Crypto Agility for Industrial & IoT:

Challenges and Opportunities when Migrating to Post-Quantum Cryptography

Joppe W. Bos
Cryptographer & Technical Director (CC C&S, CTO)
March 2025

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."

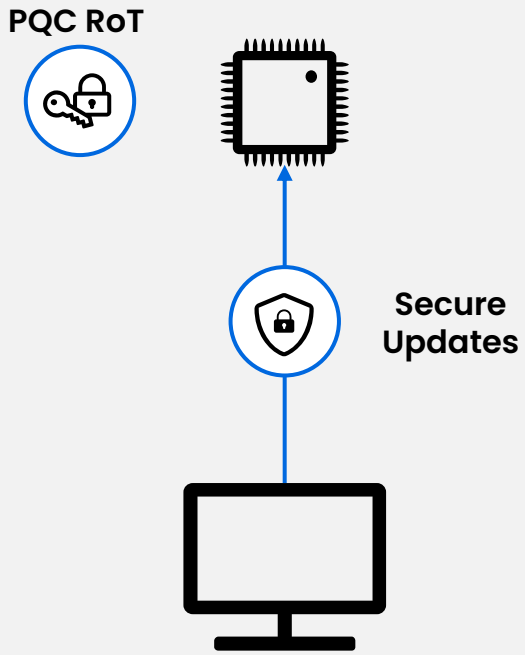
Post-Quantum Cryptography

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

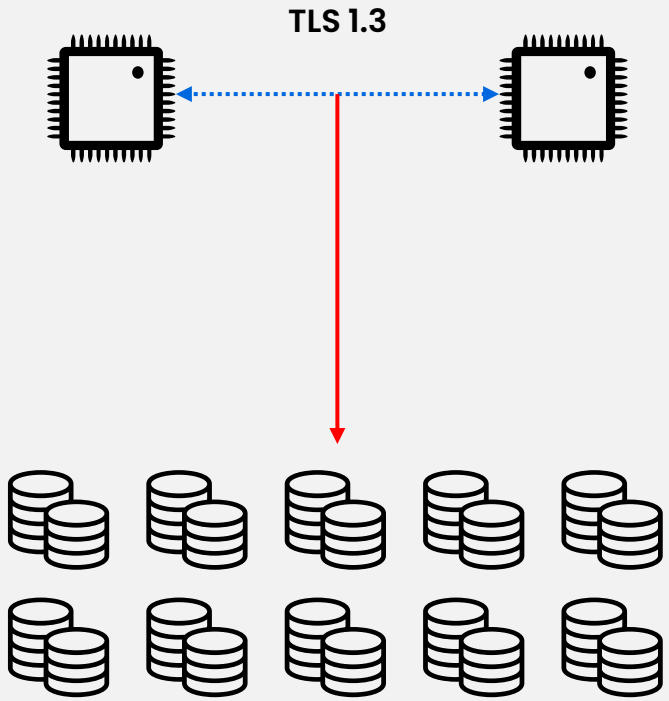
Is Post-Quantum Cryptography relevant for you?

