Balancing security and efficiency in post-quantum cryptography

Victor Dyseryn

XLIM, Université de Limoges, France

Télécom SudParis Seminar - 21/11/2023

Introduction to post-quantum cryptography

Post-quantum cryptography

- Euclidean lattices?

Post-quantum cryptography

- Euclidean lattices?
- Goppa error correcting codes?

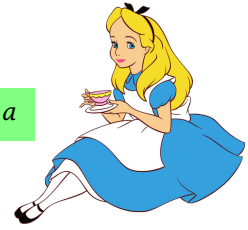
Post-quantum cryptography

- Euclidean lattices?
- Goppa error correcting codes?
- Supersingular isogenies?

Diffie-Hellman

Diffie-Hellman

Public parameter: g

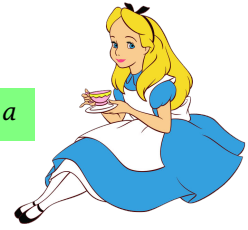


a

b

Diffie-Hellman

Public parameter: g



a

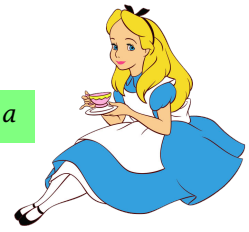
g^a

b

g^b

Diffie-Hellman

Public parameter: g



a

g^a

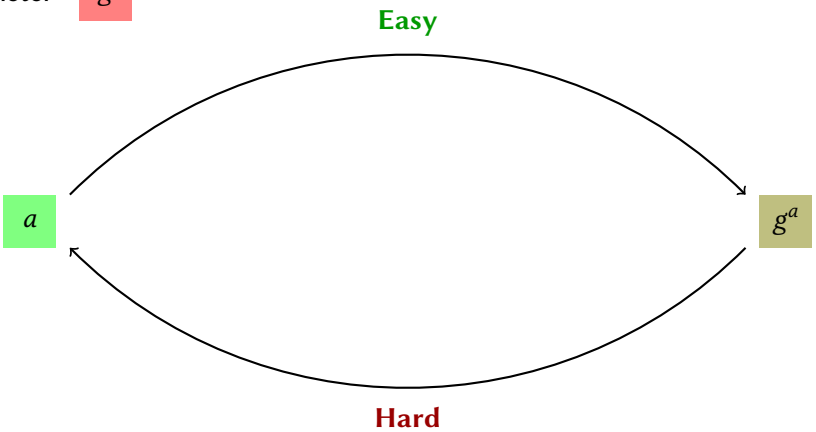
g^b

b

Shared secret: g^{ab}

Discrete logarithm

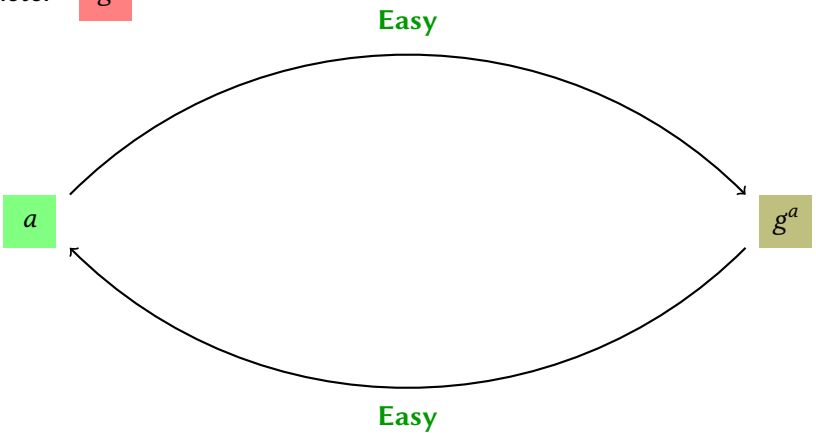
Public parameter: g



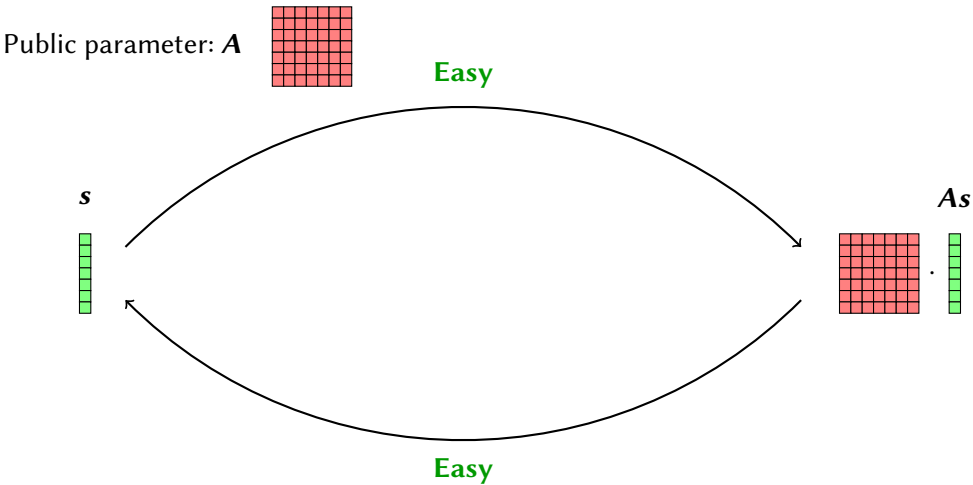
