

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

- Euclidean lattices?

Post-quantum cryptography

- Euclidean lattices?
- Goppa error correcting codes?

Post-quantum cryptography

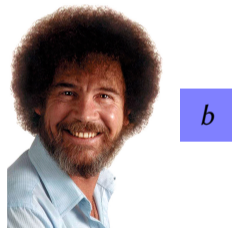
- Euclidean lattices?
- Goppa error correcting codes?
- Supersingular isogenies?

Diffie-Hellman



Diffie-Hellman

Public parameter: g



Diffie-Hellman

Public parameter: g



Diffie-Hellman

Public parameter: g



g^a



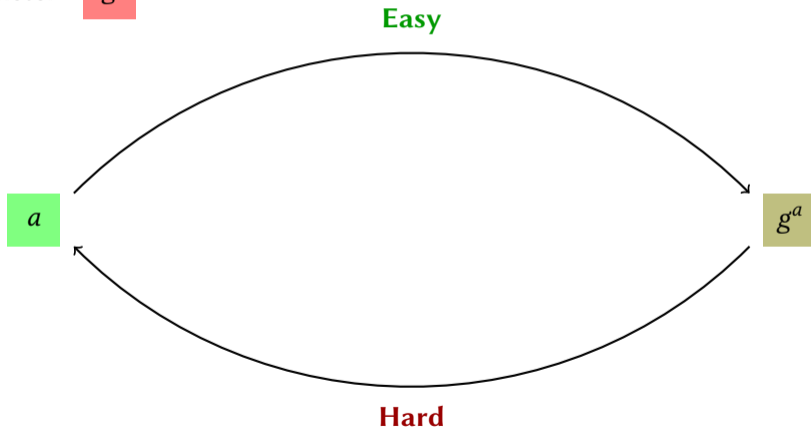
g^b

Shared secret: g^{ab}

Discrete logarithm

Public parameter:

g



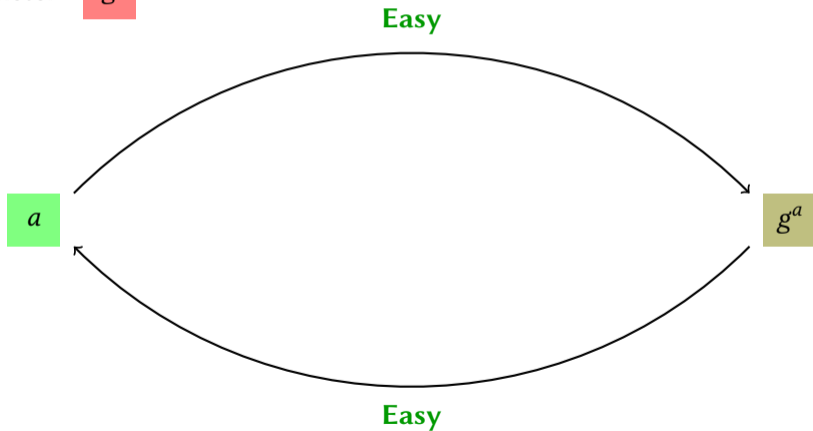
Quantum Computer



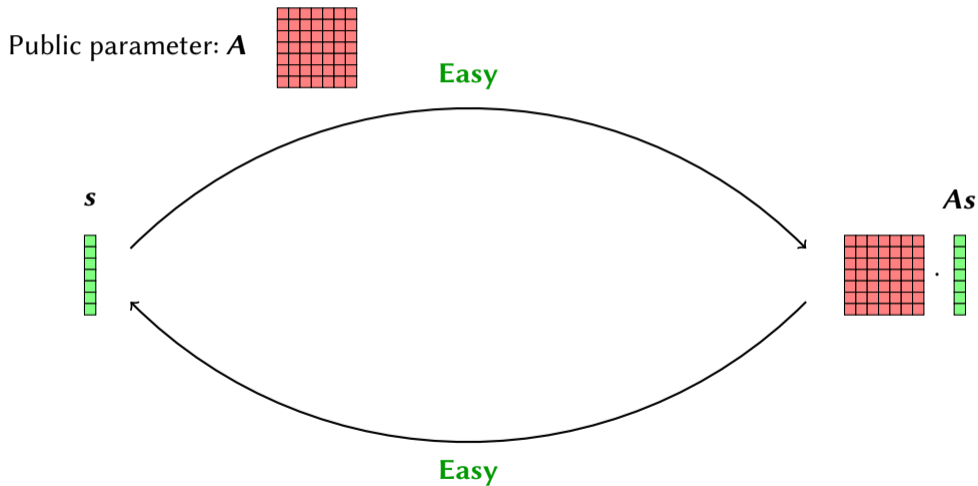
Discrete logarithm

Public parameter:

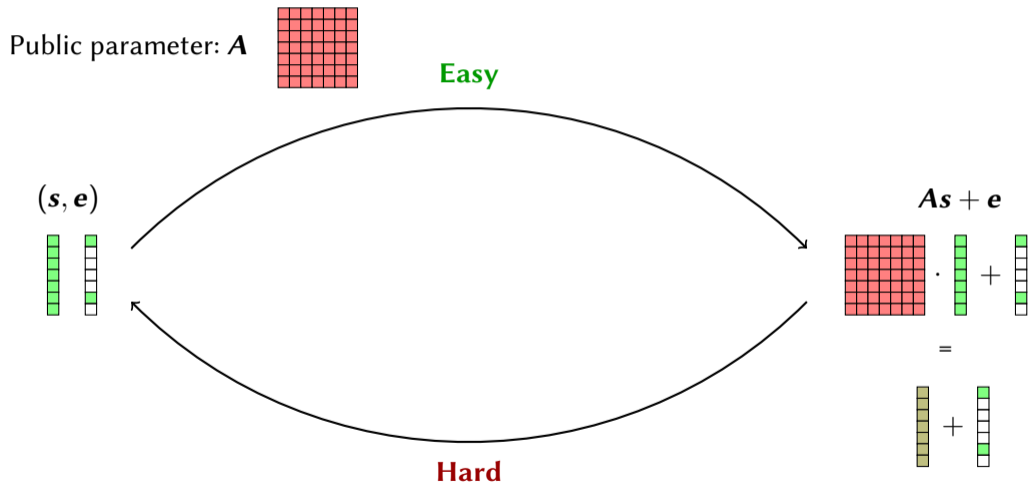
g



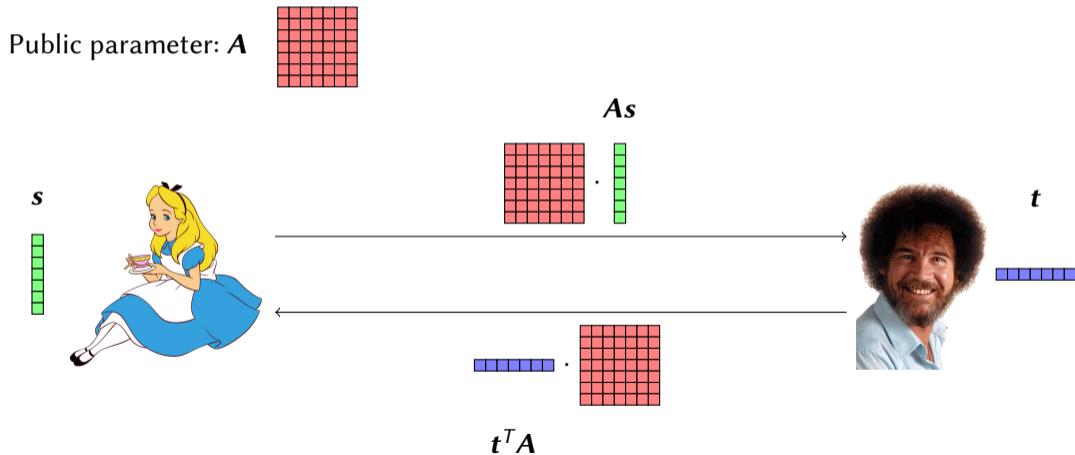
Linear algebra



Linear algebra with noise



Diffie-Hellman with linear algebra



Diffie-Hellman with linear algebra

Public parameter: A



s



As



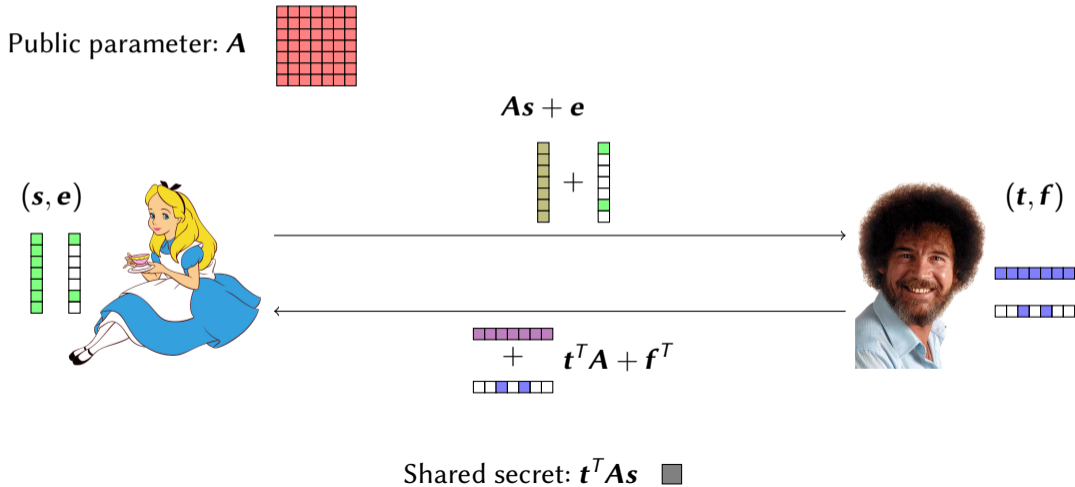
t



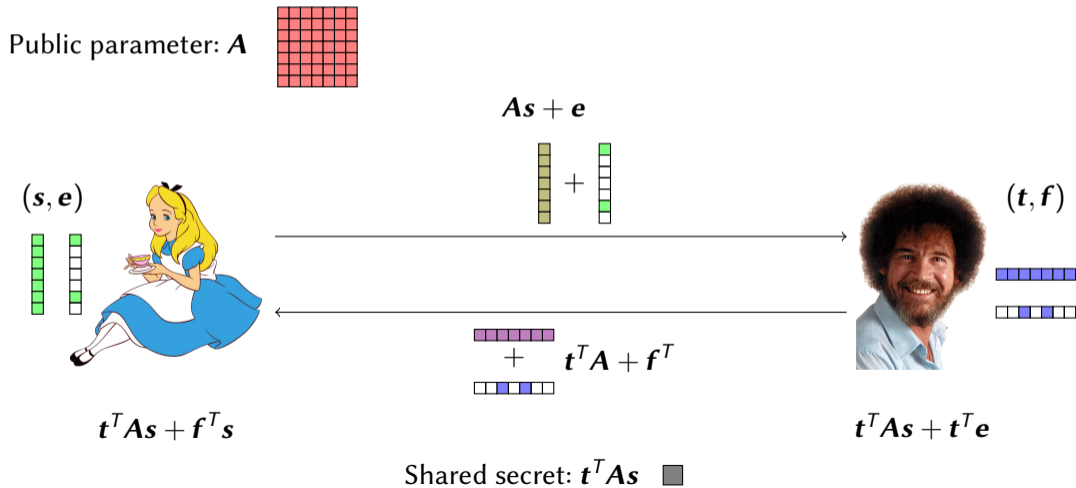
$t^T A$

Shared secret: $t^T A s$ ■

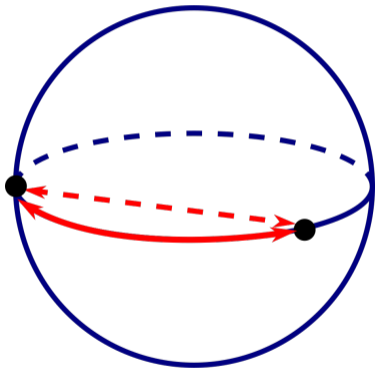
Noisy Diffie-Hellman



Noisy Diffie-Hellman



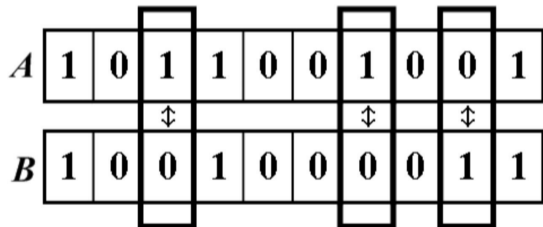
Euclidean lattices



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

Error-correcting codes

