Lattice Codes for Lattice-Based PKE

Shanxiang Lyu[1,2*], Ling Liu[3], Cong Ling[4], Junzuo Lai[1] and Hao Chen[1]

[1*]College of Cyber Security, Jinan University, Guangzhou, 510632, China.
[2*]State Key Laboratory of Cryptology, P. O. Box 5159, Beijing, 100878, China.
[3] College of Computer Science and Software Engineering, Shenzhen University, Shenzhen, 518060, China.
[4]Department of Electrical and Electronic Engineering, Imperial College London, London, SW7 2AZ, United Kingdom.

*Corresponding author(s). E-mail(s): lsx07@jnu.edu.cn;

Abstract

Existing error correction mechanisms in lattice-based public key encryption (PKE) rely on either trivial modulation or its concatenation with error correction codes (ECC). This paper demonstrates that lattice coding, as a combined ECC and modulation technique, can replace trivial modulation in current lattice-based PKEs, resulting in improved error correction performance. We model the FrodoPKE protocol as a noisy point-to-point communication system, where the communication channel resembles an additive white Gaussian noise (AWGN) channel. To utilize lattice codes for this specific channel with hypercube shaping, we propose an efficient labeling function that converts binary information bits to lattice codewords and vice versa. The parameter sets of FrodoPKE are enhanced to achieve higher security levels or smaller ciphertext sizes. For instance, the proposed Frodo-1344-E_8 offers a 10-bit classical security improvement over Frodo-1344.

Keywords: public key encryption (PKE), lattice-based cryptography (LBC), lattice codes, coded modulation

1 Introduction

The impending realization of scalable quantum computers has posed a significant challenge for modern public key cryptosystems. Shor's quantum algorithm [1] can solve the prime factorization and discrete logarithm problems in polynomial time, rendering conventional public-key cryptosystems based on these problems insecure. Although it is difficult to predict when large-scale quantum computers will be built, it is essential to start preparing the next generation quantum-safe cryptosystem as soon as possible. Historical experiences have shown that deploying modern public key cryptography infrastructures takes a considerable amount of time.

Reacting to this urgency, the field of post-quantum cryptography (PQC) has been systematically developed in the last decade [2, 3]. PQC aims to design cryptosystems that are secure against quantum attacks while remaining compatible with classical computers. Since 2016, the National Institute of Standards and Technology (NIST) has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. This process primarily revolves around proposals for public key encryption/key encapsulation mechanism (PKE/KEM) and digital signatures.

Recently, NIST has announced four post-quantum cryptography standardization candidates [4]: CRYSTALS-Kyber for PKE/KEM, CRYSTALS-Dilithium, FALCON, and SPHINCS+ for digital signatures. The first three candidates are all based on lattice-based cryptography (LBC), which represents a significant victory for lattice-based cryptography due to its prominent advantages. LBC offers strong security proofs based on the hardness of worst-case problems, efficient implementations compared to other post-quantum constructions, and extended functionality for advanced constructions such as identity-based encryption and fully homomorphic encryption (FHE).

In lattice-based PKE/KEM, the decryption process may not always produce a 100% correct message. The encryption-decryption process can be seen as message transmission through an additive noise channel, and error correction techniques are employed to mitigate decryption failures, either implicitly or explicitly. Since high decryption failure rates (DFRs) can be exploited by adversaries to extract secrets, achieving a very small DFR (e.g., smaller than 2^{-128} or 2^{-140}) [5, 6] is of utmost importance. Hence, there is significant value in improving the error correction mechanism in lattice-based PKE/KEM schemes to attain better trade-off parameters:

- **Security Strength:** If the error correction mechanism can enhance the noise tolerance while maintaining a low DFR, the PKE/KEM scheme achieves a higher security level.
- **Communication Bandwidth:** If the error correction mechanism can reduce the modulus while ensuring a small DFR, it results in smaller ciphertext sizes, thereby reducing communication bandwidth requirements.

By enhancing the error correction mechanism in lattice-based PKE/KEM, we aim to address these objectives and optimize the trade-off parameters of security strength and communication bandwidth.

1.1 Related Works

Key encapsulation mechanisms (KEMs) can simultaneously output a session key along with a ciphertext that can be used to recover the session key. Two major approaches to designing lattice-based KEMs are PKEs (KEMs without reconciliation) [7–10], and key exchanges (KEMs with reconciliation) [11–13]. In this work, we focus on PKEs as they offer simplicity by avoiding the error-reconciliation mechanism.

Most lattice-based Public Key Encryption (PKE) schemes employ an error correction mechanism known as "trivial modulation." This technique involves mapping a binary string to different positions within the set $\{0, 1, \ldots, q-1\}$. If the noise amplitude is smaller than the error correction radius, successful decryption is achieved. Consequently, a larger value of q enables higher error correction capabilities. One example is Regev's Learning with Errors (LWE) based PKE scheme [2], which modulates a single bit μ to $(q/2)\mu$. Kawachi et al. [14] extended this scheme to support multi-bit modulation and conducted an evaluation of the trade-offs between decryption errors and security.

In recent years, researchers have realized that (digital) error correction codes (ECC) can be concatenated with modulations to obtain better error correction performance. For instance, the LAC [15] PKE employs BCH codes for error correction, which helps to reduce the modulo size q from 12289 to 251. The reason behind the small q is that, although the modulation level has minus error correction capability, the induced ECC helps to achieve a smaller DFR. Other examples can be found in the repetition codes based NewHope-Simple [8], XE5 based HILA5 [16], and the Polar codes based NewHope-Simple [17]. The downside of an extra modern ECC is an increased complexity of the program code and a higher sensitivity to side-channel attacks [18] (information is obtained through physical channels such as power measurements, variable execution time of the decoding algorithm, etc).

Using Error Correcting Codes (ECC) and modulation in a concatenated manner can limit the overall system performance, leading to issues such as a less flexible number of encoded bits and the independent decoding nature of modulation and ECC. However, a solution called "coded modulation" has been extensively studied in information theory and wireless communications for several decades, offering a joint design approach for ECC and modulation.

In the 1980s, Ungerboeck's pioneering work [19] demonstrated significant performance gains achieved through coded modulation. Building on that foundation, Forney [20, 21] systematically studied coded modulation schemes using coset codes and lattice codes. A remarkable breakthrough in information theory was made by Erez and Zamir [22], who showed that high-dimensional random lattice codes can achieve the capacity of additive white Gaussian noise (AWGN) channels. Additionally, recent years have witnessed the successful utilization of Polar lattices [23] and LDPC lattices [24] to achieve the capacity of AWGN channels. From the perspective of coset codes, lattice codes represent an elegant combination of linear codes and modulation. In this approach, if points in the constellation are closely located, they benefit from ECC protection, while information bits are directly mapped to points that are farther away. This blending of concepts allows lattice codes to provide an efficient and effective solution.

It should be noted that incorporating lattice codes into lattice-based Public Key Encryption (PKE) systems is not a straightforward task. This is because the previous literature on lattice coding [25] primarily focused on physical layer considerations where the transmission power of the codes is a crucial factor. In contrast, the modulo q arithmetic in lattice-based cryptography (LBC) operates at a higher layer. Nevertheless, in recent years, there have been notable efforts to employ lattice codes in PKE schemes. In 2016, van Poppelen introduced a Leech lattice-based PKE [9], and in 2021, Saliba et al. designed an E_8-lattice-based PKE [10]. It is worth mentioning that the choice of using the E_8 and Leech lattices aligns with significant advancements in mathematics: the proof that these lattices offer the best sphere packing density in dimensions 8 and 24 [26, 27]. However, there are certain limitations in the existing approaches. The Leech lattice-based PKE [9] suffers from a lack of a labeling technique, and the labeling technique employed for E_8 in [10] is nonlinear and not homomorphic. As a result, there is a clear demand for a comprehensive formulation of error correction based on lattice codes, along with the development of an efficient linear labeling method, in order to significantly improve lattice-based PKEs.

1.2 Contributions

This paper makes the following contributions, advocating the replacement of trivial modulation in lattice-based PKE with coded modulation:

- We analyze the plain-LWE scheme Frodo [7] and treat it as a communication system, with the communication channel resembling the AWGN channel. By introducing lattice-based coded modulation, we demonstrate that the error correction performance can be significantly enhanced compared to the use of trivial modulation. Additionally, ring-based or module-based schemes like NewHope-Simple [8] and Kyber [28] can also benefit from lattice-based coded modulation.
- We introduce a universal and efficient labeling technique for cubic-shaping based lattice codes. Our proposed linear labeling function maintains the homomorphic property. In LBC, due to the modulo q arithmetic, hypercube shaping using a simple integer lattice $q\mathbb{Z}^n$ is employed. While identifying the number of lattice codewords is straightforward in hypercube shaping, an efficient labeling function has been lacking in the literature. To address this, we propose a labeling function that establishes a one-to-one mapping between the binary information bits and the set of lattice vectors. This

labeling technique is applicable to a wide range of lattices, such as D_4, E_8, BW_{16}, Λ_{24}, and more.

