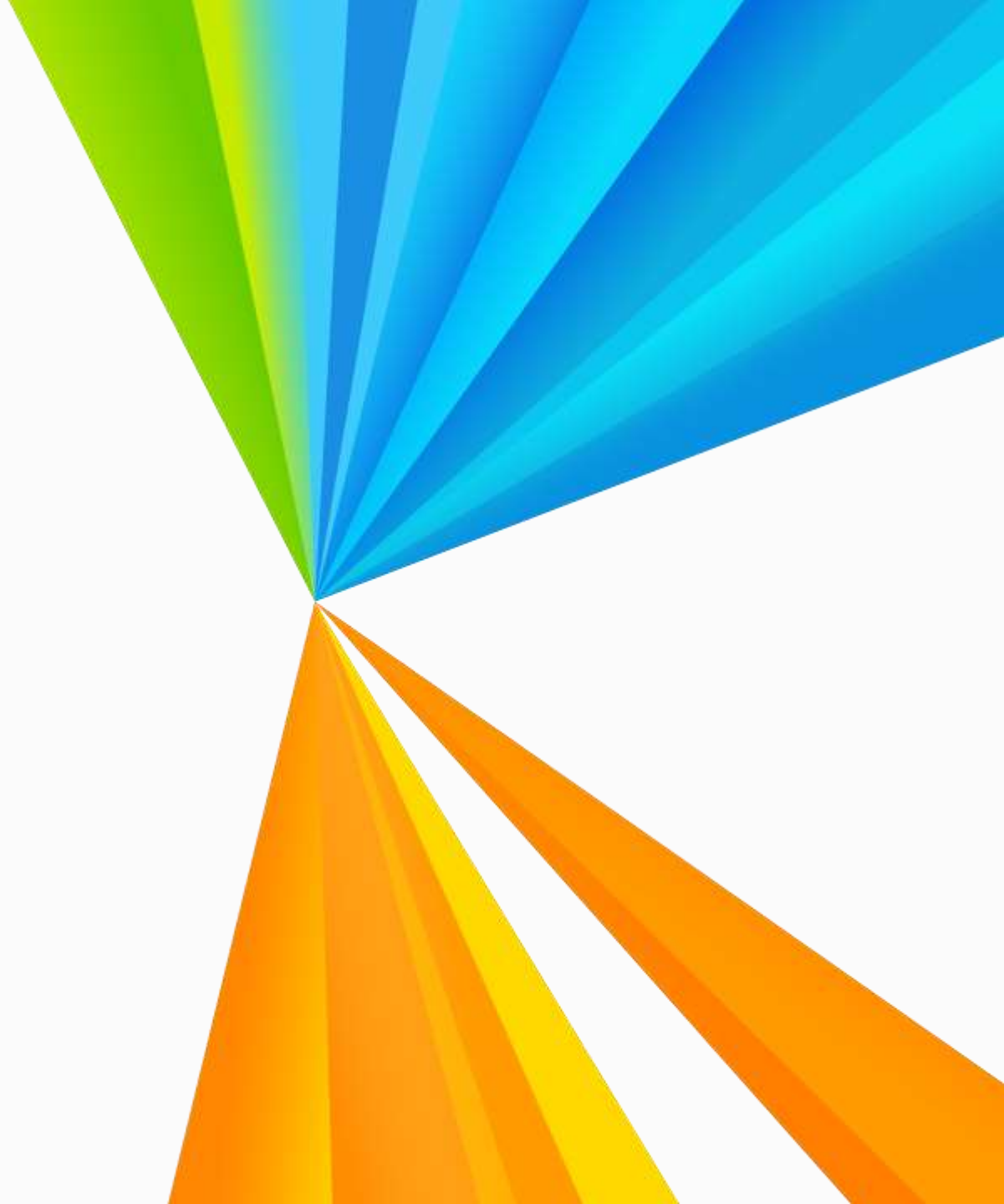


Embedded Post-Quantum Cryptography

Joppe W. Bos

Technical Director, CCC&S, CTO
March 2024

Physics and Security
From Random Numbers to Secure Communication

Agenda

NXP

PQC: General Introduction

- Quantum Threat
- Post-Quantum Cryptography (PQC)
- Standardization & Migration
- LWE 101

PQC: Embedded Use-cases

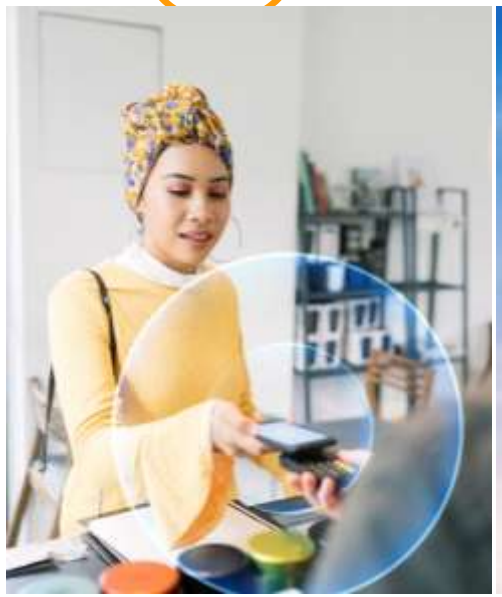
- HW Re-Use
- Memory challenges
- Automotive

SECURE CONNECTIONS FOR A SMARTER WORLD

Our digitally enhanced world is evolving to anticipate and automate

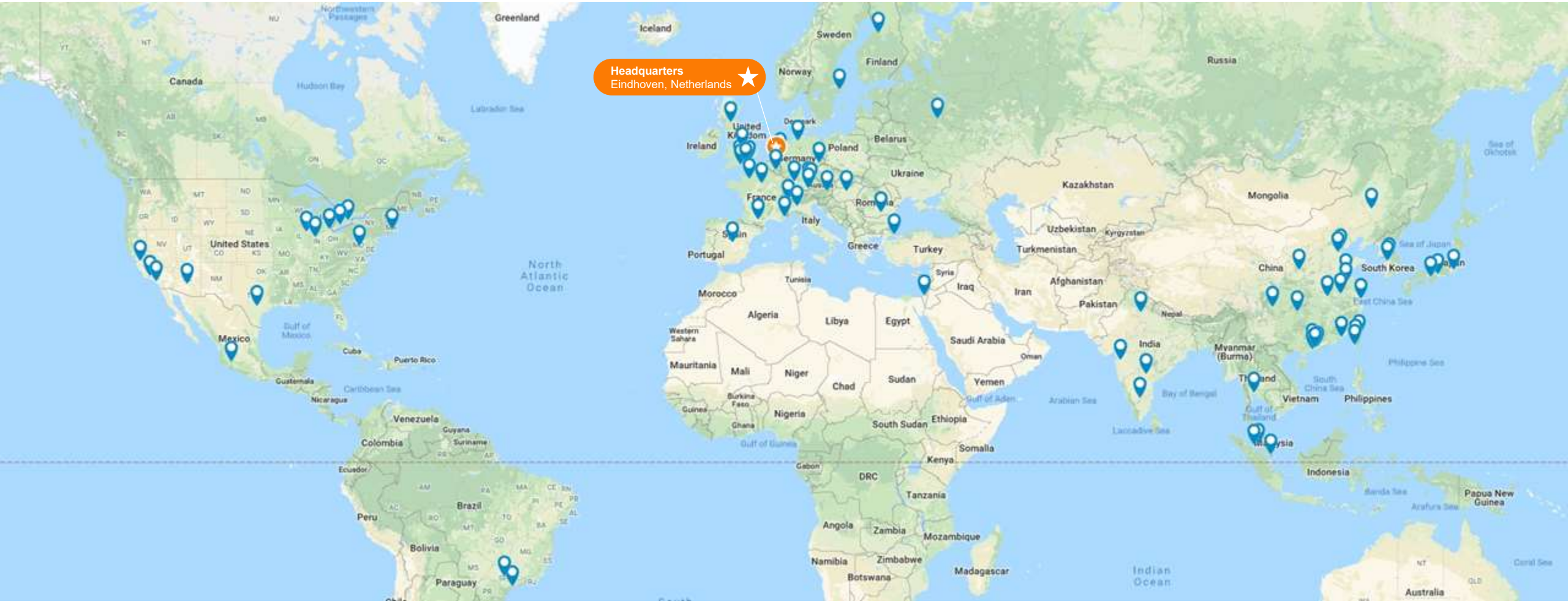
NXP Semiconductors N.V. (NASDAQ: NXPI) enables a smarter, safer and more sustainable world through innovation. As the world leader in secure connectivity solutions for embedded applications, NXP is pushing boundaries in the automotive, industrial & IoT, mobile, and communication infrastructure markets.



