



HAL
open science

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

► **To cite this version:**

A. Ras, Mikael Carmona, Antoine Loiseau, Simon Pontie, Guenael Renault, et al.. Secure, optimized and Agile HW/SW implementation for post-quantum cryptography. CHES 2023, Sep 2023, Prague, Czech Republic. 2023. cea-04521354

HAL Id: cea-04521354

<https://cea.hal.science/cea-04521354>

Submitted on 26 Mar 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

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

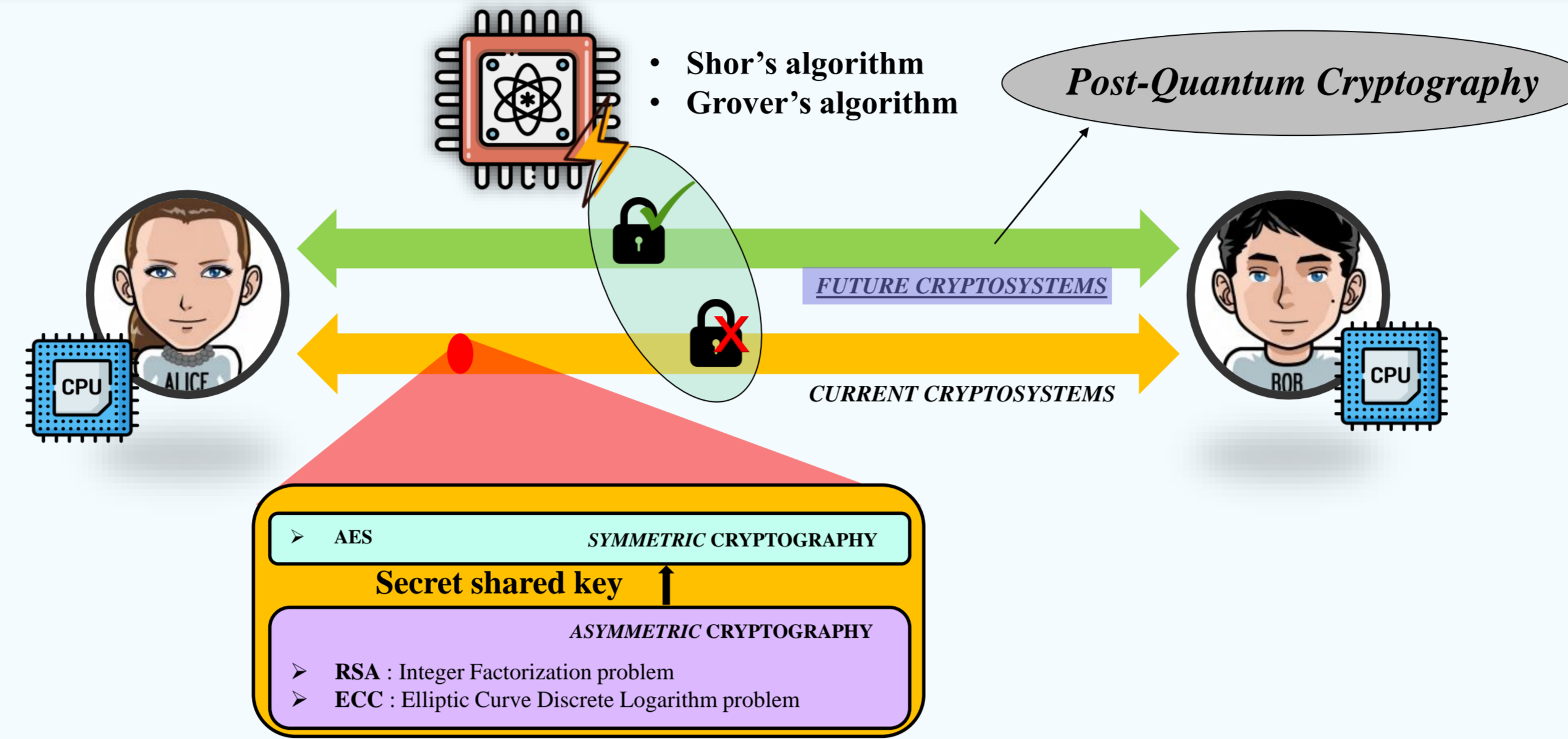


RAS Antonio
Laboratory of Security of Components (LSCO)

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.

