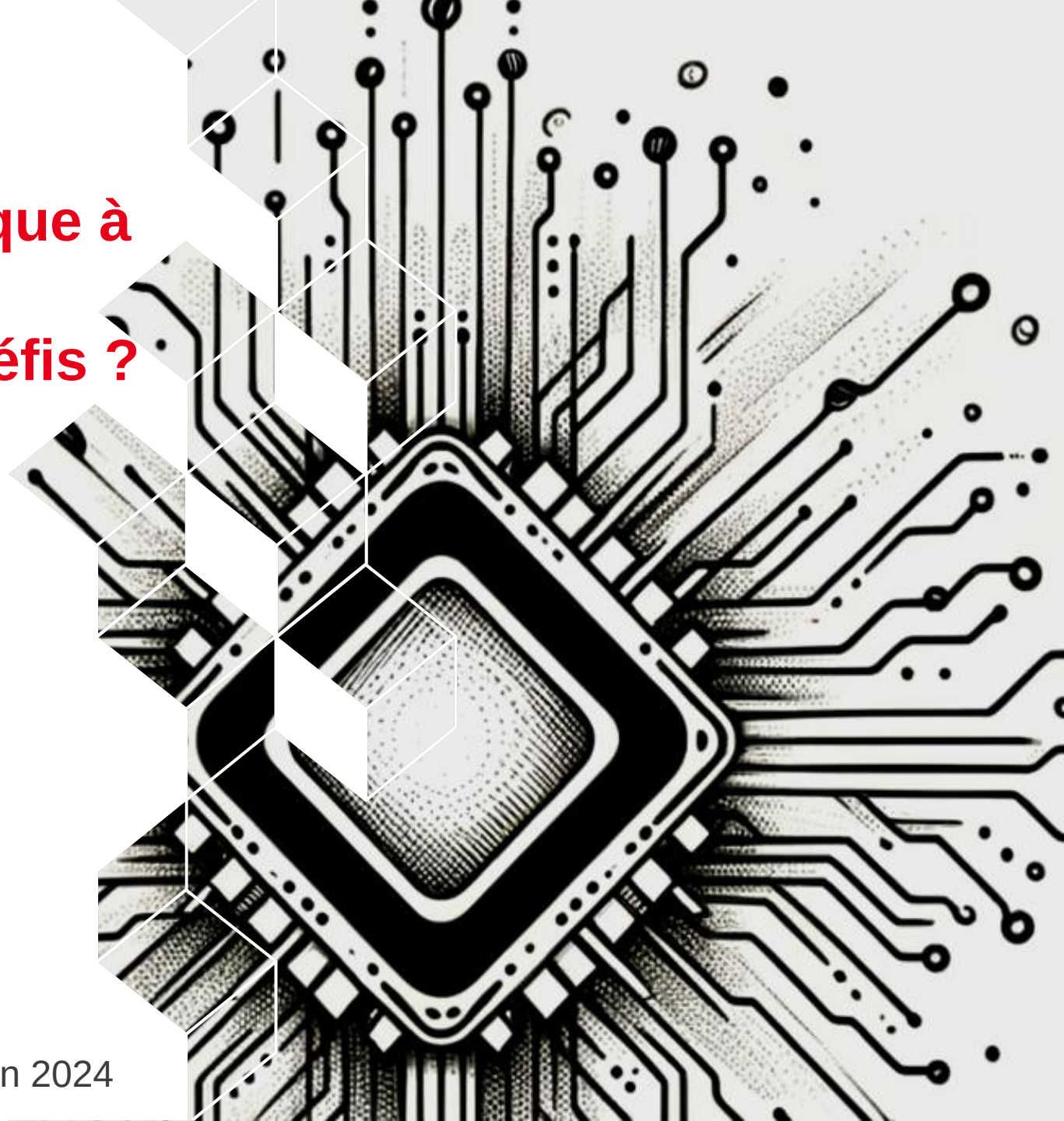
Conférence

"Sécurité numérique à l'ère quantique : opportunités et défis ?



Quelques enjeux technologiques de la transition post-quantique

Mikael CARMONA

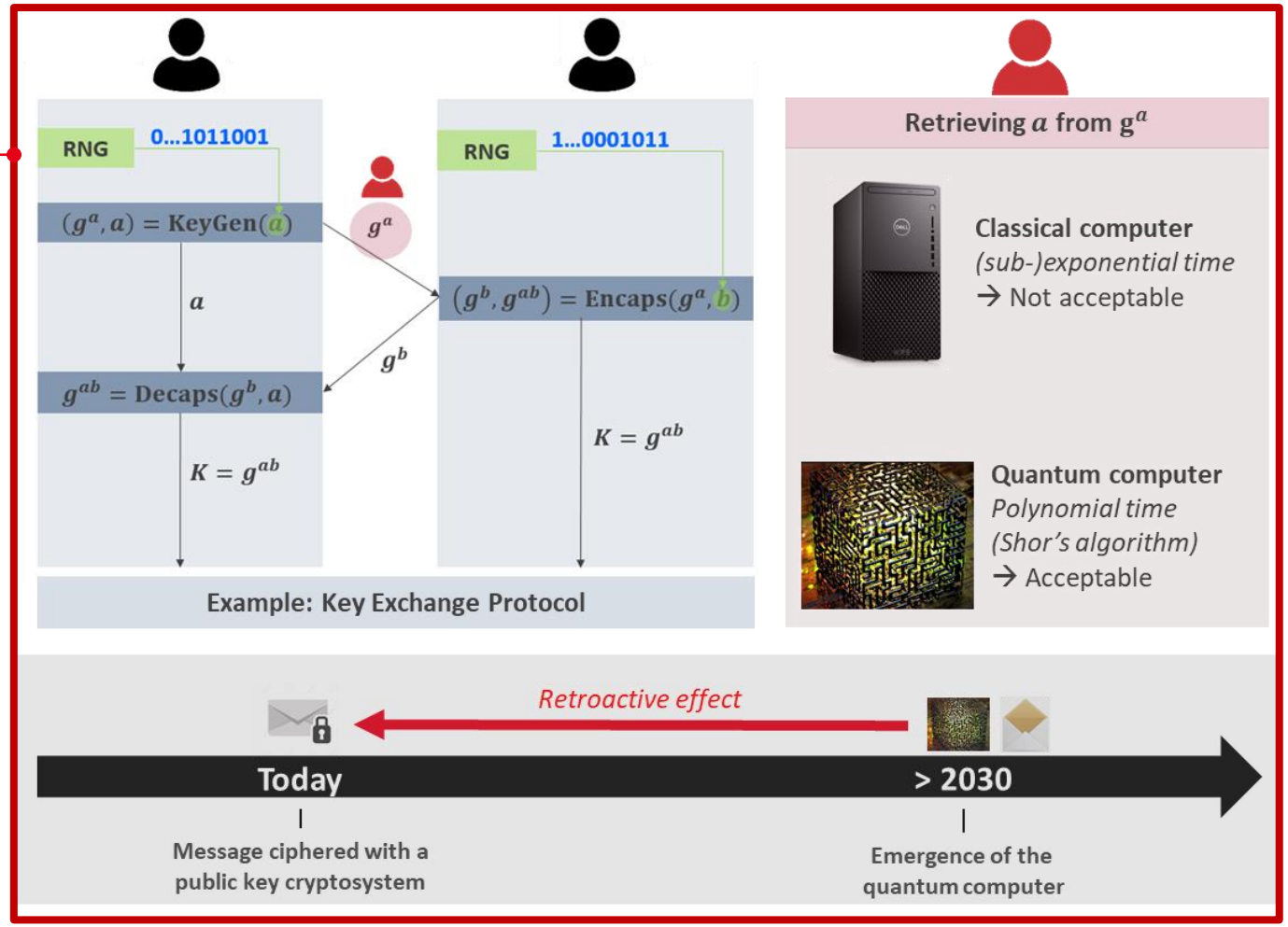
Responsable du Laboratoire Sécurité des Composants

