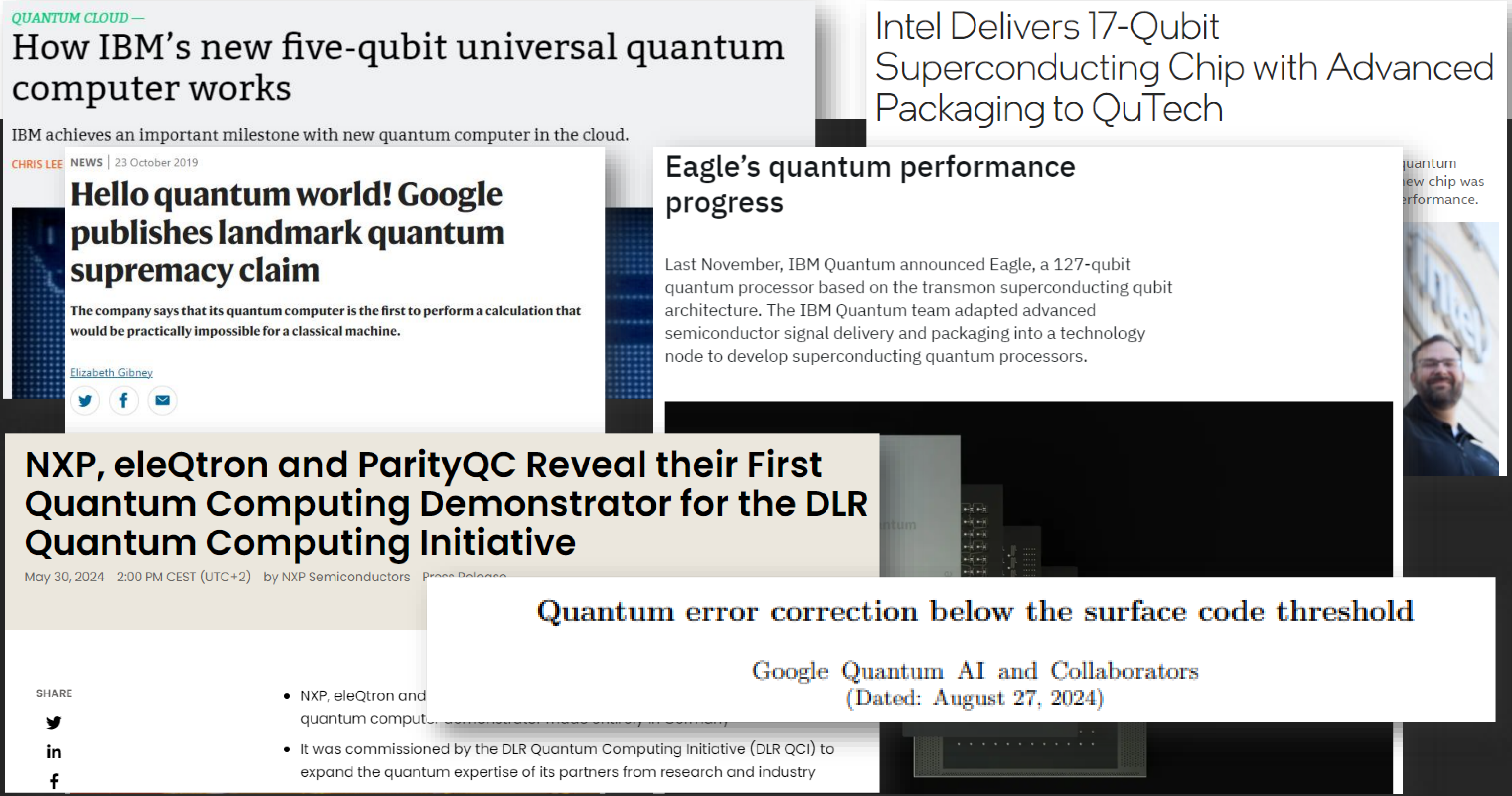
The First Generation of PQC-enabled Chips: Lessons Learned

Christine Cloostermans

Cryptographer & Security Architect (CC C&S, CTO)

December 2024



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

"This document specifies the bare-minimum security requirements expected of System-on-Chips (SoC) across multiple markets." [1]

Security Goals	
Cryptographic Identity	Rollback Protection
Security Lifecycle	Security By Isolation
Attestation	Secure Interfaces
Secure Boot	Binding
Secure Update	Trusted Services

arm Platform Security Requirements 1.0

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."

