SECURE-IC
THE SECURITY SCIENCE COMPANY

Transitioning Embedded Systems to Post Quantum Cryptography

Speaker: Sylvain GUILLEY, Ph.D.,
Co-Founder & CTO

Date: November 19th, 2024

Place: Couvent des Jacobins, Rennes

European Cyber Week by Pôle d'excellence CYBER
THE SOVEREIGN CYBER & DEFENCE AI FORUM

Version 2.3

AGENDA

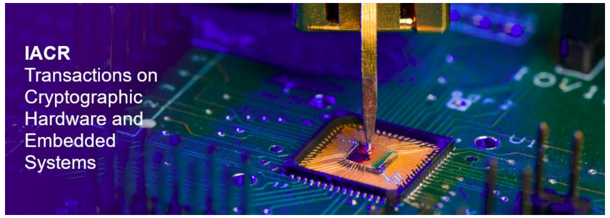
1. Introduction
2. PQC risk analysis
3. PQC technologies completeness
4. PQC technologies consistency
5. Conclusions and perspectives

AGENDA

1. Introduction
2. PQC risk analysis
3. PQC technologies completeness
4. PQC technologies consistency
5. Conclusions and perspectives

What are Embedded Systems?

- According to **Embedded France** association:
  - Les systèmes embarqués englobent tous les dispositifs combinant électronique, logiciels de contrôle/commande et communications, opérant sous des contraintes strictes telles que le temps réel, la rapidité et la fiabilité. C'est un domaine d'excellence française.
  - Embedded systems encompass all devices combining electronics, control/command software and communications, operating under strict constraints such as real time, speed and reliability. It is an area of French excellence.

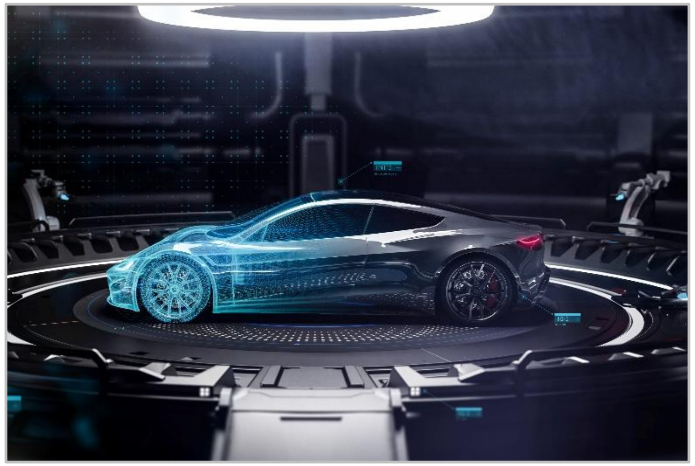


- According to **IACR**:
  - Cryptographic Hardware and Embedded Systems (CHES) conference is the premier venue for research on both design and analysis of cryptographic hardware and software implementations. As an area conference of the **International Association for Cryptologic Research** (IACR), CHES bridges the cryptographic research and engineering communities, and attracts participants from academia, industry, government and beyond.

- In general, Embedded Systems are the deepest technologies:
  - In charge of **secure bring-up** and **cyber maintenance** of the complete system.

