, \\ \, \end{pmatrix}} = \underset{\mathbb{Z}_{13}^{7\times 1}}{\begin{pmatrix} 4 \\ 8 \\ 1 \\ 10 \\ 4 \\ 12 \\ 9 \end{pmatrix}}$$

Linear system problem: given **blue**, find **red**

Solving systems of linear equations

secret

$$\underset{\mathbb{Z}_{13}^{7\times 4}}{\begin{pmatrix} 4 & 1 & 11 & 10 \\ 5 & 5 & 9 & 5 \\ 3 & 9 & 0 & 10 \\ 1 & 3 & 3 & 2 \\ 12 & 7 & 3 & 4 \\ 6 & 5 & 11 & 4 \\ 3 & 3 & 5 & 0 \end{pmatrix}} \times \underset{\mathbb{Z}_{13}^{4\times 1}}{\begin{pmatrix} 6 \\ 9 \\ 11 \\ 11 \end{pmatrix}} = \underset{\mathbb{Z}_{13}^{7\times 1}}{\begin{pmatrix} 4 \\ 8 \\ 1 \\ 10 \\ 4 \\ 12 \\ 9 \end{pmatrix}}$$

Easily solved using Gaussian elimination (Linear Algebra 101)

Linear system problem: given **blue**, find **red**

Learning with errors problem

random		secret		small noise		
$\mathbb{Z}_{13}^{7\times4}$		$\mathbb{Z}_{13}^{4\times1}$		$\mathbb{Z}_{13}^{7\times1}$		$\mathbb{Z}_{13}^{7\times1}$

$$
\begin{bmatrix} 4 & 1 & 11 & 10 \\ 5 & 5 & 9 & 5 \\ 3 & 9 & 0 & 10 \\ 1 & 3 & 3 & 2 \\ 12 & 7 & 3 & 4 \\ 6 & 5 & 11 & 4 \\ 3 & 3 & 5 & 0 \end{bmatrix}
\times
\begin{bmatrix} 6 \\ 9 \\ 11 \\ 11 \end{bmatrix}
+
\begin{bmatrix} 0 \\ -1 \\ 1 \\ 1 \\ 1 \\ 0 \\ -1 \end{bmatrix}
=
\begin{bmatrix} 4 \\ 7 \\ 2 \\ 11 \\ 5 \\ 12 \\ 8 \end{bmatrix}
$$

Learning with errors problem

random $\mathbb{Z}_{13}^{7\times 4}$ × **secret** $\mathbb{Z}_{13}^{4\times 1}$ + **small noise** $\mathbb{Z}_{13}^{7\times 1}$ = $\mathbb{Z}_{13}^{7\times 1}$