CEA-Leti

Mardi 25 juin 2024

Agenda

1. **The quantum threat**
2. **Emergence of PQC**
3. **Technological challenges**
4. **Conclusions & Next steps**



P. Shor, **Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer**, Symposium of Foundations on Computer Science, 1994.

The quantum threat

Impact

- **Making asymmetric crypto. vulnerable**
  - Authentication, signature, public key encryption
  - Secure communications (TLS, authentication and key exchange), firmware signature

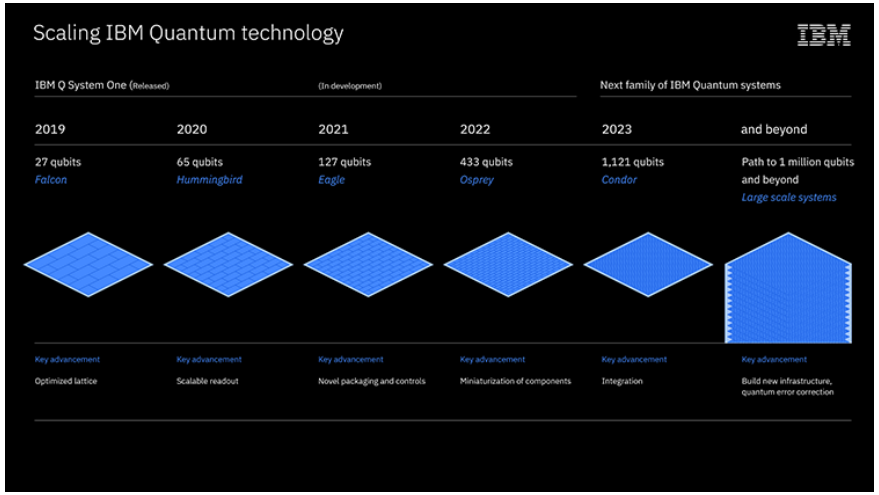
- **Weakens symmetric cryptography**
  - Secure communications (TLS, data encryption and integrity), authenticated encryption (AE)

Algorithm	Key Length	Effective Key Strength / Security Level	
		Conventional Computing	Quantum Computing
RSA-1024	1024 bits	80 bits	0 bits
RSA-2048	2048 bits	112 bits	0 bits
ECC-256	256 bits	128 bits	0 bits
ECC-384	384 bits	256 bits	0 bits
AES-128	128 bits	128 bits	64 bits
AES-256	256 bits	256 bits	128 bits

*Security level regarding classical and quantum computing of standardized primitives (from **NIST PQC Specifications**).*

Effectiveness

- In 20 years or more…but…it is better to anticipate the transition now ! (Mosca's theorem)



IBM roadmap on Quantum computer and effective qubits.

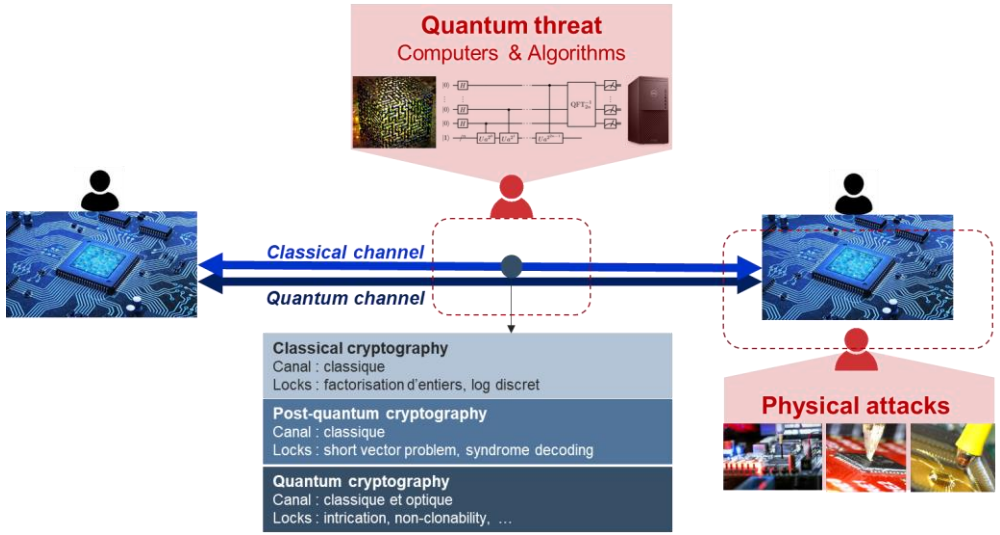
- Advances in quantum computing accelerate the emergence of the threat

@CEA: E. Gouzien, N. Sangouard, ***Factoring 2048-bit RSA Integers in 177 Days with 13436 Qubits and a Multimode Memory***, Physical Review Letters, 2021