Standards & Compliance

Crypto Agility



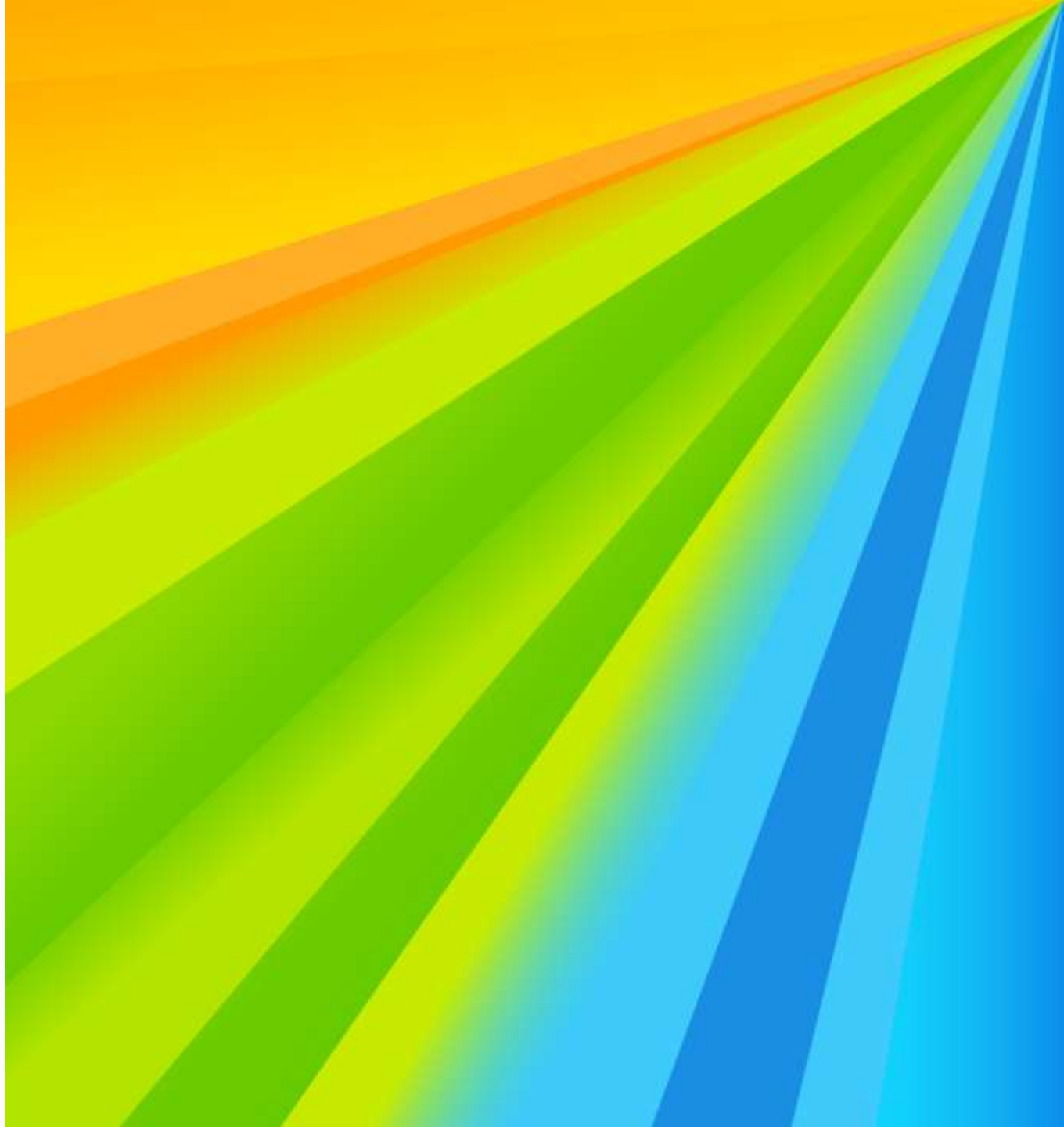
Store Now Decrypt Later



Post-quantum crypto standards are coming
It doesn't matter if you believe in quantum computers or not

More standards are not necessarily better

Lesson 1



PQC standards

Key Exchange

Digital Signature

NIST
SP 800-208
Stateful Hash-Based Signature Schemes

2020

XMSS

LMS

ML-KEM FIPS 203 (Kyber)

ML-DSA FIPS 204 (Dilithium)

SLH-DSA FIPS 205 (SPHINCS+)

2024

NIST PQC Standards

Further NIST PQC Standards
Round 4 KEM, Signature On-Ramp

FN-DSA FIPS 206 (Falcon)

Kpqc

NTRU+ | SMAUG-T

AIMer | HAETAE

2025-2028

Asia
More PQC standards from China and India expected

ISO
Push from EU to include additional schemes in ISO standard

3-2030

FrodoKEM

Classic McEliece

PQC fragmentation doesn't help migration.

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

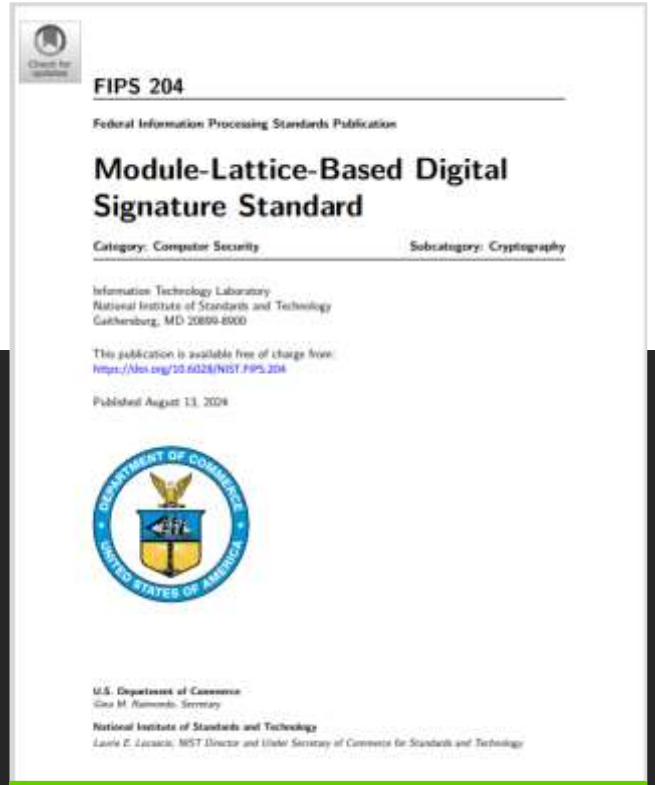
This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.203