Quantum Computer

Discrete logarithm

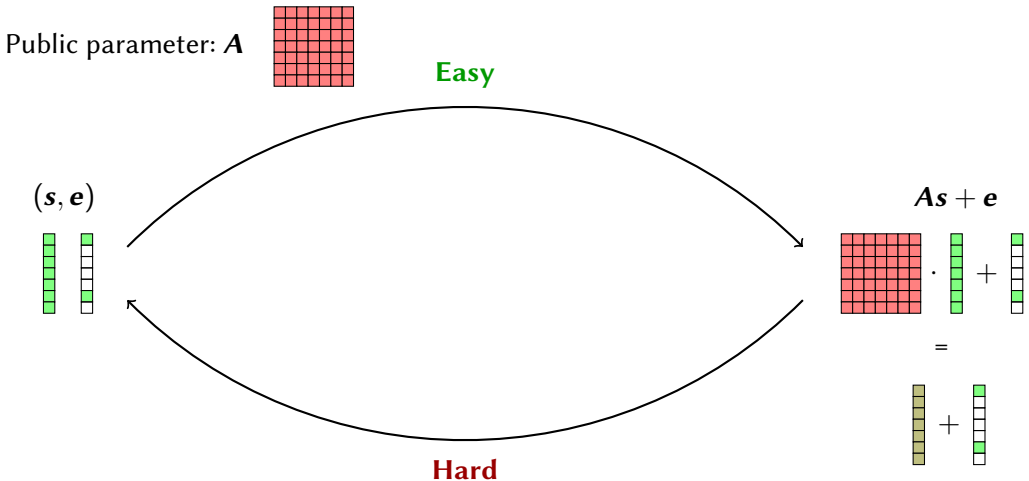
Public parameter: g



Linear algebra



Linear algebra with noise



Diffie-Hellman with linear algebra

Public parameter: $\boldsymbol{A}$

$\boldsymbol{As}$

$\boldsymbol{s}$

$\boldsymbol{t}$

$\boldsymbol{t}^T\boldsymbol{A}$

Diffie-Hellman with linear algebra

Public parameter: $\boldsymbol{A}$

$\boldsymbol{As}$

$\boldsymbol{s}$

$\boldsymbol{t}$

$\boldsymbol{t}^T\boldsymbol{A}$

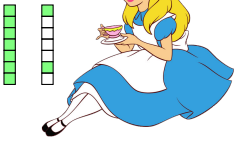
Shared secret: $\boldsymbol{t}^T\boldsymbol{As}$ 

Noisy Diffie-Hellman

Public parameter: $\boldsymbol{A}$

$\boldsymbol{As} + \boldsymbol{e}$

$(\boldsymbol{s}, \boldsymbol{e})$



$+$

$(\boldsymbol{t}, \boldsymbol{f})$

$+$ $\boldsymbol{t}^T\boldsymbol{A} + \boldsymbol{f}^T$

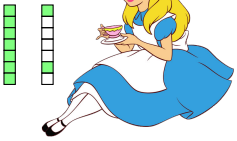
Shared secret: $\boldsymbol{t}^T\boldsymbol{As}$ 