Hamming distance = 3 —



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

Rank metric error-correcting codes

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

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



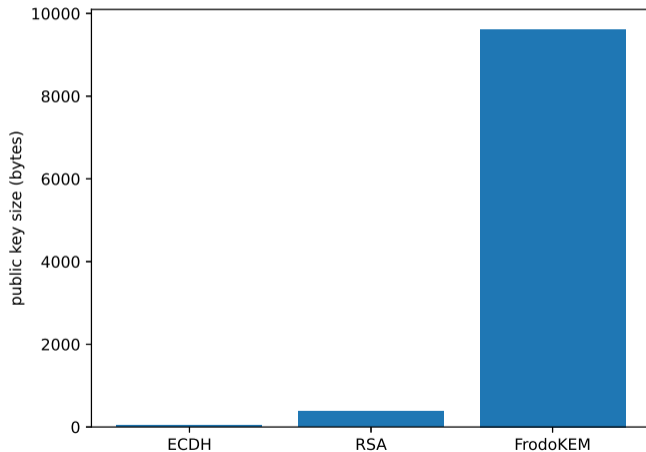
- 2017: Candidate submissions
- 2017-2019: Round 1
- 2019-2020: Round 2
- 2020-2022: Round 3
- 2022: Announcement of selected algorithms
- 2022-...: Round 4

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

1	3	4	2	0

Circulant matrices

1	3	4	2	0
0	1	3	4	2

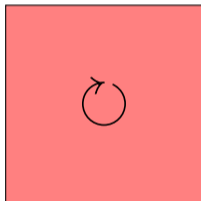
Circulant matrices