- We derive a unified decoding failure rate (DFR) formula for analyzing the DFR of lattice-code based FrodoPKE over AWGN channels. The DFR formula only requires the Hermite parameter and the kissing number of lattices. Previously, DFR calculations relied on computationally intensive case-by-case analyses. With the DFR formula, we obtain better parameter sets for FrodoPKE. Notably, the implementations based on E_8 or BW_{16} are particularly appealing, as they offer simple encoding and decoding procedures while achieving higher security levels or smaller ciphertext sizes in the modified PKE.

The remainder of this paper is organized as follows: Section II provides background information on lattice codes and PKE. Section III introduces and analyzes the proposed labeling technique. Section IV presents a coset-based lattice decoding formulation and the pseudocode for decoding BW_{16}. Section V presents the improved parameter sets for FrodoPKE. Finally, Section VI concludes the paper.

2 Preliminaries

2.1 Lattice Codes

Definition 1 (Lattices)**.** A rank n lattice Λ is a discrete additive subgroup of $\mathbb{R}^m$, $m \geq n$. For simplicity, it is assumed that $m = n$ throughout.

Based on n linearly independent vectors $\mathbf{b}_1, \dots, \mathbf{b}_n$, Λ can be written as

$$\Lambda = \mathcal{L}(\mathbf{B}) = z_1\mathbf{b}_1 + z_2\mathbf{b}_2 + \cdots + z_n\mathbf{b}_n, \tag{1}$$

where $z_1, \dots, z_n \in \mathbb{Z}$, and $\mathbf{B} = [\mathbf{b}_1, \dots, \mathbf{b}_n]$ is referred to as a basis of Λ.

Definition 2 (Basic Cell (Fundamental Region))**.** A basic cell (or fundamental region) of the lattice Λ is a bounded set $\mathcal{P}_\Lambda$ that satisfies the following properties: i) Covering Property: $\cup_{\mathbf{v}\in\Lambda}(\mathbf{v} + \mathcal{P}_\Lambda) = \mathbb{R}^n$. ii) Partitioning Property: for all $\mathbf{v}, \mathbf{w} \in \Lambda$, if $\{\mathbf{v} + \mathcal{P}_\Lambda\} \cap \{\mathbf{w} + \mathcal{P}_\Lambda\} \neq \emptyset$, then $\mathbf{v} = \mathbf{w}$.

For example, a basic cell in the form of a parallelotope comprises linear combinations of the basis vectors, where the coefficients range from zero to one: $\left\{\mathbf{x} : \mathbf{x} = \sum_{i=1}^{n} \alpha_i \mathbf{b}_i,\ 0 \leq \alpha_i < 1\right\}$. Another example of a fundamental region is the Voronoi cell $\mathcal{V}_\Lambda$. This cell encompasses the set of points in $\mathbb{R}^n$ that are closer to a specific lattice point (known as the generating lattice point) within Λ than to any other lattice point. Essentially, it defines the region surrounding each generating lattice point where it is the closest lattice point.

Definition 3 (Closest Vector Problem)**.** Considering a query vector $\mathbf{t}$ and a lattice Λ, the closest vector problem is to find the closest vector to $\mathbf{t}$ in Λ.

The function $Q_\Lambda(\cdot)$, which solves the CVP problem, is called a decoder when used for error correction and a quantizer when employed for vector quantization.

Definition 4 (Nested lattices)**.** Two lattices Λ_f and Λ_c are nested if $\Lambda_c \subset \Lambda_f$. The denser lattice Λ_f is called the *fine/coding* lattice, and Λ_c is called the *coarse/shaping* lattice.

Lattice codes are the Euclidean space counterpart of linear codes, and they provide a unified framework to describe the coded modulation techniques [20, 21]. The inherent structure is a one-level/multi-level binary encoder and subset partitioning, which can encode more than n information bits to n symbols.

Definition 5 (Lattice code)**.** A lattice code $\mathcal{C}(\Lambda_f, \Lambda_c)$ is the finite set of points in Λ_f that lie within a basic cell of Λ_c:

$$\mathcal{C}(\Lambda_f, \Lambda_c) = \Lambda_f \cap \mathcal{P}_{\Lambda_c}. \tag{2}$$

If $\Lambda_c = p\mathbb{Z}^n$, then the lattice code $\mathcal{C}(\Lambda_f, \Lambda_c)$ is said to be generated from hypercube shaping. We illustrate a 2-dimensional example in Fig. 1, where the purple points represent Λ_f. The region enclosed by dashed black lines corresponds to a basic cell of $7\mathbb{Z}^2$, while the region enclosed by dashed peach lines represents a basic cell of $14\mathbb{Z}^2$. By adjusting the size of the shaping, we can obtain two sets of lattice codes: $\mathcal{C}(\Lambda_f, 7\mathbb{Z}^2)$ and $\mathcal{C}(\Lambda_f, 14\mathbb{Z}^2)$.

The information rate (averaged number of encoded bits) per dimension is defined as

$$B = \frac{1}{n}\log_2\left(\frac{\mathrm{Vol}(\Lambda_c)}{\mathrm{Vol}(\Lambda_f)}\right). \tag{3}$$

The Hermite parameter of a lattice, also identified as the coding gain, is defined as

$$\gamma(\Lambda) = \lambda_1(\Lambda)^2/\mathrm{Vol}(\Lambda)^{2/n} \tag{4}$$

where $\lambda_1(\Lambda)$ denotes the length of a shortest non-zero vector in Λ, and $\mathrm{Vol}(\Lambda) = |\det(\mathbf{B})|$ denotes the volume of Λ. The coding gain $\gamma(\Lambda)$ measures the increase in density of Λ over the baseline integer lattice $\mathbb{Z}$ (or $\mathbb{Z}^n$). Note that the supremum of $\lambda_1(\Lambda)^2/\mathrm{Vol}(\Lambda)^{2/n}$ over all n-dimensional lattices is known as Hermite's constant.

2.2 PKE/KEM in LBC

FrodoKEM [7] is a simple and conservative Key Encapsulation Mechanism (KEM) based on generic lattices. It is one of the post-quantum algorithms recommended by the German Federal Office for Information Security (BSI) as being cryptographically suitable for long-term confidentiality [29]. The underlying encryption scheme of FrodoKEM is called FrodoPKE, which achieves chosen-plaintext security (IND-CPA) and is closely related to the hardness of a corresponding LWE problem. Compared to other PKE/KEM schemes based

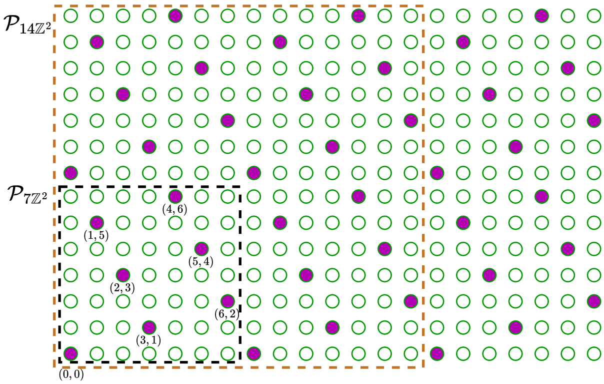

Fig. 1: Example of hypercube shaping in a 2-dimensional lattice.

on ring or module LWE, FrodoPKE offers security estimates that rely on fewer assumptions due to the lack of algebraic structure.

A public-key encryption scheme PKE consists of three algorithms: key generation, encryption and decryption.

In the key generation algorithm, random matrices $\mathbf{S}$ and $\mathbf{E}$ are sampled from the discrete Gaussian distribution $\chi_\sigma^{n' \times \bar{n}}$ with width σ, and a matrix $\mathbf{A}$ is sampled from a uniform distribution in $\mathbb{Z}_q^{n' \times n'}$. The algorithm computes $\mathbf{B} = \mathbf{AS} + \mathbf{E} \in \mathbb{Z}_q^{n' \times \bar{n}}$ as the public key $pk = (\mathbf{B}, \mathbf{A})$, and the secret key is $sk = \mathbf{S}$.

