# Secure, optimized and Agile HW/SW implementation for post-quantum cryptography

A. Ras, Mikael Carmona, Antoine Loiseau, Simon Pontie, Guenael Renault, Benjamin Smith, Emanuele Valea

# Secure, Optimized and Agile HW/SW Implementation for Post-quantum Cryptography

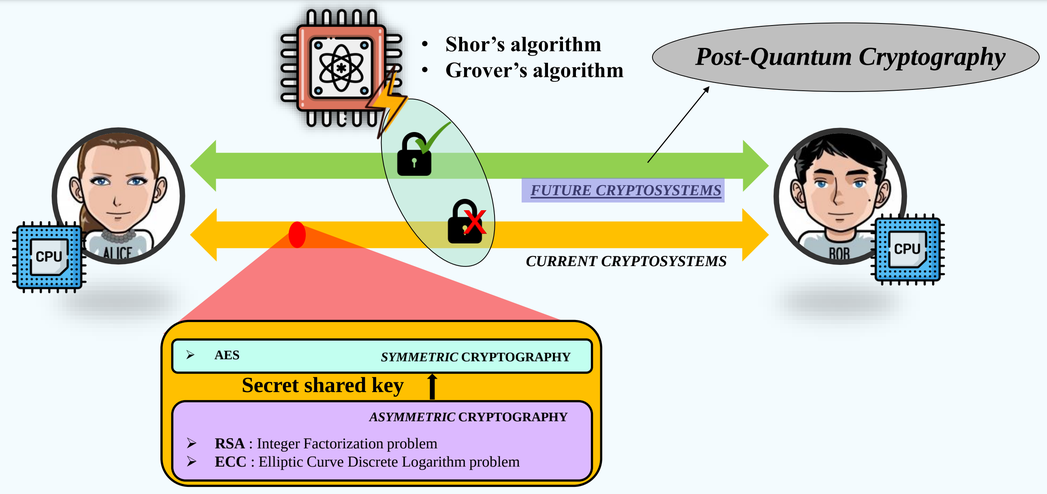
Follow us @CEA-Leti

**RAS Antonio**
Laboratory of Security of Components (LSCO)

## Context

### *Post-Quantum Cryptography* (PQC)

- Branch of cryptography, introduced due to cyber threats of **quantum computers**
  - ✓ Optimistic estimates of two decades to *break the cryptographic algorithms*
- Focus on **designing quantum-resistant** cryptographic algorithms that can be run on classical processors.
- The security of future cryptosystems rely on mathematical problems based on different approaches.