Noisy Diffie-Hellman

Public parameter: $\boldsymbol{A}$

$\boldsymbol{As} + \boldsymbol{e}$

$(\boldsymbol{s}, \boldsymbol{e})$



$+$

$(\boldsymbol{t}, \boldsymbol{f})$

$+$

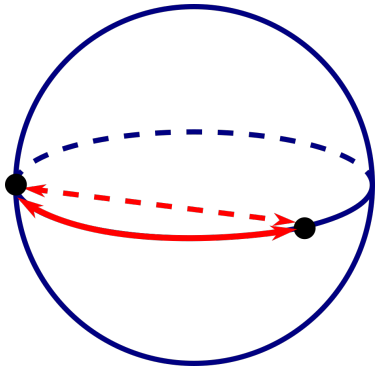
$\boldsymbol{t}^T\boldsymbol{A} + \boldsymbol{f}^T$

$\boldsymbol{t}^T\boldsymbol{As} + \boldsymbol{f}^T\boldsymbol{s}$

$\boldsymbol{t}^T\boldsymbol{As} + \boldsymbol{t}^T\boldsymbol{e}$

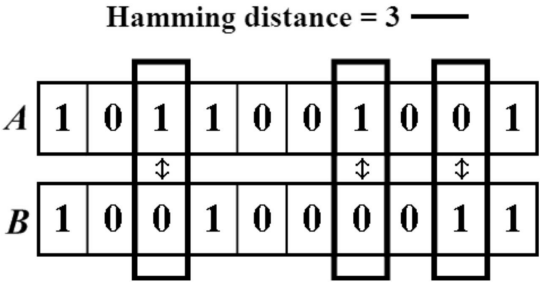
Shared secret: $\boldsymbol{t}^T\boldsymbol{As}$

Euclidean lattices



$$\|\boldsymbol{x}\| = \sqrt{\sum_i x_i^2}$$

Error-correcting codes



$$\|\boldsymbol{x}\| = \#\{i \mid x_i \neq 0\}$$

Rank metric error-correcting codes

$$A = \begin{bmatrix} 1 & 2 & 3 & -1 \\ 0 & -1 & -1 & 1 \\ 2 & 3 & 5 & -1 \end{bmatrix}$$

$$\|\boldsymbol{x}\| = \mathsf{rank}(\mathbf{Mat}(\boldsymbol{x}))$$

NIST standardization process

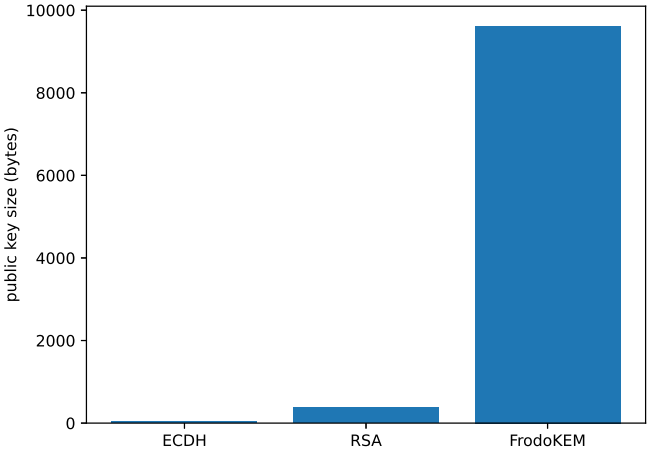
- 2017: Candidate submissions
- 2017-2019: Round 1
- 2019-2020: Round 2
- 2020-2022: Round 3
- 2022: Announcement of selected algorithms
- 2022-...: Round 4

NIST standardization process

	Round 1	Round 2	Round 3	Selected	Round 4
Lattices	21	9	5	1	0
Codes (Hamming)	13	5	3	0	3
Codes (Rank)	4	2	0	0	0
Other	7	1	1	0	1