4	1	11	10
5	5	9	5
3	9	0	10
1	3	3	2
12	7	3	4
6	5	11	4
3	3	5	0

×

+

=

4
7
2
11
5
12
8

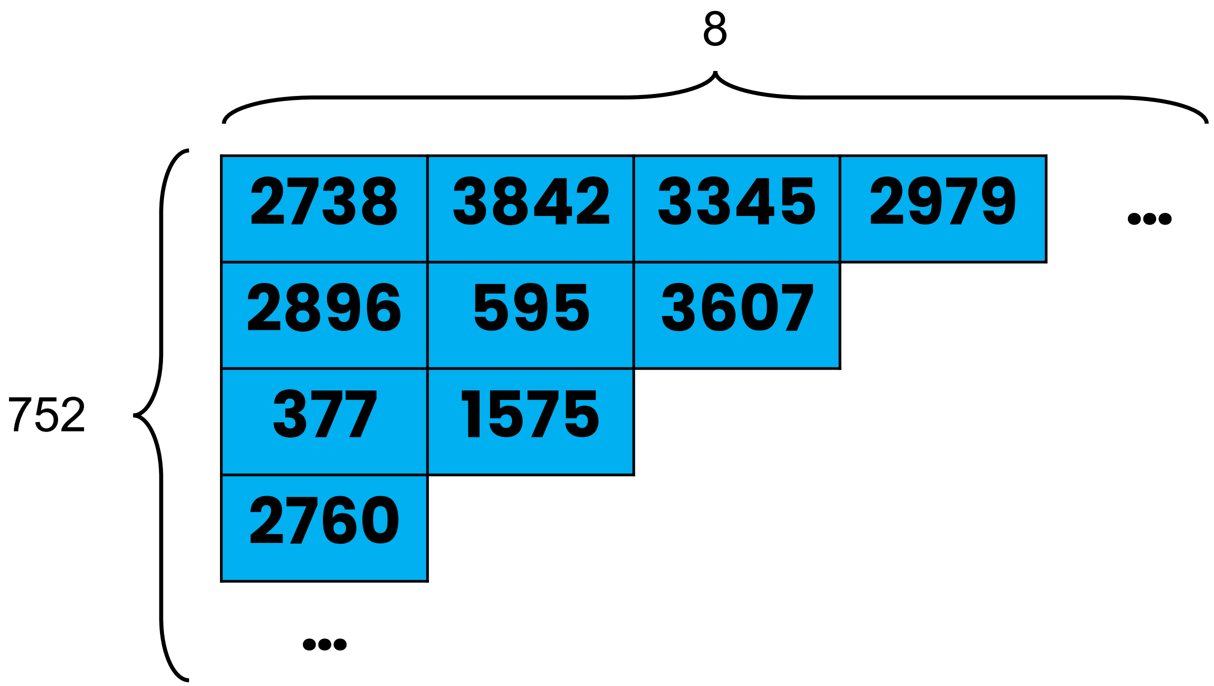
Computational LWE problem: given blue, find red

Toy example versus real-world example

$\mathbb{Z}_{13}^{7\times 4}$

4	1	11	10
5	5	9	5
3	9	0	10
1	3	3	2
12	7	3	4
6	5	11	4
3	3	5	0

$\mathbb{Z}_{2^{15}}^{752\times 8}$



752 × 8 × 15 bits = **11 KiB**

Ring learning with errors problem

random
$\mathbb{Z}_{13}^{7\times 4}$

4	1	11	10
10	4	1	11
11	10	4	1
1	11	10	4
4	1	11	10
10	4	1	11
11	10	4	1

Each row is the cyclic shift of the row above

Ring learning with errors problem

random

$\mathbb{Z}_{13}^{7\times 4}$

4	1	11	10
3	4	1	11
2	3	4	1
12	2	3	4
9	12	2	3
10	9	12	2
11	10	9	12

Each row is the cyclic shift of the row above

…

with a special wrapping rule: x wraps to $-x$ mod 13.

Ring learning with errors problem

random
$\mathbb{Z}_{13}^{7\times 4}$

4	**1**	**11**	**10**

Each row is the cyclic shift of the row above
…
with a special wrapping rule:
x wraps to –*x* mod 13 (→ $\mathbb{Z}_{13}[x]/\langle x^4+1\rangle$)

So I only need to tell you the first row.

Ring learning with errors problem

$$\mathbb{Z}_{13}[x]/\langle x^4 + 1 \rangle$$

	$4 + 1x + 11x^2 + 10x^3$	**random**
$\times$	$6 + 9x + 11x^2 + 11x^3$	**secret**
$+$	$0 - 1x + 1x^2 + 1x^3$	**small noise**
$=$	$10 + 5x + 10x^2 + 7x^3$	

Ring learning with errors problem

$\mathbb{Z}_{13}[x]/\langle x^4+1\rangle$

	$4 + 1x + 11x^2 + 10x^3$	**random**
×		**secret**
+		**small noise**
=	$10 + 5x + 10x^2 + 7x^3$	