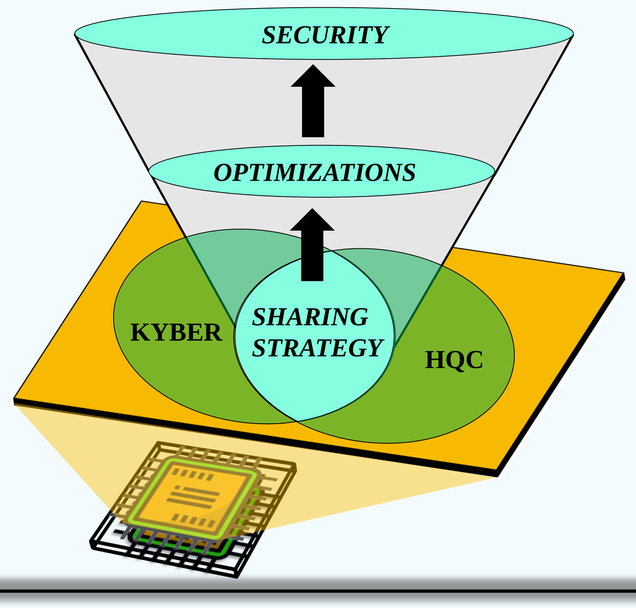


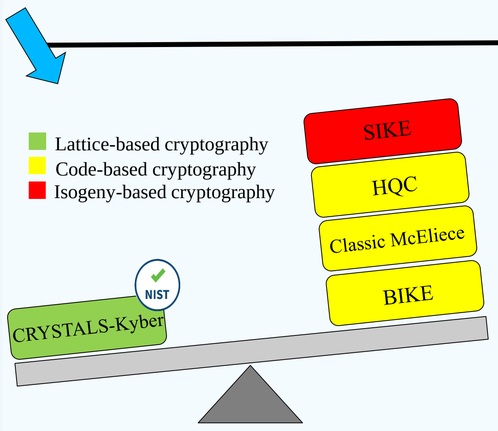

### *Motivations of Crypto-agility*

- Uncertain security of cryptosystems
- Standardization of many cryptosystems

### *Three main sphere of actions*

1. ***Sharing Strategy*** : mutualization of lower-level cryptographic primitives
2. ***Optimizations*** : Memory footprint, area surface and performance as main metrics
3. ***Security*** : side channel and fault injection attacks

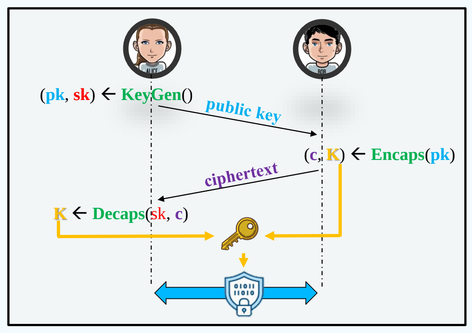



*NIST PQC competition : Round 4*

### *NIST PQC standardization project*

- Launched in 2016 to define new PQC cryptosystems that are meant to underpin the security of our future communications
- It involves two categories :
  - **Key Encapsulation Mechanisms** (KEM) and Digital Signatures (DS) algorithms
- **CRYSTALS-Kyber** [1] as first selected algorithm
- Three alternative candidates based on the theory of error-correcting codes, including **HQC** [2], may also be selected.




*KEM scheme*

## Targeted Crypto-Agility & State of the Art

**CRYSTALS-Kyber :** *Module-Learning with Error,* lattice-based problem

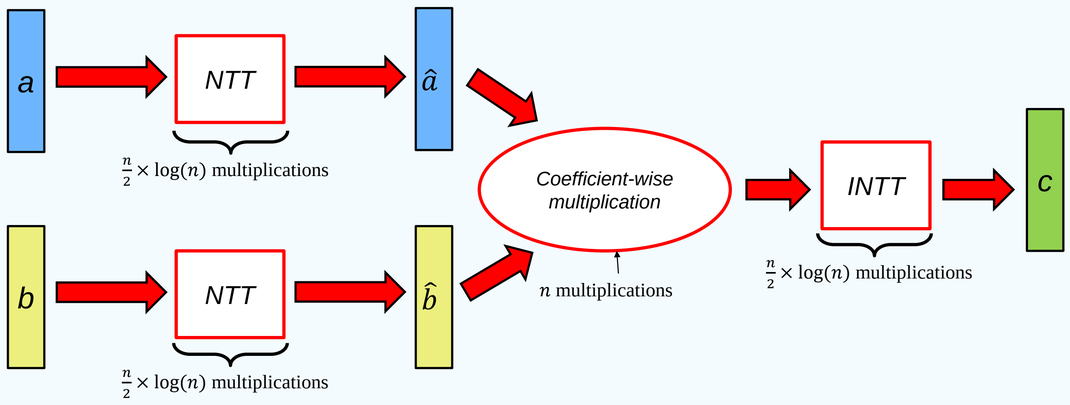
For a polynomial ring $R_q = \frac{\mathbb{Z}_q}{X^n+1}$. Given :

- A public $\boldsymbol{A} \in R_q^{kxk}$ and a secret $\boldsymbol{s} \in R_q^k$ obtained uniformly
- A small error $\boldsymbol{e} \in R_q^k$ whose coefficients are obtained from a binomial distribution $\chi^k$