Examples of Embedded Systems

Automotive



Edge / AI / OT

IoT

Mobile / High Security

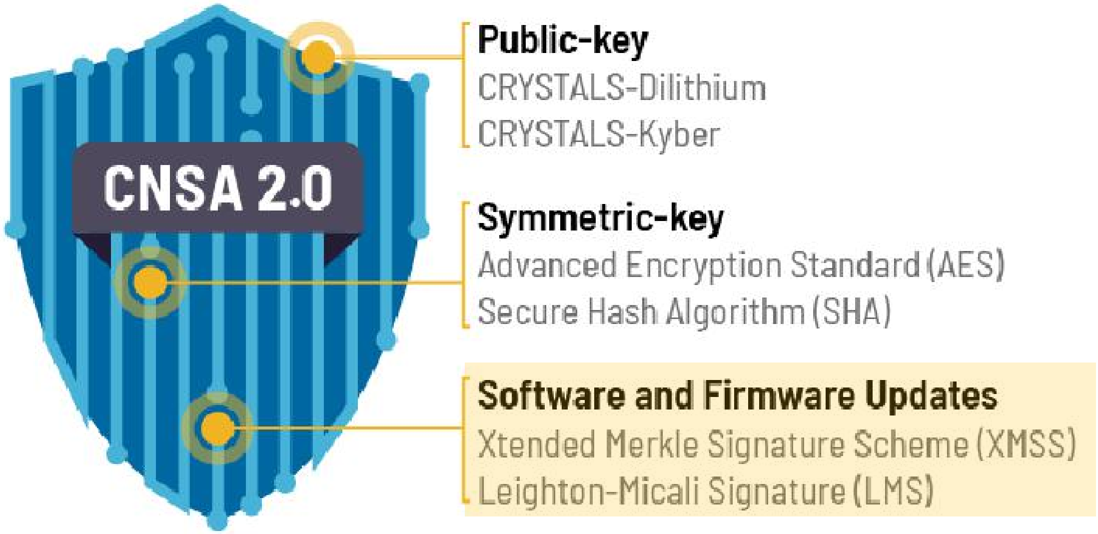
Networking / Server

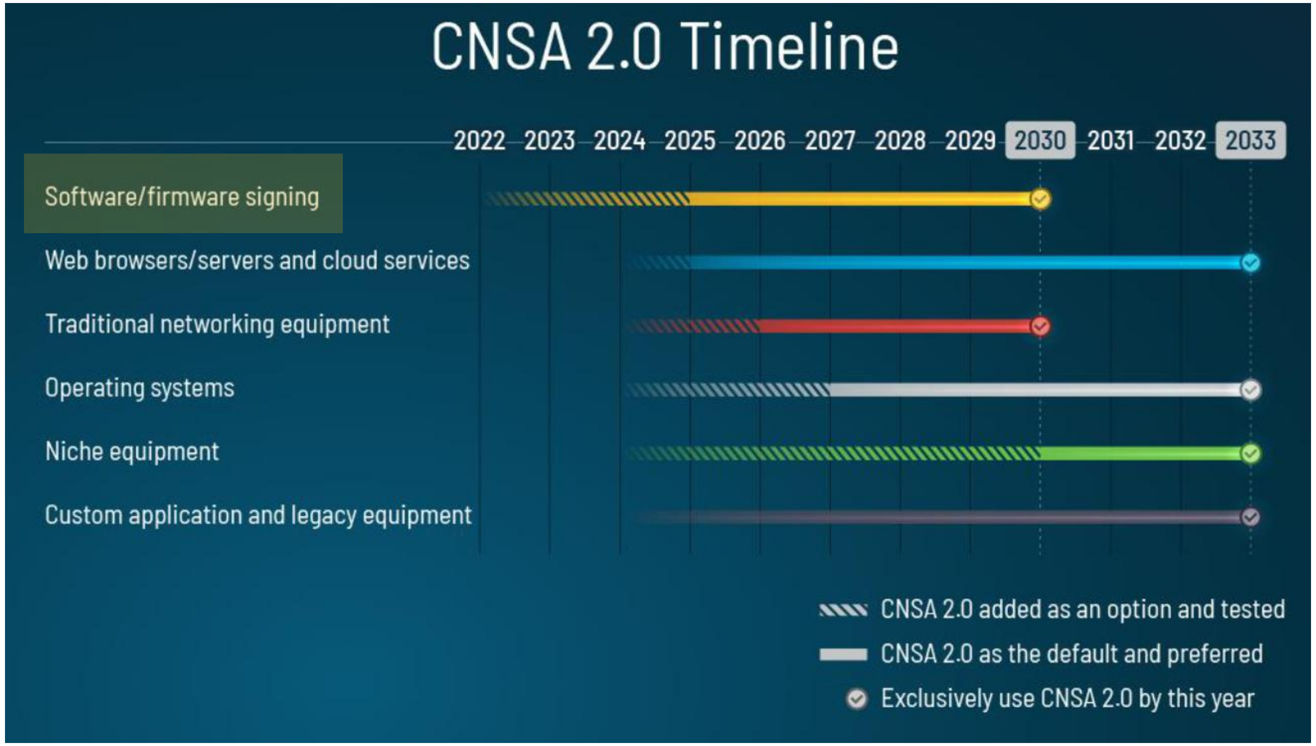
Additional Markets

- Healthcare
- Defense & Government
- Industry & Factory Automation
- Memory & Storage
- Critical Infrastructures
- Media & Entertainment
- Smart Grid & Smart Cities
- Academics & Research