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

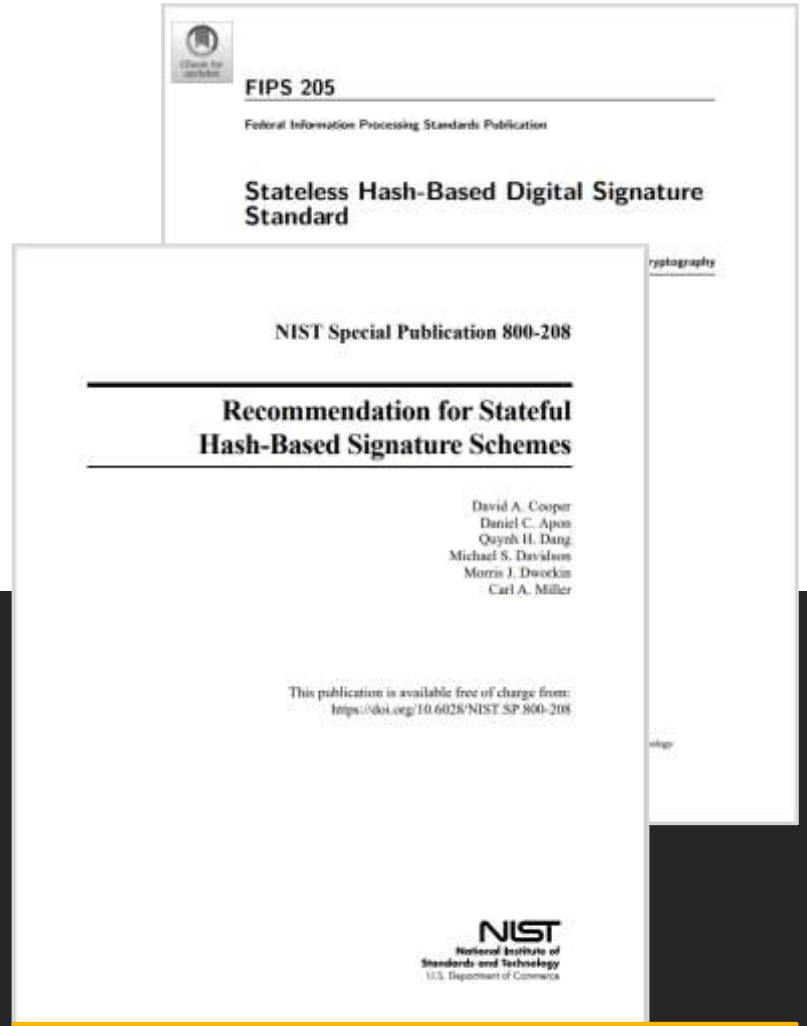
This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.204

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)


FIPS 205

Federal Information Processing Standards Publication

Stateless Hash-Based Digital Signature Standard

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

PQC migration guidance

USA (NSA)

- NSA recommendation available
- Commercial National Security Algorithm Suite 2.0
- **Begin transitioning immediately**
- PQC FW signature supported **by 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
- "QKD is only suitable for specific use cases"

France (ANSSI)