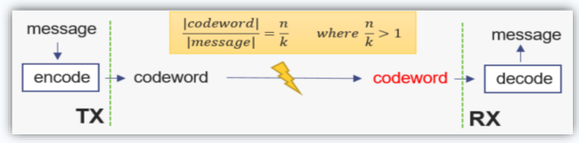
**Knowing $\mathbf{t} = \boldsymbol{As} + \boldsymbol{e}$ and $\boldsymbol{A}$, it is difficult to find $\boldsymbol{s}$**

**Polynomial multiplication with NTT (Number Theoretic Trasform)**

- NTT/INTT operations to switch data in the desired domain. Based on FFT, it has a regular structure, composed of butterfly units
- Coefficient-wise multiplication is performed using NTT operation structure




**Hamming Quasi-Cyclic :** *Quasi-Cyclic Syndrome Decoding,* code-corrector problem



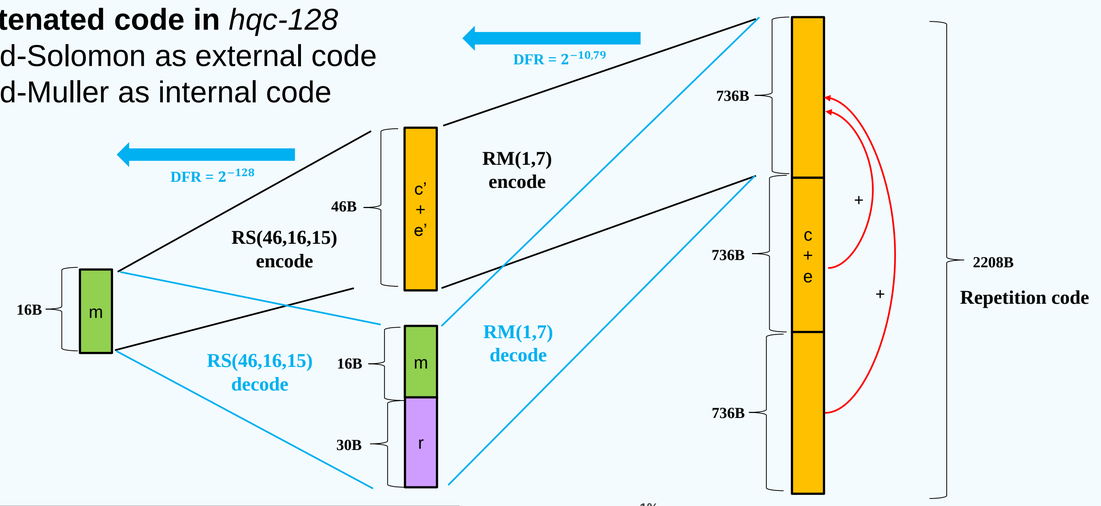

Given a random l-quasi-cyclic code $C(n, k, d)_q$ with parity-check matrix $H$, and a uniform $e \in \mathbb{F}_q^n$ with Hamming weight lower that $\omega$

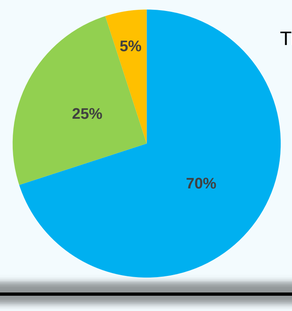
- *d* is the minimal distance of the code
- *H* is the matrix used to characterize the error

**Knowing $\boldsymbol{s} = \boldsymbol{eH^t}$ and $\boldsymbol{H}$, it is a difficult problem to find the small $\boldsymbol{e}$**