The quantum threat

2 answers

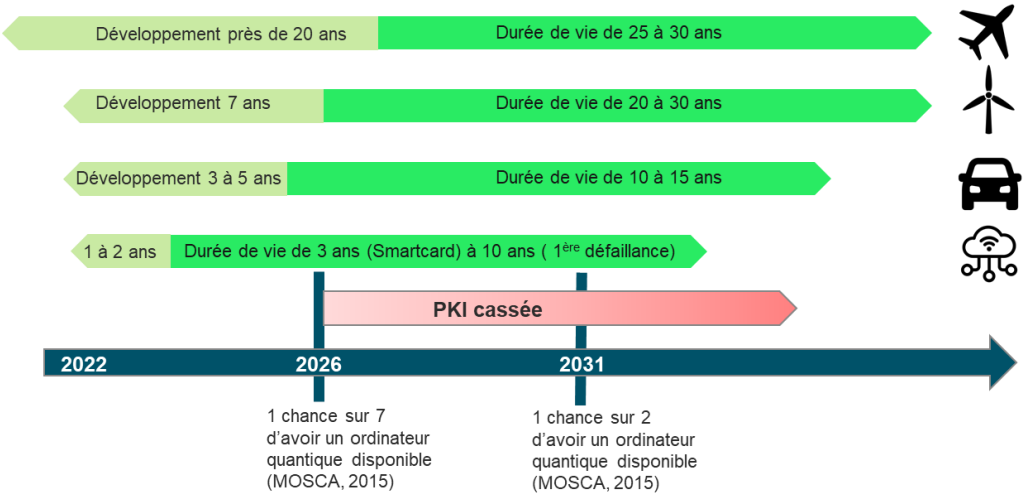
- **Post-quantum Cryptography (PQC):** changing mathematical problems underlying the security
- **Quantum Key Distribution (QKD):** changing paradigm of security using physical properties



Cryptographies *(Classical, Post-quantum and Quantum) and* ***Threats*** *(Classical and Quantum computers, Physical attacks)*

Context impact and constrains

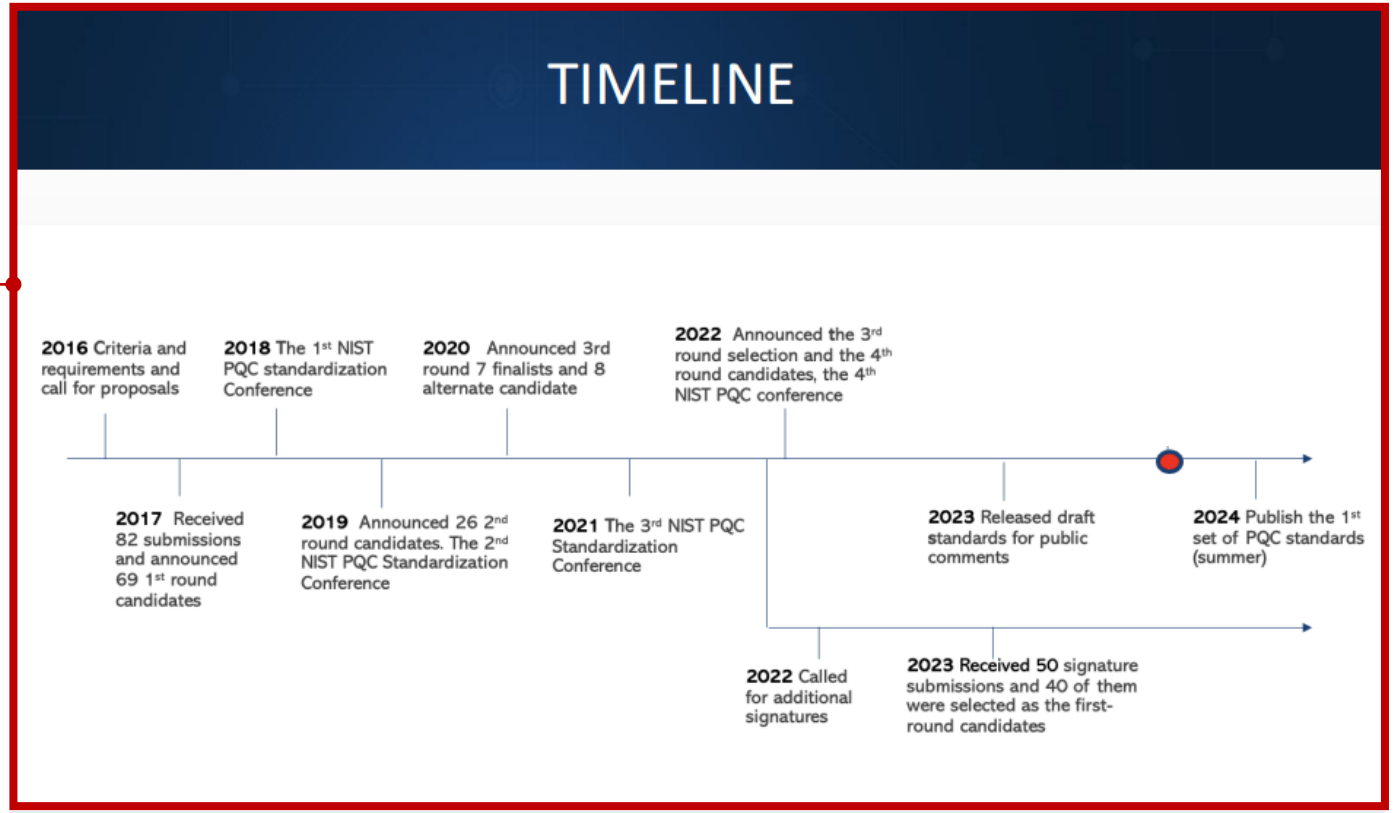
- Resilience to **classical & quantum** computers
- Resilience to **physical attacks**
- **Security-perf.-cost** compromise optimization
- New **Protection Profile and Standards**



Development and operating lifetime for some market VS predicted availability of a quantum computer (from ***CEA Marketing Unit****).*

Agenda

1. The quantum threat
2. Emergence of PQC
3. Technological challenges
4. Conclusions & Next steps



Ilustration from NIST, ***Are we there yet? An Update on the NIST PQC Standardization Project****, 5th NIST PQC conference, 04 2024.*