[1] Arm Platform Security Requirements 1.0 (DEN 0106)

Post-Quantum Cryptography

Requirement 1

Run on classical hardware

Requirement 2

Be secure against adversaries armed with classical computers

Requirement 3
NEW

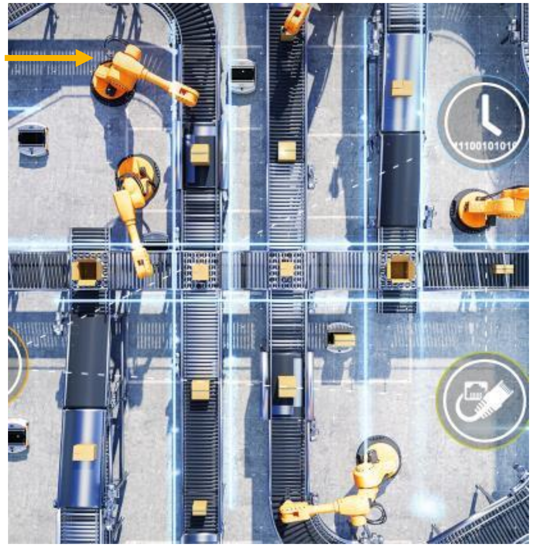
Be secure against adversaries armed with quantum computers

Requirement 4

Be secure against Side-Channel Analysis (SCA) and Fault Injection (FI) attacks

i.MX 94 Family of Applications Processors Delivers Safe and Secure Industrial and Automotive Connectivity with Real-Time Control

Samples available in 1H, 2025



Networking

- First i.MX applications processor with a TSN Switch
- Multi-protocol networking support

Security

- First NXP apps processor supporting Post-Quantum Cryptography
- EdgeLock Secure Enclave with Cyber Resilience Recovery Module

Performance + Safety

- High performance multi-core
- Integrated functional safety island
- Targeting **IEC61508** SIL2 (hardware integrity); SIL3 (systematic capability) and **ISO26262** ASIL-B

i.MX 94 Family Target Applications

Factory Automation

Servo Motor Drive

IO Controller

Programming Logic Controllers

Gateway

Industrial HMI

Building Automation

Building Control

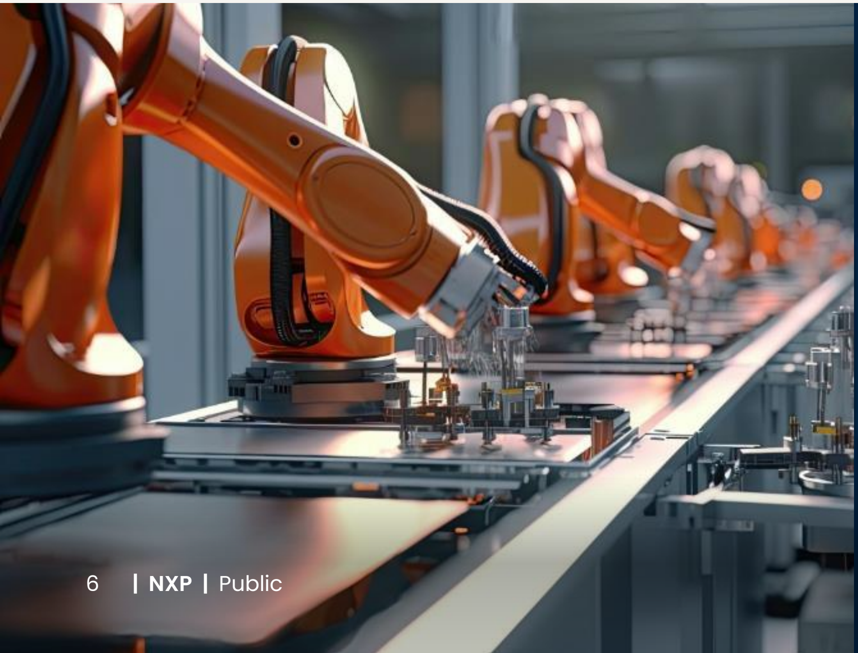
Energy Management

Climate Control (HVAC)