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

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 \times vector

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

Circulant matrices with noise

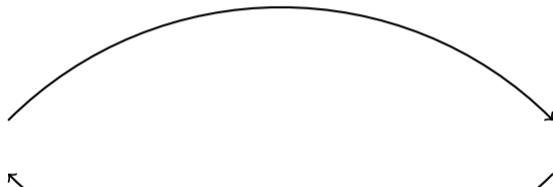
Public parameter: A



(s, e)

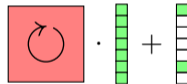


Easy



Hard

$As + e$



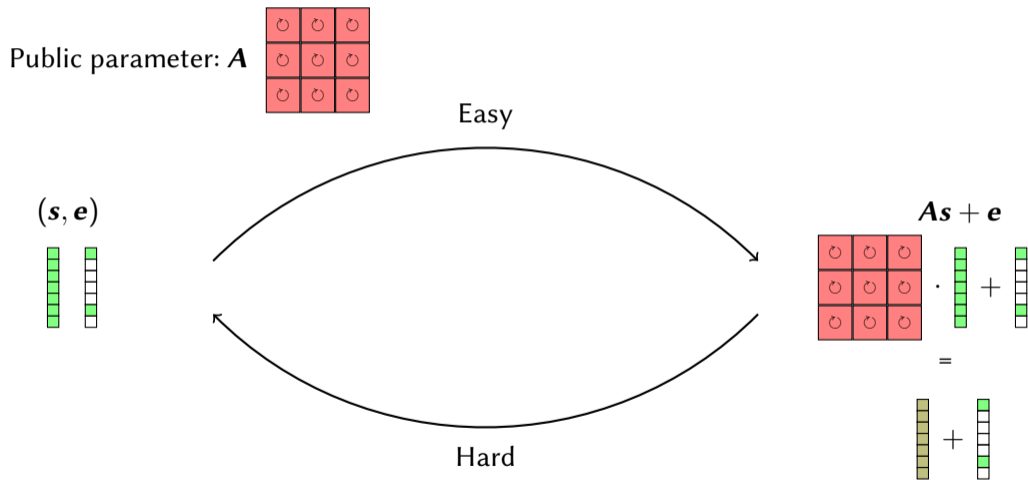
=



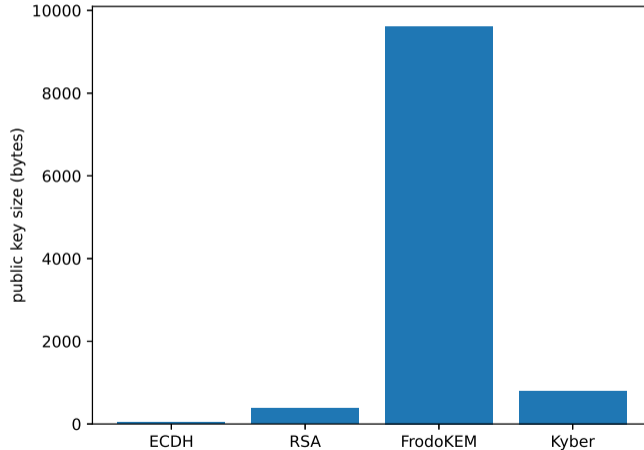
Quasi-cyclic matrix

⊕	⊕	⊕	⊕	⊕
⊕	⊕	⊕	⊕	⊕
⊕	⊕	⊕	⊕	⊕
⊕	⊕	⊕	⊕	⊕
⊕	⊕	⊕	⊕	⊕

Quasi-cyclic matrices with noise



Comparison of sizes



Is it really secure?