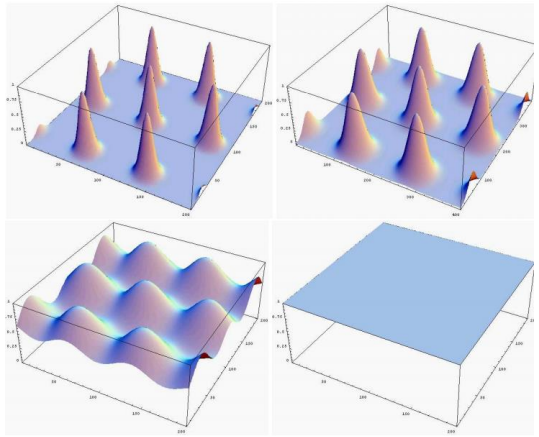
Emergence of PQC

$$\begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \cdots & \vdots \\ a_{n1} & \cdots & a_{nm} \end{bmatrix} \begin{bmatrix} s_1 \\ \vdots \\ s_m \end{bmatrix} + \begin{bmatrix} e_1 \\ \vdots \\ e_n \end{bmatrix} \bmod q$$

Relation between instances of a LWE Problem

➢ The LWE Problem

- The **LWE problem** has the following instances:
  - $n, m \geq n$, and q strictly positive integers.
  - $\boldsymbol{A} \in \mathbb{Z}_q^{nxm}$ uniform random matrix.
  - $\boldsymbol{s} \in \mathbb{Z}_q^m$ uniform random vector.
  - $\boldsymbol{e} \in \mathbb{Z}_q^n \sim D_{\mathbb{Z}_q^n,0,\alpha}$ discrete Gaussian vector with $\alpha > 0$
  - $\boldsymbol{b} = \boldsymbol{A}\,\boldsymbol{s} + \boldsymbol{e} \bmod q$.



Period discrete Gaussian law for different variance, from Regev

- The problem $\mathrm{LWE}(n, m, q, \alpha)$ has two versions:
  - **Search**: to retrieve $\boldsymbol{s}$ knowing $(\boldsymbol{A}, \boldsymbol{b}, \alpha)$ → *public/private keys generation*
  - **Decision**: to distinguish $\boldsymbol{b}$ distribution VS random distribution → *arithmetic masking*

- LWE reduces to **NP-complete problems if $\alpha q > 2\sqrt{n}$.**

O. Regev, **On lattices, learning with errors, random linear codes, and cryptography**, Journal of ACM, 2009.

- If $\boldsymbol{s}$ is a discrete Gaussian vector, the problem is called **normal form** of LWE. Other forms of LWE exist.

Emergence of PQC

Impact on metrics

- **Instance sizes:** post-quantum cryptography increases significantly the sizes
- **Execution time:** lattice-based cryptography is highly efficient even regarding classical cryptography
- **Memory consumption** and **entropy consumption** increase significantly for secure implementation

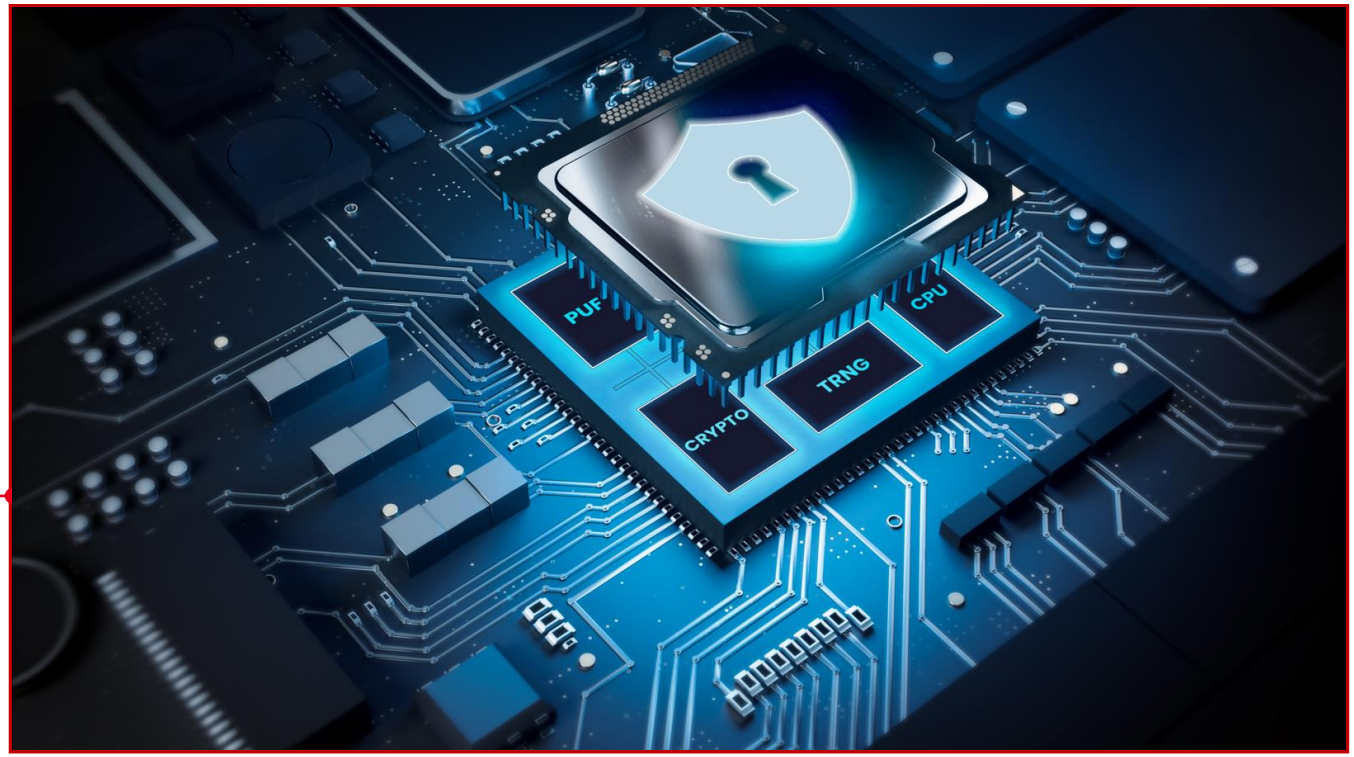
	KEM	Framework (& Security)	PK Size (bytes)	SK Size (bytes)	Ciphertext size (bytes)	Security Level
Selected →	**CRYSTALS-KYBER**	**Lattice-based (MLWE)**	**800**	**1 632**	**768**	**128 bits (Lev1)**
	CLASSIC McELIECE	Code-based (Goppa codes)	261 120	6 492	128	128 bits (Lev1)
	BIKE	Code-based (QC-MDPC)	1 540	280	1 572	128 bits (Lev1)
	HQC	Code-based (QCSD)	2 249	40	4 481	128 bits (Lev1)
Pre-quantum (for comparison) →	**X25519**	**Elliptic Curve-based**	**32**	**32**	**32**	**128 bits**