Elevator Control

Automotive IoT

Connectivity Domain Controller (Telematics)



i.MX 9 Series Applications Processors
Broad, Scalable Offerings

GREENER

EDGE AI

SAFETY

SECURITY

NXP **i.MX 95** Applications Processor Series

Advanced Platform for Vision and HMI

33K DMIPS, 7-15 TOPs (sparse) NPU, 128GFLOPS GPU, 4K Vision, Functional Safety, **PQC by EdgeLock Secure Enclave**, Heterogenous Compute

Target: Machine Vision, Data Aggregation, Intuitive HMI, Audio Applications

NXP **i.MX 94** Applications Processor Series

Real-time Control and Networking

20K DMIPS, 0.5 TOPs NPU, Multi-port Ethernet Switch, Wide Range of Industrial Protocols support,, Heterogenous Compute, Configurable Functional Safety Partition, **PQC by EdgeLock Secure Enclave**, V2X Authentication

Target: PLCs, Servo Drives, Gateways, Building Control, Automotive Telematics

NXP **i.MX 91/93** Applications Processor Series

Essential Compute Everywhere

5K-20K DMIPS, 1-4 TOPs NPU, Industrial IO, Switch, Programmable Industrial Protocols, **PQC by EdgeLock Secure Enclave**, Heterogenous Compute

Target: Cost-sensitive applications that need a range of performance and I/Os

Remainder of this talk: what did we learn from the journey to that first chip?

Lesson 1: often size is a bigger issue than speed

Lesson 2: use case, use case, use case

Lesson 3: scattered standards will be a problem

Lesson 4: side-channels are a moving target

Size and speed are malleable

Lesson 1

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

NXP PQC [A]		Slower	Smaller
Runtime	RAM	Runtime	RAM
61 ms	5 kB	3.2x	10.0x
16 ms	3 kB	2.3x	3.7x
119 ms	7 kB	3.8x	9.9x
29 ms	3 kB	2.4x	3.3x
168 ms	8 kB	4.0x	15.4x
50 ms	3 kB	2.4x	4.0x

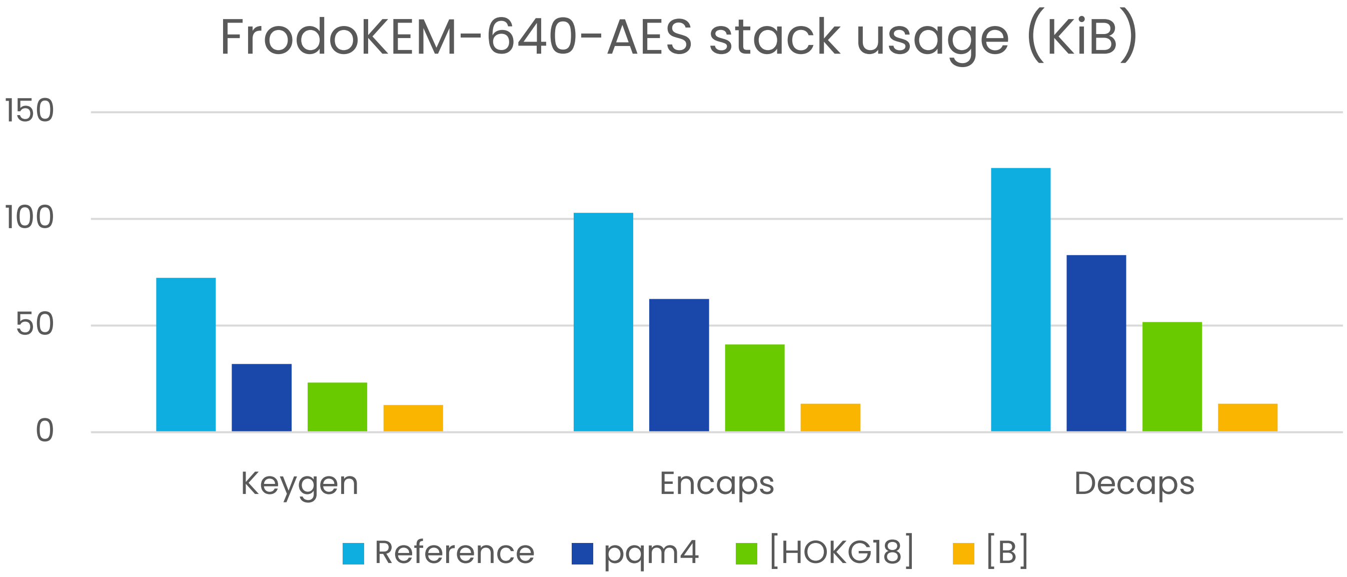
All Dilithium parameter sets will fit on a device with ~8KB memory.