Computational ring-LWE problem: given **blue**, find **red**

Basic ring-LWE-DH key agreement

- Reformulation of Peikert's ring-LWE KEM (*PQCrypto 2014*)

public: "big" a in $R_q = \mathbf{Z}_q[x]/(x^n+1)$

Alice

secret:
random "small" s, e in R_q

Bob

secret:
random "small" s', e' in R_q

$b = a \cdot s + e$ →

← $b' = a \cdot s' + e'$

Alice

shared secret:
$s \cdot b' = s \cdot (a \cdot s' \cdot e') \approx s \cdot a \cdot s'$

Bob

shared secret:
$b \cdot s' \approx s \cdot a \cdot s'$

These are only approximately equal ⇒ need rounding

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		NXP PQC [A]		Slower	Smaller
		Runtime	RAM	Runtime	RAM	Runtime	RAM
Dilithium-2	Sign	19 ms	50 kB	61 ms	5 kB	3.2x	10.0x
	Verify	7 ms	11 kB	16 ms	3 kB	2.3x	3.7x
Dilithium-3	Sign	31 ms	69 kB	119 ms	7 kB	3.8x	9.9x
	Verify	12 ms	10 kB	29 ms	3 kB	2.4x	3.3x
Dilithium-5	Sign	42 ms	123 kB	168 ms	8 kB	4.0x	15.4x
	Verify	21 ms	12 kB	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

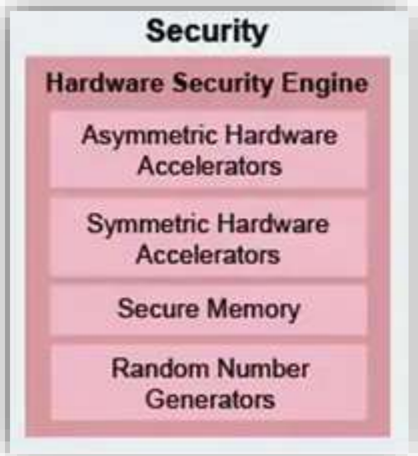
[A] NXP PQC: Bos, J.W., Renes, J. and Sprenkels, A., 2022. Dilithium for memory constrained devices. In International Conference on Cryptology in Africa (pp. 217-235)

Example of what we do at NXP

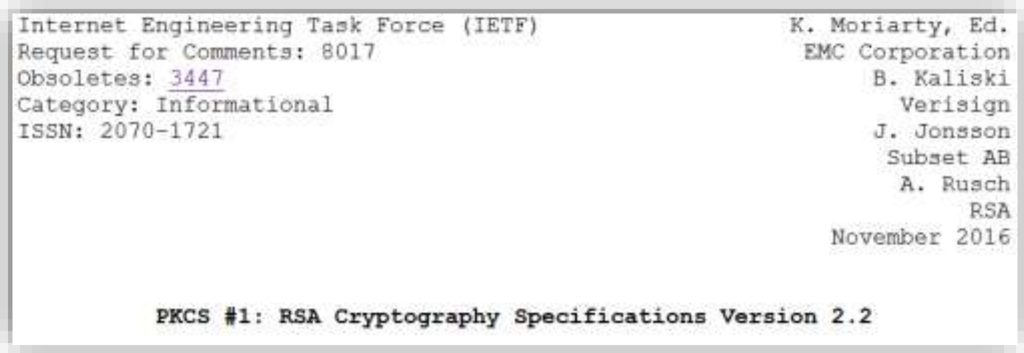
Joppe W. Bos, Joost Renes and Christine van Vredendaal: *Polynomial Multiplication with Contemporary Co-Processors: Beyond Kronecker, Schönhage-Strassen & Nussbaumer*. USENIX Security Symposium 2022.