	DS	Framework (& Security)	PK Size (bytes)	SK Size (bytes)	Signature size (bytes)	Security Level
	CRYSTALS-DILITHIUM	**Lattice-based (MLWE and MSISSelfTarget)**	**1 312**	**2 528**	**2 420**	**>128 bits (Lev2)**
	FALCON	**Lattice-based (R-SIS)**	**897**	**7553**	**666**	**128 bits (Lev1)**
	SPHINCS+	**Hash-based (stateless, ROM)**	**32**	**64**	**7856**	**128 bits (Lev1)**
Pre-quantum (for comparison) →	**Ed25519**	**Elliptic Curve-based**	**32**	**32**	**64**	**128 bits**

Instances sizes *for selected and alternate candidates for KEM and DS.* ***Comparison with classical crypto****.*

Agenda

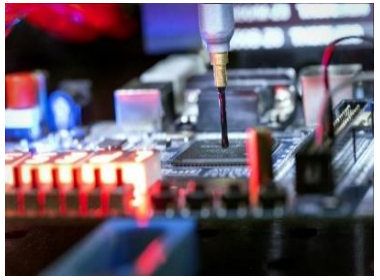
1. The quantum threat
2. PQC: principle and timeline
3. Technological challenges
4. Conclusions & Next steps

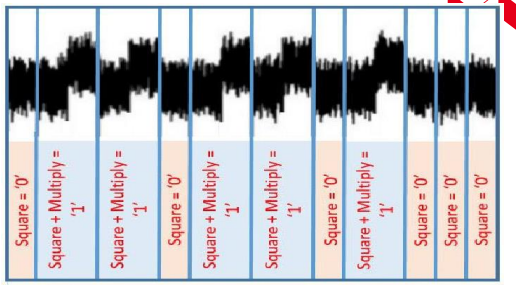


Technological challenges

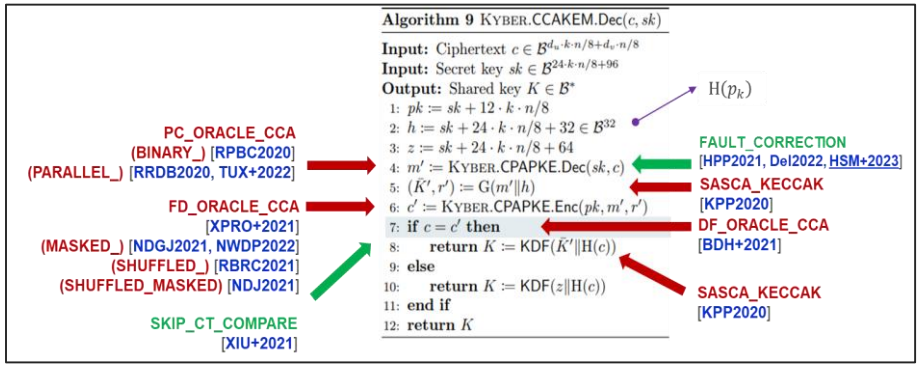
➢ Security against physical attacks: part 1

- Physical attacks are a main threat for security-oriented components
- Post-quantum quantum cryptography comes wits own attack surface
- > 20 attacks on KYBER & > 15 attacks on DILITHIUM → **the first « wave » is not finished !**
- **Amplification of advance attacks:** IA-based, SASCA-based, combination SCA & FIA

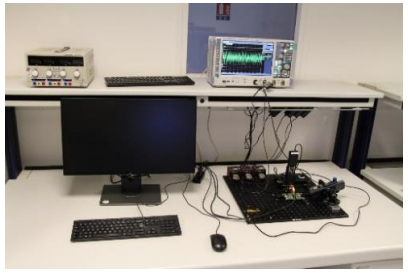




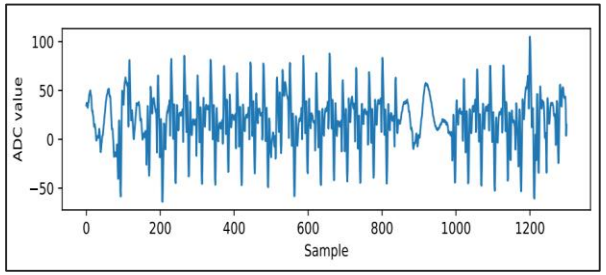
From M. Randolph, W. Dielph, **Power Side-Channel Attack Analysis: A Review of 20 Years of Study for the Layman**, *MDPI Cryptography, 2020.*



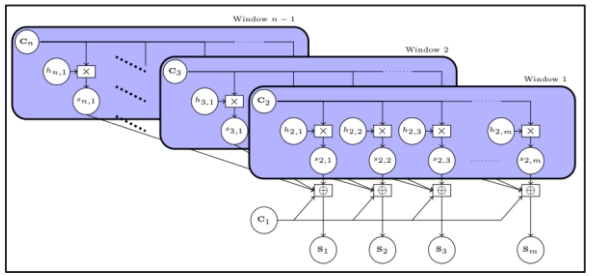
Identified physical attacks on KYBER.DECAPS @01 2024.



