Crypto Agility for Embedded Systems

Melissa Azouaoui, Joppe W. Bos, Christine Cloostermans, Gareth T. Davies

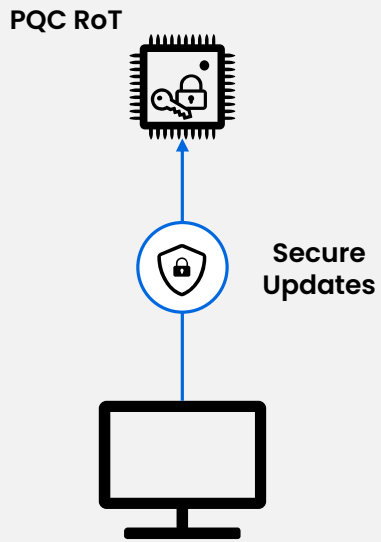
NXP PQC Team (CC C&S, CTO)

April 2025

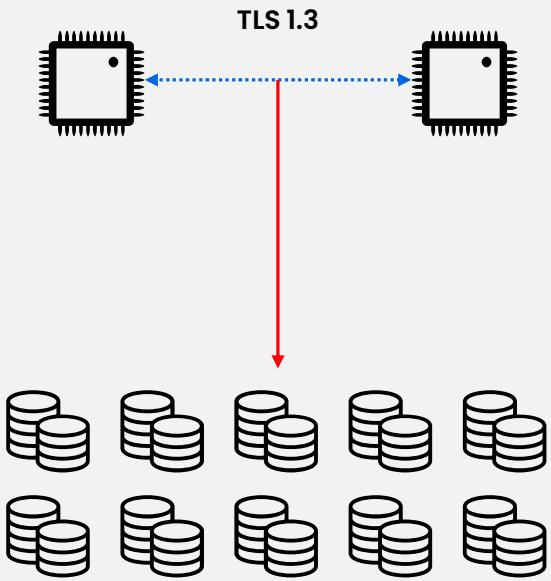
What drives migration to Post-Quantum Cryptography?

Standards & Compliance

Trust Anchor / Hardware



Store Now Decrypt Later

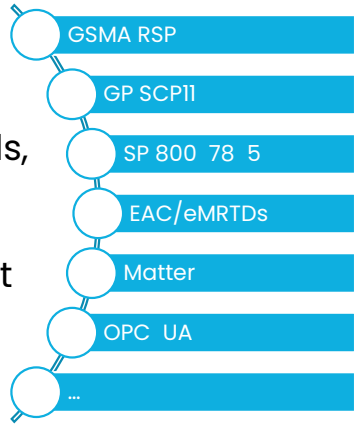


Cryptographic Agility: Priorities

Well-covered in NIST SCWP 39:
- System-level crypto agility
- Protocol-level crypto agility
  - -> Generic use of KEMs
  - -> hybrid support

Agility in TLS 1.3/IKEv2 and the broader applications/systems that use them is by now understood, fast progress made already

PQC versions of many KE protocols, frameworks and other important standards are not (yet) mature



'Advanced crypto' can benefit from agility being part of standards/design process
- ➔ PAKE
- ➔ Auth mode for HPKE
- ➔ Blind signatures, OPRFs and NIKE

...will all run better in HW if built from standard components (like PQ KEMs, signature schemes or their subroutines)

Now | Next | Later

When is Crypto Agility Hard?