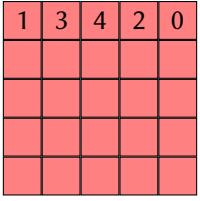
Table: Encryption schemes in the NIST standardization process

A problem of size

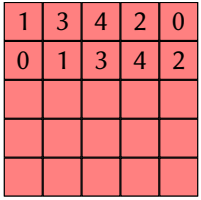


Reducing the size with cyclic structure

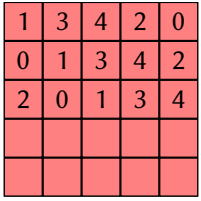
Circulant matrices



Circulant matrices



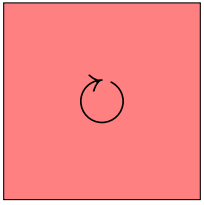
Circulant matrices



Circulant matrices

1	3	4	2	0
0	1	3	4	2
2	0	1	3	4
4	2	0	1	3
3	4	2	0	1

Circulant matrices



Circulant matrix × vector

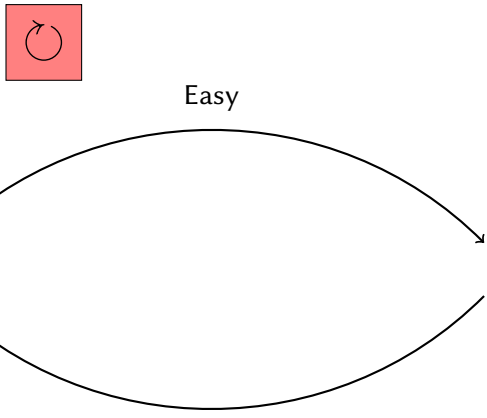
1	3	4	2	0
0	1	3	4	2
2	0	1	3	4
4	2	0	1	3
3	4	2	0	1