In the encryption algorithm, random matrices $\mathbf{S}'$ and $\mathbf{E}'$ are sampled from the discrete Gaussian distribution $\chi_\sigma^{\bar{m} \times n'}$, and a matrix $\mathbf{E}''$ is sampled from $\chi_\sigma^{\bar{m} \times \bar{n}}$. The algorithm computes $\mathbf{C}_1 = \mathbf{S}'\mathbf{A} + \mathbf{E}'$ and $\mathbf{V} = \mathbf{S}'\mathbf{B} + \mathbf{E}''$. To encrypt a message $\mu \in \mathcal{M} = \{0, 1\}^{\bar{m}\bar{n}B}$, the ciphertext is generated as

$$c = (\mathbf{C}_1, \mathbf{C}_2 = \mathbf{V} + \mathsf{Frodo.EncodeM}(\mu)). \tag{5}$$

The function Frodo.EncodeM represents a matrix encoding function of bit strings. Each B-bit value is transformed into the B most significant bits of the corresponding entry modulo q. This encoding scheme is referred to as "trivial modulation," as it amounts to a special case of lattice code-based encoding that employs hypercube shaping, with $\Lambda_f = \frac{q}{2^B}\mathbb{Z}^{64}$ and $\Lambda_c = q\mathbb{Z}^{64}$.

To decrypt, the secret key $\mathbf{S}$ and the ciphertext $\mathbf{C}_1, \mathbf{C}_2$ are used to compute

$$\hat{\mu} = \mathsf{Frodo.DecodeM}(\mathbf{C}_2 - \mathbf{C}_1\mathbf{S}), \tag{6}$$

where Frodo.DecodeM standards for the demodulation function. The FrodoPKE protocol is summarized in Fig. 2.

When targeting security levels 1, 3, and 5 in the NIST call for proposals, which aim to match or exceed the brute-force security of AES-128, AES-192, Input Parameters: q, n', $\bar{n}$, $\bar{m}$, χ_σ.

Alice		Bob
$\mathbf{A} \leftarrow_{\$} \mathbb{Z}_q^{n' \times n'}$		
$\mathbf{S}, \mathbf{E} \leftarrow_{\$} \chi_\sigma^{n' \times \bar{n}}$		$\mathbf{S}', \mathbf{E}' \leftarrow_{\$} \chi_\sigma^{\bar{m} \times n'}$
$\mathbf{B} = \mathbf{AS} + \mathbf{E}$	$\xrightarrow{\mathbf{A},\mathbf{B}}$	$\mathbf{E}'' \leftarrow_{\$} \chi_\sigma^{\bar{m} \times \bar{n}}$
		$\mathbf{C}_1 = \mathbf{S}'\mathbf{A} + \mathbf{E}'$
		$\mathbf{V} = \mathbf{S}'\mathbf{B} + \mathbf{E}''$
		$\mu \in \{0,1\}^{\bar{m}\bar{n}B}$
$\mathbf{Y} = \mathbf{C}_2 - \mathbf{C}_1\mathbf{S}$	$\xleftarrow{\mathbf{C}_1,\mathbf{C}_2}$	$\mathbf{C}_2 = \mathbf{V} + \mathsf{Frodo.EncodeM}(\mu)$
$\hat{\mu} = \mathsf{Frodo.DecodeM}(\mathbf{Y})$		

Fig. 2: The FrodoPKE protocol.

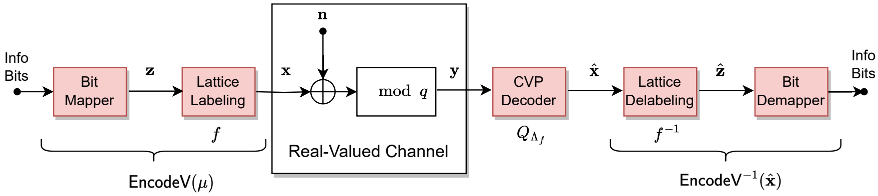

Fig. 3: The equivalent communication system model.

and AES-256, the recommended parameters for FrodoPKE are as follows:

$$\begin{aligned}
&\text{Frodo-640}: \ n' = 640, \bar{n} = 8, \bar{m} = 8, q = 2^{15}, \sigma = 2.75, \mathcal{M} = \{0,1\}^{128} \\
&\text{Frodo-976}: \ n' = 976, \bar{n} = 8, \bar{m} = 8, q = 2^{16}, \sigma = 2.3, \mathcal{M} = \{0,1\}^{192} \\
&\text{Frodo-1344}: \ n' = 1344, \bar{n} = 8, \bar{m} = 8, q = 2^{16}, \sigma = 1.4, \mathcal{M} = \{0,1\}^{256}.
\end{aligned}$$

3 The Proposed Scheme

3.1 Equivalent Communication Model

Recall that the decryption algorithm of FrodoPKE computes

$$\begin{aligned}
\mathbf{Y} &= \mathbf{C}_2 - \mathbf{C}_1\mathbf{S} \\
&= \mathsf{Frodo.EncodeM}(\mu) + \mathbf{S}'\mathbf{E} + \mathbf{E}'' - \mathbf{E}'\mathbf{S},
\end{aligned} \tag{7}$$

whose addition is over the modulo q domain. From the perspective of communications, this amounts to transmitting the modulated μ through an additive noise channel. Specifically, Eq. (7) can be formulated as

$$\mathbf{y} = \mathbf{x} + \mathbf{n} \mod q, \tag{8}$$

where $\mathbf{x} = \mathsf{EncodeV}(\mu) \in \mathbb{R}^{\bar{m}\bar{n}}$ denotes a general error correction function, and $\mathbf{y}$, $\mathbf{n}$ represent the vector form of $\mathbf{Y}$ and $\mathbf{S}'\mathbf{E} + \mathbf{E}'' - \mathbf{E}'\mathbf{S}$, respectively. Since the element-wise modulo q is equivalent to hypercube shaping via the lattice $q\mathbb{Z}^{\bar{m}\bar{n}}$, $\mathsf{EncodeV}$ can be designed from the perspective of lattice codes.

The flowchart of the communication model is plotted in Fig. 3, which contains the following operations:

- *Bit Mapper and Demapper*: The former maps binary information bits to an information vector $\mathbf{z}$ defined over integers, while the latter performs the inverse operation. These operations are straightforward.
- *Lattice Labeling and Delabeling*: Given a message index $\mathbf{z}$, lattice labeling finds its corresponding lattice codeword $\mathbf{x} \in \mathcal{C}(\Lambda_f, \Lambda_c = q\mathbb{Z}^{\bar{m}\bar{n}})$. Delabeling denotes the inverse of labeling.
- *CVP Decoder*: It returns the closet lattice vector to $\mathbf{y}$ over Λ_f. The CVP algorithm of $Q_{\Lambda_f}(\cdot)$ will be examined in Section 3.4.

The conventional method $\mathsf{Frodo.EncodeM}$ utilizes $\Lambda_f = q/(2^B)\mathbb{Z}^{\bar{m}\bar{n}}$ for simpler labeling functions. However, our research aims to improve the error correction performance by employing a more sophisticated Λ_f. As a result, the associated labeling function and CVP decoder become more intricate.

3.2 Lattice Labeling and Delabeling

In this section, we demonstrate that for any fine lattice with a basis in rectangular form, a linear labeling from specific index sets to lattice codewords can be generically defined.

Definition 6 (Rectangular Form)**.** A lattice basis $\mathbf{B}$ is said to be in rectangular form if it can be expressed as

$$\mathbf{B} = \mathbf{U} \cdot \mathrm{diag}(\pi_1, \pi_2, \ldots, \pi_n), \tag{9}$$

where $\mathbf{U} \in \mathrm{GL}_n(\mathbb{Z})$ is a unimodular matrix, and $\pi_1, \pi_2, \ldots, \pi_n \in \mathbb{Q}^+$.

Any lattice with a rational basis can be put into rectangular form. Specifically, if we consider the Smith Normal Form factorization of a lattice basis $\mathbf{B}^* \in \mathbb{Q}^{n\times n}$, we have

$$\mathbf{B}^* = \mathbf{U} \cdot \mathrm{diag}(\pi_1, \pi_2, \ldots, \pi_n) \cdot \mathbf{U}', \tag{10}$$

where $\mathbf{U}, \mathbf{U}' \in \mathrm{GL}_n(\mathbb{Z})$[1]. Since lattice bases are equivalent up to unimodular transformations, the term $\mathbf{U}'$ can be canceled out, resulting in the rectangular form.