Decoding One C

INRIA Paris-IdRocq
Nicolas
alliaux

Mildly Short Vectors in Cyclotomic Ideal Lattices in Quantum Polynomial Time

RONALD CRAMER, CWI, Amsterdam and Leiden University, The Netherlands
LÉO DUCAS, CWI, Amsterdam, CNRS, IMB, UMR 5071 and INRIA, LIPN, France
BENJAMIN WESOLOWSKI, Univ. Bordeaux, CNRS, IMB, UMR 5071 and INRIA, LIPN, 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 algorithm can only reach an approximation factor $\exp(\tilde{O}(m))$. Following a recent series of attacks, these results call into question the hardness of various problems over structured lattices, such as Ideal-SVP and Ring-LWE, upon which relies the security of a number of cryptographic schemes.

NOTE. This article is an extended version of a conference paper [11]. 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 [40].

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

Additional Reference format:
Ronald Cramer, Léo Ducas, and Benjamin Wesolowski. 2020. Mildly Short Vectors in Cyclotomic Ideal Lattices in Quantum Polynomial Time. *J. ACM* 63, 2, Article 8 (January 2021), 26 pages.
<https://doi.org/10.1145/3451725>

1 Introduction
Lattice-based cryptography has attracted a lot of interest in the past few years due to the use of one-way functions. In this paper, we study the security of the one-way function based on the hardness of finding a short vector in a lattice. We consider the case of cyclotomic ideal lattices. 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 algorithm can only reach an approximation factor $\exp(\tilde{O}(m))$. Following a recent series of attacks, these results call into question the hardness of various problems over structured lattices, such as Ideal-SVP and Ring-LWE, upon which relies the security of a number of cryptographic schemes.

NOTE. This article is an extended version of a conference paper [11]. 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 [40].

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

Additional Reference format:
Ronald Cramer, Léo Ducas, and Benjamin Wesolowski. 2020. Mildly Short Vectors in Cyclotomic Ideal Lattices in Quantum Polynomial Time. *J. ACM* 63, 2, Article 8 (January 2021), 26 pages.
<https://doi.org/10.1145/3451725>

Is it really secure?



Federal Office
for Information Security

The illustration depicts a stylized scene where several figures are engaged with a large, glowing purple key. One figure stands on a ladder, another is seated at a desk with a laptop, and a third is standing nearby. In the background, a quantum atom symbol is visible, suggesting a connection to quantum computing or cryptography. The overall theme is the intersection of traditional security and quantum technology.

Quantum-safe cryptography – fundamentals, current developments and recommendations

Mildly Short Vectors in Cyclotomic Ideal Lattices in Quantum Polynomial Time

RONALD CRAMER, CWI, Amsterdam and Leiden University, The Netherlands
LÉO DUCAS, CWI, Amsterdam, CNRS, IMB, UMR 5074 and INRIA, LIPN, Paris
BENJAMIN WESOLOWSKI, Univ. Bordeaux, CNRS, IMB, UMR 5074 and INRIA, LIPN, Paris

In this article, we study the geometry of units and ideals of cyclotomic rings and derive an algorithm for finding a mildly short vector in any given cyclotomic ideal lattice in quantum polynomial time, under some number-theoretic assumptions. More precisely, given an ideal lattice of the cyclotomic ring of integers, the algorithm finds an approximation of the shortest vector by a factor $\exp(\sqrt{m})$. This result improves the hardness gap between these structured lattices and general lattices. The best known attack on generic lattice algorithms can only reach an approximation factor $\exp(\sqrt{m})$. Following a series of attacks, these results call into question the hardness of various problems over structured lattices, such as the Shortest Vector Problem (SVP) and Ring-LWE, upon which relies the security of a number of cryptographic schemes.

Notes. This article is an extended version of a conference paper [11]. The results are general to any 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 extend the results in the Ph.D. dissertation of the third author [40].