1
2
1
4
0

4
1
0
2
3

Circulant matrices with noise

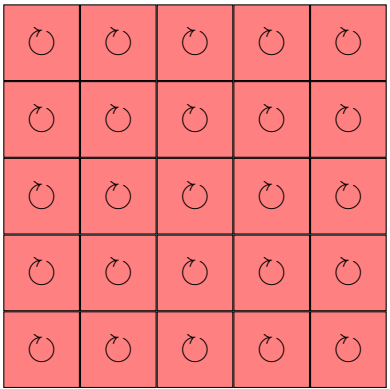
Public parameter: $\boldsymbol{A}$



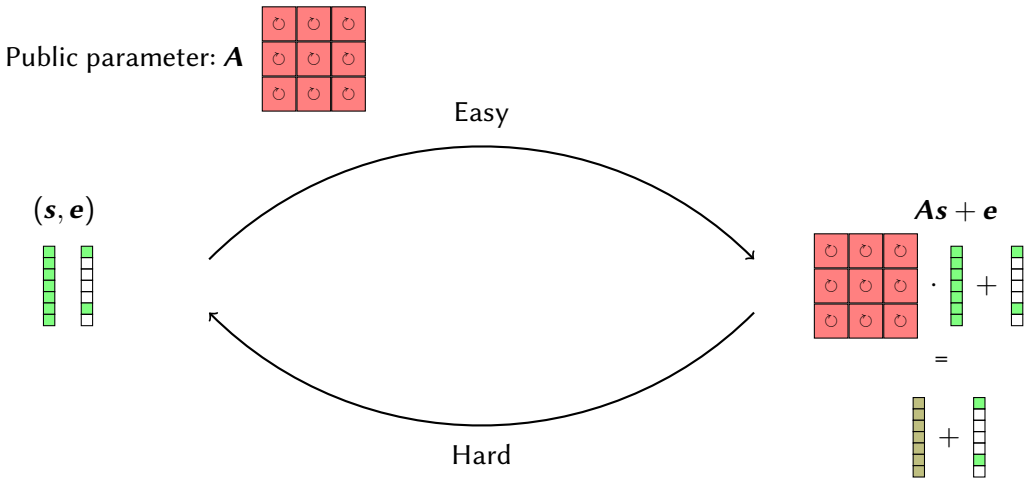
$(\boldsymbol{s}, \boldsymbol{e})$

$\boldsymbol{As} + \boldsymbol{e}$

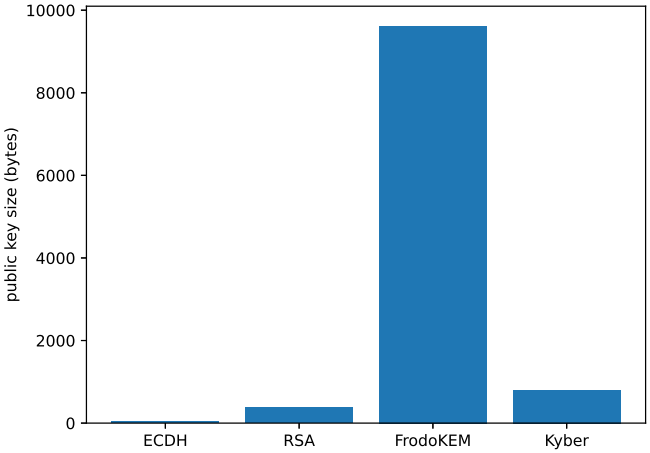
Quasi-cyclic matrix



Quasi-cyclic matrices with noise



Comparison of sizes



Is it really secure?

Decoding One Out of Many

Nicolas Sendrier
INRIA Paris-Rocquencourt, Project-Team SECRET
nicolas.sendrier@inria.fr

Abstract. Generic decoding of linear codes is the best known attack against most code-based cryptosystems. Understanding and measuring the complexity of the best decoding technique is thus necessary to select secure parameters. We consider here the possibility that an attacker has access to many cryptograms and is satisfied by decrypting (i.e. decoding) only one of them. We show that, in many cases of interest in cryptology, a variant of Stern's collision decoding can be adapted to gain a factor almost $\sqrt{N}$ when N instances are given. If the attacker has access to an unlimited number of instances, we show that the attack complexity is significantly lower, in fact raised by a power slightly larger than 2/3. Finally we give indications on how to counter those attacks.

1 Introduction

Is it really secure?

Decoding One C

INRIA Paris-Rocquencourt

Mildly Short Vectors in Cyclotomic Ideal Lattices in Quantum Polynomial Time

RONALD CRAMER, CWI, Amsterdam and Leiden University, The Netherlands
LÉO DUCAS, CWI, Amsterdam, The Netherlands
BENJAMIN WESOLOWSKI, Univ. Bordeaux, CNRS, IMB, UMR 5251 and INRIA, LFANT, France

In this article, we study the geometry of units and ideals of cyclotomic rings and derive an algorithm to find a mildly short vector in any given cyclotomic ideal lattice in quantum polynomial time, under some plausible number-theoretic assumptions. More precisely, given an ideal lattice of the cyclotomic ring of conductor m, the algorithm finds an approximation of the shortest vector by a factor $\exp(\tilde{O}(\sqrt{m}))$. This result exposes an unexpected hardness gap between these structured lattices and general lattices. The best known polynomial time generic lattice algorithms can only reach an approximation factor $\exp(\tilde{O}(m))$. This result exposes an of attacks; these results call into question the hardness of a number of cryptographic schemes. Following a recent series Ideal-SVP and Ring-LWE, upon which relies the security of a conference paper [32]. The results are generalized to arbitrary cyclotomic fields. In particular, we also extend some results of Reference [10] to arbitrary cyclotomic fields. In addition, we prove the numerical stability of the method of Reference [10]. These extended results appeared in the Ph.D. dissertation of the third author [46].

CCS Concepts: • **Mathematics of computing** → **Discrete mathematics** • **Security and privacy** → **Cryptanalysis and other attacks**;

Additional Key Words and Phrases: Shortest vector problem, ideal lattices, cyclotomic fields

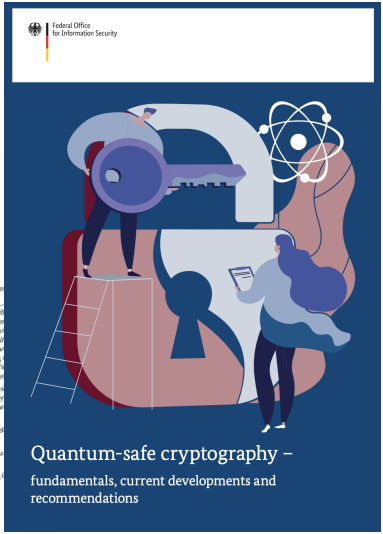
ACM Reference format:
Ronald Cramer, Léo Ducas, and Benjamin Wesolowski. 2020. Mildly Short Vectors in Cyclotomic Ideal Lattices in Quantum Polynomial Time. J. ACM 68, 2, Article 8 (January 2021), 26 pages.
https://doi.org/10.1145/3431725

Is it really secure?