**Concatenated code in** *hqc-128*

- Reed-Solomon as external code
- Reed-Muller as internal code

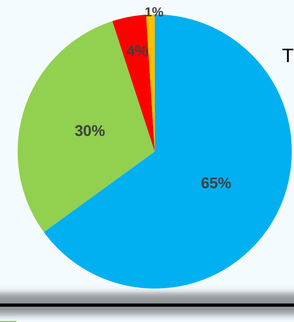



Time-consuming operation in CRYSTALS-Kyber

- Hash functions
- Polyn. Mult.with NTT
- Others

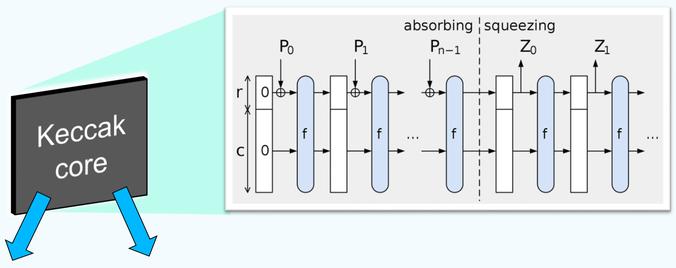
| | Crystal-Kyber | HQC | Lattice-code agility (focus of this PhD) |
|---|---|---|---|
| Hardware implementation | ~40 implementations | 1 implementation | No state of the art for this targeted agility |
| Hardware implementation + Security | ~10 implementations | / | |




Time-consuming operation in HQC

- Hash functions
- Polynomial Multiplication
- Decoding function
- Others

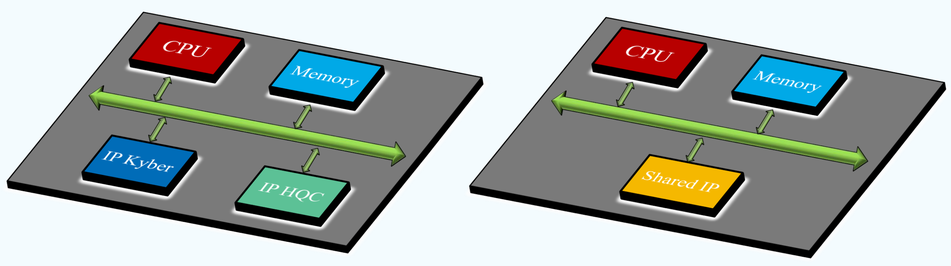
## First sharing analysis




***Hash functions***

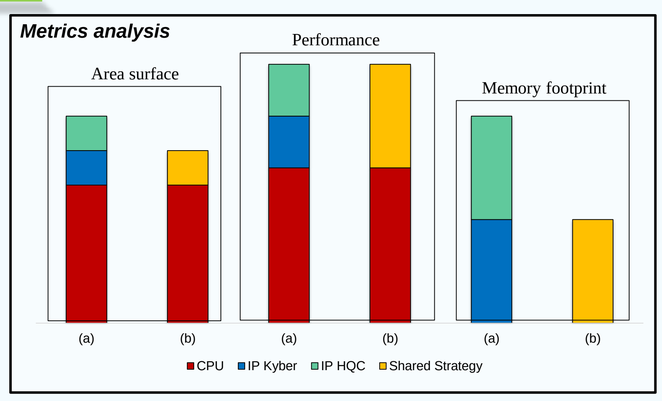
- ***SHAKE*** with fixed output size

***Pseudo-random number generation***




(a) Crypto-agility with optimizations

(b) Crypto-agility with optimizations and sharing strategy




**M. Carmona[1], A. Loiseau[1], S. Pontié[1,3], A. Ras[1], G. Renault[4,5], B. Smith[4], E. Valea[2]**

**1** Univ. Grenoble Alpes, CEA-Leti, Grenoble, France **2** Univ. Grenoble Alpes, CEA-List, Grenoble, France

**3** CEA-Leti, Centre CMP, Equipe Commune CEA Leti-Mines Saint-Etienne, Gardanne, France

**4** LIX, INRIA, CNRS, Ecole Polytechnique, Institut Polytechnique de Paris, France

**5** ANSSI, Paris, France

## Reference

[1] R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J.M. Schanck, P. Schwabe, G. Seiler, and D. Stehl´e, "CRYSTALS-Kyber:Algorithm Specifications and Supporting Documentation," 2020.

[2] C. Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J-C.Deneuville, P. Gaborit, E. Persichetti, G. Z´emor, and J. Bos. "HQC: Technical report, National Institute of Standards and Technology", 2020..