Implementing Classical cryptography

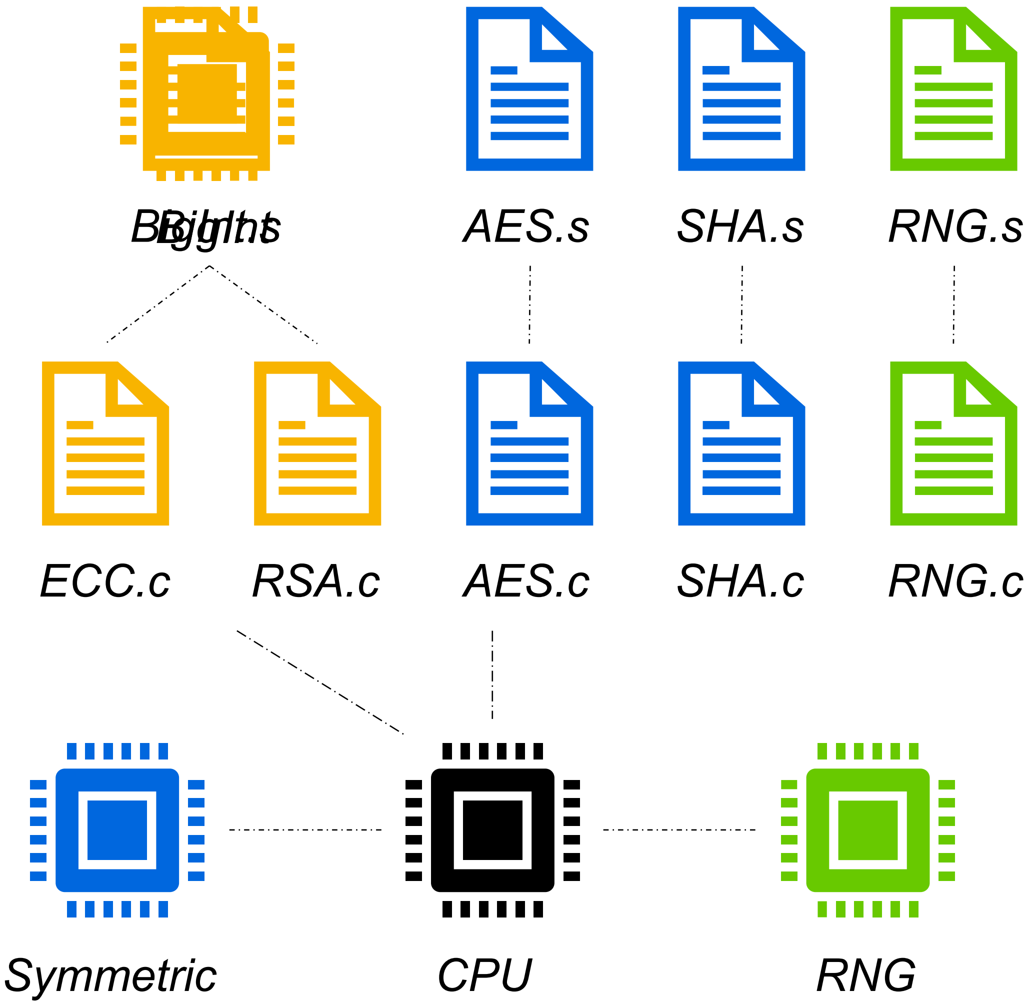

NIST
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER
PUBLICATIONS
FIPS 186-5 (Draft)
Digital Signature Standard (DSS)