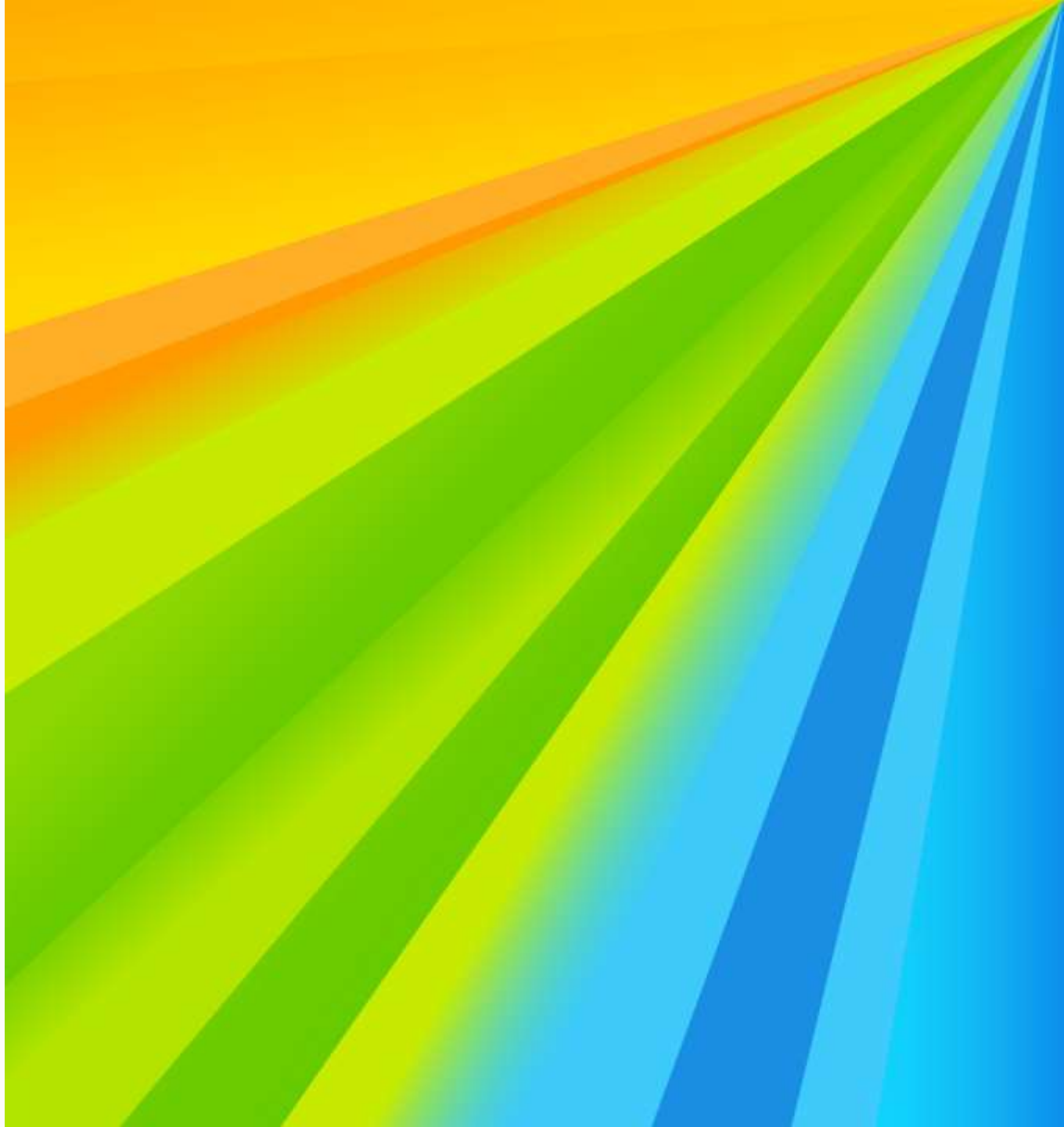
- PQC recommendations for security products
- **"As soon as possible"** when long-lasting protection is required
- Others to **migrate to classic-PQC hybrid in 2025 – 2030**
- Switch to PQC-only expected by 2030

NIST IR 8547 (Initial Public Draft)
Transition to Post-Quantum Cryptography Standards

Key Establishment Scheme	Parameters	Transition
Finite Field DH and MQV [SP80056A]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
Elliptic Curve DH and MQC [SP80056A]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
RSA [SP80056B]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035

Use case, use case, use case

Lesson 2



Typical embedded use cases for new algorithms

Many more ongoing and upcoming!

		FIPS 203 ML-KEM	FIPS 204 ML-DSA	FIPS 205 (Verify) SLH-DSA	SP 800-208 (Verify) XMSS / LMS
Security Goals	Secure Boot	✓	✓	✓	✓
	Secure Update	✓	✓	✓	✓
	Secure Attestation	×	✓	×	×
	Secure Debug / Test	✓	✓	×	×
	Certificates (PKI)	×	✓	✓	✓**
	Runtime Crypto API	✓	✓	✓	✓
Protocols	TLS 1.3 (Hybrid)	✓	✓*	×	×
	IKEv2 (Hybrid)	✓	✓*	×	×
	GSMA eSIM	✓	✓	×	×
	GlobalPlatform: TEE/MCU	✓	✓	✓	✓

** Signatures for client authentication excluded from initial proposals, discussions ongoing*
*** Possible but the number of issued certificates should be carefully managed (e.g., Root CA)*

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
EC-P384	No	"Fast"	"Fast"	48 B	48 B	96 B
FIPS 203 (ML-KEM)	Yes	4 ms	4 ms	2 400 B	1 184 B	1 088 B