PQC Compliance of Embedded Systems

- CNSA 2.0 - aligned

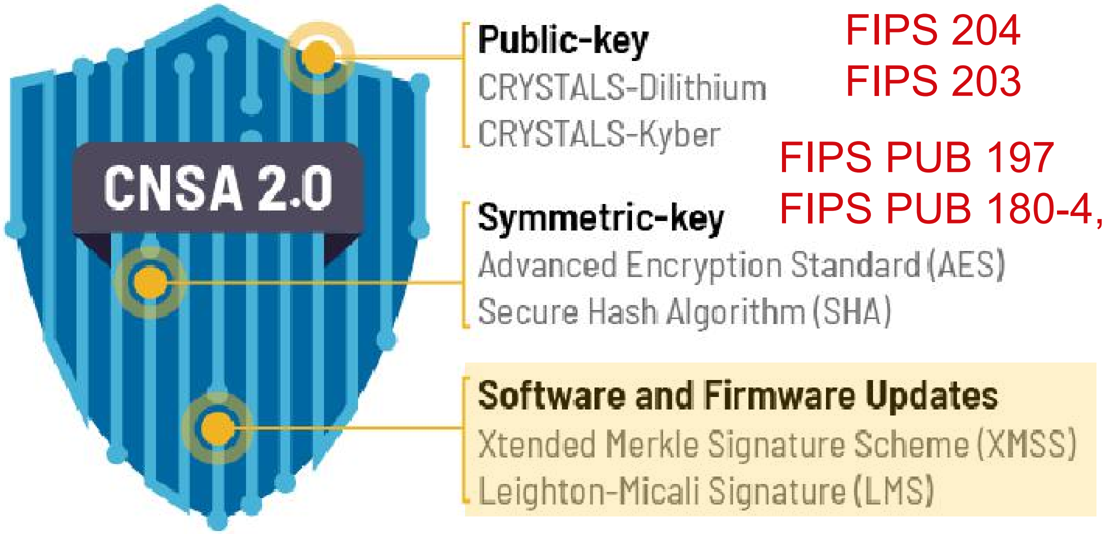




- By a cursory glance or examination, it looks like SW & FW signatures verification at boot and at updates are sufficient
- But the problem is wider, as provisioning of embedded system is also leveraging asymetrical cryptographic algorithms

PQC Compliance of Embedded Systems

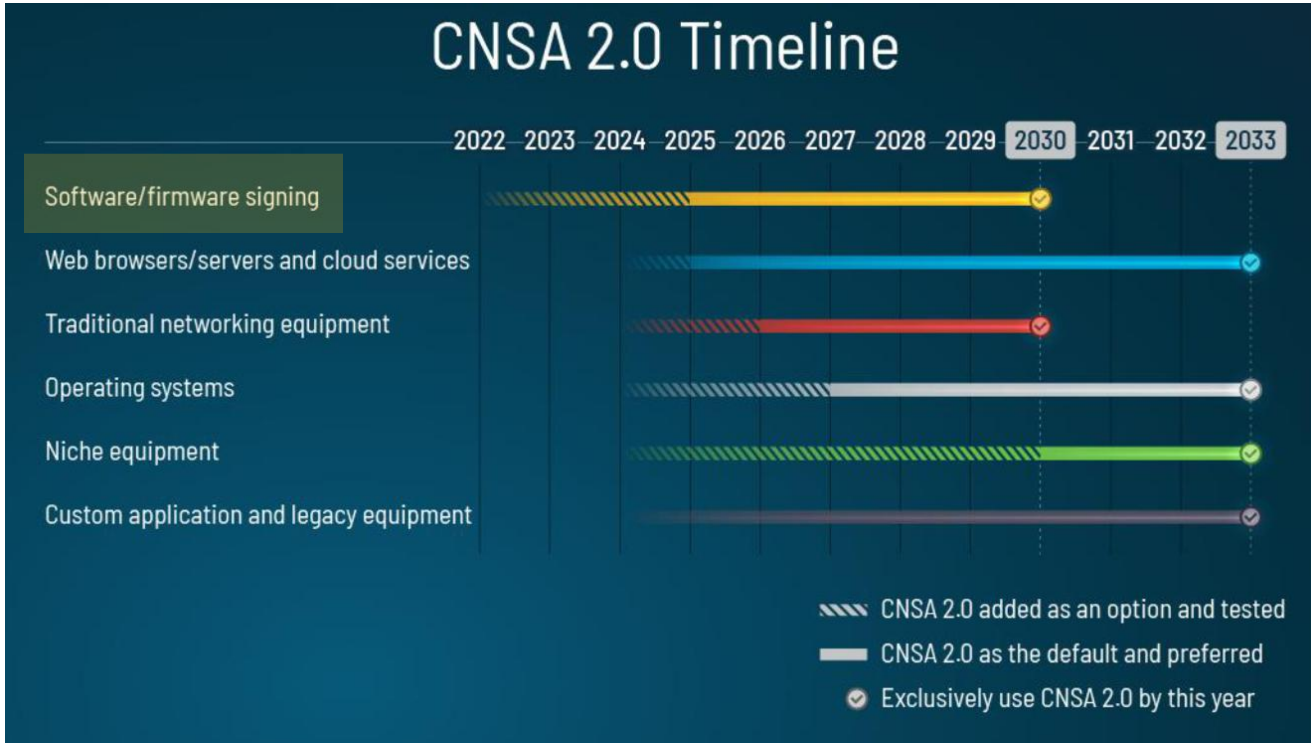
- CNSA 2.0 - aligned



FIPS 204
FIPS 203

FIPS PUB 197
FIPS PUB 180-4, 202

NIST SP 800-208



- By a cursory glance or examination, it looks like SW & FW signatures verification at *boot time* and at *updates* are sufficient
- But the problem is wider, as provisioning of embedded system is also leveraging asymetrical cryptographic algorithms

Certificate of Compliance

A6046

- Secure-IC is the first IP vendor to get hardware type CAVP for PQC algorithms!
  - Bonus: two bugs related to padding identified in NIST ACVP servers!