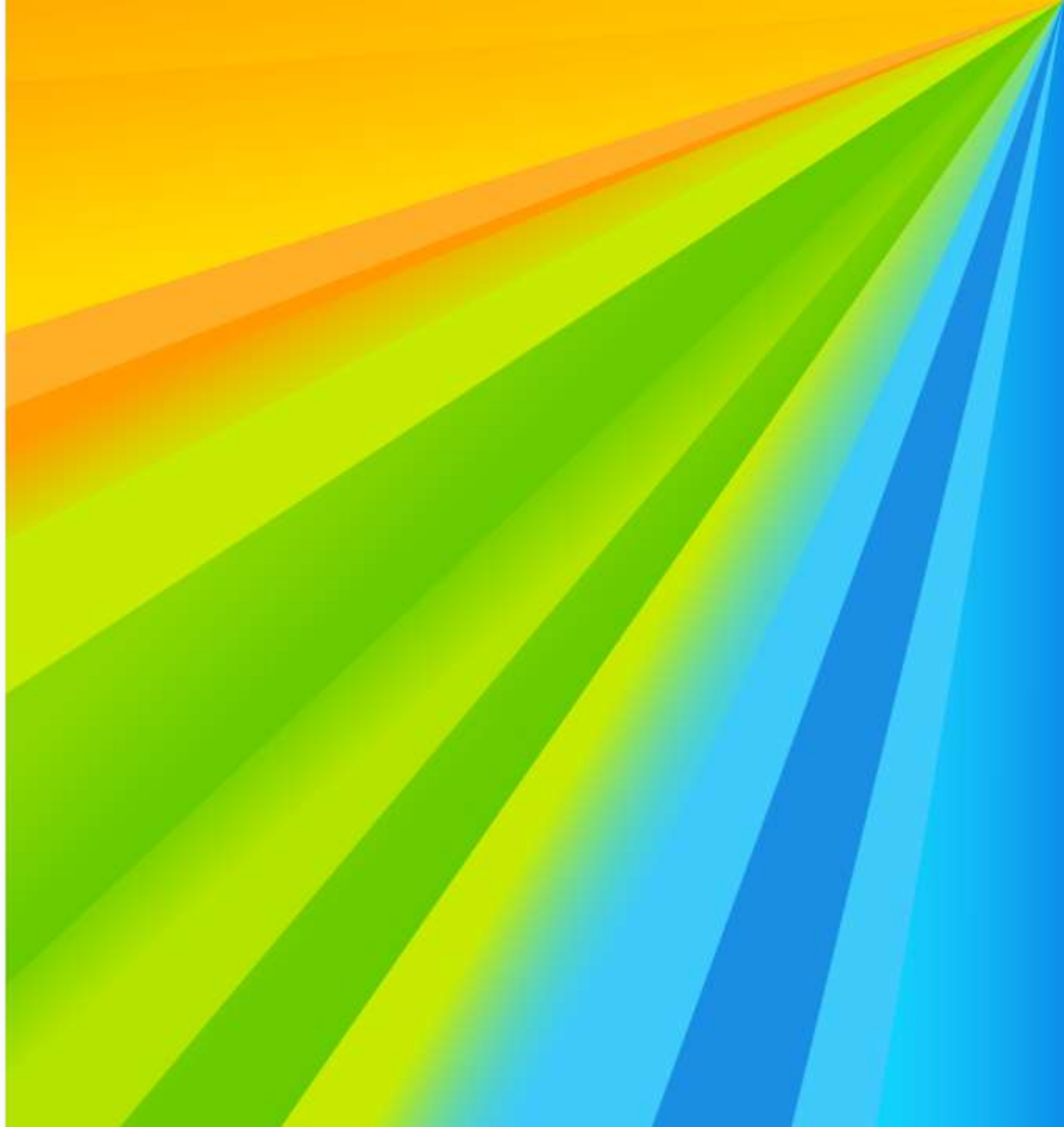


NXP Locations

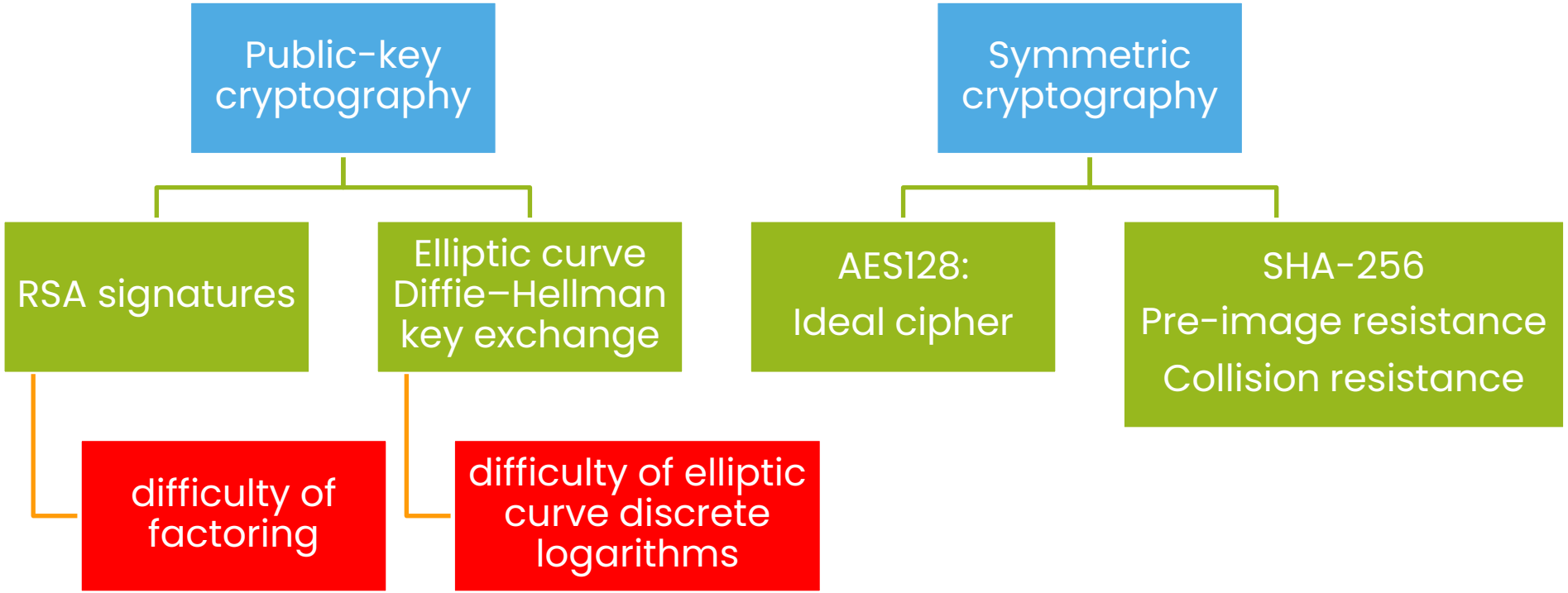
~34,000 employees with operations in more than 30 countries