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)

Frodo low-cost stack usage

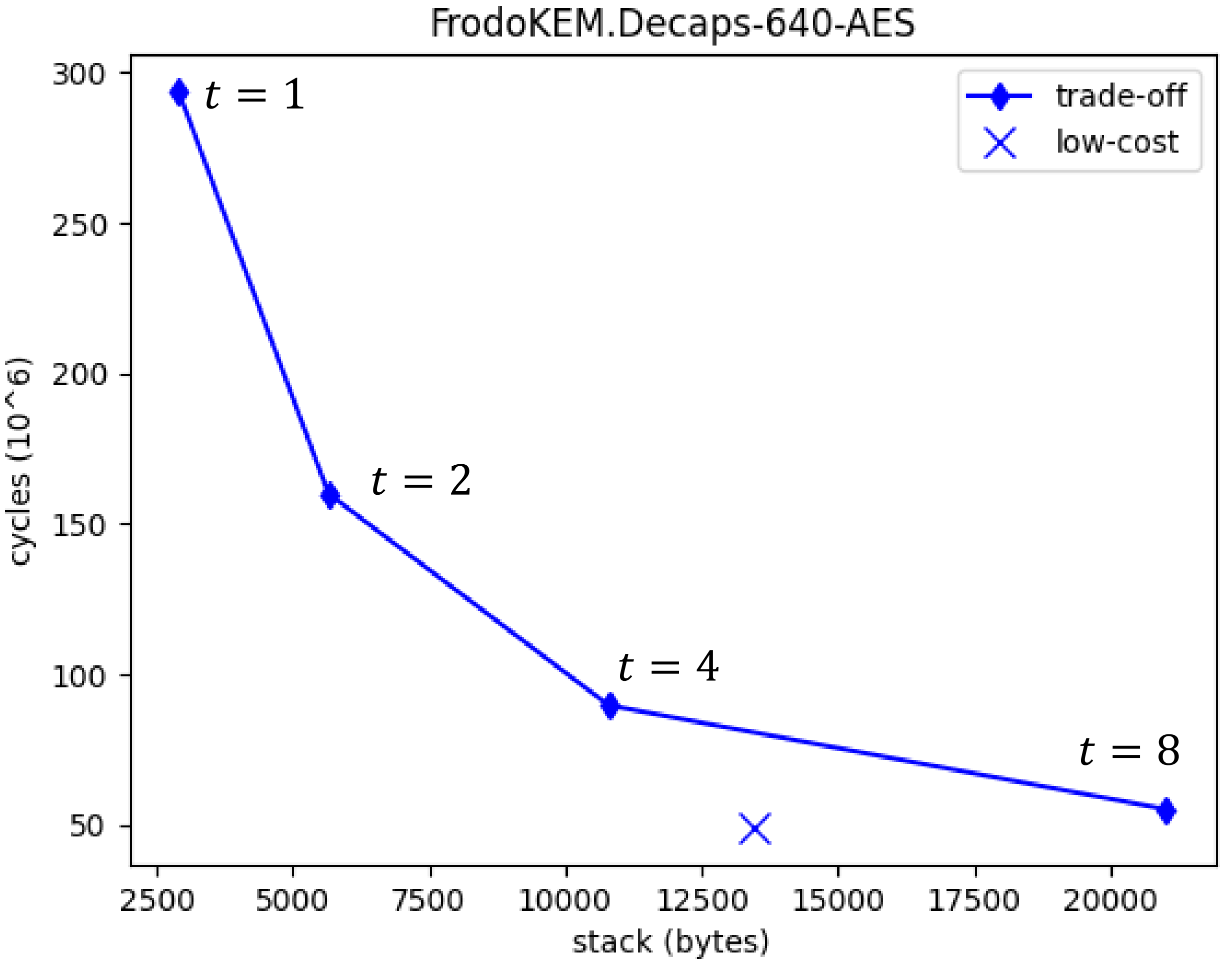
- Benchmark on Cortex-M4 platforms
- Cycle count within 5% range compared to pqm4 (40-50m cycles)