Mildly Short Vectors in Cyclotomic Ideal Lattices in Quantum Polynomial Time

RONALD CRAMER, CWI, Amsterdam and Leiden University, The Netherlands
LÉO DUCAS, CWI, Amsterdam, The Netherlands
BENJAMIN WESOLOWSKI, Univ. Bordeaux, CNRS, IMB, UMR 5251 and INRIA, LFANT, Franc

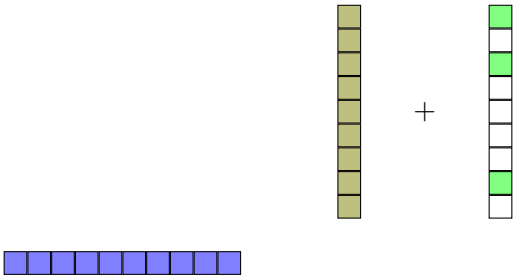
1 Introduction



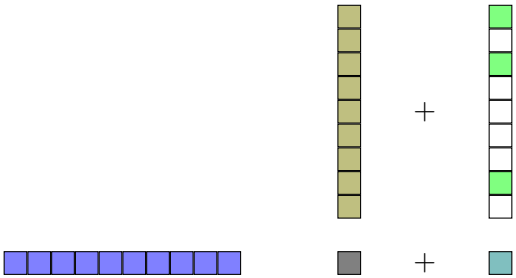
Is it really secure?