PQC:
General Introduction

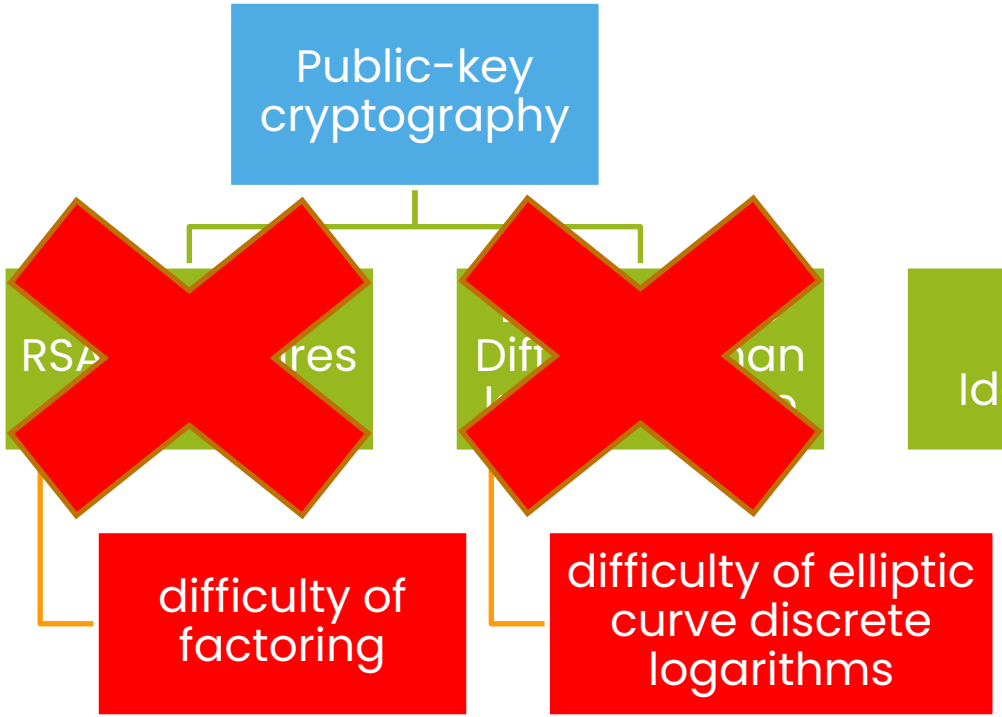


Contemporary Cryptography
TLS-ECDHE-RSA-AES128-GCM-SHA256

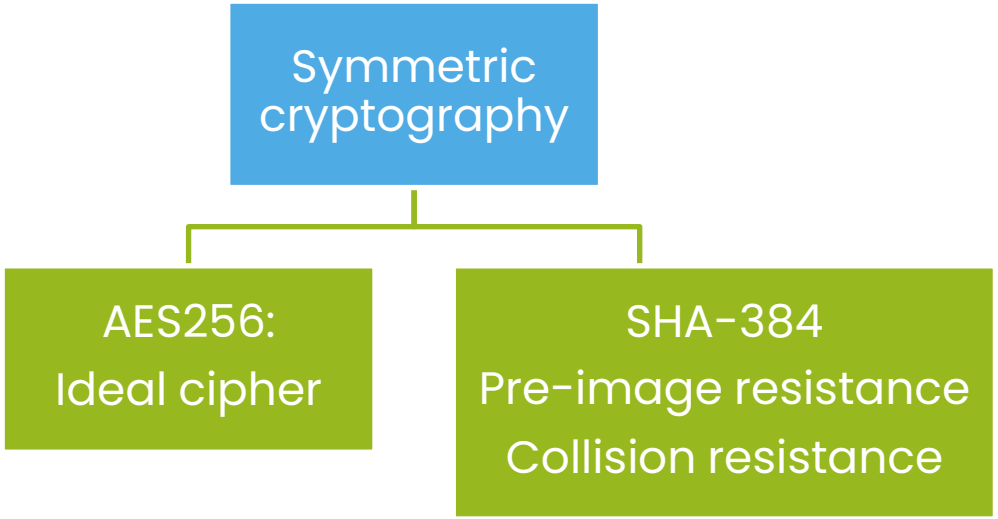


Contemporary cryptography
TLS-~~ECDHE-RSA~~-AES256-GCM-SHA384

"Double" the key sizes



Shor's algorithm (1994)



Grover's algorithm (1996)

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 Migration Drivers

Standards

Prävention Detektion Reaktion

NIST

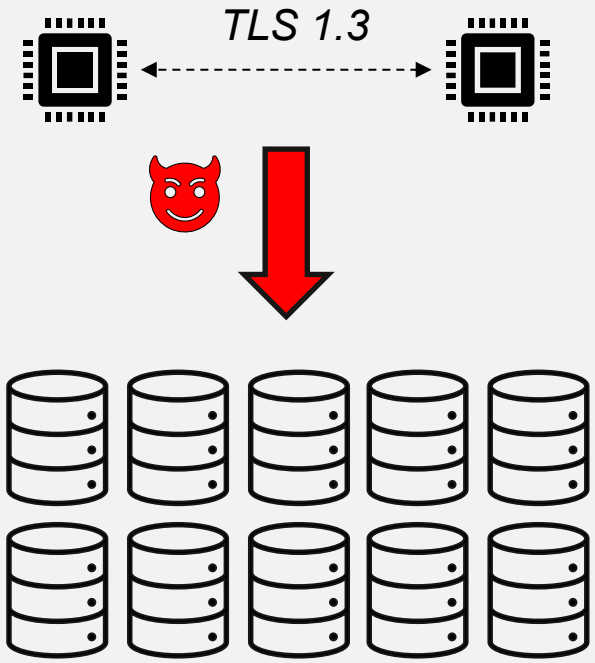
NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA

International Organization for Standardization ISO

ANSSI

Crypto Agility

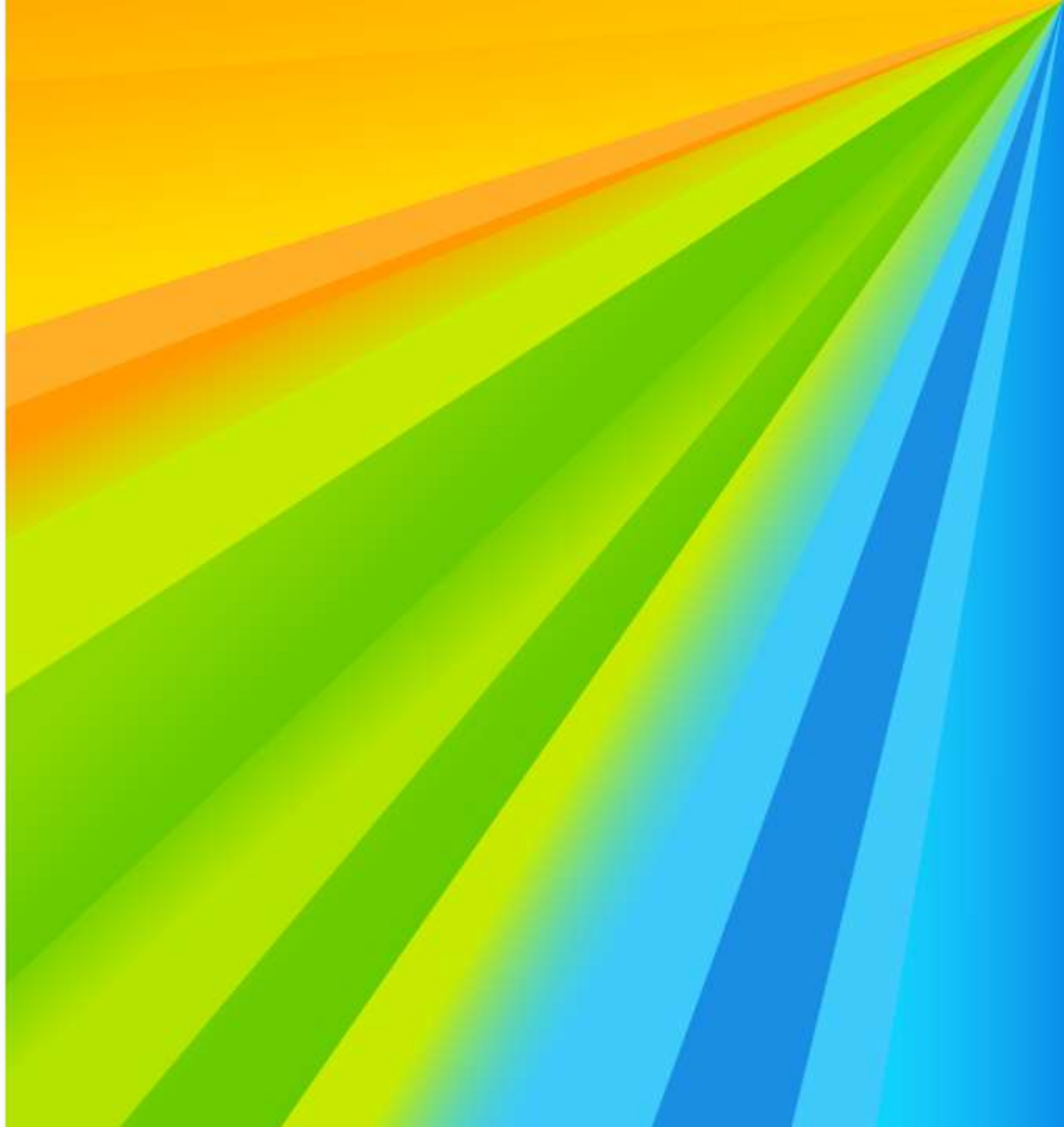
Store now decrypt later



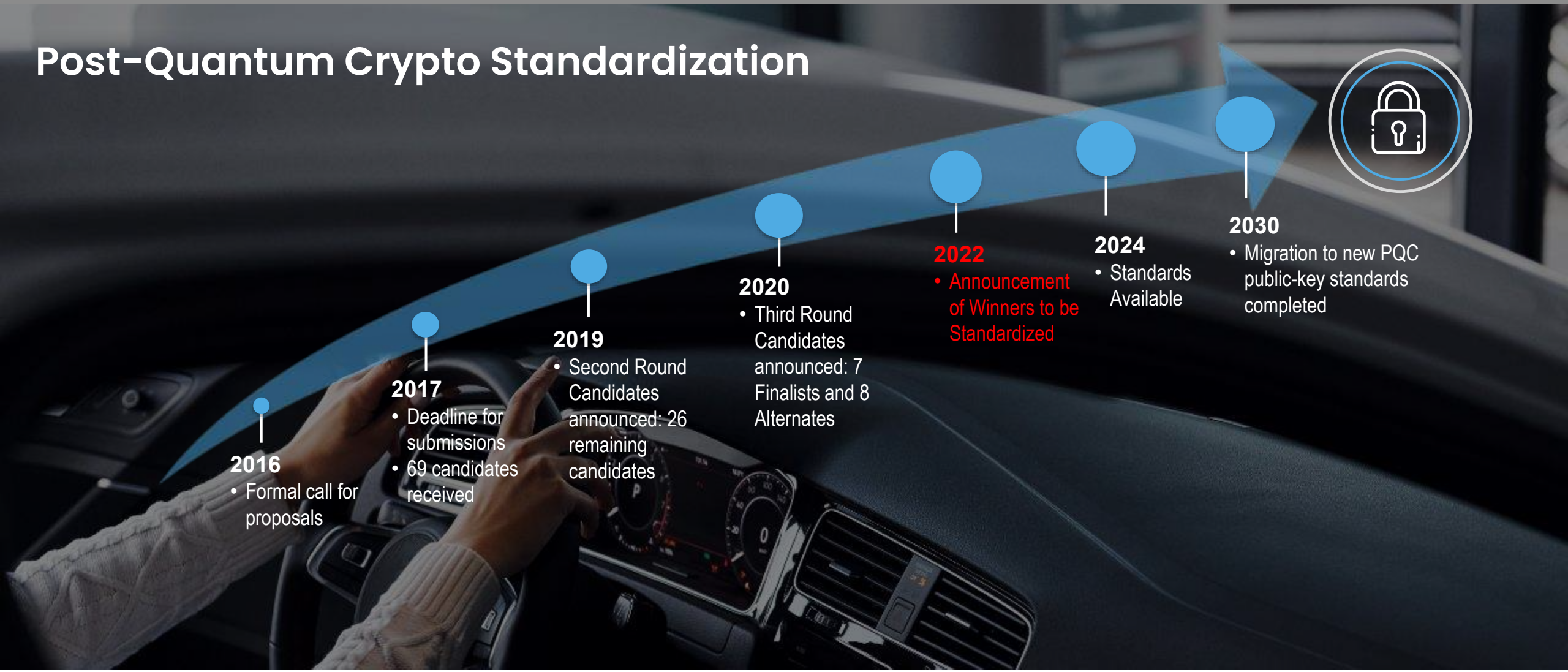
Post-Quantum Crypto Standards Are Coming

It doesn’t matter if you believe in quantum computers or not

PQC Standards



Post-Quantum Crypto Standardization



NIST
National Institute of Standards and Technology

PQC STANDARDS – NIST

Winners

- CRYSTALS-Kyber
- CRYSTALS-Dilithium

Secondary Winners

- Falcon
- SPHINCS+

Round 4 Candidates

- HQC
- BIKE
- Classic McEliece
- SIKE

Digital Signature Competition

Proposals June '23: 40 "complete & proper" submissions

2024 | 2025? | 2028? | 2030?

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

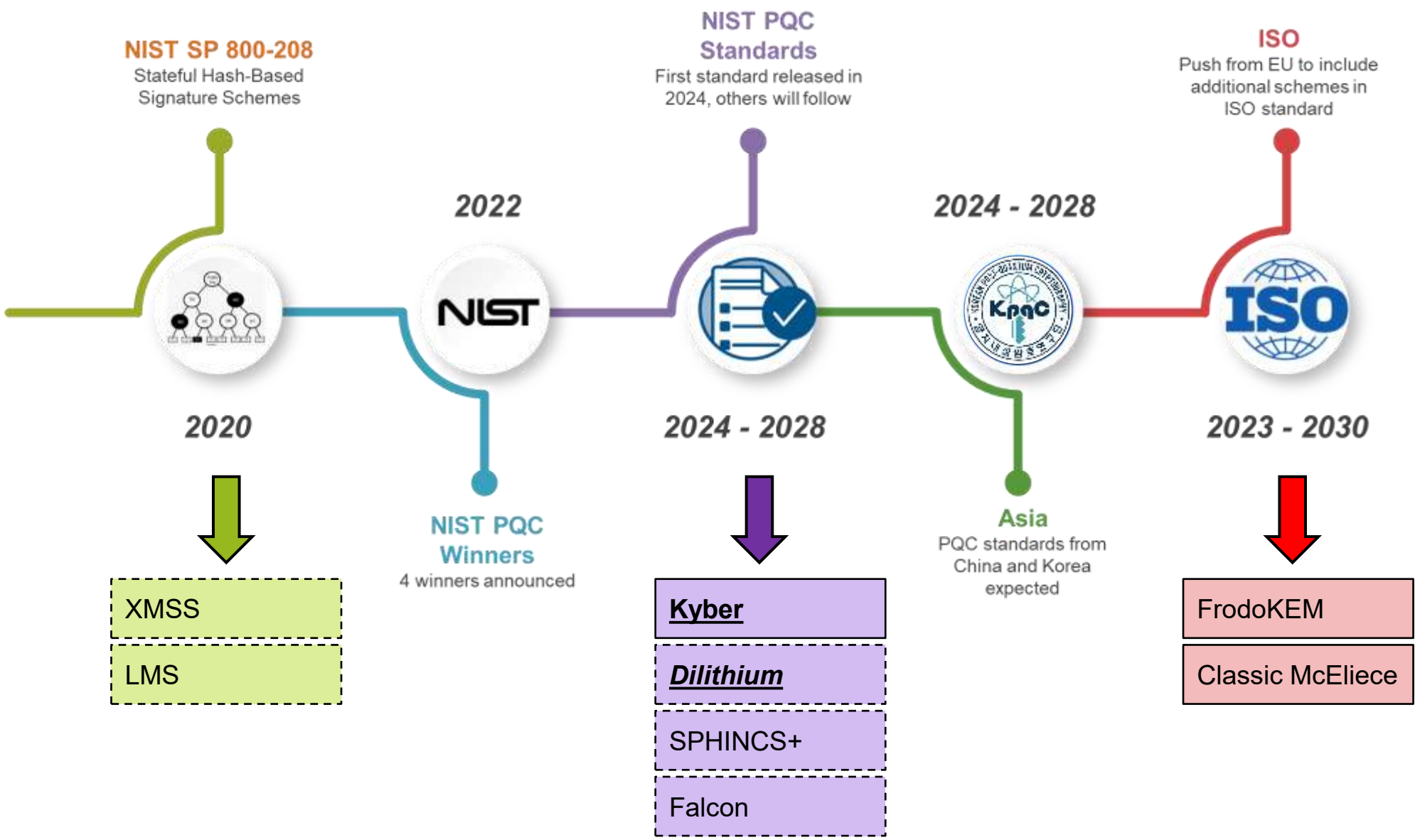
PQC Standard #2 (Digital Signatures)