S32G2 automotive processor spec

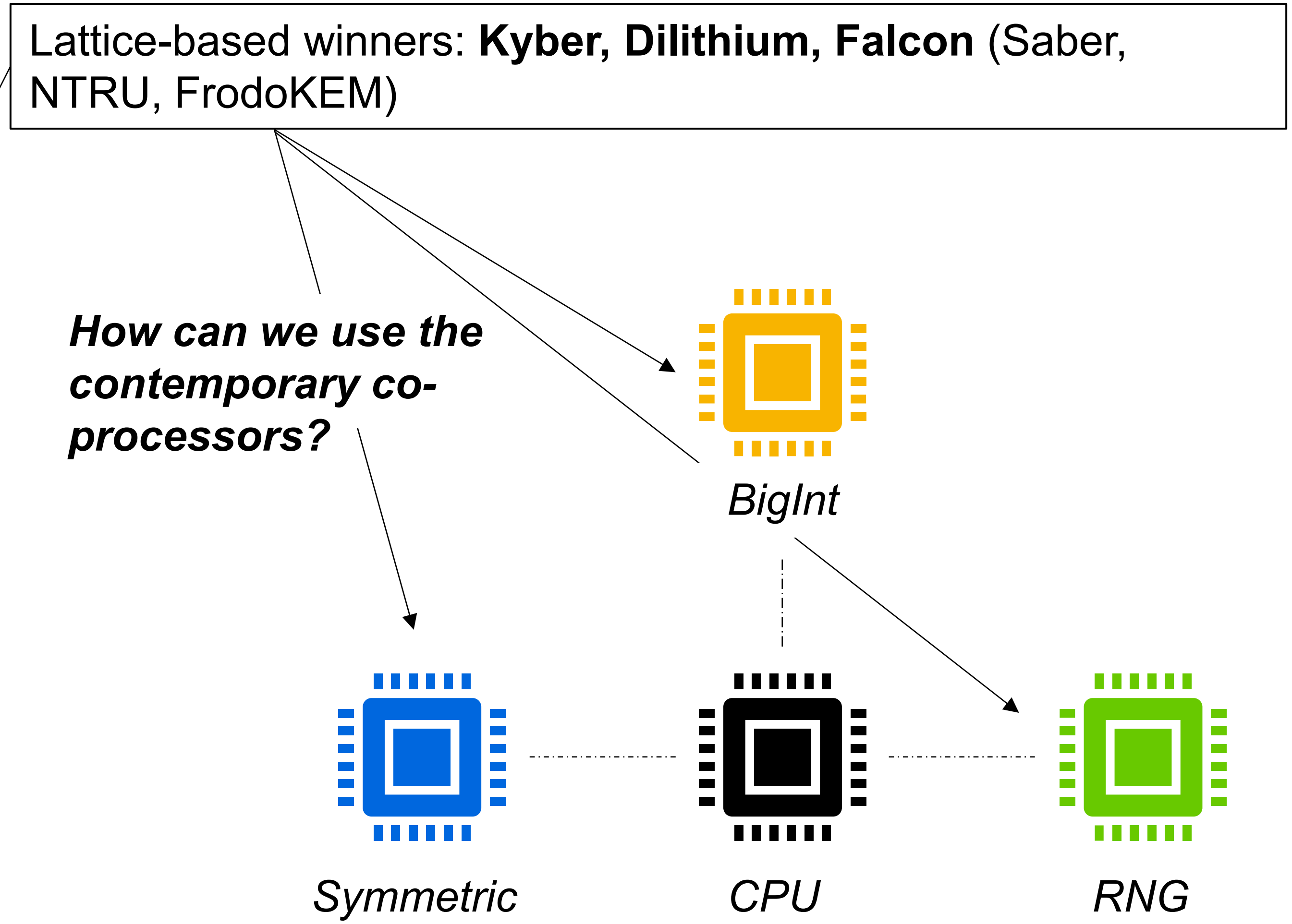

Internet Engineering Task Force (IETF) K. Moriarty, Ed.
Request for Comments: 8017 EMC Corporation
Obsoletes: 3447 B. Kaliski
Category: Informational Verisign
ISSN: 2070-1721 J. Jonsson
Subset AB
A. Rusch
RSA
November 2016

PKCS #1: RSA Cryptography Specifications Version 2.2



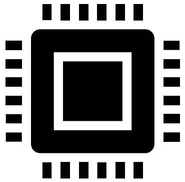
1. https://www.nxp.com/products/processors-and-microcontrollers/arm-processors/s32g-vehicle-network-processors:S32G-PROCESSORS

Implementing post-quantum cryptography



Re-using existing HW

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 chips

Can we use this?