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

PROJECTS | CRYPTOGRAPHIC ALGORITHM VALIDATION PROGRAM

Cryptographic Algorithm Validation Program CAVP

PROJECT LINKS

Overview

Presentations

Implementation Name	Secure-IC PQC Solutions
Description	The "Secure-IC PQC Solutions" comprising ML-KEM, ML-DSA, SLH-DSA and LMS PQC algorithms support the maximum message lengths with adaptive key sizes and are optimized for a faster throughput in hardware implementations and operational environments. The "Secure-IC PQC solutions" are embedded in the Secure-IC's integrated Secure Elements (Securyzr™ iSEs) including S100, S300, S700, and S900 neo series, and in the Securyzr™ Crypto Solutions/Crypto co-processors, strictly following the NIST PQC requirements.
Version	1.0
Type	HARDWARE

Vendor: Secure-IC
801 avenue des Champs Blancs
Digital Park B - ZAC Atalante via Silva
Cesson-Sévigné, Bretagne 35510
FR

Contacts:
karine lorvellec
karine.lorvellec@secure-ic.com
+33 2 99 12 18 72
Ritu-Ranjan SHRIVASTWA
ritu-ranjan.shrivastwa@secure-ic.com
+33 2 99 12 18 72
Sylvain GUILLEY
sylvain.guilley@secure-ic.com
+33 6 75 25 27 49

A6046 First Validated: 10/30/2024

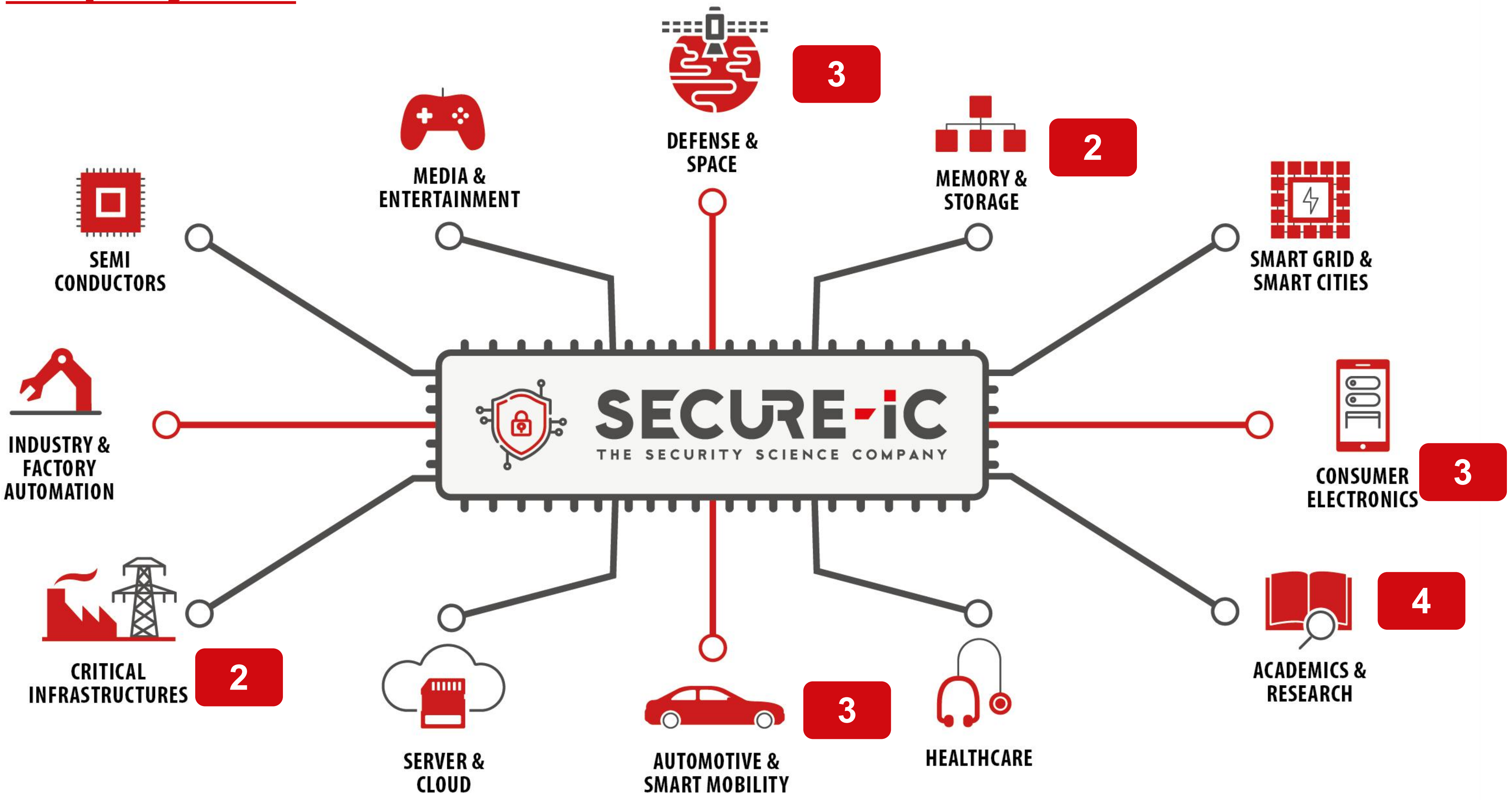
Collapsed | Expanded | Aggregated

Operating Environment	Algorithm Capabilities
XC7Z020 (xc7z020clg484-1)	ML-DSA KeyGen
XC7Z020 (xc7z020clg484-1)	ML-DSA SigGen
XC7Z020 (xc7z020clg484-1)	ML-DSA SigVer
XC7Z020 (xc7z020clg484-1)	ML-KEM EncapDecap
XC7Z020 (xc7z020clg484-1)	ML-KEM KeyGen
XC7Z020 (xc7z020clg484-1)	SHA3-224
XC7Z020 (xc7z020clg484-1)	SHA3-256
XC7Z020 (xc7z020clg484-1)	SHA3-384
XC7Z020 (xc7z020clg484-1)	SHA3-512
XC7Z020 (xc7z020clg484-1)	SHAKE-128
XC7Z020 (xc7z020clg484-1)	SHAKE-256