[B] NXP PQC: Joppe W. Bos, Olivier Bronchain, Frank Custers, Joost Renes, Denise Verbakel, Christine van Vredendaal: Enabling FrodoKEM on Embedded Devices. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2023(3): 74-96 (2023)

Stack usage and performance – trade-off

- Pqm4: 83kB, 47m cycles



Use case, use case, use case

Lesson 2

Typical embedded use cases for new algorithms

Many more ongoing and upcoming!

		FIPS 203	FIPS 204	FIPS 205 (Verify)	SP 800-208 (Verify)
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.
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	(variable) 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

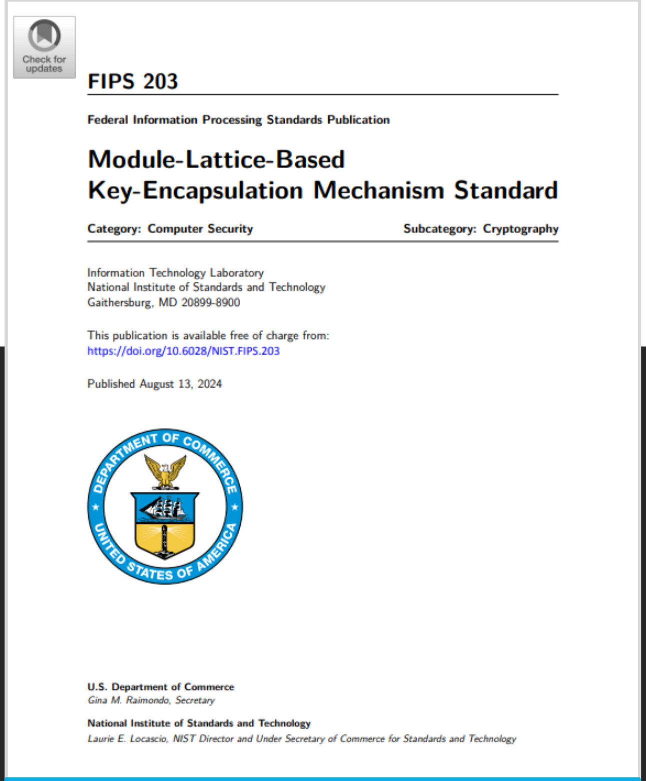
** NIST Level 3 parameter sets*
*** Significant reduction possible by increasing memory consumption for state*
**** New parameter sets coming that will improve performance & signature size!*