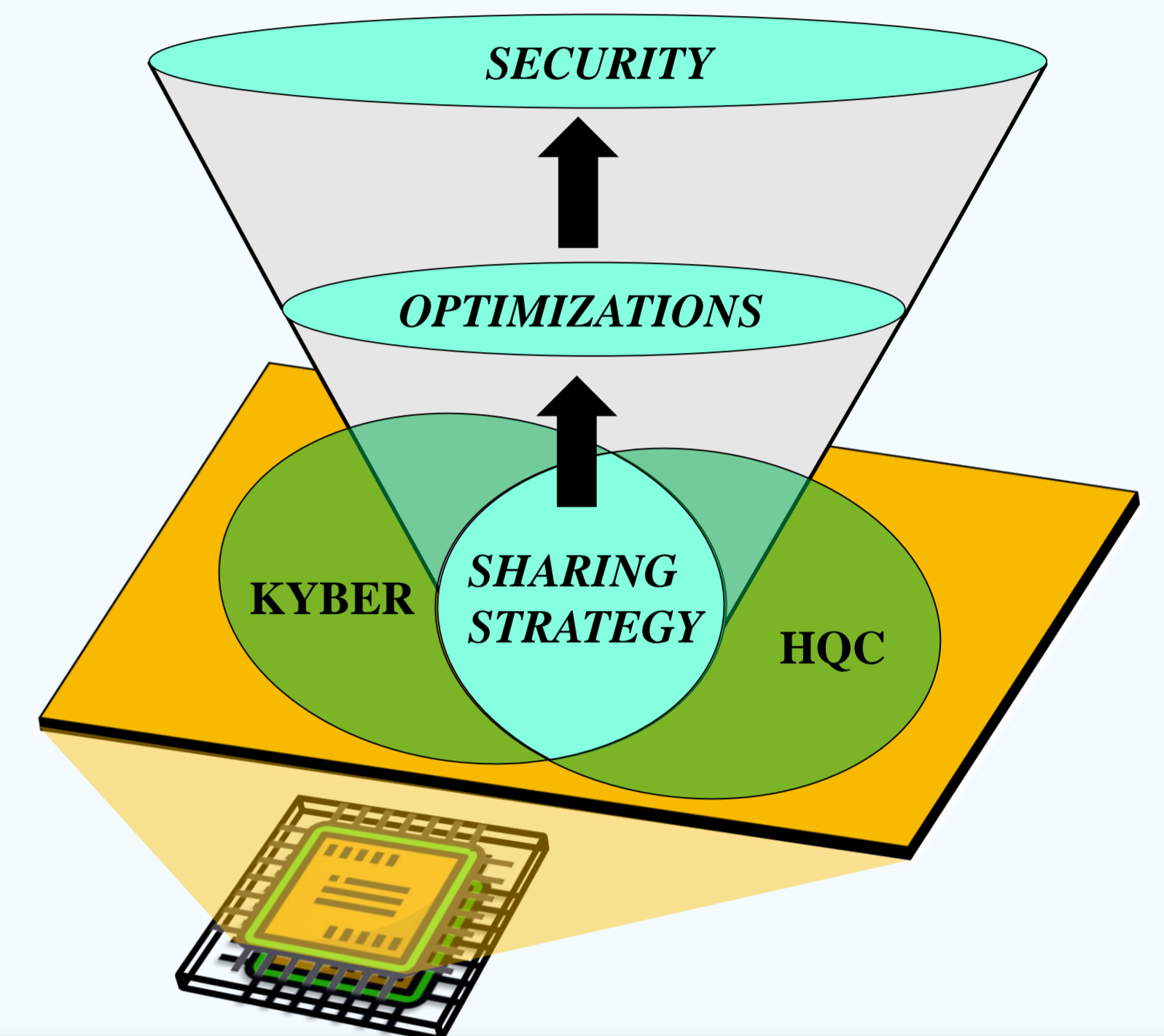


Motivations of Crypto-agility

- Uncertain security of cryptosystems
- Standardization of many cryptosystems

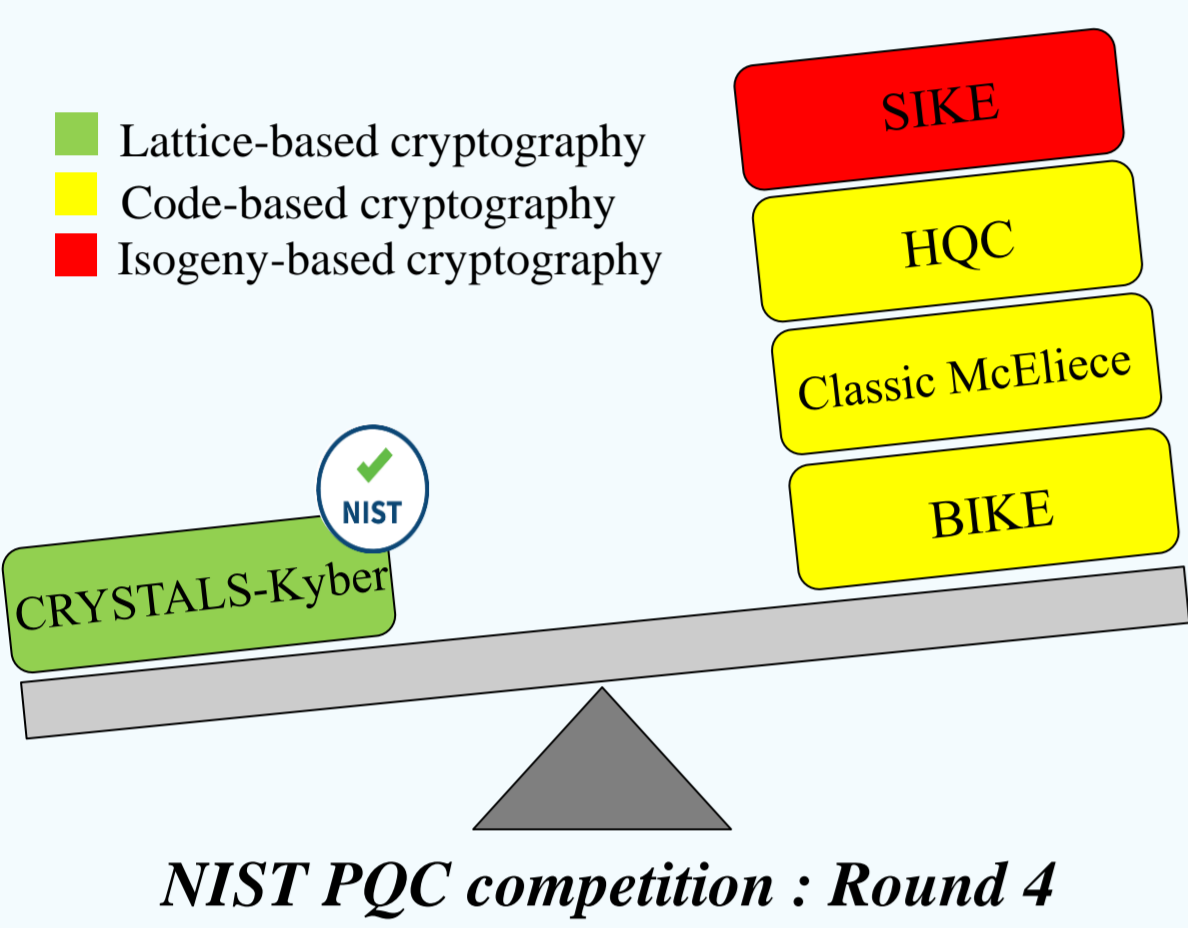