Kronecker substitution

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

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

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

✖

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

Kronecker domain (with evaluation point 100)

$$f(100) = 4030201$$

$$g(100) = 8070605$$

✖

$$fg(100) = 32526160341605$$

Polynomial multiplication techniques

Kronecker evaluation at 2^{32}

Multiplication with a 256-bit multiplier

$$\frac{\mathbb{Z}[X]}{(X^{256}+1)} \xrightarrow{\text{Kronecker}} \frac{\mathbb{Z}}{(2^{8192}+1)} \xrightarrow{\text{Schön.-Strassen}} \frac{\mathbb{Z}/(2^{544}+1)[X]}{(X^{32}+1)}$$

$$\frac{\mathbb{Z}[Y]/(Y^{8}+1)[X]}{(X^{32}-Y)} \xrightarrow{\text{Kronecker}} \frac{\mathbb{Z}/(2^{256}+1)[X]}{(X^{32}-2^{32})} \xrightarrow{\text{Twist}} \frac{\mathbb{Z}/(2^{256}+1)[X]}{(X^{32}-1)}$$

Nussbaumer

$$\frac{\mathbb{Z}[Y]/(Y^{8}+1)[X]}{(X^{64}-1)} \xrightarrow{\text{Kronecker}} \frac{\mathbb{Z}/(2^{256}+1)[X]}{(X^{64}-1)}$$

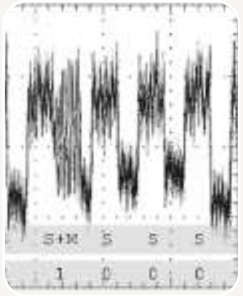
Kronecker+

Algorithm	# Muls	# Bits
Kron. + Schoolbook	1024	256
Kron. + Karatsuba	243	256
Kron. + Toom-Cook	63	256
Kron. + Schön.-Strassen	32	544
Nussbaumer + Kron.	64	256
Kronecker+	**32**	**256**

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

[B] Harvey. Faster polynomial multiplication via multipoint Kronecker substitution. J. of Sym. Comp. 2009.

Resistance against physical & logical attacks

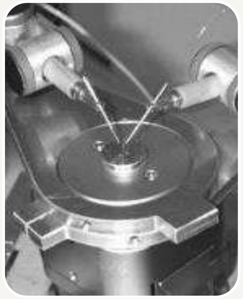


Side-channel attacks

- Power analysis (SPA, DPA)
- Electromagnetic analysis (SEMA, DEMA)
- Timing Analysis
- Photo-emission microscopy (high-end)
- Profiled, unprofiled and ML-assisted variants

Fault injection attacks

- Voltage or clock glitching
- Electromagnetic fault injection (EMFI)
- Body bias injection
- Laser fault injection
- Single and multi-shot scenarios



Invasive attack

- Focused Ion Beam (FIB) modifications
- Micro/Nano-probing of internal signals
- Signal forcing
- Delayering
- Reverse-engineering

Embedded cryptography and implementation attacks

Attacks

Deep understanding in both academia and industry.

Classic Cryptography

AES 3DES
DSA… ECDSA
RSA ECC

Countermeasures

Practically secure and certified implementations.

Embedded cryptography and implementation attacks

Attacks

Deep understanding in both academia and industry.

Classic Cryptography

AES 3DES
DSA… ECDSA
RSA ECC

Countermeasures

Practically secure and certified implementations.