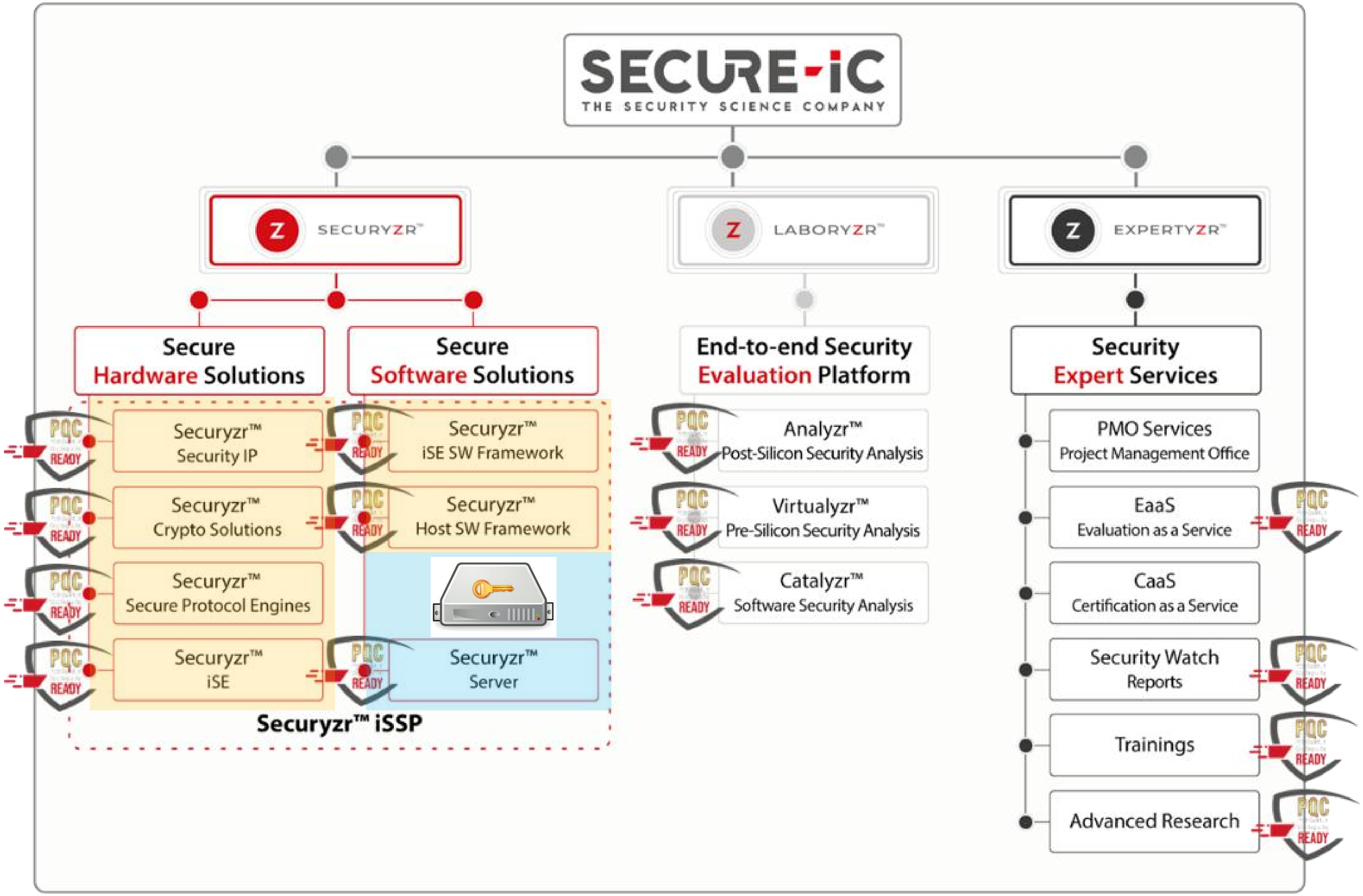
SERMA SAFETY & SECURITY

Secure-IC's industrial backlog on PQC

- <u>17 projects</u>



Secure-IC portofolio, ported to PQC already



Caption:

Embarked

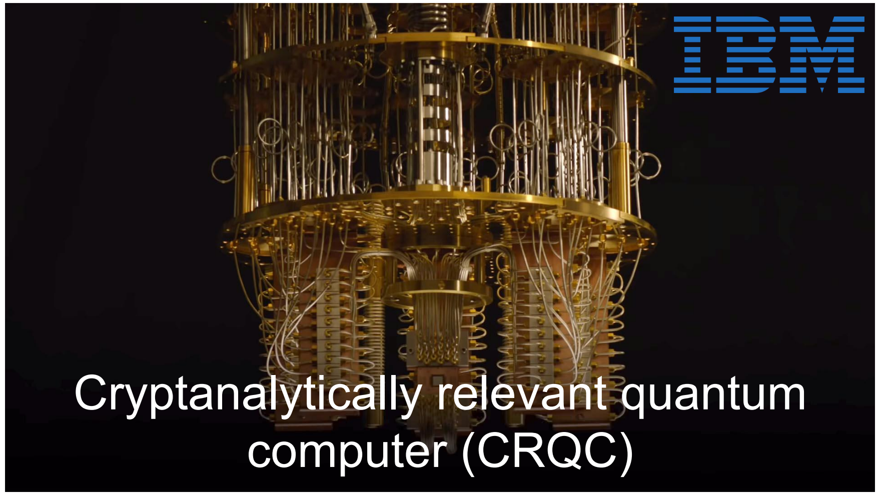
Debarked

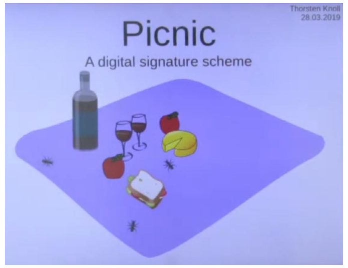
AGENDA

1. Introduction
2. PQC risk analysis
3. PQC technologies completeness
4. PQC technologies consistency
5. Conclusions and perspectives

Risk Analysis

- **NIST**: Classical digital signature and key exchange can be broken by a quantum computer
  - → **Standardize PQC**
- **ANSSI**: PQC algorithms are young
  - → **Hybridize PQC**
- **Secure-IC**: Transition needs to be exhaustive, for embedded systems. Gaps are the weakest points
  - → **Ensure PQC completeness & consistency**





SECURE-iC
THE SECURITY SCIENCE COMPANY

AGENDA

1. Introduction
2. PQC risk analysis
3. PQC technologies completeness
4. PQC technologies consistency
5. Conclusions and perspectives

SECURE-IC
THE SECURITY SCIENCE COMPANY

System-level impact of PQC transitioning

Pre-silicon stage

Debarked

HSM:
- roles management,
- backup, etc.

FIPS 140-3. Otherwise a PQC attacker will extract keys from there

Generates Chip/System Manufacturer PK_0/SK_0

Integrated

ROM
...
$Hash(PK_0)$

Hardware PQC signature verification

Otherwise attacker can stub digital signature as «return true»

R2: hardware because is checking the firmware (HW CAVP)

R1: security by default

Provisioning stage

OSAT (assumed not in secure premises) HSM for diversified CM/SM PK/SK, and for other keys as well (e.g., Endorsement Key)

Secure channel: PQC KEM needed

OTP
...
$Hash(PK_i)$ with $i>0$

OTP
...
EK pub
EK priv

R3: end-to-end security

R5: comply to ANSSI's view in terms of hybridization for **R3** and **R4**

Mission mode

CM/SM (not in secure premises)

(Unbounded number of signed commands: ML-DSA or hybrid)

ECDSA + ML-DSA

Otherwise the assurance continuity stops dead after some time. Non compliance to EU CRA directive!

Otherwise an attacker can spy on a confidential data (SK) or change / choiose the data (PK)

R4: (unbounded) assurance continuity

Caption: To be transitioned to PQC / System-level requirements

Pre-silicon Authentication Algorithms for Injection

- Pre-silicon: chip manufacturer / system manufacture key pairs are generated
  - We made an abstraction:
    - Can be any amongst: `ed25519 ecdsa_p256 ecdsa_p384 ecdsa_p521 ecdsa_p521_sha3 rsa_4k xmss_10 xmss_16 mldsa44 mldsa65 mldsa87 ecdsa_p256+mldsa44`
- The HSM must not be the weakest point!
  - Its CMVP appliance must not only support PQC, but
  - also have all its FIPS 140-3 services be PQC!
- Secure-IC offers Securyzr Server, fully PQC ready!
  - CMVP certification to be announced early 2025


Secure-IC HQ datacenter

Common Criteria
ALC_DVS
SERMA
SAFETY & SECURITY


https://www.wired.com/2015/02/

WIRED

Gemalto Confirms It Was Hacked But Insists the NSA Didn't Get Its Crypto Keys

As the the company confirmed the hacks, it downplayed their significance, insisting that the attackers failed to get inside the network where cryptographic keys are stored to protect mobile communications.

Firmware Management Algorithms must be Hardware

- According to FIPS 140 (ISO/IEC 19790), from level 3 onwards, FW verification must rely on asymmetric cryptography

Approved digital signature-based integrity test.

Table 1 - Summary of security requirements

	Security Level 1	*Security Level 2*	*Security Level 3*	*Security Level 4*
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, approved security functions, and normal and degraded modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. All services provide status information to indicate when the service utilises an approved security function or process in an approved manner.			
Cryptographic Module Interfaces	Required and optional interfaces. Specification of all interfaces.		Plaintext trusted path.	
Roles, Services, and Authentication	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	Multi-factor authentication.
Software/Firmware Security	Approved integrity technique. Defined module interface.	Approved digital signature or keyed message authentication code-based integrity test.	Approved digital signature-based integrity test.	