Color key: Mathematical approach — Lattice | Hash | Code

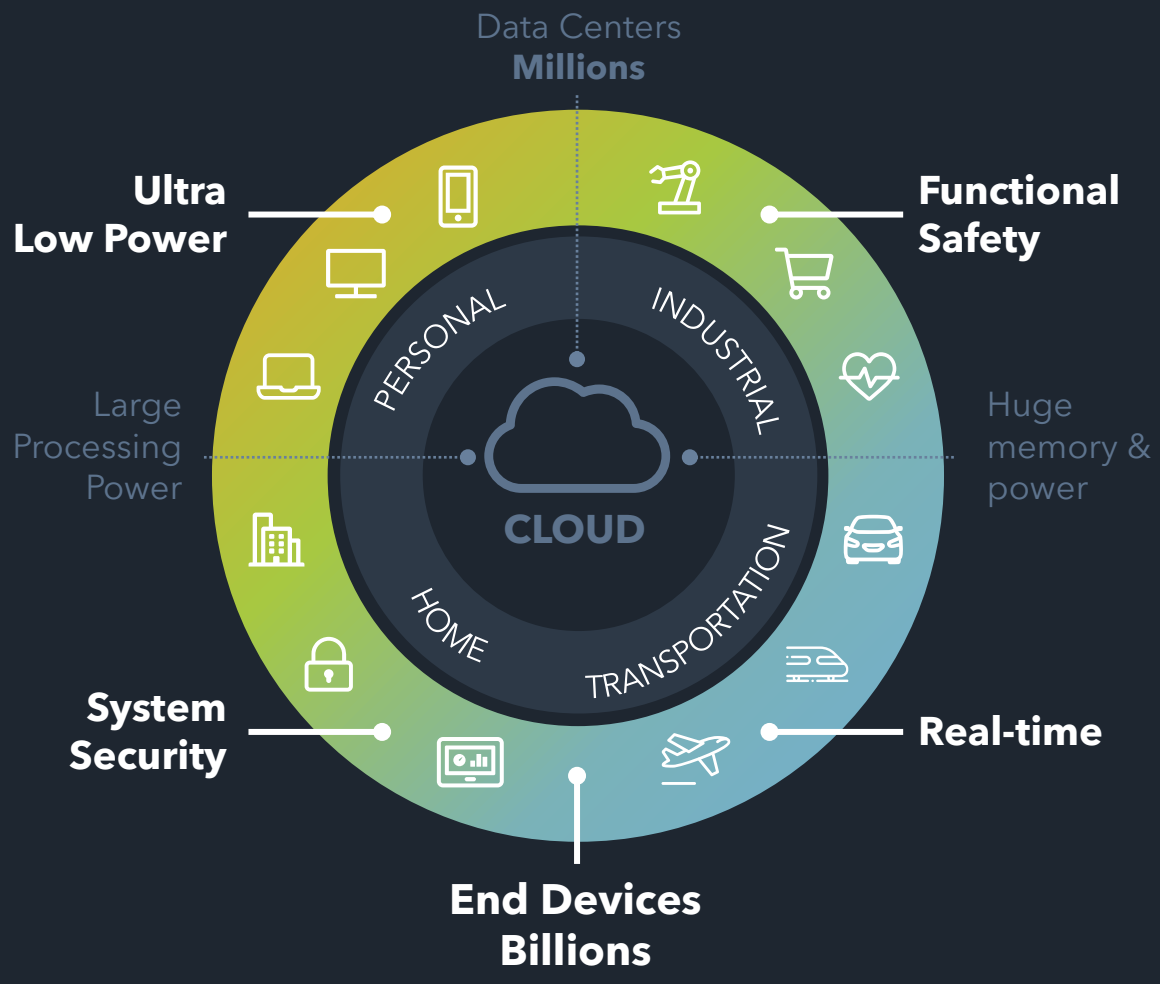
Algorithm selection

Key Exchange

Digital signature



Impact of PQC on embedded 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

Bandwidth & Power

Larger signatures (up to 4.6KB) → more bandwidth required → increase in power usage

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

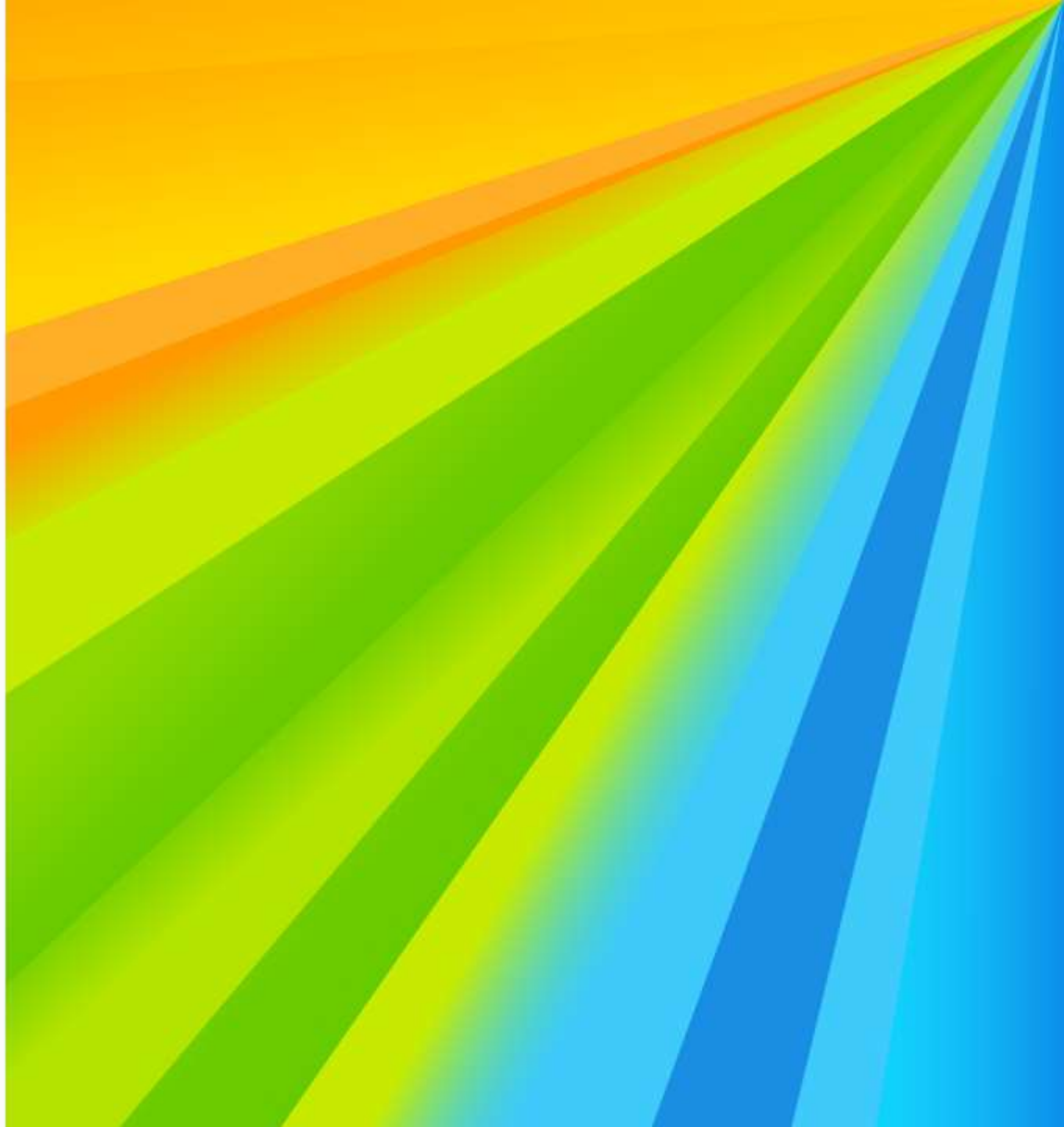
Germany (BSI)