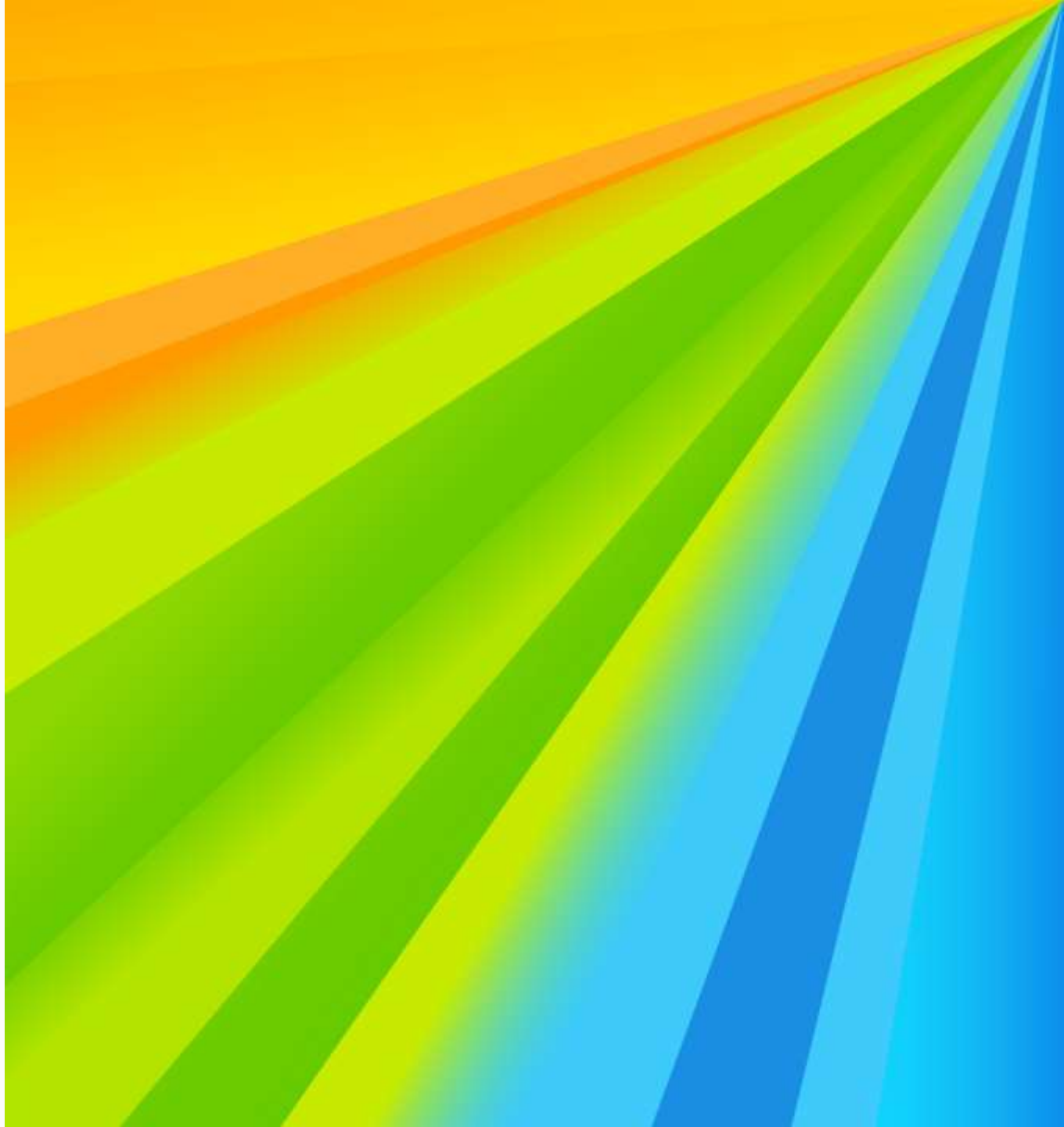
Algorithm	PQC	Sign	Verify	SK	PK	Sig
ECDSA-P384	No	"Fast"	"Fast"	48 B	48 B	96 B
FIPS 204 (ML-DSA)	Yes	31 ms	12 ms	4 032 B	1 952 B	3 309 B
FIPS 205 (SLH-DSA)***	Yes	77 s	68 ms	96 B	48 B	16 224 B
SP 800-20 (LMS/XMSS)	Yes	**(Stateful) 19 s	13 ms	48 B	48 B	1 860 B

** 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

Size and speed are malleable

Lesson 3



From theory to practice: small-memory implementations

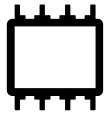
Do these implementations actually run on embedded systems?