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

Standards will be an issue

Lesson 3

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

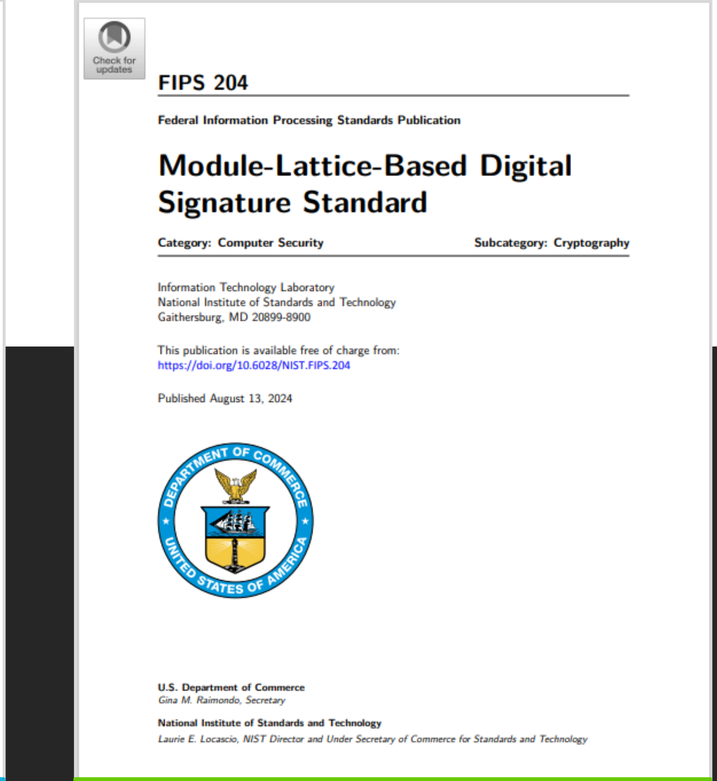
This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.203

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

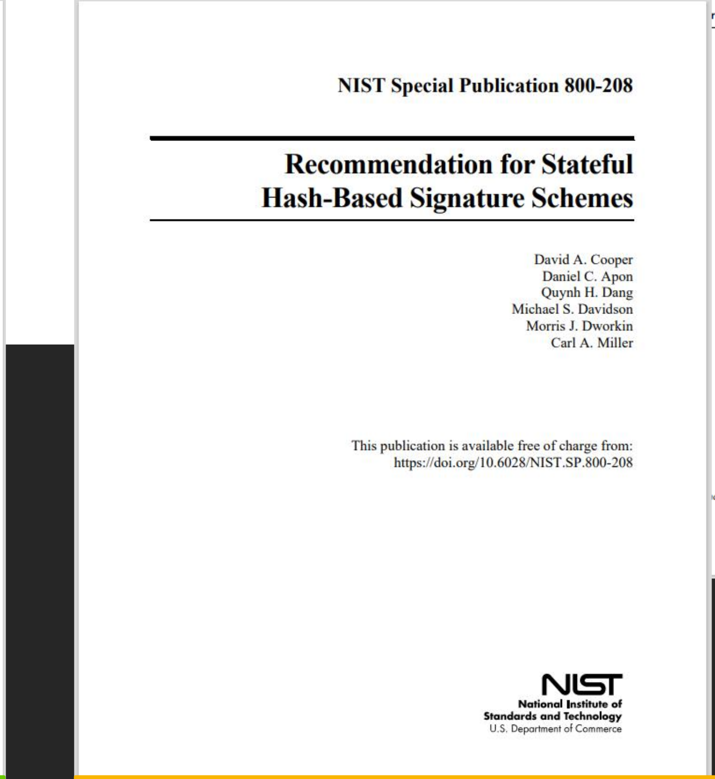
National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

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)

[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

More ongoing and upcoming

Enabling and accelerating all on each and every chip seems infeasible

- Regional chips?
- Market chips?
- Interoperability?

US/NIST

- **FIP 206 (Falcon)**
- **Additional Digital Signature Schemes**
- **PQC Standardization Process: Fourth Round Candidates**
- **More?**