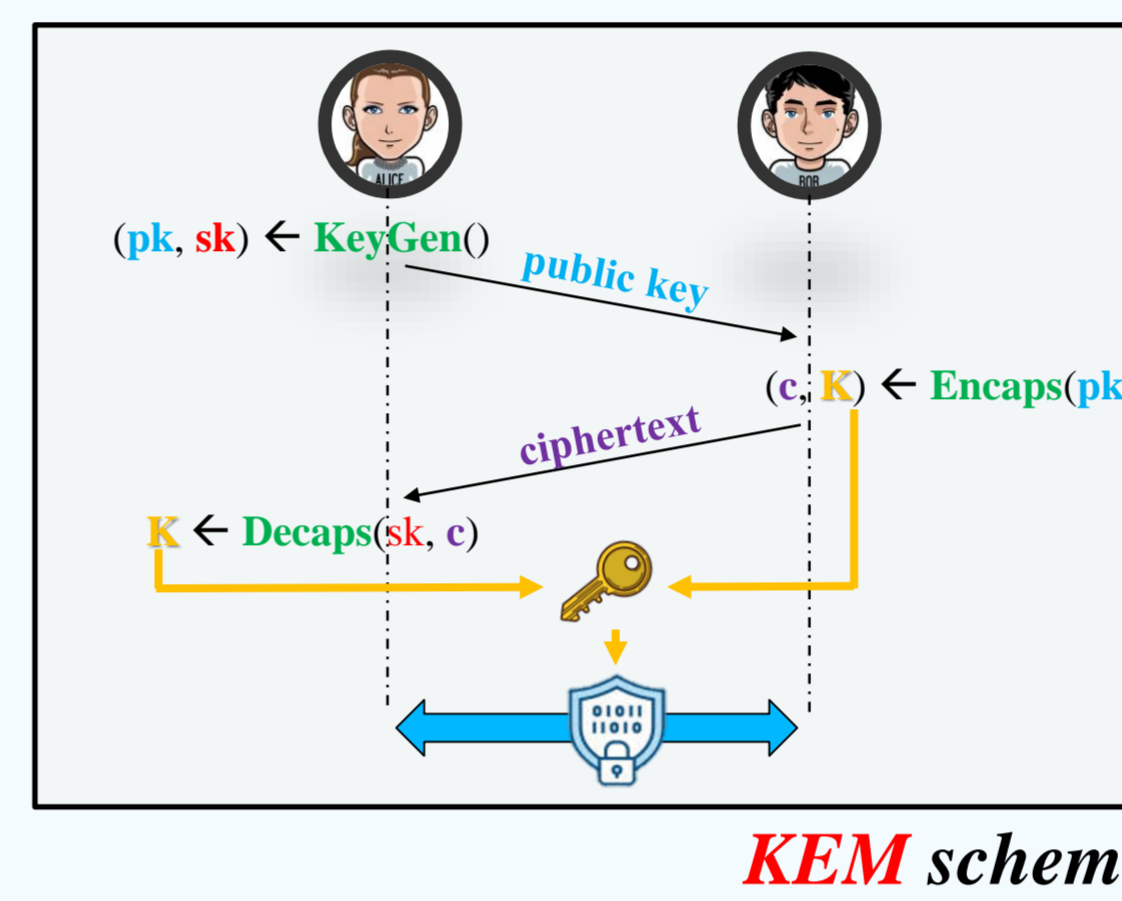
Three main sphere of actions

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



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.