CCS Concepts • Mathematics of computing → Discrete mathematics; • Security and privacy → Cryptography; • Mathematics of computing → Discrete mathematics; • Security and privacy → Cryptography

Additional Key Words and Phrases: Shortest vector problem, ideal lattices, cyclotomic rings, quantum polynomial time

ACM Reference format:
Ronald Cramer, Léo Ducas, and Benjamin Wesolowski. 2020. Mildly Short Vectors in Quantum Polynomial Time. J. ACM 63, 2, Article 8 (January 2021), 26 pages.
<https://doi.org/10.1145/3441725>

Is it really secure?



Decoding One C

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, LIPANZ, France

In this article, we study the geometry of units and ideals of cyclotomic rings and derive an algorithm that finds an approximation of the shortest vector in an ideal lattice of a cyclotomic ring of integers. More precisely, given an ideal lattice of the cyclotomic ring of integers, our algorithm finds an approximation of the shortest vector by a factor $\exp(\sqrt{m})$. This result improves the hardness gap between these structured lattices and general lattices. The best known generic lattice algorithm can only reach an approximation factor $\exp(\sqrt{m})$. Following this result, these results call into question the hardness of various problems over structured lattices, such as the hardness of the Shortest Vector Problem (SVP) and Ring-LWE, upon which relies the security of a number of cryptographic schemes.

CCS Concepts • Mathematics of computing → Discrete mathematics, • Security and cryptography → Cryptography
Additional Key Words and Phrases: Shortest vector problem, ideal lattices, cyclotomic rings, quantum polynomial time

ACM Reference format:
 Ronald Cramer, Léo Ducas, and Benjamin Wesolowski. 2020. Mildly Short Vectors in Cyclotomic Ideal Lattices in Quantum Polynomial Time. *J. ACM* 63, 2, Article 8 (January 2021), 26 pages.
<https://doi.org/10.1145/3441772>

Federal Office
for Information Security

ANSSI views on the Post-Quantum Cryptography transition (2023 follow up) August 29, 2023

This document is an update of ANSSI's position on the post-quantum cryptography transition in view of the recent advances in the topic. It should be read as an addition to 2022's publication [1]. We will detail our recommendations in terms of post-quantum algorithms and hybridization techniques.

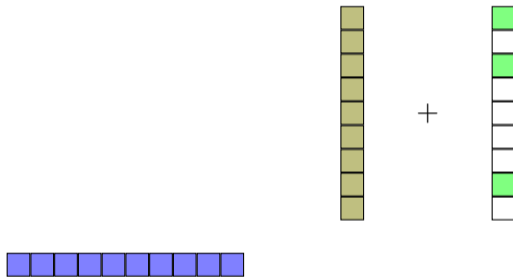
ANSSI also decided to speed-up the original approach. First French security view for products implementing hybrid post-quantum cryptography are expected to be delivered around 2024.

The impact of a potential large scale quantum computer on our current digital infrastructure has been discussed in ANSSI 2022's position paper [1]. While the quantum threat did not undergo any change since and more a reality, indeed, the research and development of post-quantum algorithms and secure implementations has highly increased in the last few years, concerning both theoretical hardness and scientific publications on the subject. This is attested by the increasing number of collaborative projects (PQTL, BERQUE, HYPERFORM, ePQDS, XTPQC) and the status of NIST first future PQC standards [2]. Cystabank [3] and other candidate algorithms will join the four future standardization efforts in hybrid post-quantum cryptography.

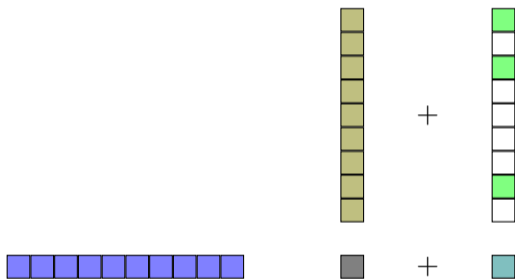
ANSSI considers that such an effort to encourage developers to start working on hybrid post-quantum solutions in 2023 and beyond 2023 on a regular basis.