For a lattice that possesses a rectangular form, an efficient labeling scheme can be constructed. The idea is that the combination of rectangular form

[1] The determinants of $\mathbf{U}$ and $\mathbf{U}'$ are 1 or -1 after incorporating the necessary rational factors into $\mathrm{diag}(\pi_1, \pi_2, \ldots, \pi_n)$.

and non-uniform labeling achieves hypercube shaping. Specifically, let the fine lattice be

$$\Lambda_f = \mathcal{L}(\mathbf{B}_f) = \mathcal{L}(\mathbf{U} \cdot \mathrm{diag}(p/p_1, p/p_2, \ldots, p/p_n)), \tag{11}$$

where $p \in \mathbb{Z}^+$ is a common multiplier of $\pi_1, \pi_2, \ldots, \pi_n$, and $p_1 = p/\pi_1, p_2 = p/\pi_2, \ldots, p_n = p/\pi_n$. If we set $\mathbf{B}_c = \mathbf{B}_f \mathrm{diag}(p_1, p_2, \ldots, p_n)$, we have

$$\begin{aligned}\Lambda_c &= \mathcal{L}(\mathbf{U} \cdot \mathrm{diag}(\pi_1, \pi_2, \ldots, \pi_n) \cdot \mathrm{diag}(p_1, p_2, \ldots, p_n)) \\ &= \mathcal{L}(p\mathbf{U}) \\ &= p\mathbb{Z}^n. \end{aligned} \tag{12}$$

The last equality holds because a unimodular matrix can be considered as a lattice basis for $\mathbb{Z}^n$. Thus, modulo Λ_c is equivalent to modulo p. This leads us to the following theorem.

Theorem 7 (Labeling Function)**.** *Let the message space be*

$$\mathcal{I} = \{0, 1, \ldots, p_1 - 1\} \times \cdots \times \{0, 1, \ldots, p_n - 1\}, \tag{13}$$

and let the pair of nested lattices be $\Lambda_f = \mathcal{L}(\mathbf{B}_f) = \mathcal{L}(\mathbf{U} \cdot \mathrm{diag}(p/p_1, p/p_2, \ldots, p/p_n))$ *and* $\Lambda_c = \mathcal{L}(p\mathbf{U}) = p\mathbb{Z}^n$*. With* $\mathbf{z} \in \mathcal{I}$*, the function* $f : \mathcal{I} \to \mathcal{C}(\Lambda_f, \Lambda_c)$*,*

$$f(\mathbf{z}) = [\mathbf{B}_f \mathbf{z}] \mod p, \tag{14}$$

is bijective.

Proof We aim to prove that f is both injective and surjective.

"Injective" means that no two elements in the domain of the function are mapped to the same image. For $\mathbf{z}_1, \mathbf{z}_2 \in \mathcal{I}$, we want to show that if $\mathbf{z}_1 \neq \mathbf{z}_2$, then $f(\mathbf{z}_1) \neq f(\mathbf{z}_2)$. We can prove this by contradiction. Suppose $f(\mathbf{z}_1) = f(\mathbf{z}_2)$. It implies that there exist $\mathbf{z}_1, \mathbf{z}_2 \in \mathcal{I}$ and $\mathbf{z}_3 \in \mathbb{Z}^n$ such that $\mathbf{B}_f(\mathbf{z}_1 - \mathbf{z}_2) = \mathbf{B}_f \cdot \mathrm{diag}(p_1, p_2, \ldots, p_n) \cdot \mathbf{z}_3$, which amounts to

$$\mathbf{z}_1 - \mathbf{z}_2 = \mathrm{diag}(p_1, p_2, \ldots, p_n) \cdot \mathbf{z}_3. \tag{15}$$

However, (15) has a solution only when $\mathbf{z}_3 = \mathbf{0}$, which leads to $\mathbf{z}_1 = \mathbf{z}_2$. Therefore, the injective property holds.

"Surjective" means that every element in the range of the function is mapped to by the function. Recall that the number of coset representatives of Λ_f/Λ_c is given by:

$$\frac{|\det(\mathbf{B}_c)|}{|\det(\mathbf{B}_f)|} = p_1 p_2 \cdots p_n. \tag{16}$$

Since $|\mathcal{I}| = p_1 p_2 \cdots p_n$, it follows from the injective property that all the coset representatives have been uniquely mapped. Hence, the surjection is proved. □

Denote $\mathbf{x} = f(\mathbf{z})$. The inverse of f is given by

$$\mathbf{z} = f^{-1}(\mathbf{x}) \triangleq \mathbf{B}_f^{-1}\mathbf{x} \mod (p_1, \ldots, p_n), \tag{17}$$

which stands for $z_i = \left(\mathbf{B}_f^{-1}\mathbf{x}\right)_i \mod p_i$, $i = 1, \ldots, n$. As the labeling and delabeling process also encounters an additive noise channel, we examine the correct recovery condition hereby. Assume that the receiver's side has the noisy observation $\mathbf{x} + \mathbf{n}$, with $\mathbf{x} \in \Lambda_f$ and $\mathbf{n}$ being the additive noise.

Theorem 8 (Correct Decoding)**.** *If* $Q_{\Lambda_f}(\mathbf{n}) \in \Lambda_c$*, then* $f^{-1}(Q_{\Lambda_f}(\mathbf{x} + \mathbf{n})) = f^{-1}(\mathbf{x})$*.*

Proof Notice that:

$$Q_{\Lambda_f}(\mathbf{x} + \mathbf{n}) = \mathbf{x} + Q_{\Lambda_f}(\mathbf{n}), \tag{18}$$

which implies:

$$f^{-1}(Q_{\Lambda_f}(\mathbf{x} + \mathbf{n})) = \mathbf{B}_f^{-1}\mathbf{x} + \mathbf{B}_f^{-1}Q_{\Lambda_f}(\mathbf{n}) \mod (p_1, \ldots, p_n). \tag{19}$$

The condition $Q_{\Lambda_f}(\mathbf{n}) \in \Lambda_c$ implies that this vector of the coarse lattice can be written as $\mathbf{B}_f \mathrm{diag}(p_1, p_2, \ldots, p_n)\mathbf{k}$ for $\mathbf{k} \in \mathbb{Z}^n$. Therefore, $Q_{\Lambda_f}(\mathbf{n}) \mod (p_1, \ldots, p_n) = \mathbf{0}$, and the theorem is proved. □

Theorem 8 states that if the noise vector $\mathbf{n}$ satisfies $Q_{\Lambda_f}(\mathbf{n}) \in \Lambda_c$, then the inverse function f^{-1} correctly recovers the original message $\mathbf{x}$ from the received vector $\mathbf{x} + \mathbf{n}$. We can summarize two cases for the correct recovery of messages: i) Small noise: $Q_{\Lambda_f}(\mathbf{n}) = \mathbf{0}$. ii) Large noise within the coarse lattice: $Q_{\Lambda_f}(\mathbf{n}) \neq \mathbf{0}$, $Q_{\Lambda_f}(\mathbf{n}) \in \Lambda_c$.
Example: Consider the D_4 lattice, whose lattice basis and its inverse are given by

$$\mathbf{B}_{D_4} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} \cdot \mathrm{diag}(1, 1, 1, 2), \tag{20}$$

$$\mathbf{B}_{D_4}^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -0.5 & -0.5 & -0.5 & 0.5 \end{bmatrix}. \tag{21}$$

To encode 7 bits over 4 dimensions, let the pair of nested lattices be $(\Lambda_f, \Lambda_c) = (D_4, 4\mathbb{Z}^4)$, and the message space be

$$\mathcal{I} = \{0, 1, 2, 3\}^3 \times \{0, 1\}. \tag{22}$$

W.l.o.g, let the input binary string be $\{0, 1, 1, 0, 1, 1, 1\}$. Then the "Bit Mapper" transforms the bits to a vector in $\mathcal{I}$:

$$\mathbf{z} = [1, 2, 3, 1]^\top.$$

By using lattice labeling in Eq. (14), we have

$$\mathbf{x} = f(\mathbf{z}) = [1, 2, 3, 0]^\top.$$

In the noiseless case where $\mathbf{n} = 0$, we have

$$\begin{aligned} f^{-1}(\mathbf{x}) &= f^{-1}([1, 2, 3, 0]^\top) && (23)\\ &= [1, 2, 3, -3]^\top \mod (4, 4, 4, 2) && (24)\\ &= [1, 2, 3, 1]^\top. && (25) \end{aligned}$$

In the large-noise case where $\mathbf{n} = [4, 4, 4, 4]^\top$, we have $Q_{\Lambda_f}(\mathbf{n}) \in \Lambda_c$, and

$$\begin{aligned} f^{-1}(Q_{\Lambda_f}(\mathbf{x} + \mathbf{n})) &= f^{-1}([5, 6, 7, 4]^\top) && (26)\\ &= [9, 10, 11, -7]^\top \mod (4, 4, 4, 2) && (27)\\ &= [1, 2, 3, 1]^\top. && (28) \end{aligned}$$

Finally, the "Bit Demapper" transforms the information integers back to bits, resulting in the original input.