Targeted Crypto-Agility & State of the Art

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

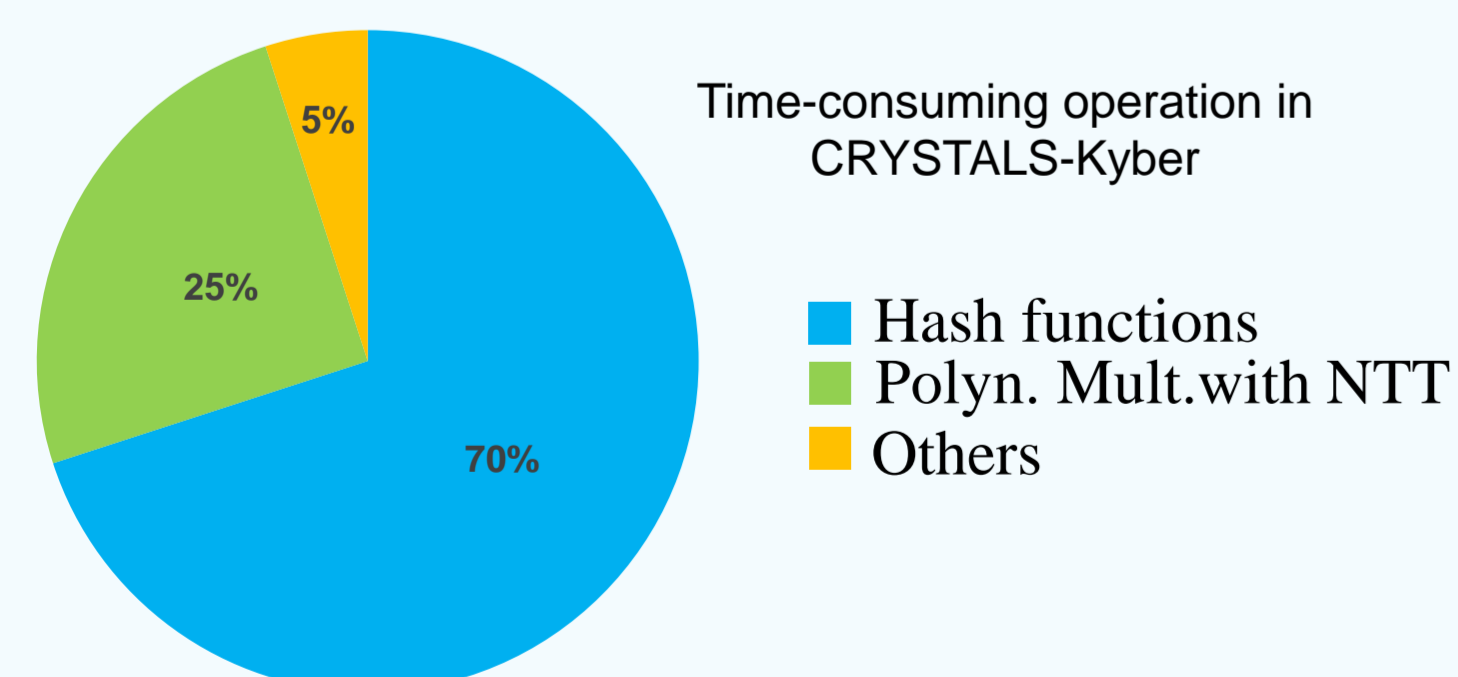
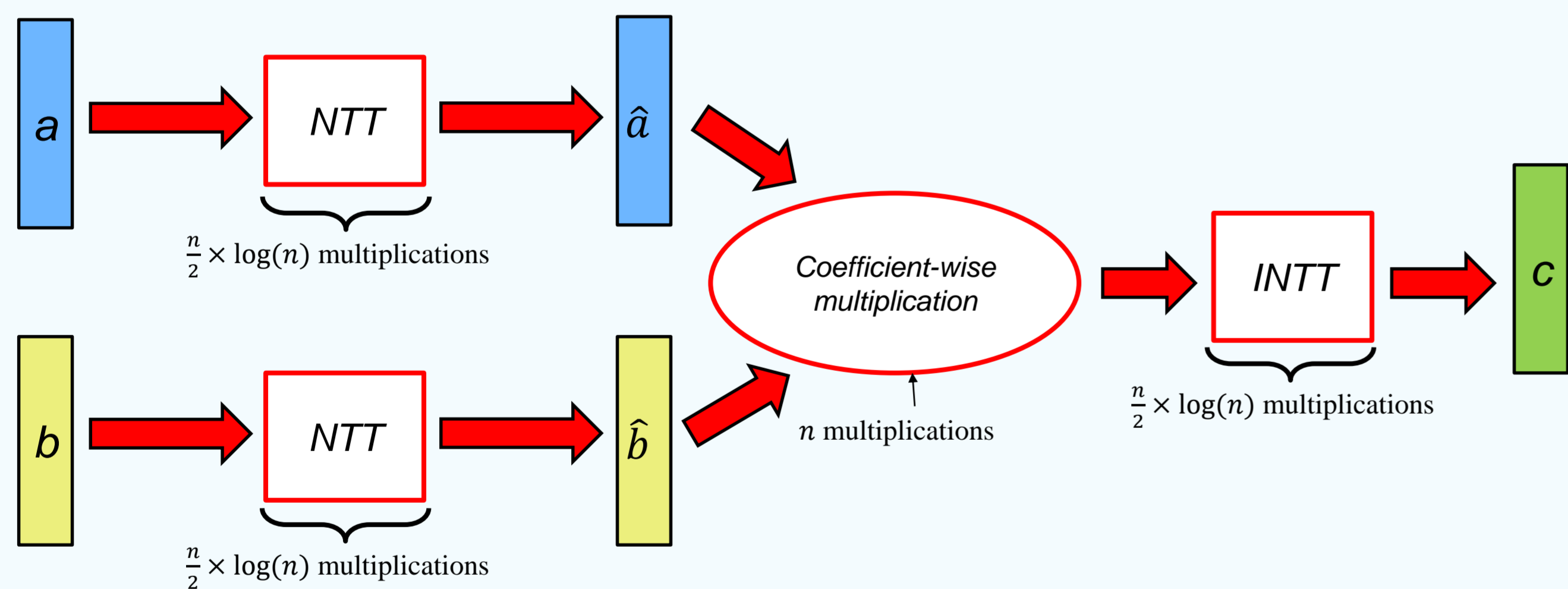
For a polynomial ring $R_q = \frac{\mathbb{Z}_q}{x^{n+1}}$. Given :