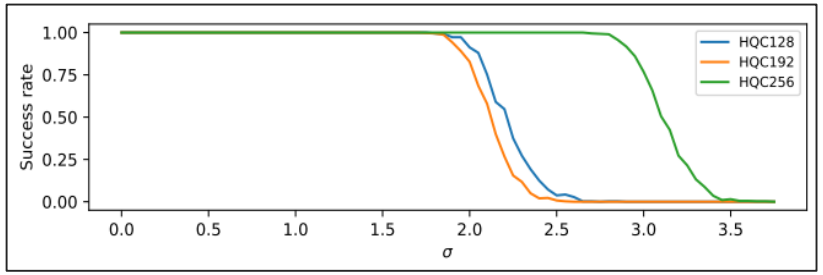
1. Experimental setup for side-channel analysis



2. Observed & Computed traces



3. Formalizing & injecting known information

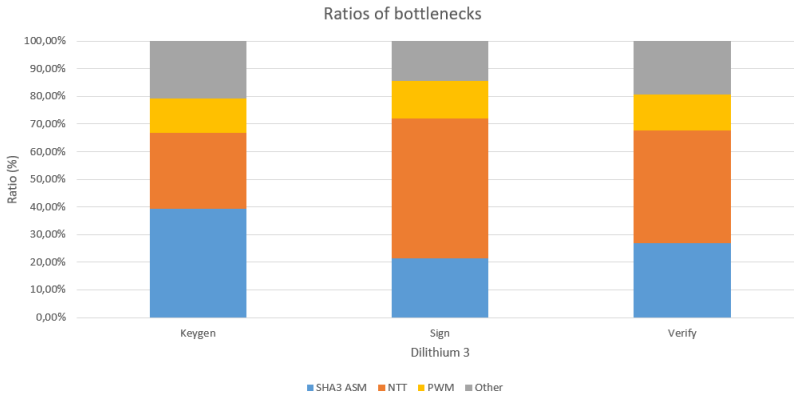


4. Retrieving secret information from data fusion and leakage models

Technological challenges

➢ HW acceleration for efficient implementations

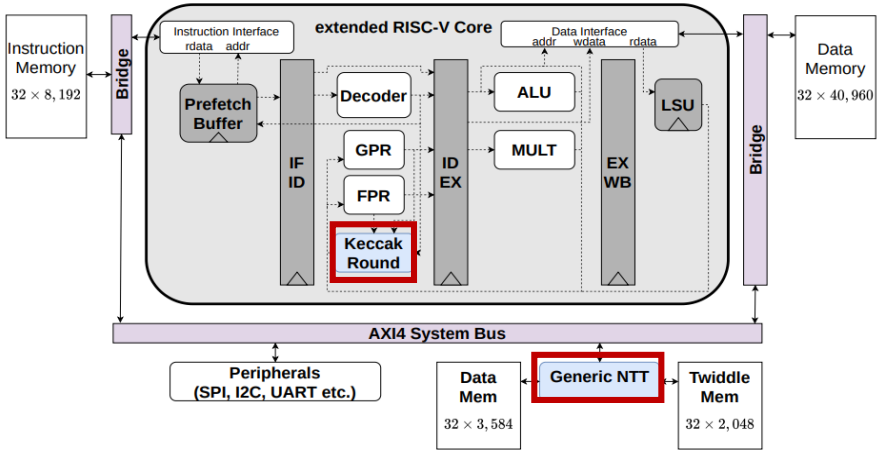
- Bottlenecks of PQC are identified
  - **Hash (70%)** → no SHA-3 on many existing HW!
  - **Polynomial multiplication**
  - **Non-uniform sampling & modular arithmetic**
  - **Security against side-channel attacks !**



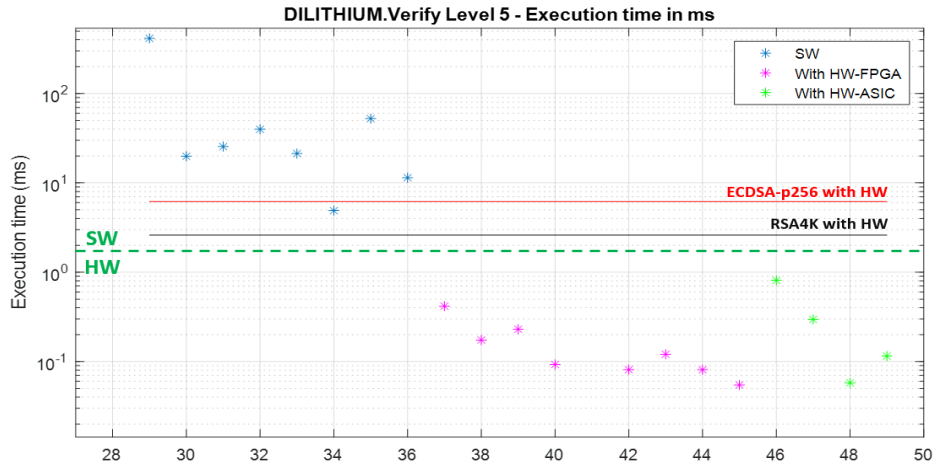
Bottlenecks analysis of DILITHIUM in Software on STM32H7 (from CEA)

- They are critical for **constrained devices** (SE) and **applications** (secure boot for automotive, TLS for cloud services)

- Accelerations strategies are multiple and amplified with RISC-V emergence



Example of one of the most advanced architecture [KSFS2023] accelerating KYBER in HW and RISC-V based

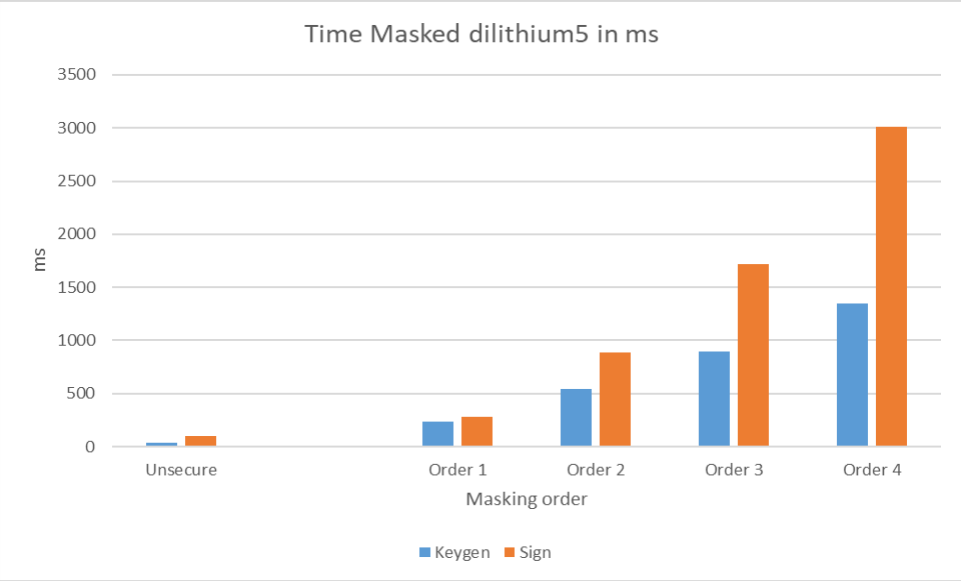


Performances analysis of existing implementations of DILITHIUM (from CEA). Comparison with existing embedded classical cryptography.