3.3 Rectangular Forms of Code-Based Lattices

The proposed labeling is applicable to a wide range of lattices, including low-dimensional optimal lattices such as D_2, D_4, E_8, Λ_{24}, as well as the general Construction-A and Construction-D lattices. Construction A and Construction D are popular techniques for lifting linear codes to lattices. These techniques have been used to construct remarkable lattices with large coding gains, such as the Barnes-Wall lattices [21, 30, 31] and the polar lattices [23, 32]. Let C be a linear binary code of length n, dimension k, and minimum distance d, denoted as (n, k, d).

Definition 9 (Construction A [33])**.** A vector $\mathbf{y}$ is a lattice vector of the Construction-A lattice over C if and only if $\mathbf{y}$ modulo 2 is congruent to a codeword of C.

Let $\phi(\cdot)$ be a natural mapping function from $\mathbb{F}_2$ to $\mathbb{R}$ with $\phi(0) = 0, \phi(1) = 1$ for a scalar input, and $\phi(\cdot)$ is applied element-wise for a vector/matrix input. Let $\mathbf{G}$ be the generator matrix of C. By reformulating it as the Hermite normal form of $\{\mathbf{I}, \mathbf{A}\}$, the Construction-A lattice of C can be written as

$$\Lambda_A = \mathcal{L}\left(\begin{bmatrix} \phi(\mathbf{I}) & \mathbf{0} \\ \phi(\mathbf{A}) & 2\mathbf{I} \end{bmatrix}\right). \tag{29}$$

The lattice basis of Λ_A is therefore of a rectangular form. The volume of Λ_A is

$$V(\Lambda_A) = 2^{n-k}. \tag{30}$$

Definition 10 (Construction D [33]). Let $C_0 \subset C_1 \subset \cdots \subset C_a = \mathbb{F}_2^n$ be a family of nested binary linear codes, where C_i has parameters (n, k_i, d_i) and C_a is the trivial $(n, n, 1)$ code. A vector $\mathbf{y}$ is a lattice vector of the Construction-D lattice over $(C_0, \ldots, C_a)$ if and only if $\mathbf{y}$ is congruent (modulo 2^a) to a vector in $C_0 + 2C_1 + \cdots + 2^{a-1}C_{a-1}$.

Denote the generator matrices of C_0, C_i, and C_a as

$$\mathbf{G}_0 = \begin{bmatrix} | & | & & | \\ \mathbf{g}_1 & \mathbf{g}_2 & \cdots & \mathbf{g}_{k_0} \\ | & | & & | \end{bmatrix} \tag{31}$$

$$\mathbf{G}_i = \begin{bmatrix} | & | & & | & & | \\ \mathbf{g}_1 & \mathbf{g}_2 & \cdots & \mathbf{g}_{k_0} & \cdots & \mathbf{g}_{k_i} \\ | & | & & | & & | \end{bmatrix} \tag{32}$$

$$\mathbf{G}_a = \begin{bmatrix} | & | & & | & & | & & | \\ \mathbf{g}_1 & \mathbf{g}_2 & \cdots & \mathbf{g}_{k_0} & \cdots & \mathbf{g}_{k_i} & \cdots & \mathbf{g}_{k_a} \\ | & | & & | & & | & & | \end{bmatrix}, \tag{33}$$

where $1 \leq k_0 \leq k_1 \leq \cdots \leq k_a = n$. Then the code formula of a Construction-D lattice is

$$\Lambda_D = \bigcup_{\mathbf{u}_i \in \{0,1\}^{k_i}} \left(\sum_{i=0}^{a-1} 2^i \phi(\mathbf{G}_i)\mathbf{u}_i \right) + 2^a \mathbb{Z}^n \tag{34}$$

$$= \mathcal{L}(\phi(\mathbf{G}_a) \cdot \mathrm{diag}(2^0 \mathbf{1}_{k_0}, \ldots, 2^a \mathbf{1}_{k_a - k_{a-1}})), \tag{35}$$

where $\mathbf{1}_{k_i}$ denotes an all-one vector of dimension k_i, $\phi(\mathbf{G}_a)$ is a unimodular matrix. Thus $2^a\mathbb{Z}^n \subset \Lambda_D$ and the volume of a Construction-D lattice is

$$V(\Lambda_D) = 2^{an - \sum_{i=0}^{a-1} k_i}. \tag{36}$$

By using Construction D over Reed-Muller codes, the Barnes–Wall lattices can be obtained [21] [2]. Some low-dimensional examples are

$$BW_8 = (8, 4, 4) + 2\mathbb{Z}^8 \approxeq E_8 \tag{37}$$

$$BW_{16} = (16, 5, 8) + 2(16, 15, 2) + 4\mathbb{Z}^{16} \approxeq \Lambda_{16} \tag{38}$$

$$BW_{32} = (32, 6, 16) + 2(36, 26, 4) + 4\mathbb{Z}^{32} \tag{39}$$

$$BW_{64} = (64, 7, 32) + 2(64, 42, 8) + 4(64, 63, 2) + 8\mathbb{Z}^{64}, \tag{40}$$

where $\approxeq$ denotes equality up to rotations. The rectangular-form lattice basis in (35) can be derived by considering the Kronecker product based construction of Reed-Muller codes [35, Section I-D]. The explicit rectangular forms of the lattice bases for E_8, BW_8, and BW_{16} are provided in Appendix A.

[2] Barnes–Wall lattices can also be defined recursively [34, Definition 1.1].

3.4 CVP Decoding

Enumeration and sieving are two popular types of CVP algorithms for decoding random lattices [36, 37]. However, for code-based lattices used in error correction, these algorithms can be further optimized by leveraging the strong structures inherent in these lattices. While bounded distance decoding (BDD) techniques exist for Barnes–Wall lattices [34, 38], they fail to achieve the DFR of CVP decoding. Exploiting the structure of cosets, efficient CVP algorithms have been developed for lattices such as E_8 and D_n [39]. In a similar vein, this section explores the CVP decoding of BW_{16}, BW_{32}, and BW_{64}.

3.4.1 Lattice Partition as Cosets

A natural and efficient approach to designing CVP algorithms for Construction-D lattices is to partition the lattice as the union of cosets. If Λ can be expressed as the union of Λ' cosets, the CVP problem for Λ can be reduced to the CVP problem for Λ' as follows:

$$\begin{aligned} Q_{\Lambda}(\mathbf{t}) &= Q_{\Lambda'+\mathbf{g}'}(\mathbf{t}), \\ \mathbf{g}' &= \operatorname{argmin}_{\mathbf{g}\in\Lambda/\Lambda'} \left\|\mathbf{t} - Q_{\Lambda'+\mathbf{g}}(\mathbf{t})\right\|, \end{aligned} \tag{41}$$

where $Q_{\Lambda'+\mathbf{g}}(\mathbf{t}) = \mathbf{g} + Q_{\Lambda'}(\mathbf{t}-\mathbf{g})$. The number of cosets in the partition is denoted as $|\Lambda/\Lambda'|$. Consequently, the computational complexity of Q_Λ is $|\Lambda/\Lambda'|$ times larger than that of $Q_{\Lambda'}$.

While all Construction-D lattices can be partitioned using $\mathbb{Z}^n$ as the base, this generally results in a large number of cosets. Whenever possible, partitioning the lattice into D_n cosets can significantly improve decoding efficiency. For instance, the CVP algorithm for E_8 [39] treats E_8 as two D_8 cosets, and D_8 can be further divided into two $\mathbb{Z}^8$ cosets. This clever partitioning strategy contributes to the faster decoding of E_8.

3.4.2 Decoding BW_{16}

Among BW_{16}, BW_{32}, and BW_{64}, only BW_{16} and BW_{64} contain D_n-based cosets:

$$BW_{16} = (16, 5, 8) + 2D_{16}, \tag{42}$$

$$BW_{64} = (64, 7, 32) + 2(64, 42, 8) + 4D_{64}. \tag{43}$$

The number of cosets for BW_{16} and BW_{64} are $|BW_{16}/2D_{16}| = 2^5$ and $|BW_{64}/4D_{64}| = 2^{49}$, respectively. In contrast, $|BW_{16}/4\mathbb{Z}^{16}| = 2^{20}$ and $|BW_{64}/8\mathbb{Z}^{64}| = 2^{112}$. Additionally, $|BW_{32}/4\mathbb{Z}^{32}| = 2^{32}$.