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

Knowing $t = As + e$ and A , it is difficult to find s

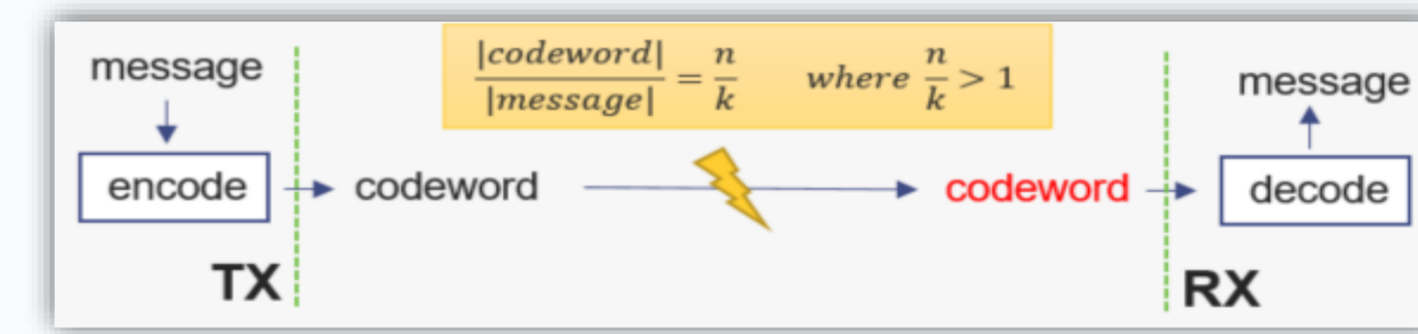
Polynomial multiplication with NTT (Number Theoretic Transform)