- 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

Learning with Errors



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

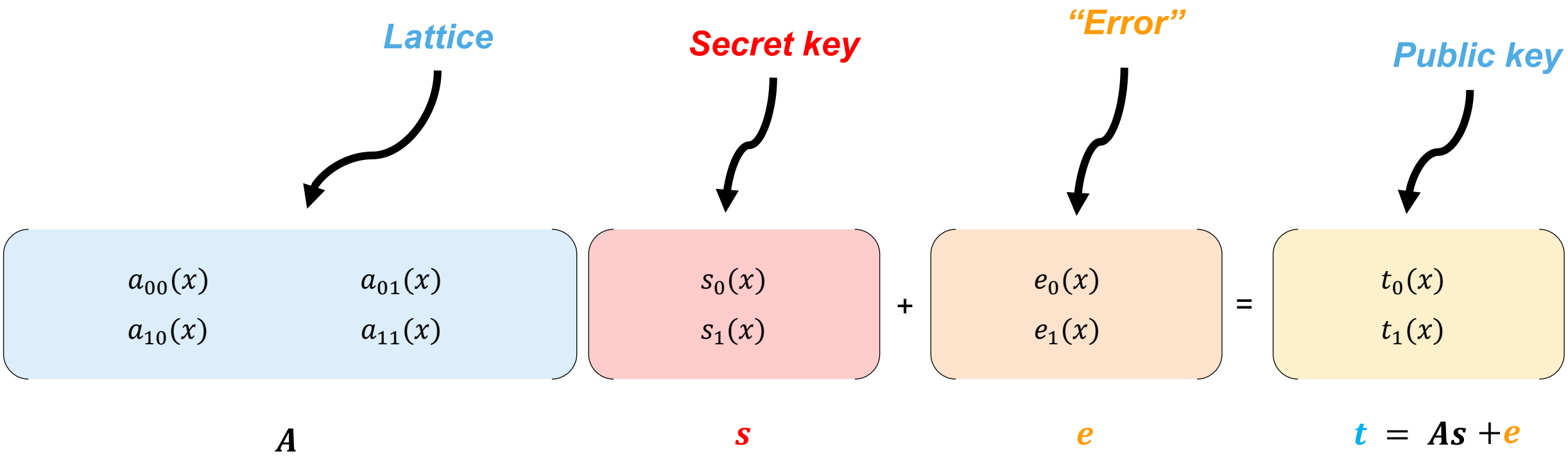
- Module Learning with Errors
- Number-Theoretic Transformations

Many new techniques to deal with!

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

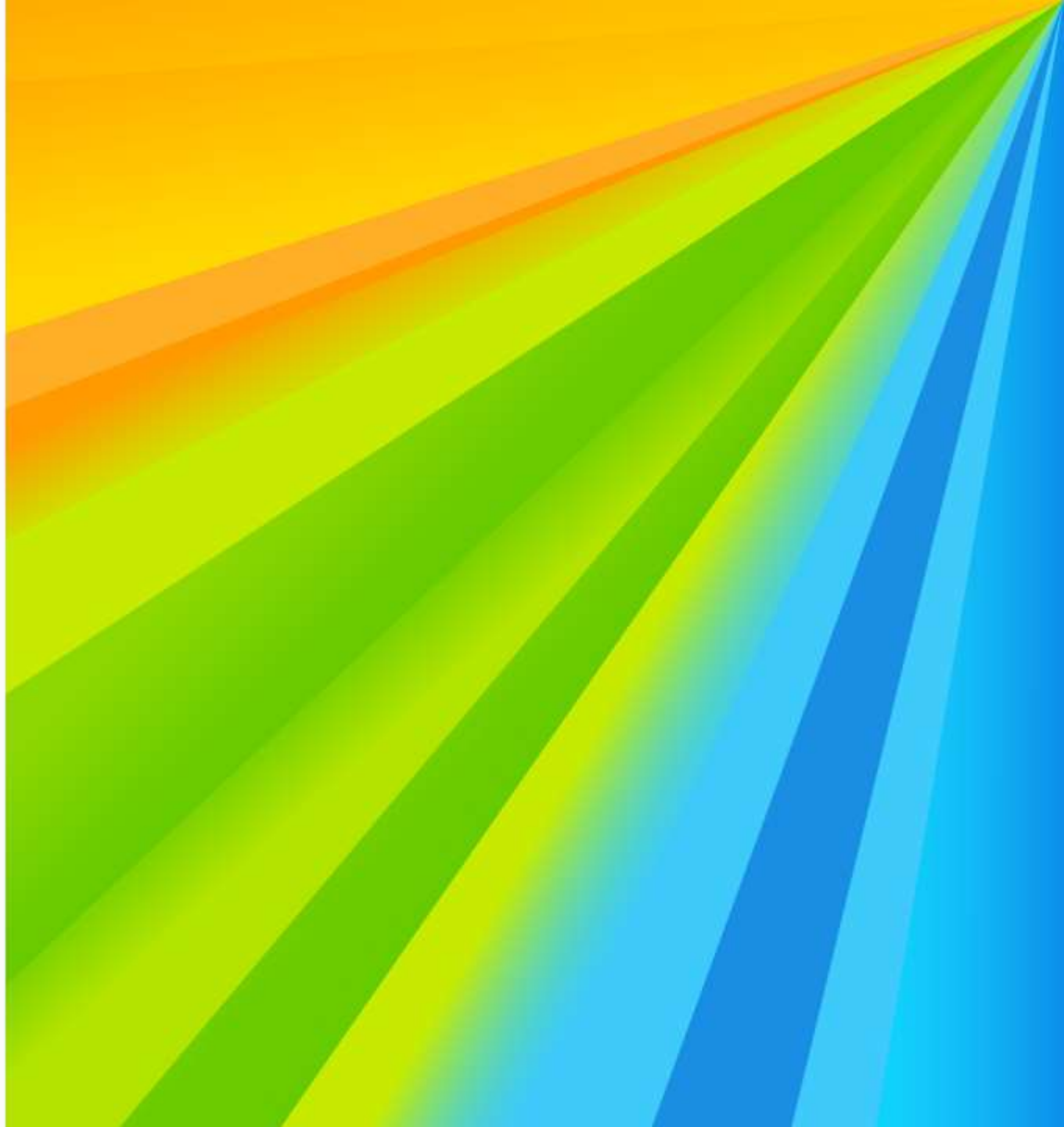
Dilithium uses 'Rejection Sampling' as a core component for producing signatures

module (ring) Learning with errors



Given **blue**, find **red** or **yellow**

PQC & HW Re-Use



IMPLEMENTING CLASSICAL CRYPTOGRAPHY

NIST

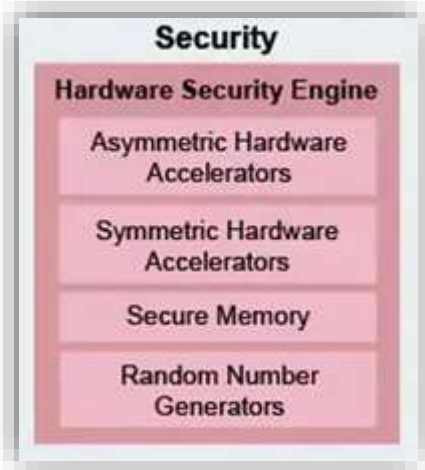
Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

PUBLICATIONS

FIPS 186-5 (Draft)