Based on the above observations, the decoding complexity of BW_{16} appears to be more manageable compared to BW_{32} and BW_{64}. Referring to Eqs. (41) and (42), we have:

$$Q_{BW_{16}}(\mathbf{t}) = Q_{2D_{16}+\mathbf{g}'}(\mathbf{t}), \tag{44}$$

$$\mathbf{g}' = \mathrm{argmin}_{\mathbf{g}\in(16,5,8)} \left\| \mathbf{t} - Q_{2D_{16}+\mathbf{g}}(\mathbf{t}) \right\|.$$

The pseudocode for the CVP algorithms $Q_{BW_{16}}$ and Q_{D_n} are presented in Algorithm 1 and Algorithm 2, respectively.

Algorithm 1 The closest vector algorithm $Q_{BW_{16}}$

Input: A query vector $\mathbf{y}$.
Output: The closest vector $\hat{\mathbf{v}}$ of $\mathbf{y}$ in BW_{16}.

```
Define the codewords of (16,5,8) as d_1, ..., d_32
for t = 1, ... 32 do
    y_t = (y - d_t)/2
    v̂_t = 2 Q_{D_n}(y_t) + d_t
    Dist_t = y - v̄_t
end for
t* = min_t Dist_t
v̂ = v̂_{t*}.
```

Algorithm 2 The closest vector algorithm Q_{D_n}.

Input: A query vector $\mathbf{y}$.
Output: The closest vector $\hat{\mathbf{v}}$ of $\mathbf{y}$ in D_n.

```
u = ⌊y⌉
δ = |y - u|
t* = max_t |y_t - u_t|
v = u
if y_{t*} - u_{t*} > 0 then
    v_{t*} ← v_{t*} + 1
else
    v_{t*} ← v_{t*} - 1
end if
if u_1 + ··· + u_n mod 2 = 0 then
    v̂ = u
else
    v̂ = v
end if
```

4 Improving FrodoPKE with Lattice Codes

4.1 DFR Analysis in the Worst Case

In FrodoPKE, χ_σ is chosen from a truncated discrete Gaussian that minimizes its Rényi divergence from the target "ideal" distribution, as the loss of security can be evaluated by computing the Rényi divergence between the two distributions [40]. To simplify the DFR analysis, χ_σ is treated as a continuous Gaussian distribution of $\mathcal{N}(0,\sigma^2)$.

Recall that Section 3.1 has formulated an $\bar{m}\bar{n}$-dimensional modulo lattice additive noise channel "$\mathbf{y}=\mathbf{x}+\mathbf{n} \mod q$". The error term $\mathbf{n}$ has $\bar{m}\bar{n}$ entries, each entry has the form of $\mathbf{s}'\mathbf{e}+e''-\mathbf{e}'\mathbf{s}$, and we have

$$\mathbb{E}(\mathbf{s}'\mathbf{e}+e''-\mathbf{e}'\mathbf{s})=0 \tag{45}$$

$$\mathbb{E}\left(\|\mathbf{s}'\mathbf{e}+e''-\mathbf{e}'\mathbf{s}\|^2\right)=2n'\sigma^4+\sigma^2. \tag{46}$$

Although the entries of $\mathbf{n}$ are not independent, we can use information theory to give a worst case analysis. The information entropy of $\mathbf{n}$ is no larger than that of the joint distribution of $\bar{m}\bar{n}$ i.i.d. $\mathcal{N}(0,2n'\sigma^4+\sigma^2)$ (also known as Hadamard's Inequality [41]). We adopt this "largest entropy" setting to approximate the DFR, which amounts to the error rate analysis of lattice codes over an AWGN channel.

The DFR of the PKE protocol can be estimated by using the decoding error probability P_e of a lattice codeword. To proceed, we set the coarse lattice $\Lambda_c=q\mathbb{Z}^n$ ($n=\bar{m}\bar{n}$) as required by the PKE protocol, and identify a general fine lattice Λ_f with kissing number τ, length of the shortest non-zero lattice vector λ_1, and volume

$$\mathrm{Vol}(\Lambda_f)=\frac{\mathrm{Vol}(\Lambda_c)}{2^{nB}}. \tag{47}$$

Based on Theorem 8, the DFR can be evaluated as

$$P_e \triangleq \Pr\left(\hat{\mu}\neq\mu\right)=\Pr\left(Q_{\Lambda_f}(\mathbf{n})\notin\Lambda_c\right)\leq\Pr\left(Q_{\Lambda_f}(\mathbf{n})\neq\mathbf{0}\right). \tag{48}$$

Assume that $\mathbf{n}$ admits an i.i.d. Gaussian noise $\mathcal{N}(0,\bar{\sigma}^2)$ with $\bar{\sigma}=\sigma\sqrt{2n'\sigma^2+1}$, it follows from [33, Chap. 3], [42, Eq. 4] that

$$\Pr\left(Q_{\Lambda_f}(\mathbf{n})\neq\mathbf{0}\right)\lesssim\frac{\tau}{2}\mathrm{erfc}\left(\frac{\lambda_1/2}{\sqrt{2}\bar{\sigma}}\right) \tag{49}$$

$$=\frac{\tau}{2}\mathrm{erfc}\left(\frac{\sqrt{\gamma}q}{2^{B+3/2}\bar{\sigma}}\right), \tag{50}$$

where the second equality is obtained by substituting $\lambda_1=\sqrt{\gamma}\left(q^n/2^{nB}\right)^{1/n}$, which is based on the definition of Hermite parameter γ and $\mathrm{Vol}(\Lambda_c)=q^n$. Note that "$\lesssim$" denotes an approximate "$\leq$", which holds in the high signal to noise ratio scenario (i.e., $\lambda_1\gg\bar{\sigma}$) [33, Chap. 3]. In Fig. 4, by using $\mathbb{Z}^8$ and E_8 as the fine lattice, respectively, we plot both their theoretical DFR upper bounds and the actual simulated DFRs, which suggests the upper bound in (49) is tight.

The DFR formula is determined by several factors, including: (i) The Hermite parameter γ, which describes the density of lattice points packed in a unit volume for a given minimum Euclidean distance. (ii) The kissing number τ, which measures the number of facets in the Voronoi region of a lattice.

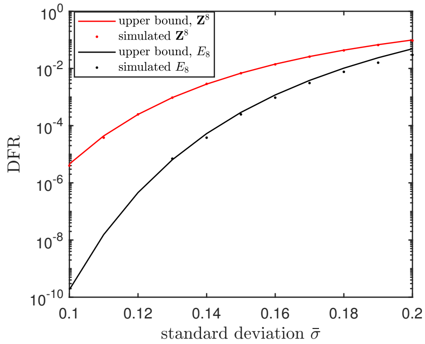

Fig. 4: The DFRs of trivial modulation and E_8 based coded modulation.

(iii) The modulus q in LBC. (iv) The averaged number of encoded bits B. (v) The standard deviation $\bar{\sigma}$ of the effective noise. These factors collectively contribute to determining the value of the DFR.

4.2 Flexible Lattice Parameter Settings

Finding the densest lattice structure is a well-studied topic, and the Hermite parameter γ and kissing number τ of some low-dimensional optimal lattices can be found in [33]. Therefore, the key challenge is to judiciously design B, q, $\bar{\sigma}$ based on chosen γ and τ.

i) On the kissing number and Hermite parameter. We adopt Barnes–Wall lattices to construct lattice codes. Though being less dense than other known packings in dimensions 32 and higher, they offer the densest packings in dimensions 2, 4, 8 and 16 [33]. Moreover, many lattice parameters are available [33][P. 151]. In dimension $n = 2^r$ with $r = 1, 2, 3, \ldots$, the kissing number is given by

$$\tau = (2+2)(2+2^2)\cdots(2+2^r), \tag{51}$$

and the Hermite parameter is defined as

$$\gamma_r = 2^{(r-1)/2}, \tag{52}$$

which increases without limit. If Λ' is constructed from the k-fold Cartesian product of $\Lambda \subset \mathbb{R}^m$, i.e, $\Lambda' = \Lambda \times \cdots \times \Lambda \subset \mathbb{R}^{km}$, then we have

$$\tau(\Lambda') = k\tau(\Lambda) \tag{53}$$

$$\gamma_r(\Lambda') = \gamma_r(\Lambda). \tag{54}$$

Table 1 summarizes the parameters of some low-dimensional optimal lattices and the Barnes–Wall lattices.

ii) On the information rate B. Since the coarse lattice in FrodoPKE is $\Lambda_c = q\mathbb{Z}^{64}$, let $2^{\Delta} = q/p$ be a power of 2 with p being a free parameter. By choosing

Table 1: Properties of selected lattices.