- 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



	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	/	

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

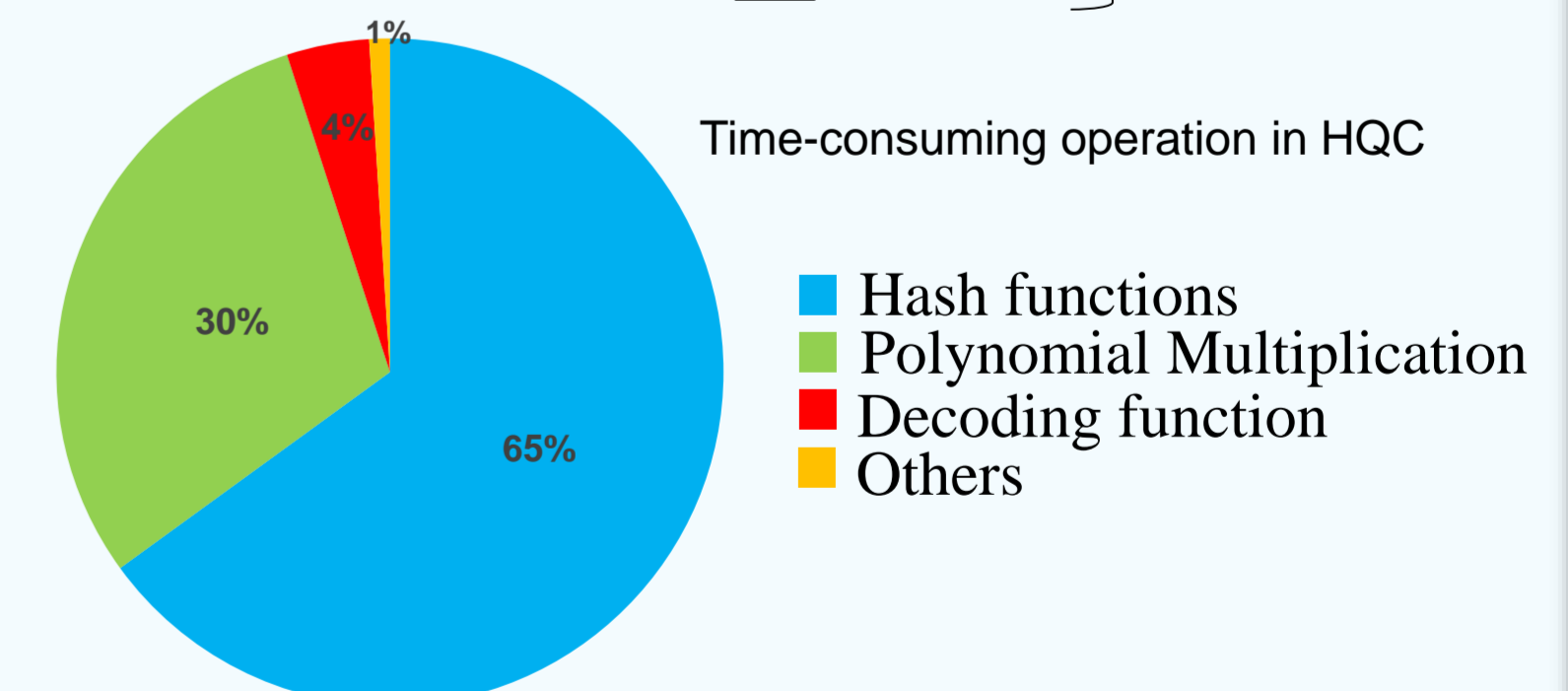
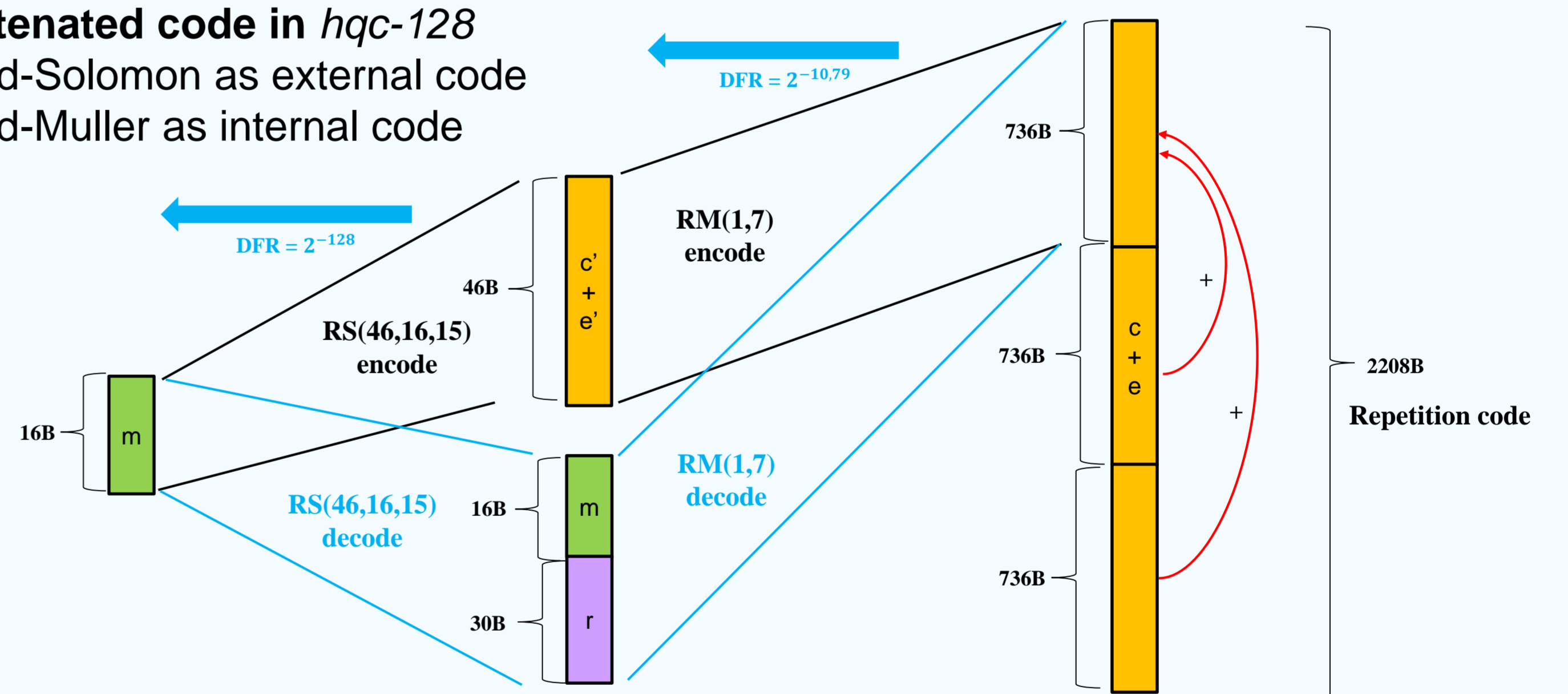


Given a random l -quasi-cyclic code $C(n, k, d)_q$ with parity-check matrix H , and a uniform $e \in \mathbb{F}_q^n$ with Hamming weight lower than ω