		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



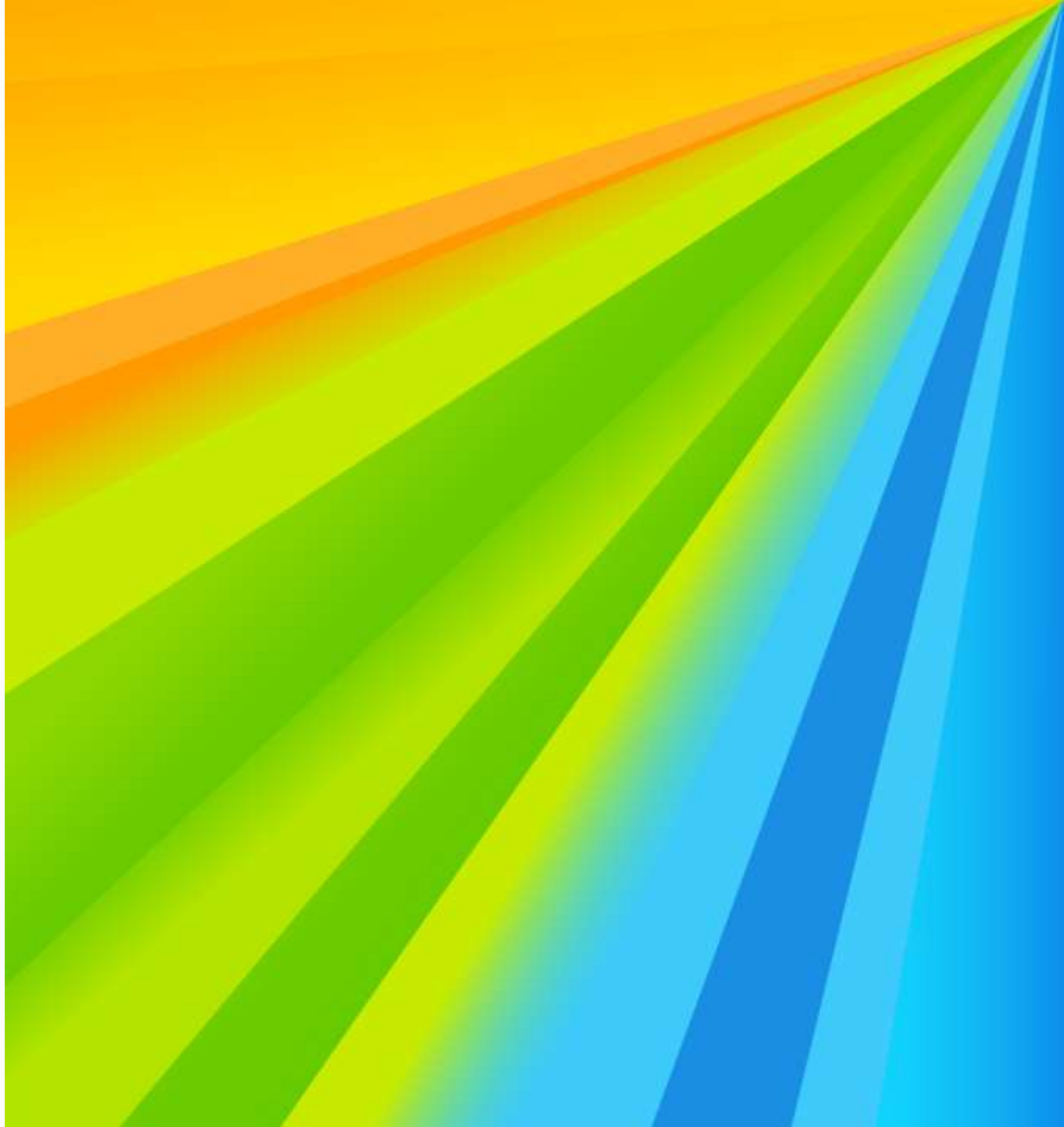
All Dilithium parameter sets will fit on a device with ~8KB memory.

Price: factor 3 to 4 in performance → HW accelerators

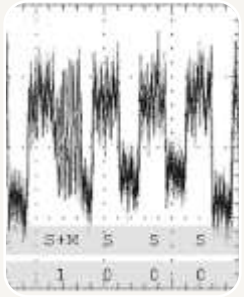
[A] NXP PQC: Bos, J.W., Renes, J. and Sprenkels, A., 2022. Dilithium for memory constrained devices. In International Conference on Cryptology in Africa (pp. 217-235)

Physical attacks

Lesson 4



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

From Theory to practice: Secure implementations (NXP PQC Team)

NIST CfP [A]: *"Schemes that can be made resistant to side-channel attack at minimal cost are more desirable"*

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 !

Q3/Q4 2024: First NXP products with PQC support announced!