The multi-dimensional approach

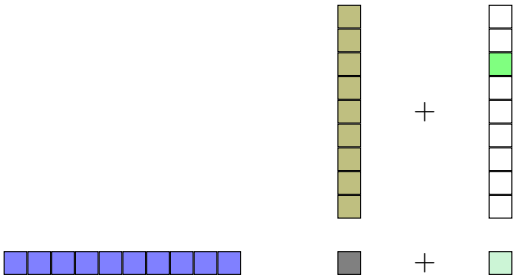
The right proportion of noise



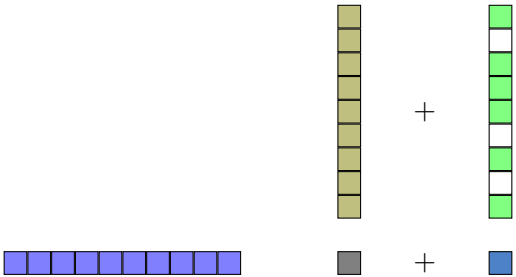
The right proportion of noise



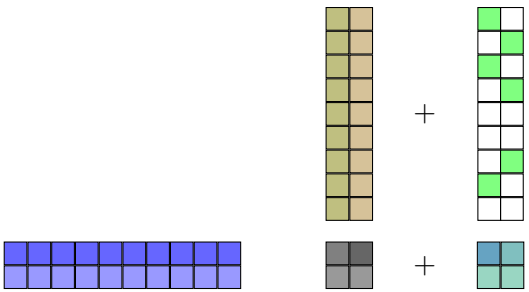
The right proportion of noise



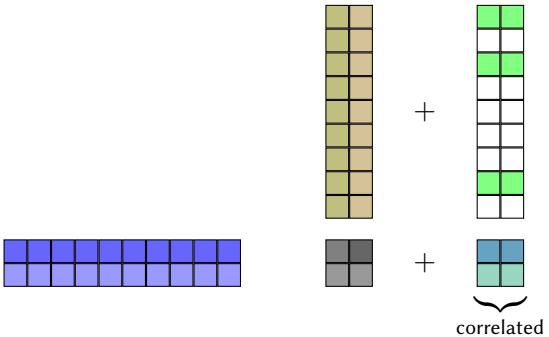
The right proportion of noise



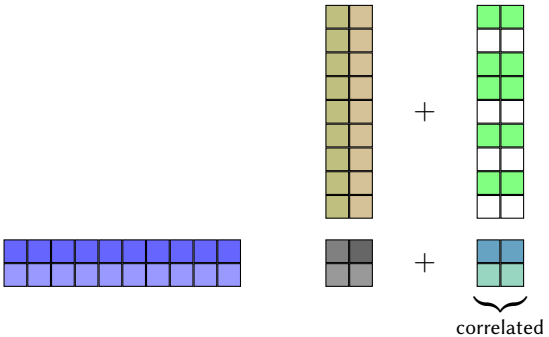
The multi-dimensional approach



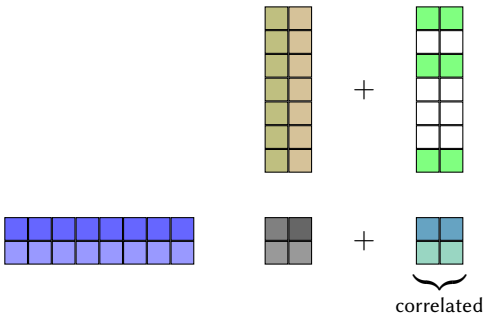
The multi-dimensional approach



The multi-dimensional approach



The multi-dimensional approach

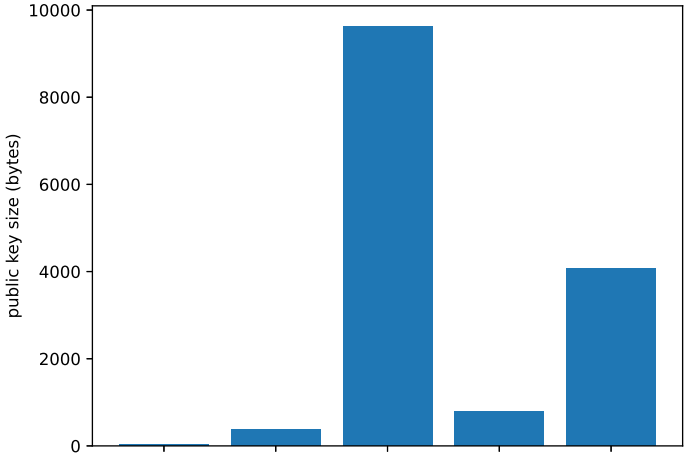


Application to efficient encryption

The multiple dimensional approach was explored in various metric and settings:

- Interleaved McEliece [HLPWZ19]
- **LowMS** [ADG+22]
- **LRPC-MS** [AMAD+22]
- Multi-UR [BBBG22]

Comparison of sizes



Open problems that interest me

- Applying multi-dimensional approach to build hash-and-sign signatures
- Applications to homomorphic encryption

Open problems that interest me

- Applying multi-dimensional approach to build hash-and-sign signatures
- Applications to homomorphic encryption

Thank you for your attention!

References I

Nicolas Aragon, Victor Dyseryn, Philippe Gaborit, Pierre Loidreau, Julian Renner, and Antonia Wachter-Zeh.
Lowms: a new rank metric code-based kem without ideal structure.
Cryptology ePrint Archive, 2022.

Carlos Aguilar-Melchor, Nicolas Aragon, Victor Dyseryn, Philippe Gaborit, and Gilles Zémor.
LRPC codes with multiple syndromes: near ideal-size KEMs without ideals.
In *International Conference on Post-Quantum Cryptography, PQCrypto*, pages 45–68. Springer, 2022.

Loïc Bidoux, Pierre Briaud, Maxime Bros, and Philippe Gaborit.
RQC revisited and more cryptanalysis for Rank-based Cryptography.
arXiv preprint arXiv:2207.01410, 2022.

References II


Lukas Holzbaur, Hedongliang Liu, Sven Puchinger, and Antonia Wachter-Zeh.
On Decoding and Applications of Interleaved Goppa Codes.
In *IEEE Int. Symp. Inf. Theory (ISIT)*, July 2019.