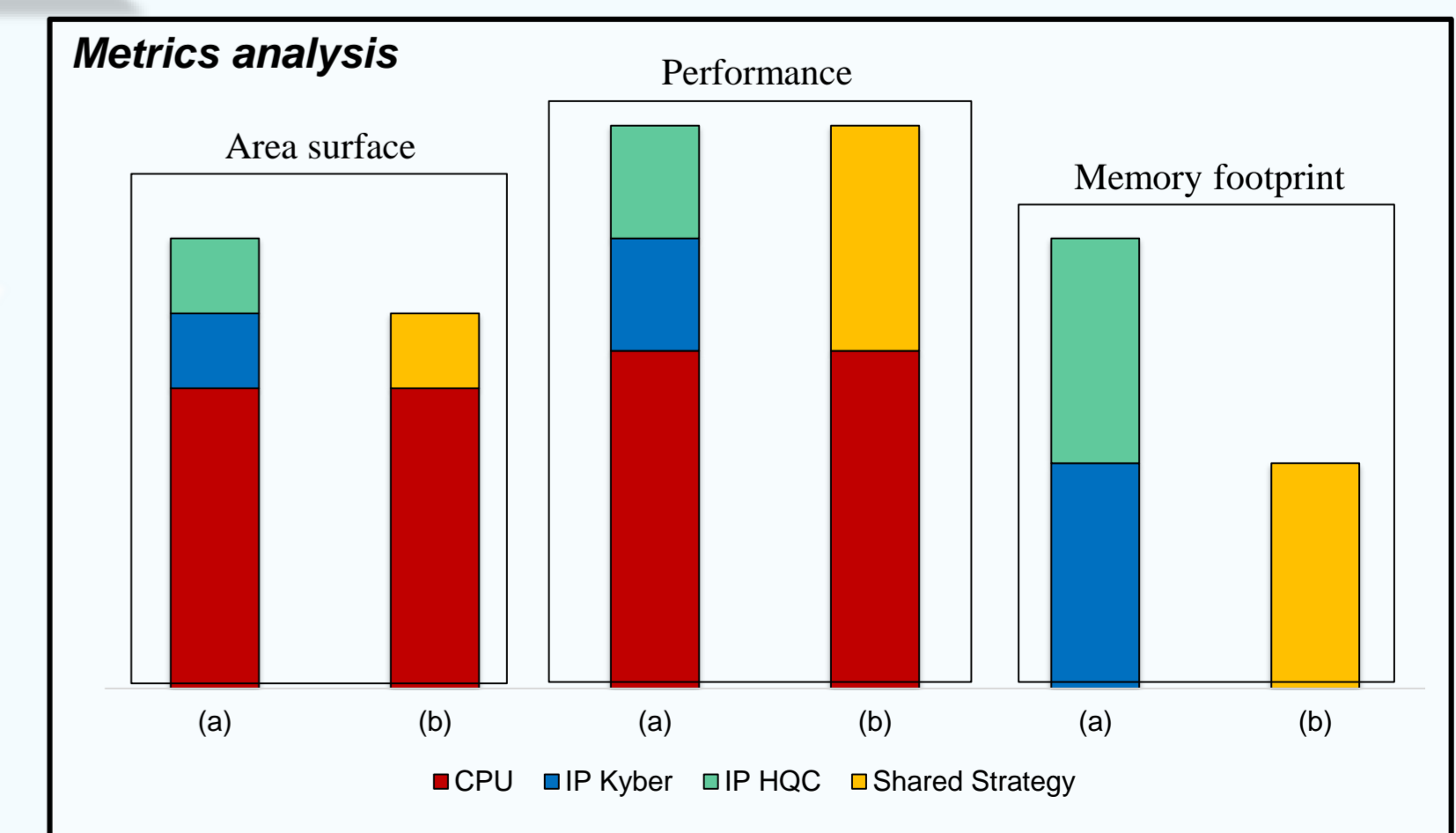
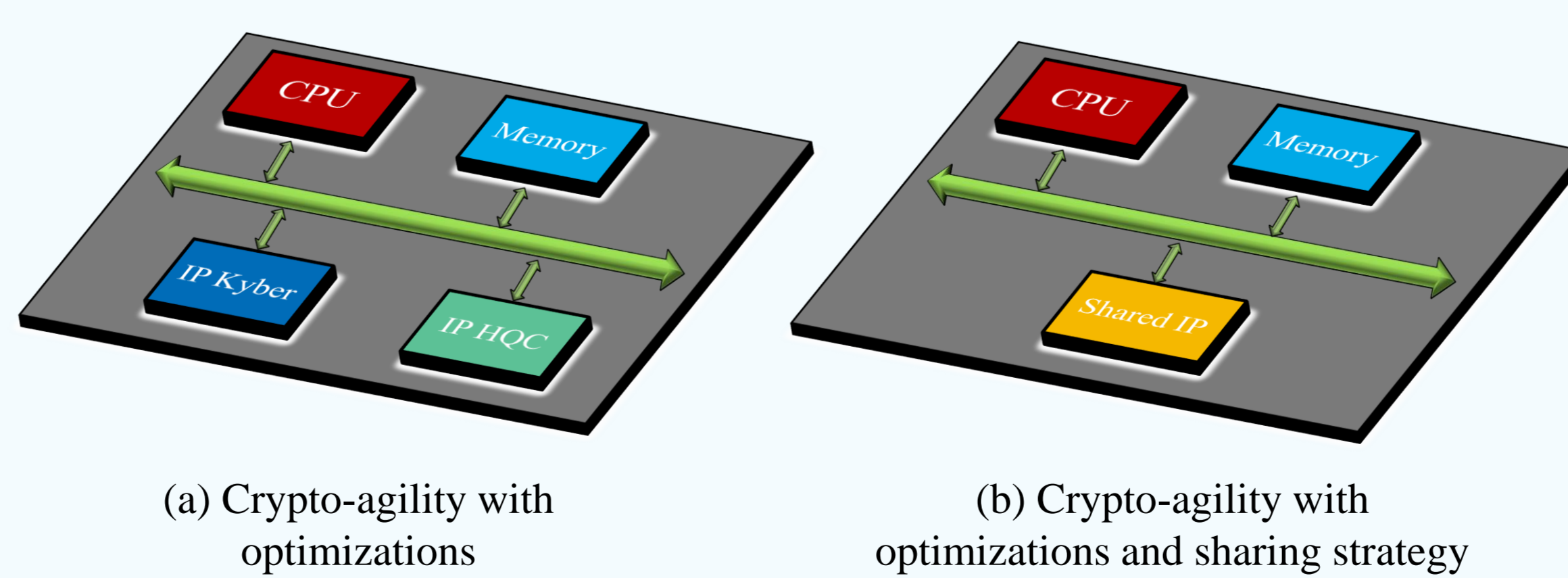
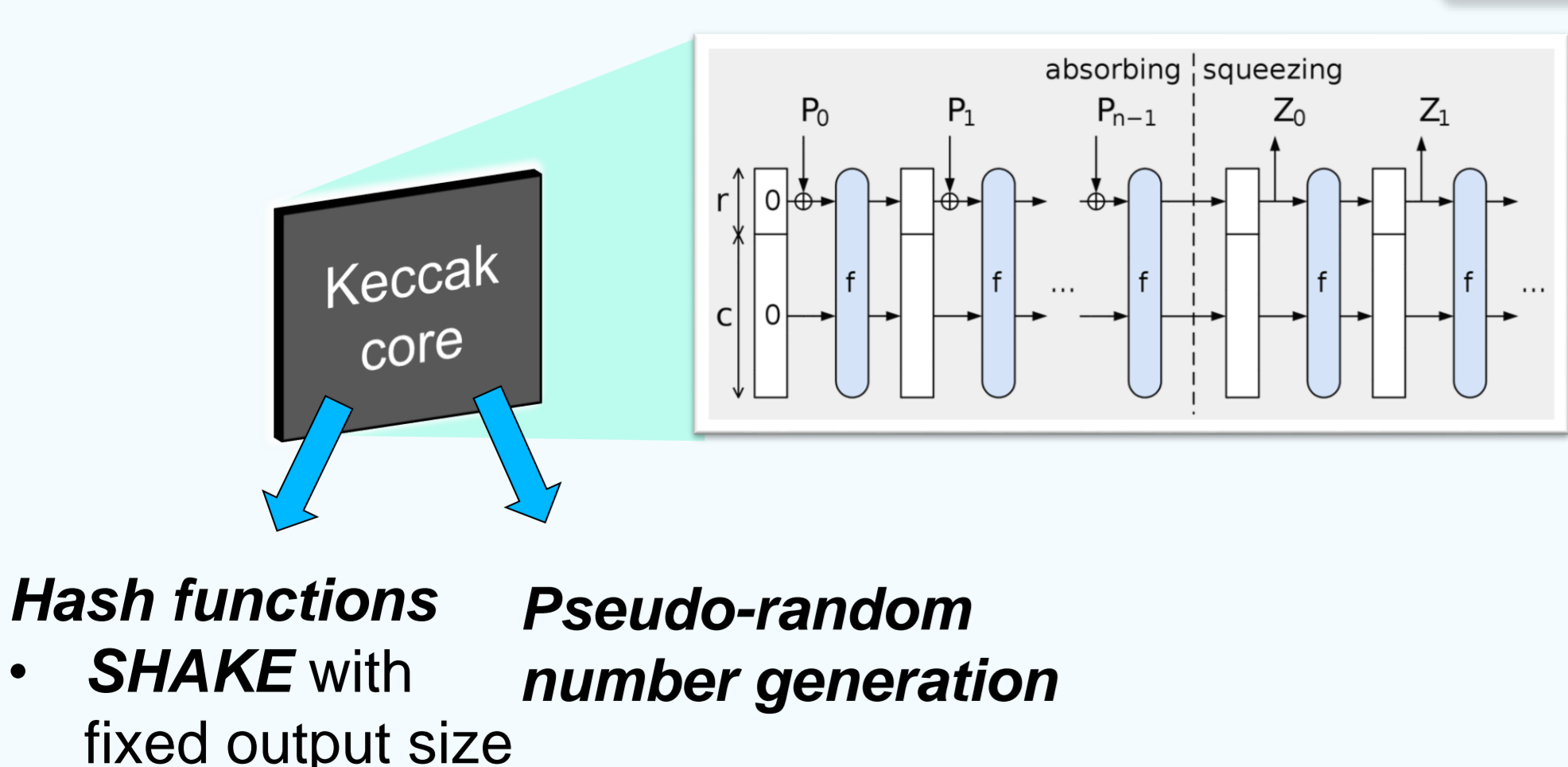
- d is the minimal distance of the code
 - H is the matrix used to characterize the error
- Knowing $s = eH^t$ and H , it is a difficult problem to find the small e

Concatenated code in hqc-128

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



First sharing analysis



M. Carmona¹, A. Loiseau¹, S. Pontié^{1,3}, A. Ras¹, G. Renault^{4,5}, B. Smith⁴, E. Vatea²

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

- R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J.M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé, "CRYSTALS-Kyber: Algorithm Specifications and Supporting Documentation," 2020.
- C. Melchor, N. Aragon, S. Betteieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, E. Persichetti, G. Zemor, and J. Bos. "HQC: Technical report, National Institute of Standards and Technology", 2020..