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

Attacks are still in active development

- Chip design goes through a careful process architecture and code development
- It can take a year between code freeze and customers getting their chips
  - And they can be on the market for over ten years

	Side-Channel Attacks		Fault Injection Attacks	
	2016-2024	2024	2016-2024	2024
ML-KEM	30	11	12	2
ML-DSA	11	6	17	3
HBS	3	0	3	0

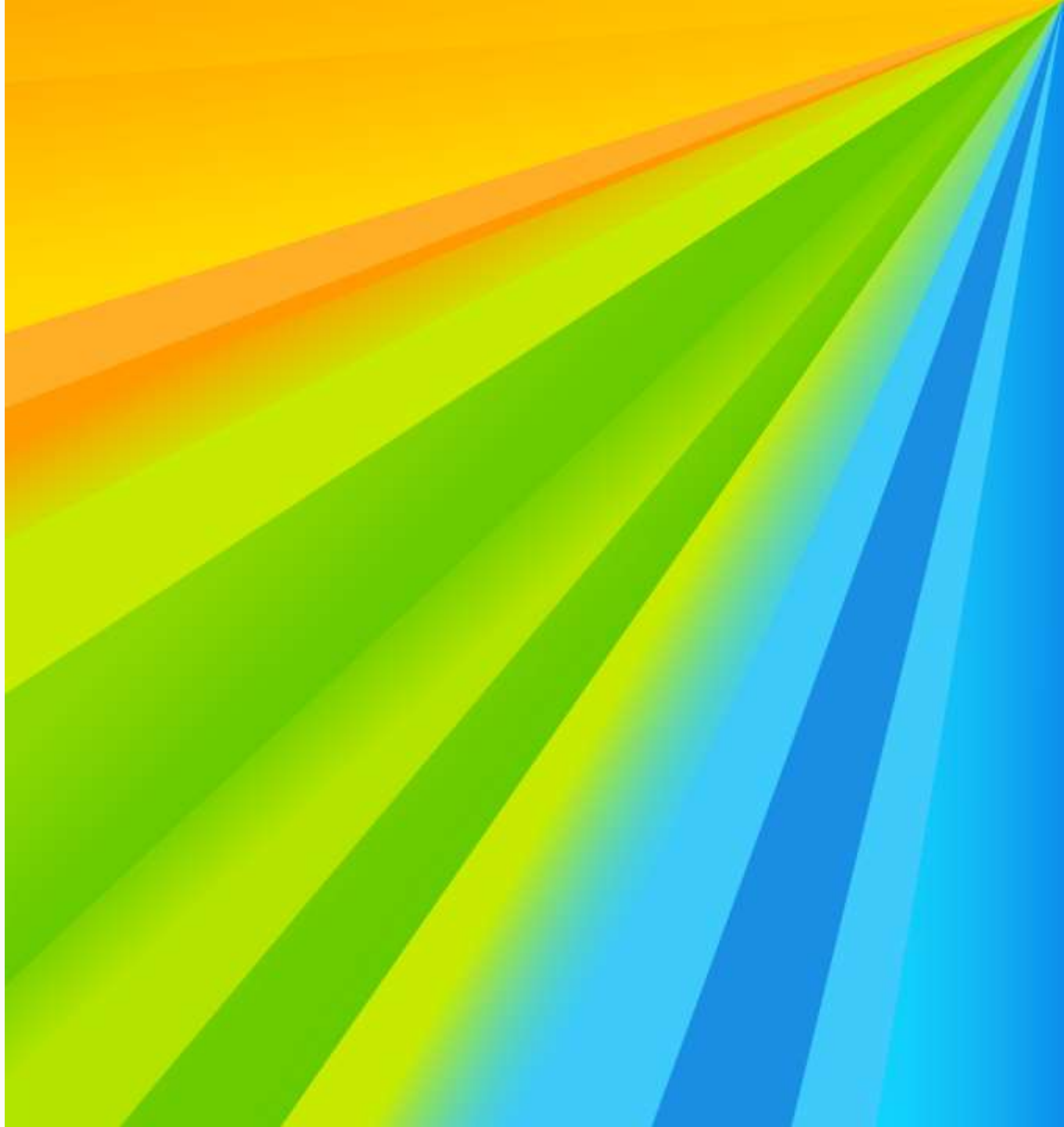
Number of publications concerning SCA and FA on PQC algorithms.*

- Crypto-agility/updateability is a solution
  - IF the capacity to do so is there, IF it fits, IF it still meets performance requirements

* Result of a manual count on eprint.iacr.org. Take error margins into account.