- As per CNSA 2.0 roadmap, all asymmetrical cryptographic checks must be PQC
- Starting from ROM, a verification chain must be implemented
  - After ROM, the next verification is named the « first mutable firmware »
  - Hence our CAVP A6046 certificate is of « hardware » type
    - Hardware + ROM is eligible
  - Future-proofness:
    - of the IP is at pre-silicon
    - of the product is at post-silicon

HW future-proofness!

Not an utopia :)

Secure Channel Establishment for Provisioning

- Provisioning environment is not always secure
  - Supply-chain attack
- Threats are:
  - During selection of ciphersuite:
    - Downgrade attack (= selection of an pre-quantum algorithm)
  - During selection of keys:
    - Provisioning is done abroad: falsification of PK (provisioning of chosen PK), or stealth of secret/private key
    - Error in written keys (default or trivial keys, mix-up between independent key sets, or re-injection of same keys)
    - Over-provisioning
- Solution:
  - Secure channel, leveraging fresh challenge-response protocol
    - Such as TLS
  - Can be based on ML-KEM and/or some hybrid version of it
    - X-Wing: general-purpose hybrid post-quantum KEM ; draft-connolly-cfrg-xwing-kem-06

Assurance Continuity

- Mandated by EU CRA regulation, adopted Oct 10, 2024
- Stateful algorithms cannot apply

Cost of cyber-crime:

Every 11 seconds there is a **ransomware attack**

Ransomware attacks alone are estimated to have cost the world roughly **€20 billion** in 2021

The **global annual cost** of cybercrime was estimated to be **€5.5 trillion** in 2021

Cost of non-compliance to EU CRA:

- **EUR 15 million** or
- **2.5 % of the total worldwide annual** turnover of the preceding fiscal year – whichever is higher.

Benefits of Secure-IC offering for device manufacturers:

- **No risk** of cyber-crime
- **No risk** of EU fines
- **Longer** product operation
- Positive impact on the **reputation**

AGENDA

1. Introduction
2. PQC risk analysis
3. PQC technologies completeness
4. PQC technologies consistency
5. Conclusions and perspectives

SECURE-iC
THE SECURITY SCIENCE COMPANY

Cryptographic consistency, single algorithms

- Multiple algorithms are used, but how to have their security level match? (sizes in bits)

Level / Mechanism	1	2	3	4	5
Symmetric encryption	128		192		256
Message Authentication tag	128		128		128
Hash function	256		384		512
PQC asymetric functions	ML-KEM-512		ML-KEM-768		ML-KEM-1024
	SLH-DSA-SHA2-128s		SLH-DSA-SHA2-192s		SLH-DSA-SHA2-256s
	ML-DSA-44		ML-DSA-65		ML-DSA-87

Table III: CNSA 2.0 quantum-resistant public-key algorithms

Algorithm	Function	Specification	Parameters
CRYSTALS-Kyber	Asymmetric algorithm for key establishment	TBD	Use Level V parameters for all classification levels.
CRYSTALS-Dilithium	Asymmetric algorithm for digital signatures	TBD	Use Level V parameters for all classification levels.

SECURE-IC
THE SECURITY SCIENCE COMPANY

Cryptographic consistency, hybridized algorithms

- Multiple algorithms are used, but how to have their security level match?

Hybridation modes

In general, as for any cryptographic function, ANSSI recommends to use **standards or well-studied modes with validated security proofs.**
➡ The implementation security (side-channel resistance) of the hybridation mode is also very important to avoid attacks that would bypass certain key encapsulations.

	IND-CPA robustness	IND-CCA robustness
CAT	×	×
XOR	✓	×
XOR then PRF	✓	(×)
Dual-PRF	✓	(✓)
CAT then KDF	✓	(✓)
CASCADE	✓	(✓)

For **IND-CCA robustness**:
- research is still ongoing
- the modes did not pass the « test of time »

In addition, XOR and XOR then PRF may be relevant to achieve **IND-CPA robustness.**

Cat then KDF and CASCADE seem as good options.
➡ Drafted for being included at a protocol level (TLS, IKE).

23

- D. Stebila, S. Fluhrer, and S. Gueron. Hybrid key exchange in TLS 1.3 (draft IETF). https://www.ietf.org/id/draft-ietf-tls-hybrid-design-03.html
- C. Tjhai, M. Tomlinson, G. Bartlett, S. Fluhrer, D. Van Geest, O. Garcia-Morchon, and V. Smyslov. Multiple Key Exchanges in IKEv2 https://datatracker.ietf.org/doc/draft-ietf-ipsecme-ikev2-multiple-ke/

Hybrid Signatures

The solutions for hybrid signatures are less diverse.
The signature scheme below is proved secure in the existential unforgery under chosen message attacks model (EUF-CMA).