Technological challenges

Security against physical attacks: part 2

- The cost of countermeasures for PQC is high for the main metrics:
  - **Performance**, **Memory**, **Entropy consumption**
  - **Surface** for HW implementations



Impact on execution time of masking for DILITHIUM Lev 5, from CEA benchmark

Order	KeyGen	Sign	Verify
0	98	123	92
1	130	178	92
2	161	233	92
3	193	288	92
4	225	344	92

Impact on RAM of masking for DILITHIUM Lev 5, from CEA benchmark

Order	KeyGen	Sign 1 loop	Sign mean	Verify
0	32	32	64	0
1	1267744	579972	2232892	0
2	3757088	2528664	9735356	0
3	7483424	6661072	25645127	0
4	12446752	13778016	53045361	0

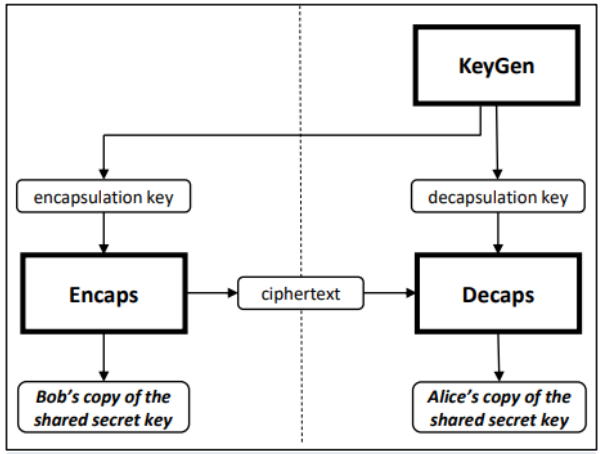
Impact on entropy of masking for DILITHIUM Lev 5, from CEA benchmark

- Innovation on **lightweight countermeaures** is fundamental

Technological challenges

Deployement

- At the **cryptosystem level**
  - Hybridization
  - Agility
- At the **protocol level (TLS, IPSec, …)**
- At the data format level (**certificates**)



KEM Description, from NIST

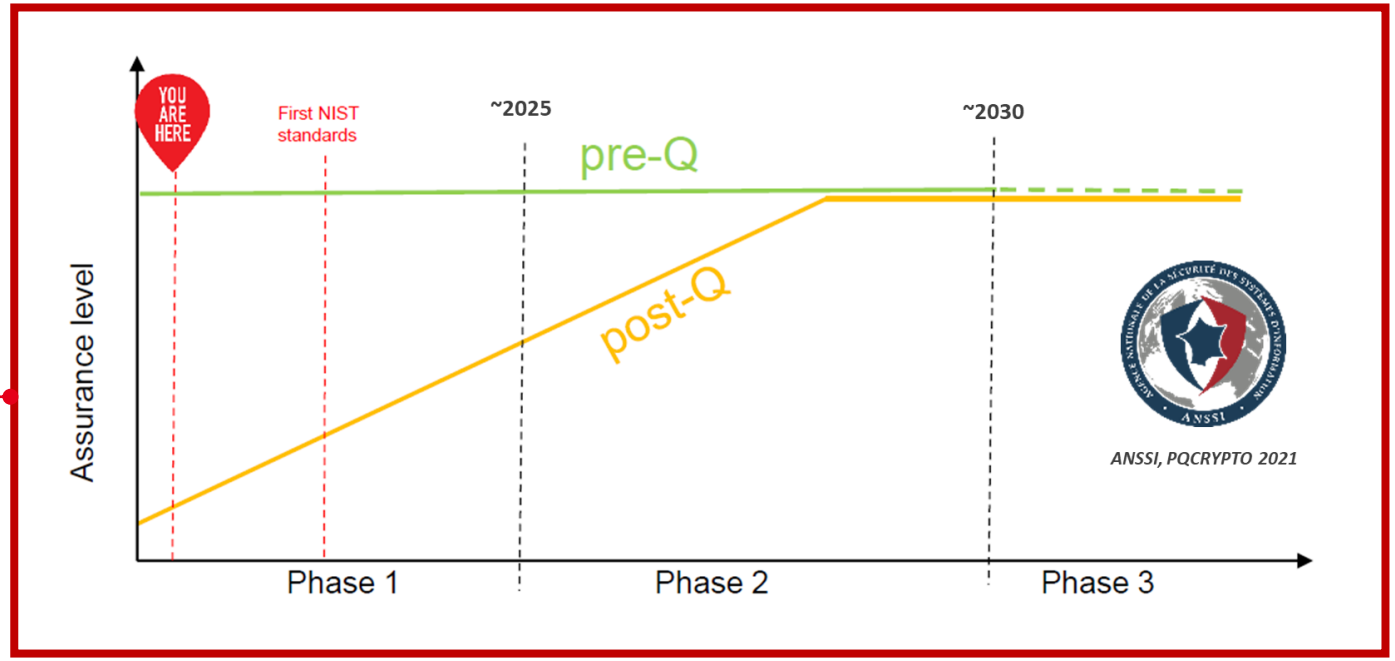
	IND-CPA robustness	IND-CCA robustness
CAT	×	×
XOR	✓	×
XOR then PRF	✓	(×)
Dual-PRF	✓	(✓)
CAT then KDF	✓	(✓)
CASCADE	✓	(✓)

Hybridization solutions and semantic security, from ANSSI

- **No evident and unique choices at each level to start the migration…..**

Agenda

1. The quantum threat
2. PQC: context
3. Technological challenges
4. Conclusions & Next steps



Conclusions & Next steps

➢ Migration has started !