Lattice	$\mathbb{Z}$	D_4	E_8	BW_{16}	Λ_{24}	BW_{32}	BW_{64}
Hermite parameter γ	1	$2^{1/2}$	2	$2^{3/2}$	4	4	$2^{5/2}$
Kissing number τ	2	24	240	4320	196560	146880	9694080
Volume $\mathrm{Vol}(\Lambda_t)$	1	2	1	2^{12}	1	2^{32}	2^{80}

a small-dimensional lattice $\Lambda_t \in \mathbb{R}^t$, where t divides 64, and $p\mathbb{Z}^t \subset \Lambda_t$, the fine lattice is a Cartesian product of Λ_t:

$$\Lambda_f = 2^{\Delta}\Lambda_t \times \cdots \times \Lambda_t. \tag{55}$$

The number of encoded bits B per dimension is dictated by p:

$$B = \frac{1}{n}\log_2\left(\frac{\mathrm{Vol}(\Lambda_c)}{\mathrm{Vol}(\Lambda_f)}\right) = \frac{1}{t}\log_2\frac{p^t}{\mathrm{Vol}(\Lambda_t)}. \tag{56}$$

For a Construction-A or Construction-D lattice, it always holds that:

$$p\mathbb{Z}^t \subset 2^a\mathbb{Z}^t \subset \Lambda_t. \tag{57}$$

While the E_8 lattice has half integers, it holds that $4\mathbb{Z}^8 \subset 2E_8$.

Based on different fine lattices, we enumerate some feasible number of encoded bits in FrodoPKE below, denoted as $64B$:

- $\Lambda_f = 2^{\Delta} \cdot \mathbb{Z}^{64}$, $64B = 64, 128, 192, 256, \ldots$
- $\Lambda_f = 2^{\Delta} \cdot D_4^{16}$, $64B = 112, 176, 240, 304, \ldots$
- $\Lambda_f = 2^{\Delta} \cdot E_8^8$, $64B = 64, 128, 192, 256, \ldots$
- $\Lambda_f = 2^{\Delta} \cdot BW_8^8$, $64B = 96, 160, 224, 288, \ldots$
- $\Lambda_f = 2^{\Delta} \cdot BW_{16}^4$, $64B = 80, 144, 208, 272, \ldots$
- $\Lambda_f = 2^{\Delta} \cdot BW_{32}^2$, $64B = 64, 128, 192, 256, \ldots$
- $\Lambda_f = 2^{\Delta} \cdot BW_{64}$, $64B = 112, 176, 240, 304 \ldots$

4.3 Improved Frodo Parameters

The Frodo-640, Frodo-976, and Frodo-1344 schemes are designed to target security levels 1, 3, and 5, respectively, as defined in the NIST PQC Standardization. To provide resistance against attacks exploiting Distinguished Field Reconstructions (DFRs) [6], the DFR bounds at levels 1, 3, and 5 should not exceed 2^{-128}, 2^{-192}, and 2^{-256}, respectively.

In our proposed scheme, we focus on modifications to the labeling function, the corresponding Closest Vector Problem (CVP) algorithm, and the parameter choices of σ, B, and q. The security levels refer to the primal and dual attack via the FrodoKEM script `pqsec.py` [43]. The subscripts C, Q and P denote "classical", "quantum" and "paranoid" estimates on the concrete bit-security given by parameters (n', σ, q). We propose three sets of parameters in Tables 2 and 3: the first aims at improving the security level and the second at reducing the communication bandwidth. Frodo-640/976/1344 are the original parameter sets. The parameters that we have changed are highlighted in bold-face blue color, and other values that have altered as a consequence of this change are marked with normal blue color.

Parameter set 1: Improved security strength

In this parameter set, we aim to enhance the security strength of Frodo-640/976/1344 by increasing the value of σ while keeping n' and q unchanged. The table below (Table 2) shows the results of error correction using different lattice structures, such as E_8, BW_{16}, and BW_{32}, which improve the security level of the original Frodo-640/976/1344 by 6 to 16 bits. It is worth noting that while $\mathbb{Z}^{64}$, E_8^8, and BW_{32}^2 naturally encode 128, 192, and 256 bits per instance, respectively, BW_{16}^4 only supports 144, 208, and 272 bits. Among these options, the parameter set based on BW_{32} offers the highest security enhancement in the table. However, its CVP decoding complexity of enumerating 2^{32} cosets may make it less attractive.

Considering the trade-off between security and complexity, we recommend the parameter sets based on E_8 and BW_{16}. Frodo-640/976/1344-E_8 provides a good balance between information rate and security level, with a classical security enhancement of 7 or 8 bits compared to the original Frodo-640/976/1344. On the other hand, Frodo-640/976/1344-BW_{16} maintains a similar security level to Frodo-640/976/1344-E_8 while offering a slightly higher information rate, with B values of 2.25, 3.25, or 4.25.

Parameter set 2: Reduced size of ciphertext

In this parameter set, we aim to reduce the size of the ciphertext by decreasing the value of q while maintaining a small DFR and a comparable security level. The table below (Table 3) shows the results of reducing q from 2^{15} to 2^{14}, which leads to a reduction in the size of the ciphertext, denoted as $|c|$. For example, in Frodo-640, the ciphertext size can be reduced from 9720 bytes to 9072 bytes, in Frodo-976 from 15744 bytes to 14760 bytes, and in Frodo-1344 from 21632 bytes to 20280 bytes. Once again, the parameter sets based on E_8 and BW_{16} are recommended.

It is worth mentioning that the lattice-code based FrodoPKE can also be extended to a KEM for symmetric lightweight cryptography algorithms. By setting $\Lambda_f = 2^\Delta \cdot BW_{16}^4$ and $\Lambda_c = 2^\Delta \cdot 4\mathbb{Z}^{64}$, it is possible to tightly exchange 80 bits for the PRESENT [44] algorithm. This highlights the versatility and potential applications of the FrodoPKE scheme.

4.4 IND-CCA Security

Lattice code-based PKE/KEM also provides chosen ciphertext secure (IND-CCA) security. Similar to the argument presented in [7], the IND-CPA security of FrodoPKE is upper bounded by the advantage of the decision-LWE problem with the same parameters and error distribution. This establishes a connection between the security of FrodoPKE and the hardness of the underlying lattice problem. To achieve IND-CCA security, the post-quantum secure version of the Fujisaki-Okamoto transform [45, 46] can be applied. This transform allows an IND-CPA encryption scheme to be transformed into an IND-CCA secure scheme. By incorporating this transformation, the encryption scheme can resist chosen ciphertext attacks.

In the context of analyzing the security of a cryptographic scheme in the quantum random-oracle model, security proofs often consider the number of decryption queries made by the chosen ciphertext adversary. In [47, Theorem 4.3], it is demonstrated that the impact of decryption failure can be quantified as $4q_G P_e$, where q_G represents the number of quantum oracle queries and P_e denotes the decryption failure rate. Based on the established bounds on decryption failure, it can be argued that such queries pose no significant danger to the overall security of the scheme.

5 Conclusions

In this paper, we have demonstrated the potential of low-dimensional structured lattices in improving the error correction performance of FrodoPKE, highlighting the benefits of lattice codes as a form of coded modulation. The connection between lattice codes and FrodoPKE (and lattice-based PKEs in general) lies in the modulo q operation, which leads to hypercube shaping. By introducing an efficient lattice labeling function and a comprehensive formula for estimating the DFR, lattice-based coded modulation becomes feasible in LBC. Through the utilization of low-dimensional optimal lattices, we have obtained several enhanced parameter sets for FrodoPKE, offering either higher security levels or smaller ciphertext sizes. Furthermore, the lattice coding techniques presented in this work can be readily applied to Ring/Module LWE-based PKEs, extending their potential applications beyond FrodoPKE.

Acknowledgments. The authors are grateful to the reviewers for their constructive suggestions that improved the presentation and quality of this paper. This work was supported in part by the National Natural Science Foundation of China (No. 61902149, 62001300, and 62032009), the Natural Science Foundation of Guangdong Province (No. 2021A1515011679), the Science and Technology Planning Project of Guangzhou (No. 202201010388), the Major Program of Guangdong Basic and Applied Research (No. 2019B030302008).

Table 2: The recommended parameter sets with higher security.