Agility inherently increases the attack surface in many hardware contexts

Devices can get FW/SW updates, but not more HW acceleration

➔ Restrictiveness of CNSA 2.0 is useful: at chip level scope for crypto agility is low

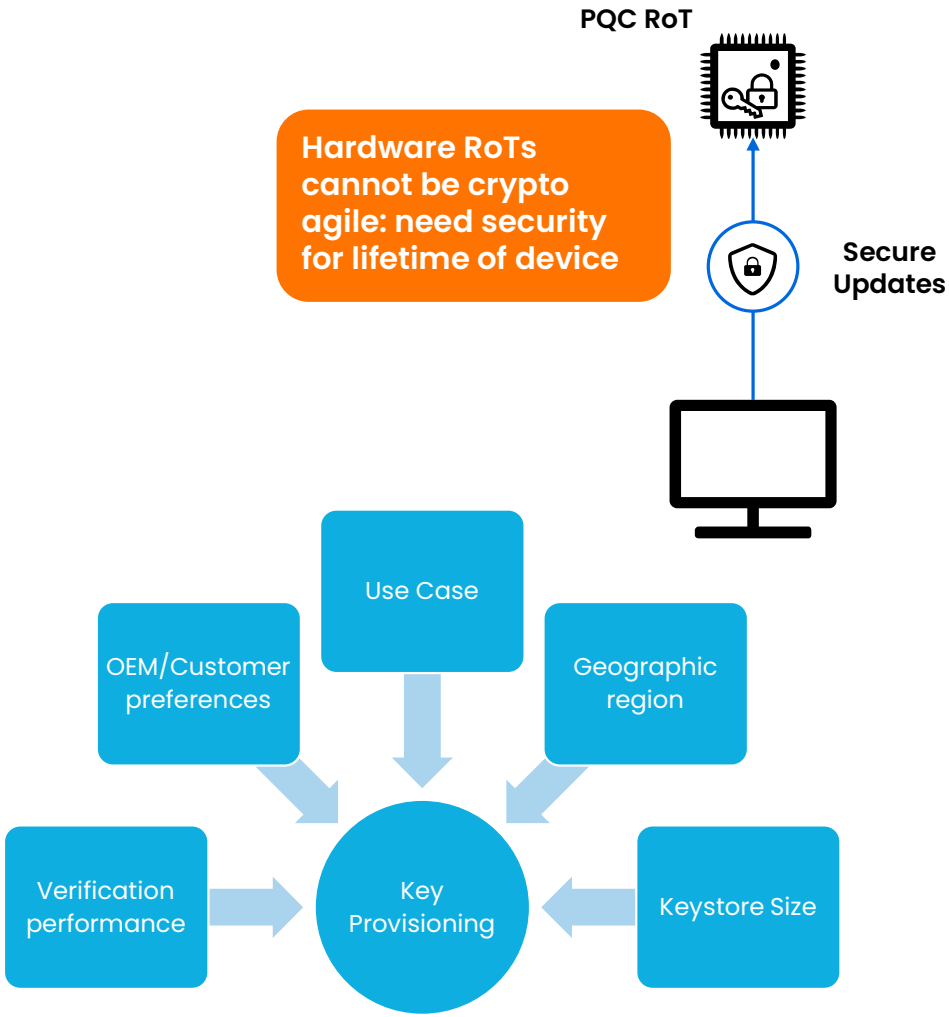
Many consequences for secure devices:

➔ Chip area for crypto acceleration limited

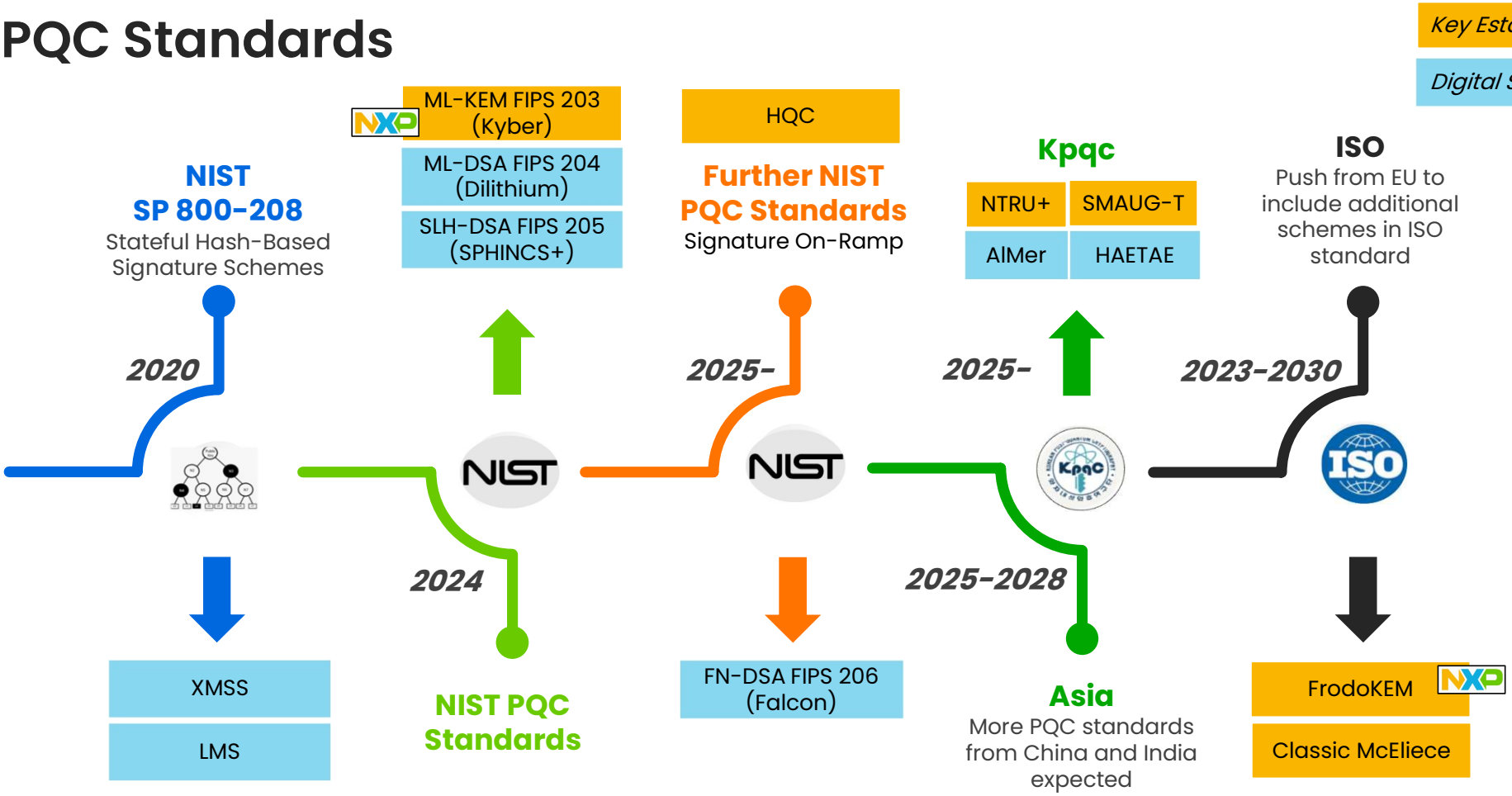
- unfortunate divergence in mathematical structure
- can't support everything

➔ Each mini-generation of chips could target different schemes for acceleration

➔ Global certification landscape not static; progresses in sync with attack literature



PQC Standards



PQC Algorithms in Typical Embedded Use Cases

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.
LMS numbers are 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
HQC	Yes	528 ms	798 ms	40 B	4 522 B	9 042 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; LMS vs XMSS: Comparison of Stateful Hash-Based Signature Schemes on ARM Cortex-M4; AfricaCrypt 2022 https://eprint.iacr.org/2020/470

From Theory to Practice: Low-Memory Implementations

Do these implementations actually run on embedded systems?