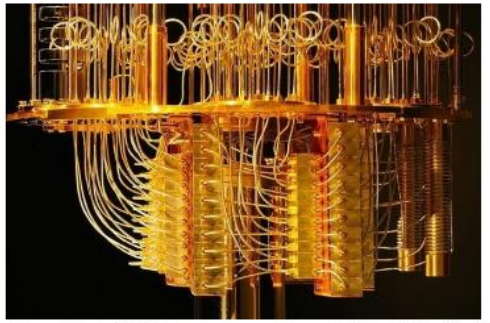
- **Standards are close to follow their initial roadmap**
  - Drafts are ready since 2023, standards waited in 2024
  - Cryptographic suites 2.0 are identified
  - PQC-oriented IETF drafts are in progress

- **Industrial starts post-quantum-ready products**
  - HW IP (Rambus, …)
  - HSM (Thalès, Ultimaco), SE (Thalès, Idemia, Infineon, …)
  - Lib crypto (CryptoNext, …), PKI & Related tools (OQS, …)
  - Alliances, structuration, consortiums, working groups, …

➢ But there is still issues

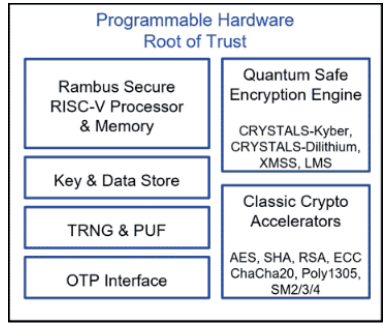
- **Security against physical attacks**
- **Performances achievement** under cost contraints
- **Standards are still moving and at different levels** (cryptosystems, protocols, certificates, …)

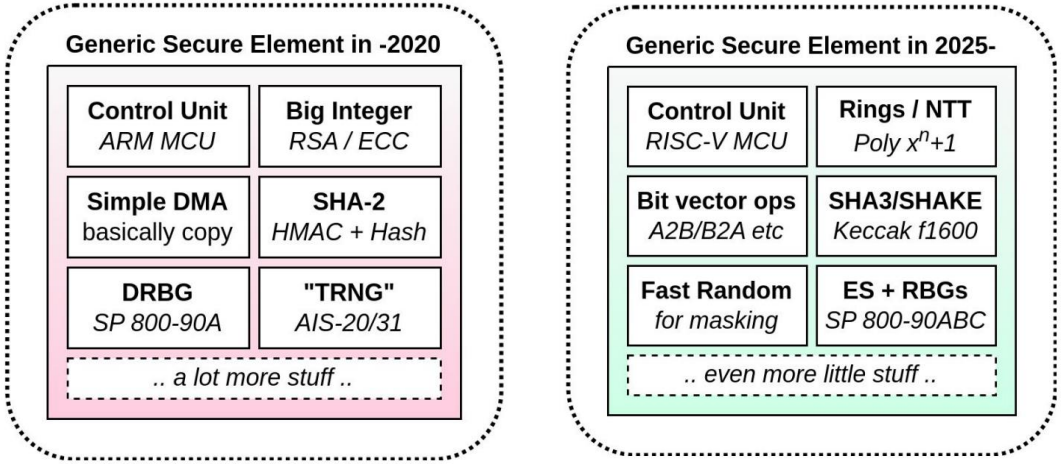
La fondation Linux a lancé une alliance pour la cryptographie post-quantique (PQCA) pour promouvoir l'avancement et l'adoption de la cryptographie post-quantique. AWS, Cisco, Google, IBM et Nvidia font partie de ses membres.



Parmi les participants à PQCA, il y a plusieurs grands noms de l'IT dont IBM. (crédit : IBM)

Rambus Delivers Quantum Safe IP Solutions with Next-Generation Root of Trust for Data Center Security





From M-J. O. Saarinen, **RISC-V Cryptography and Hardware Security**, RISC-V Technical Sessions, 2024.

Next steps @CEA

➢ Pursuing roadmaps

▪ On physical attacks

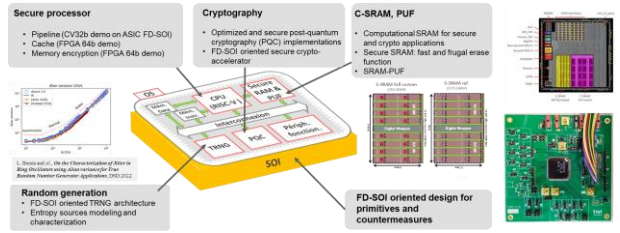
- G. Goy and *al.*, **Single-trace HQC session key recovery with SASCA**, CHES 2024 & 5th NIST PQC Conference.
- R. Carrera-Rodriguez and *al.*, **Correlation electromagnetic analysis on an FPGA implementation of CRYSTALS-Kyber**, PRIME 2023
- G. Goy and *al.*, **A New Key Recovery Side-Channel Attack on HQC with Chosen Ciphertext**, PQCrypto 2022 & 4th NIST PQC Conference.
- G. Goy and *al.*, **Estimating the Strength of Horizontal Correlation Attacks in the Hamming Weight Leakage Model: A Side-Channel Analysis on HQC**, WCC 2022.
- L. De Feo and *al.,* **SIKE channels: Zero-value side-channel attacks on SIKE**, CHES 2022.
- É. Tasso and *al.,* **Resistance of isogeny-based cryptographic implementations to a fault attack**, COSADE 2021 & 3rd NIST PQC Conference.

▪ On secure, agile and efficient SW/HW implementations

- A. Dolmeta and *al.,* **On the implementation of a lattice-based DAA for VANET system**, SECRYPT 2024.
- D. Lesaigoux and *al.,* **On the implementation of a lattice-based DAA for VANET system**, SECRYPT 2024.
- A. Loiseau and *al*, **Securing DILITHIUM against physical attacks: performances analysis**, NATO Science for Peace and Security Series 2024.
- A. Ras and *al.* **Secure, Optimized and Agile HW/SW Implementation for Post-quantum Cryptography**, CHES 2023.
- M. Carmona and *al.*, **On the implementation of a lattice-based revocable hierarchical IBE**, SECRYPT 2023.
- M. Ramirez-Corrales and *al.*, **Improving Post-Quantum Cryptography coupling Near-Memory Computing and RISC-V Cores**, RISC-V Summit 2023
- S. Pontie and *al.*, **Post-quantum cryptography: Challenges and opportunities for robust and secure HW design**, IEEE DFT 2021.

▪ On national and european projects

PQ TLS



M. CARMONA

Head of Laboratory Security of Components

mikael.carmona@cea.fr

+33 7 86 86 15 21