Hybrid migration

Lesson 5



Hybrid migration

Transition Period

ECC / RSA benefit from decades of cryptanalysis including logical / physical attacks

Can combine security of both in a hybrid mode

Hybrid Signed Container

" NIST will **accommodate** the use of a hybrid key-establishment mode and dual signatures in FIPS 140 validation when suitably combined with a NIST-approved scheme "

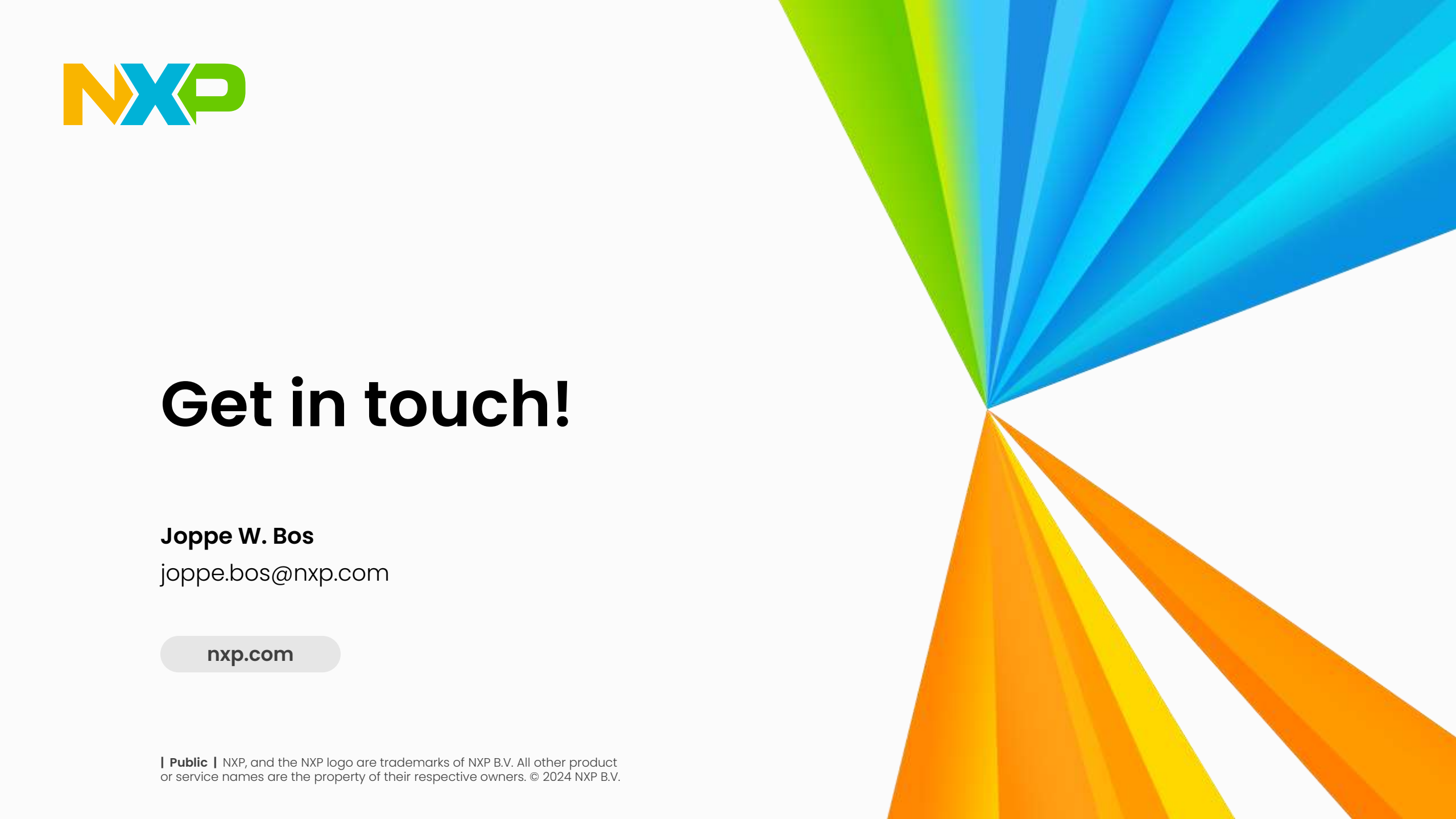
" the BSI does not recommend using post-quantum cryptography alone, but **only "hybrid"** "

" the role of hybridation in the cryptographic security is crucial and will be **mandatory** for phases 1 and 2.

public key cryptography [...] would strongly benefit from the introduction of new alternative algorithms. "

Conclusions

- Lesson 1: scattered standards will be a problem
- Lesson 2: urgency when to migrate depends on use case
- Lesson 3: often size is a bigger issue than speed
- Lesson 4: side-channels are a moving target
- Lesson 5: Migration is complicated → hybrid crypto



Get in touch!

Joppe W. Bos
joppe.bos@nxp.com

nxp.com