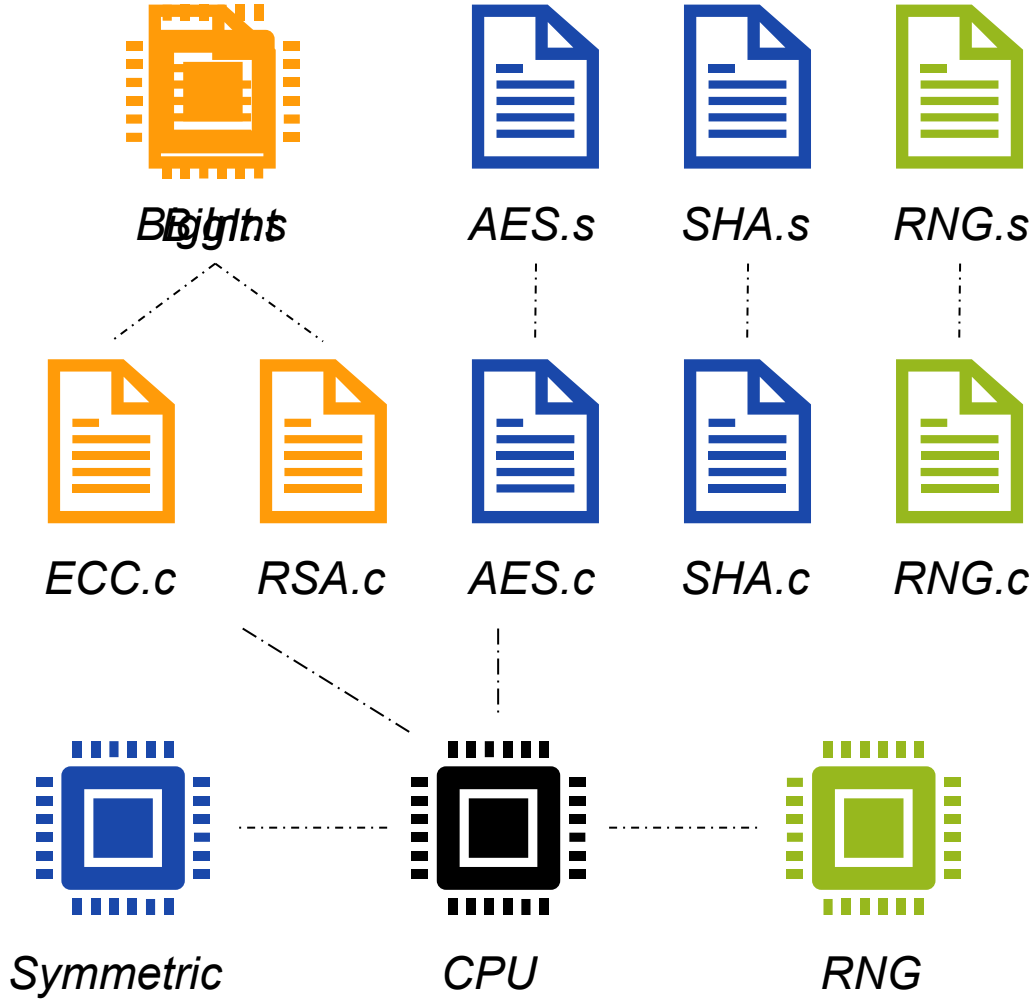
Digital Signature Standard (DSS)



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

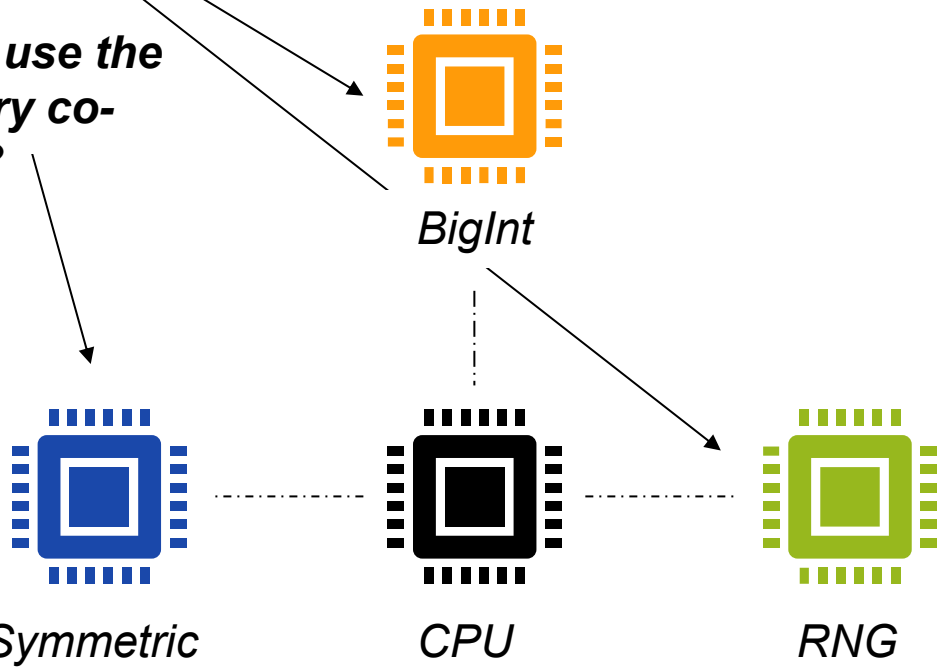


1. https://www.nxp.com/products/processors-and-microcontrollers/arm-processors/s32g-vehicle-network-processors:S32G-PROCESSORS

IMPLEMENTING POST-QUANTUM CRYPTOGRAPHY

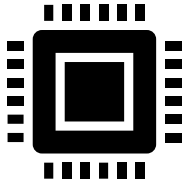
Lattice-based winners: **Kyber, Dilithium, Falcon**

How can we use the contemporary co-processors?

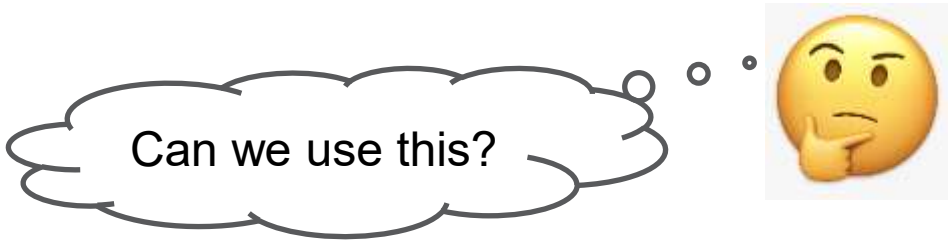


RE-USING EXISTING HW

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



Kronecker substitution

Polynomial domain

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

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

✖

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

Grundzüge einer arithmetischen Theorie der algebraischen Grössen.

(Von *L. Kronecker.*)

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

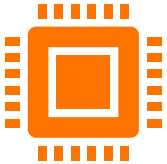
Kronecker domain (with evaluation point 100)