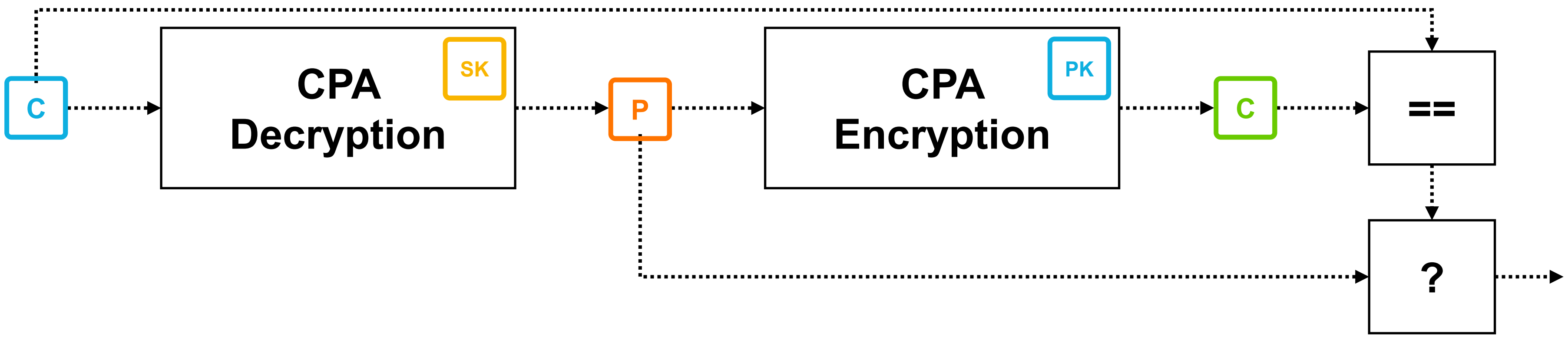
Post-Quantum Cryptography

Active research area resulting in increasingly powerful attacks.

Kyber
Dilithium …
SPHINCS+
XMSS

Early stage of academic research. Limited industrial results.

Fujisaki Okamoto transform



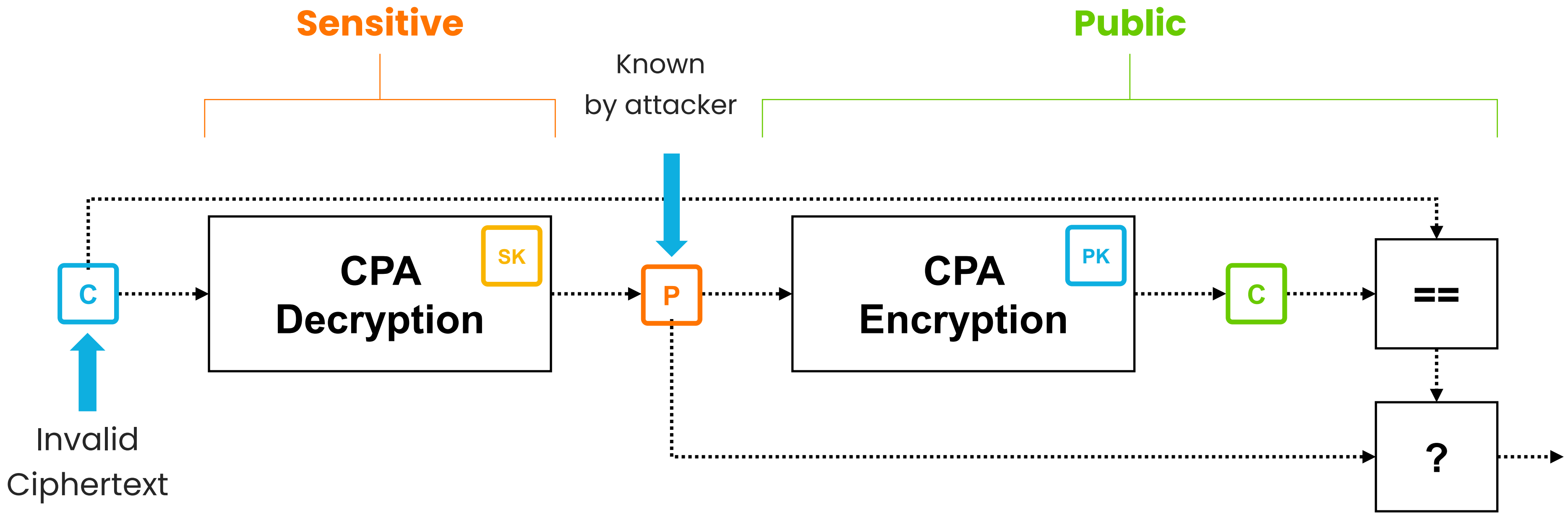
Transform a scheme which achieves **IND-CPA** ("chosen plaintext attack") security to reach **IND-CCA** ("indistinguishability against chosen-ciphertext attacks") security