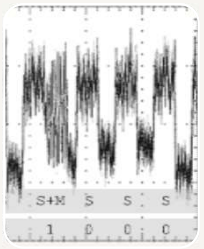
		pqm4		NXP PQC [C]		Slower	Smaller
		Runtime	RAM	Runtime	RAM	Runtime	RAM
Dilithium-2	Sign	19 ms	50 kB	61 ms	5 kB	3.2x	10.0x
	Verify	7 ms	11 kB	16 ms	3 kB	2.3x	3.7x
Dilithium-3	Sign	31 ms	69 kB	119 ms	7 kB	3.8x	9.9x
	Verify	12 ms	10 kB	29 ms	3 kB	2.4x	3.3x
Dilithium-5	Sign	42 ms	123 kB	168 ms	8 kB	4.0x	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

[C] NXP PQC: Bos, Renes; Sprenkels. Dilithium for memory constrained devices; AfricaCrypt 2022 https://eprint.iacr.org/2022/323

Resistance against Physical & Logical Attacks

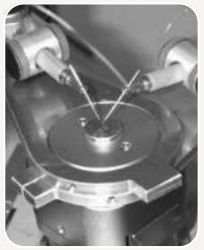


Side-channel attacks

- 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 [D]: *"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
2023	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 !

[D] NIST CfP: Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process

Conclusions

- Much focus so far on SNDL, but consideration of agility for signature use cases is also vital
- Hardware Acceleration will develop over time
- Size is often a bigger issue than speed
- Side-channels are a moving target
- Hybrid crypto increases user/customer confidence

Get in touch!

Gareth T. Davies
garethThomas.davies@nxp.com

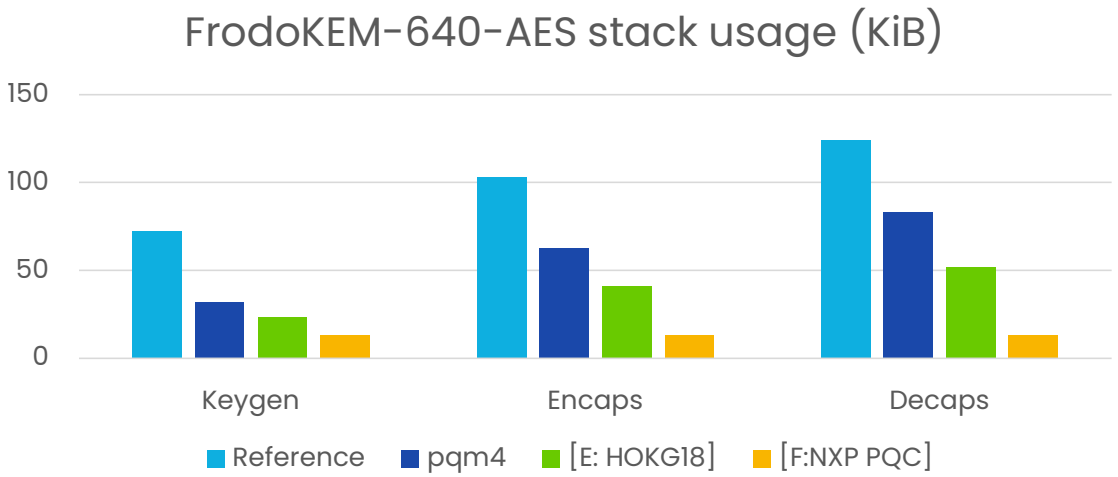
nxp.com

Additional Slides

FrodoKEM with low-cost Stack Usage

Benchmark on Cortex-M4 platforms

➔Cycle count within 5% range compared to pqm4 (40-50m cycles)



[E: HOKG18] Howe, Oder, Krausz, Güneysu; Standard Lattice-Based Key Encapsulation on Embedded Devices; IACR TCHES 2018 https://eprint.iacr.org/2018/686
[F:NXP PQC] Bos, Bronchain, Custers, Renes, Verbakel, van Vredendaal; Enabling FrodoKEM on Embedded Devices; IACR TCHES 2023 https://eprint.iacr.org/2023/158

Attacks 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
➔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.*

Update (of the implementation) is a solution
➔IF the capacity to do so is there, IF it fits, IF it still meets performance requirements

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