$$f(100) = 4030201$$

$$g(100) = 8070605$$

✖

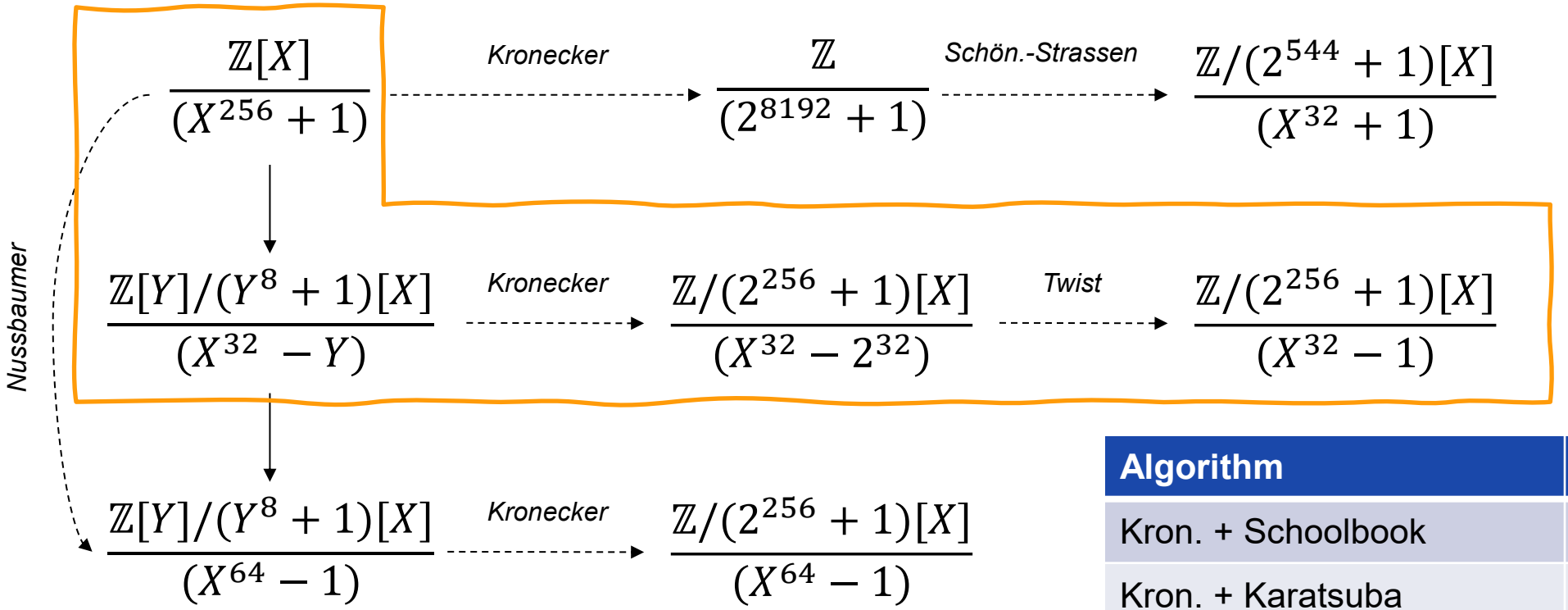
$$fg(100) = 32526160341605$$



POLYNOMIAL MULTIPLICATION TECHNIQUES

Kronecker evaluation at 2^{32}

Multiplication with a 256-bit multiplier

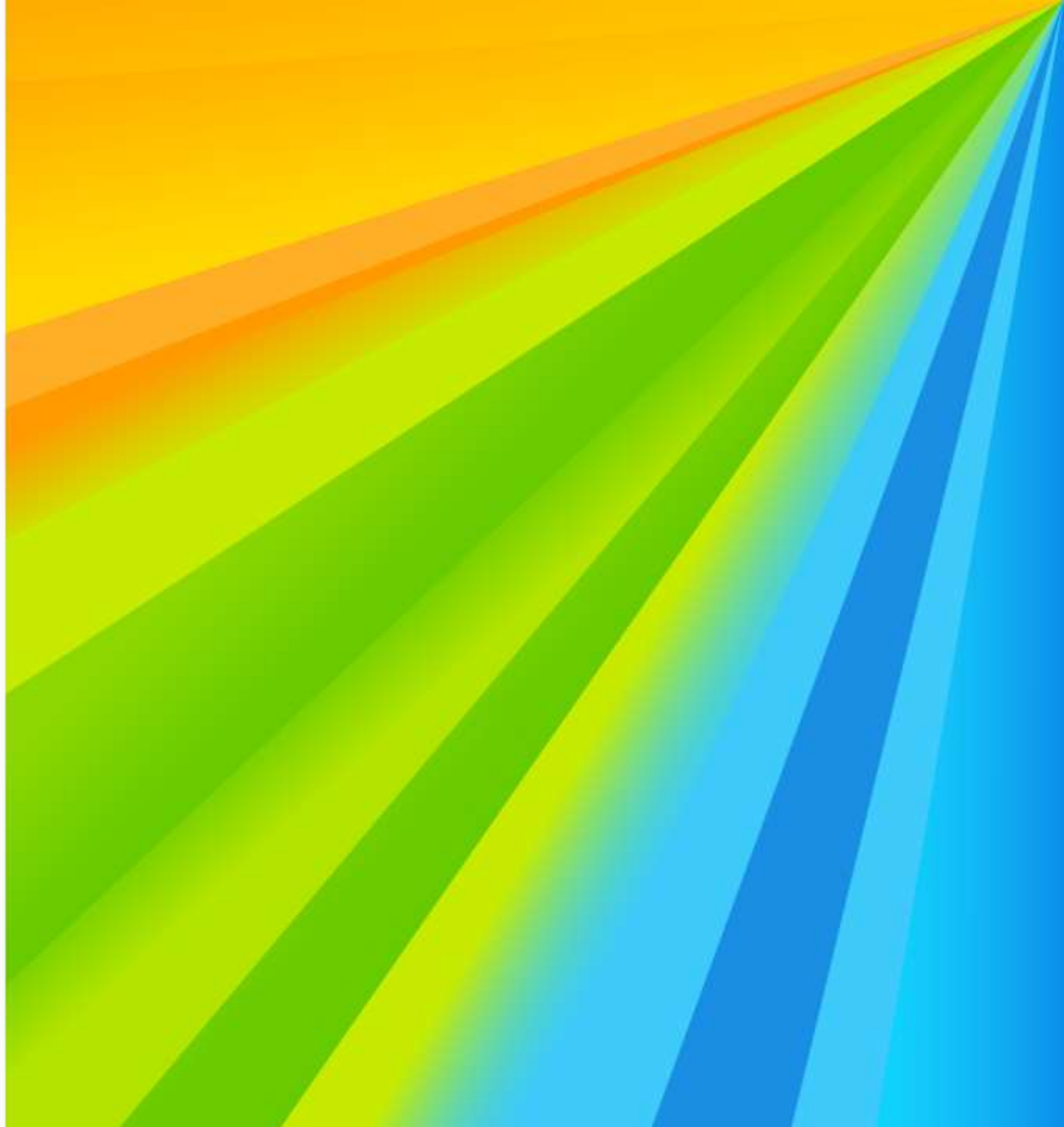


Kronecker+

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**

- Harvey. Faster polynomial multiplication via multipoint Kronecker substitution. J. of Sym. Comp. 2009.
- Albrecht, Hanser, Hoeller, Pöppelmann, Virdia, Wallner; Implementing RLWE-based schemes using an RSA co-processor. TCHES 2019
- Bos, Renes, van Vredendaal: Polynomial Multiplication with Contemporary Co-Processors: Beyond Kronecker, Schönhage-Strassen & Nussbaumer. USENIX 2022.

PQC Embedded Use Cases



SECURE ELEMENTS AND END-TO-END SERVICES

NXP propels today's on-the-go lifestyle with intelligent mobile solutions that safely connect consumers and their technology to the world around them.

SECURE ELEMENTS AND END-TO-END SERVICES

CUSTOM HIGH-PERFORMANCE INTERFACES

SMART VOICE, AUDIO, AND HAPTIC SOLUTIONS

EFFICIENT CHARGING SOLUTIONS

DEFINING WHAT'S NEXT FOR MOBILE PHONES

NXP has been driving the mobile wallet expansion, advancing analog and charging solutions add more capabilities to mobile phones, notebooks, and tablets.

- NFC, eSE, eSIM, and UWB solutions
- Advanced analog solutions for personal computing
- Fast charging with USB Type-C

WEARABLES

Thanks to secure mobile payments, advanced audio solutions and tailored MCUs, wearables naturally blend into our lives.

- NFC+eSE mobile wallet solutions
- Highly integrated Arm® based MPUs and MCUs
- MiGLO™ NFMI radios for wireless audio

ACCESSORIES

NXP's anti-counterfeiting technology, among others products, support charging cables, power adapters, and wireless charging pads for mobile phones to help OEMs protect their brand and provides safety to their customers by making trusted accessories.




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}.

PQC KEM Migration

Algorithm (Level 3)	PQ Secure?	Standard?	Efficient Encaps	Efficient Decaps	Need hybrid?	SK (Bytes)	PK (Bytes)	Ciphertext (Bytes)
ECDH	No	SP 800-56A	Yes	Yes	N/A	32	32	N/A
Kyber	Yes	FIPS 203	Yes	Yes	Yes	2 400 B	1 184 B	1 088 B
FrodoKEM	Yes	ISO/IEC 18033-2	No	No	Yes	31 296 B	15 632 B	15 792 B
McEliece	Yes	ISO/IEC 18033-2	No	No	Yes	13 608 B	524 160 B	32 B

PQC signature migration

Dilithium (migration via hybrid with ECC/RSA) the best option if signing is required

Dilithium (no signer state, hybrid with ECC/RSA) or **LMS** (signer state, no hybrid) suitable for verify-only applications

Algorithm	PQ Secure?	Standard?	Efficient Signing?	Stateful?	Efficient Verification?	Hybrid?	Public Key Size (L3)	Signature size (L3)
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
LMS / XMSS	Yes	SP 800-208	No	Yes	Yes	No	60 B	1744 B

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
    See the talk by Elisabeth yesterday!

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