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**



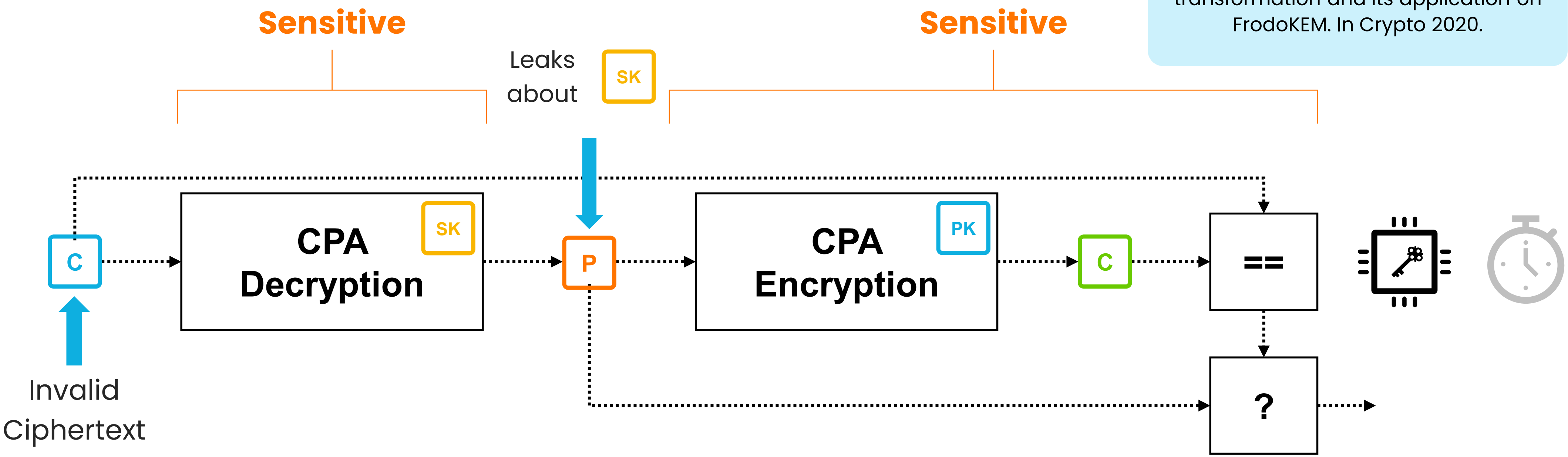
The SCA Problem of the FO-Transform

Attack 2: Chosen Ciphertext

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

P is potentially sensitive

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.



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 !

[A] Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process

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

SAFE ASSURE™ by NXP

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

- We are always looking for talented people in math / crypto!
- Need to have an applied interest as well.
- New mathematical techniques to map algorithms to resource constrained devices.

- Software / hardware skills are a plus
- Crypto / number theory knowledge is a must!

Experience shows it is easier to teach software development skills to an applied mathematician than number theory to an engineer ☺

Interested? Job? Internship? Industry PhD with KU Leuven?

Contact me: joppe.bos@nxp.com

Get in touch!

Joppe W. Bos
joppe.bos@nxp.com

nxp.com

NXP

Brighter Together