Let n signature schemes $\mathsf{SIG}_i = (\mathsf{KeyGen}_i, \mathsf{Sign}_i, \mathsf{Verif}_i)\ 1 \leq i \leq n$

$\widetilde{\mathsf{KeyGen}}()$
for $i = 1 \dots n$ **do**
$(sk_i, pk_i) \leftarrow_S \mathsf{KeyGen}()$
$\overrightarrow{sk} = (sk_i)_{1 \leq i \leq n}$
$\overrightarrow{pk} = (pk_i)_{1 \leq i \leq n}$
return $(\overrightarrow{sk}, \overrightarrow{pk})$

$\widetilde{\mathsf{Sign}}\left(\overrightarrow{sk} = (sk_i)_{1 \leq i \leq n}, m\right)$
for $i = 1 \dots n$ **do**
$\sigma_i \leftarrow \mathsf{Sign}(sk_i, m)$
return $\widetilde{\sigma} = (\sigma_i)_{1 \leq i \leq n}$

$\widetilde{\mathsf{Verif}}\left(\overrightarrow{pk} = (pk_i)_{1 \leq i \leq n}, m, \widetilde{\sigma}\right)$
for $i = 1 \dots n$ **do**
if $\mathsf{Verif}(pk_i, m, \sigma_i) = 0$ **then return** 0
return 1

24

Example: transitioning OpenSSL `TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256`

--> `ML-KEM-{512,768,1024}` `ML-DSA-{44,65,87}` `SHA3-{224,256,384,512}`

Source: PQC TRANSITION IN FRANCE, ANSSI VIEWS. Mélissa Rossi, ANSSI, France. Real World Post-Quantum Crypto March 26th 2023 Tokyo.
https://cyber.gouv.fr/en/publications/follow-position-paper-post-quantum-cryptography

AGENDA

SECURE-iC THE SECURITY SCIENCE COMPANY

Conclusions & Perspectives

- PQC transition starts by embedded devices
- It requires deep transformations:
  - Cryptographic primitives to be evolved, from symmetric (larger key lengths) to asymmetric (novel algorithms, some of them not standardized yet, with varying parameter sized)
  - Must be thought at an holistic level, whereby all cryptographic mechanisms in place must be questioned (authentication & provisioning, authorization, secure channel, attestation, ...)
  - Given the fragmentation of regulations, crypto-agility is required, especially to meet the hybridization requirement from ANSSI / ENISA

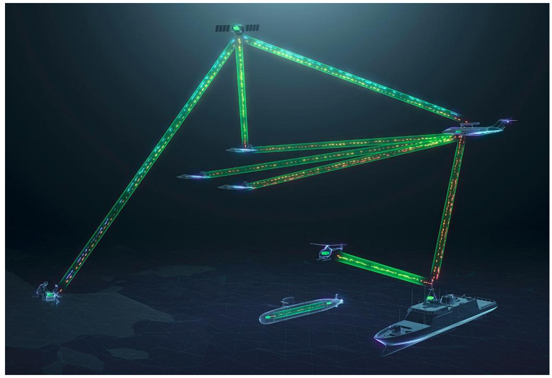
« ANSSI is currently speeding-up the original agenda. First phase-2 security visas for products implementing hybrid post-quantum cryptography are expected to be delivered around 2024-2025. » [ANSSI]

- Secure-IC analysed the need under the prism of 5 system-level requirements
- Implementation of Securyzr neo Core Platform is already complying
- Perspectives: involving our Customers into their own PQC transition

[ANSSI] https://cyber.gouv.fr/sites/default/files/document/follow_up_position_paper_on_post_quantum_cryptography.pdf

Acknowledgments

- Acknowledgments to BPI, for X7PQC project
  - With Hensoldt France
- Acknowledgements to Embedded France
  - [GT cyber]
- Secure-IC is PI (leader) of project QUASAR:
  - European call `HORIZON-CL3-2024-CS-01-02`
  - Partners: Leonardo, Italtel, CNIT, DNSC (Cyber Agency of Romania), etc.
- Secure-IC is also delegate and active contributor of AFNOR for:
  - ISO/IEC JTC 1/SC 27/WG 2 - Cryptography and security mechanisms
  - ISO/IEC JTC 1/SC 27/WG 3 - Security evaluation, testing and specification



Regarding tools, see:

- A. Facon, S. Guilley, M. Lec'Hvien, A. Schaub and Y. Souissi, "Detecting Cache-Timing Vulnerabilities in Post-Quantum Cryptography Algorithms," 2018 IEEE 3rd International Verification and Security Workshop (IVSW), Costa Brava, Spain, 2018, pp. 7-12, DOI: 10.1109/IVSW.2018.8494855.

SECURE-IC

THE SECURITY SCIENCE COMPANY

THANK YOU FOR YOUR ATTENTION

CONTACTS

EMEA	sales-EMEA@secure-IC.com
APAC	sales-APAC@secure-IC.com
CHINA	sales-CHINA@secure-IC.com
JAPAN	sales-JAPAN@secure-IC.com
AMERICAS	sales-US@secure-IC.com

European Cyber Week by Pôle d'Excellence Cyber

THE SOVEREIGN CYBER & DEFENCE AI FORUM