The multi-dimensional approach

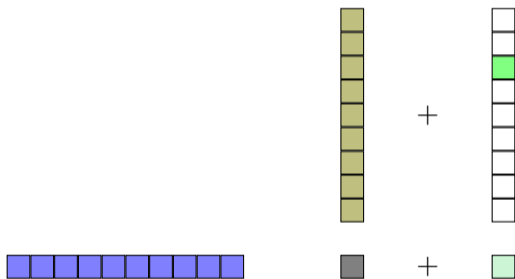
The right proportion of noise



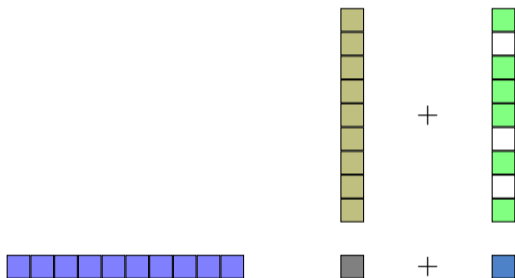
The right proportion of noise



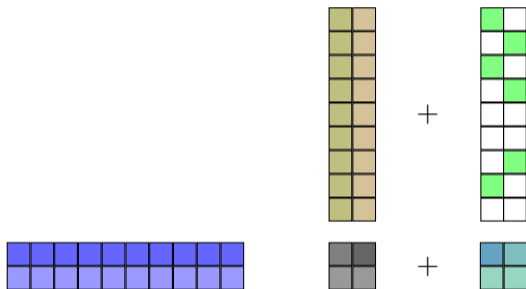
The right proportion of noise



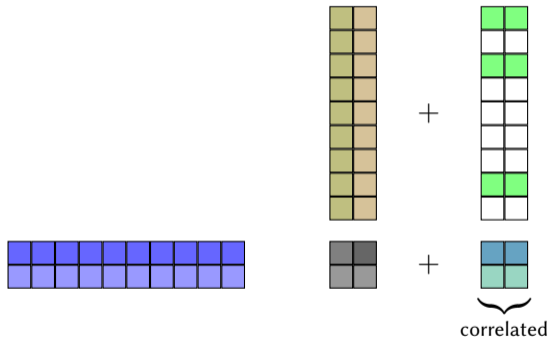
The right proportion of noise



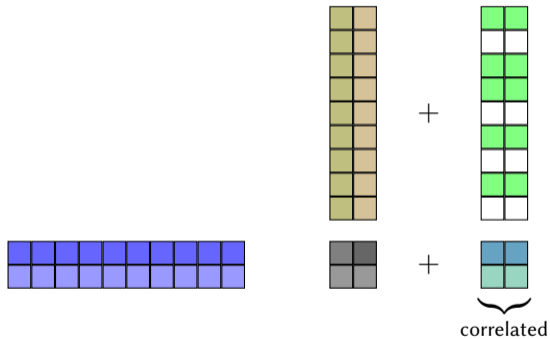
The multi-dimensional approach



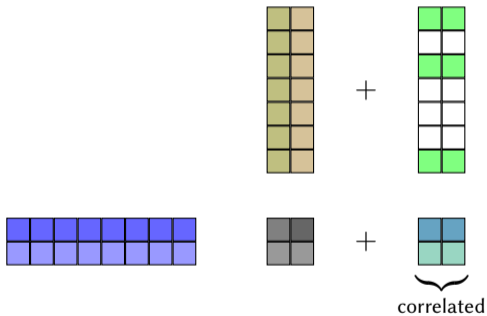
The multi-dimensional approach



The multi-dimensional approach



The multi-dimensional approach

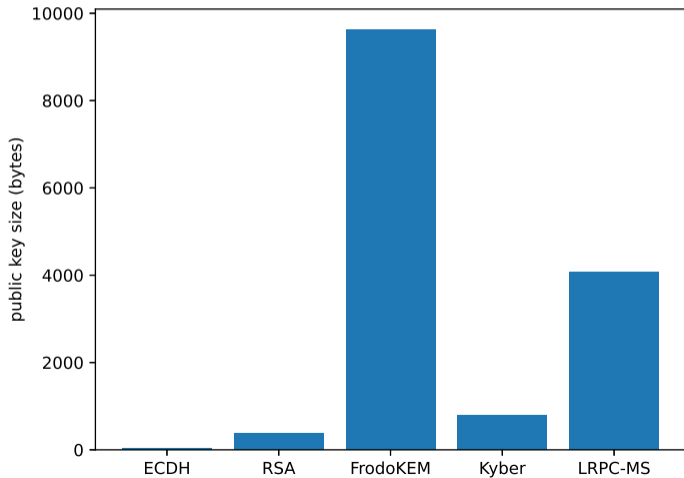


Application to efficient encryption

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

- 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.

-  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.