EU

- **ISO: FrodoKEM, Classic McEliece**

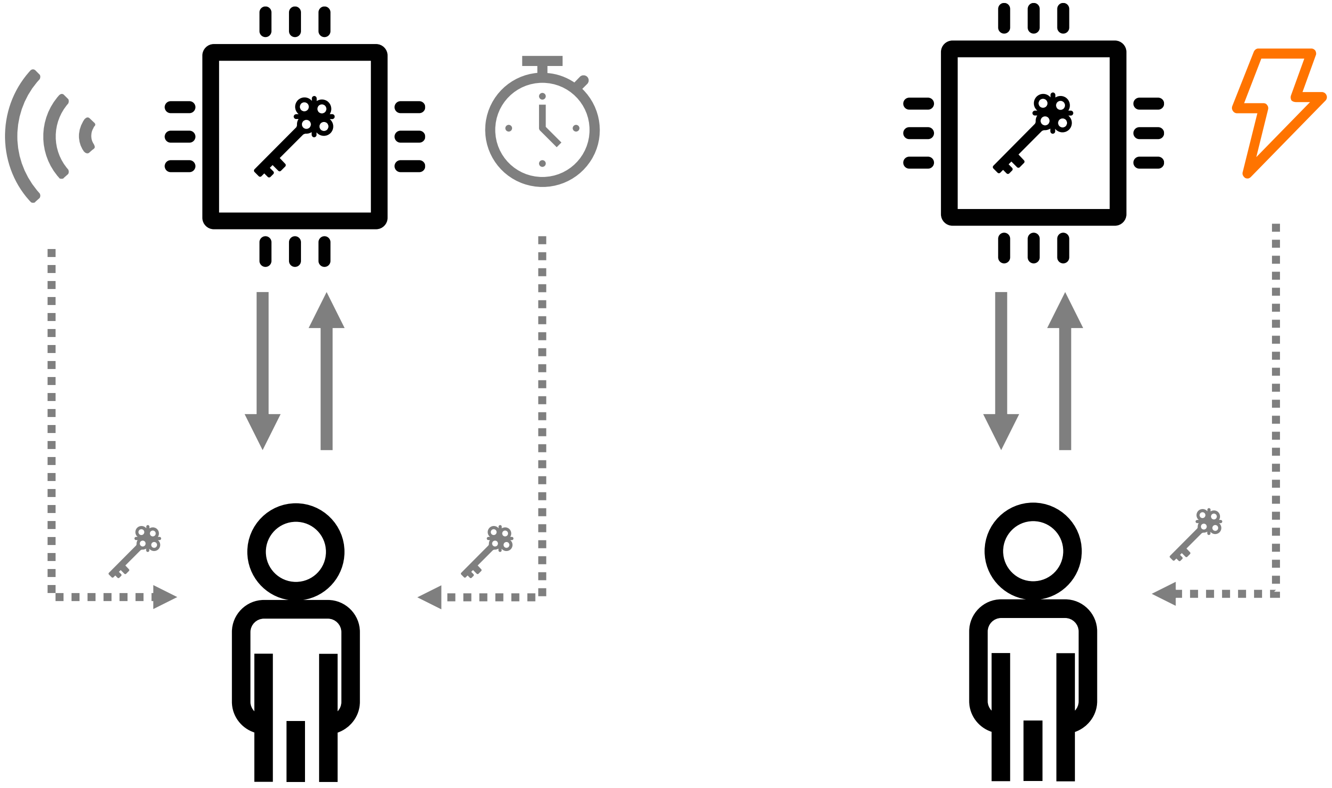
Asia

- **Korean standards**
- **Chinese standards**
- **Indian standards?**

Physical attacks

Lesson 4

From theory to practice: Secure implementations



Side-Channel Attacks (SCA)

Fault Injection (FI)

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 Learned from Protecting CRYSTALS-Dilithium
2024	TCHES		🟦	Exploiting Small-Norm Polynomial Multiplication with Physical Attacks
2024	RWC	🟩	🟦	Challenges of Migration to PQ Secure Embedded Systems
2024	PROOFS	🟩	🟦	The long and winding road to physically secure PQC - An industrial perspective

Completely masked implementation of Dilithium / FIPS 204 !

[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.

Conclusions

Lesson 1: often size is a bigger issue than speed

Lesson 2: use case, use case, use case

Lesson 3: scattered standards will be a problem

Lesson 4: side-channels are a moving target

Get in touch!

Christine Cloostermans

Christine.cloostermans@nxp.com

nxp.com