	Structure of lattice code		$n', \bar{n}, \bar{m}$	q	σ	B	DFR	$\lvert c \rvert$	Security		
	Λ_f	Λ_c						(bytes)	C	Q	P
Frodo-640	$2^{13} \cdot \mathbb{Z}^{64}$	$2^{15} \cdot \mathbb{Z}^{64}$	$640, 8, 8$	2^{15}	2.75	2	2^{-164}	9720	149	136	109
Frodo-640-E_8	$2^{13} \cdot E_8^8$	$2^{15} \cdot \mathbb{Z}^{64}$	$640, 8, 8$	2^{15}	**3.25**	2	2^{-164}	9720	156	142	113
Frodo-640-BW_{16}	$2^{12} \cdot BW_{16}^4$	$2^{15} \cdot \mathbb{Z}^{64}$	$640, 8, 8$	2^{15}	**3.23**	**2.25**	2^{-164}	9720	155	142	113
Frodo-640-BW_{32}	$2^{12} \cdot BW_{32}^2$	$2^{15} \cdot \mathbb{Z}^{64}$	$640, 8, 8$	2^{15}	**3.83**	2	2^{-164}	9720	162	148	118
Frodo-976	$2^{13} \cdot \mathbb{Z}^{64}$	$2^{16} \cdot \mathbb{Z}^{64}$	$976, 8, 8$	2^{16}	2.3	3	2^{-220}	15744	216	196	156
Frodo-976-E_8	$2^{13} \cdot E_8^8$	$2^{16} \cdot \mathbb{Z}^{64}$	$976, 8, 8$	2^{16}	**2.72**	3	2^{-220}	15744	224	204	162
Frodo-976-BW_{16}	$2^{12} \cdot BW_{16}^4$	$2^{16} \cdot \mathbb{Z}^{64}$	$976, 8, 8$	2^{16}	**2.71**	**3.25**	2^{-220}	15744	224	204	161
Frodo-976-BW_{32}	$2^{12} \cdot BW_{32}^2$	$2^{16} \cdot \mathbb{Z}^{64}$	$976, 8, 8$	2^{16}	**3.21**	3	2^{-220}	15744	232	211	167
Frodo-1344	$2^{12} \cdot \mathbb{Z}^{64}$	$2^{16} \cdot \mathbb{Z}^{64}$	$1344, 8, 8$	2^{16}	1.4	4	2^{-290}	21632	282	256	203
Frodo-1344-E_8	$2^{12} \cdot E_8^8$	$2^{16} \cdot \mathbb{Z}^{64}$	$1344, 8, 8$	2^{16}	**1.66**	4	2^{-290}	21632	292	265	210
Frodo-1344-BW_{16}	$2^{11} \cdot BW_{16}^4$	$2^{16} \cdot \mathbb{Z}^{64}$	$1344, 8, 8$	2^{16}	**1.66**	**4.25**	2^{-290}	21632	292	265	210
Frodo-1344-BW_{32}	$2^{11} \cdot BW_{32}^2$	$2^{16} \cdot \mathbb{Z}^{64}$	$1344, 8, 8$	2^{16}	**1.97**	4	2^{-290}	21632	302	275	217

Table 3: The recommended parameter sets with smaller size of ciphertext.

	Structure of lattice code		$n', \bar{n}, \bar{m}$	q	σ	B	DFR	$\|c\|$	Security		
	Λ_f	Λ_c						(bytes)	C	Q	P
Frodo-640	$2^{13} \cdot \mathbb{Z}^{64}$	$2^{15} \cdot \mathbb{Z}^{64}$	$640, 8, 8$	2^{15}	2.75	2	2^{-164}	9720	149	136	109
Frodo-640-E_8	$2^{12} \cdot E_8^8$	$2^{14} \cdot \mathbb{Z}^{64}$	$640, 8, 8$	$\mathbf{2^{14}}$	2.30	2	2^{-164}	9072	156	143	114
Frodo-640-BW_{16}	$2^{11} \cdot BW_{16}^4$	$2^{14} \cdot \mathbb{Z}^{64}$	$640, 8, 8$	$\mathbf{2^{14}}$	2.29	**2.25**	2^{-164}	9072	156	143	114
Frodo-640-BW_{32}	$2^{11} \cdot BW_{32}^2$	$2^{14} \cdot \mathbb{Z}^{64}$	$640, 8, 8$	$\mathbf{2^{14}}$	2.71	2	2^{-164}	9072	163	149	118
Frodo-976	$2^{13} \cdot \mathbb{Z}^{64}$	$2^{16} \cdot \mathbb{Z}^{64}$	$976, 8, 8$	2^{16}	2.3	3	2^{-220}	15744	216	196	156
Frodo-976-E_8	$2^{12} \cdot E_8^8$	$2^{15} \cdot \mathbb{Z}^{64}$	$976, 8, 8$	$\mathbf{2^{15}}$	1.93	3	2^{-220}	14760	225	205	162
Frodo-976-BW_{16}	$2^{11} \cdot BW_{16}^4$	$2^{15} \cdot \mathbb{Z}^{64}$	$976, 8, 8$	$\mathbf{2^{15}}$	1.92	**3.25**	2^{-220}	14760	224	204	162
Frodo-976-BW_{32}	$2^{11} \cdot BW_{32}^2$	$2^{15} \cdot \mathbb{Z}^{64}$	$976, 8, 8$	$\mathbf{2^{15}}$	2.27	3	2^{-220}	14760	233	212	168
Frodo-1344	$2^{12} \cdot \mathbb{Z}^{64}$	$2^{16} \cdot \mathbb{Z}^{64}$	$1344, 8, 8$	2^{16}	1.4	4	2^{-290}	21632	282	256	203
Frodo-1344-E_8	$2^{11} \cdot E_8^8$	$2^{15} \cdot \mathbb{Z}^{64}$	$1344, 8, 8$	$\mathbf{2^{15}}$	1.18	4	2^{-290}	20280	291	265	210
Frodo-1344-BW_{16}	$2^{10} \cdot BW_{16}^4$	$2^{15} \cdot \mathbb{Z}^{64}$	$1344, 8, 8$	$\mathbf{2^{15}}$	1.17	**4.25**	2^{-290}	20280	291	265	209
Frodo-1344-BW_{32}	$2^{10} \cdot BW_{32}^2$	$2^{15} \cdot \mathbb{Z}^{64}$	$1344, 8, 8$	$\mathbf{2^{15}}$	1.39	4	2^{-290}	20280	302	275	217

Appendix A

The lattice bases for E_8, BW_8, and BW_{16} are as follows:

$$\begin{bmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0.5 \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0.5 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0.5 \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0.5 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0.5 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0.5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0.5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0.5 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 \\ 1 & 1 & 1 & 0 & 2 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 2 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 2 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1&1&1&1&1&2&2&2&2&2&2&2&2&2&2&4 \\ 1&1&1&1&0&2&2&0&2&0&0&2&0&0&0&0 \\ 1&1&1&0&1&2&0&2&0&2&0&0&2&0&0&0 \\ 1&1&1&0&0&2&0&0&0&0&0&0&0&0&0&0 \\ 1&1&0&1&1&0&2&2&0&0&2&0&0&2&0&0 \\ 1&1&0&1&0&0&2&0&0&0&0&0&0&0&0&0 \\ 1&1&0&0&1&0&0&2&0&0&0&0&0&0&0&0 \\ 1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 1&0&1&1&1&0&0&0&2&2&2&0&0&0&2&0 \\ 1&0&1&1&0&0&0&0&2&0&0&0&0&0&0&0 \\ 1&0&1&0&1&0&0&0&0&2&0&0&0&0&0&0 \\ 1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 1&0&0&1&1&0&0&0&0&0&2&0&0&0&0&0 \\ 1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0 \\ 1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \end{bmatrix}.$$

References

[1] Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. **26**(5), 1484–1509 (1997). https://doi.org/10.1137/S0097539795293172

[2] Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: Proceedings of the 37th Annual ACM Symposium on Theory of Computing (STOC), Baltimore, MD, USA, pp. 84–93. ACM, New York (2005). https://doi.org/10.1145/1060590.1060603

[3] Peikert, C.: A decade of lattice cryptography. Found. Trends Theor. Comput. Sci. **10**(4), 283–424 (2016). https://doi.org/10.1561/0400000074

[4] Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., Kelsey, J., Lichtinger, J., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., Smith-Tone, D., (NIST), Y.-K.L.: Status report on the third

round of the nist post-quantum cryptography standardization process. US Department of Commerce, NIST (2022)

[5] Fritzmann, T., Pöppelmann, T., Sepúlveda, J.: Analysis of error-correcting codes for lattice-based key exchange. In: Selected Areas in Cryptography - SAC 2018 - 25th International Conference, Calgary, AB, Canada. Lecture Notes in Computer Science, vol. 11349, pp. 369–390. Springer, Heidelberg (2018). https://doi.org/10.1007/978-3-030-10970-7_17

[6] D'Anvers, J., Vercauteren, F., Verbauwhede, I.: On the impact of decryption failures on the security of LWE/LWR based schemes. IACR Cryptol. ePrint Arch. (2018)

[7] Naehrig, M., Alkim, E., Bos, J., Ducas, L., Easterbrook, K., LaMacchia, B., Longa, P., Mironov, I., Nikolaenko, V., Peikert, C., et al.: Frodokem. Technical report, National Institute of Standards and Technology (2017)

[8] Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P.: Newhope without reconciliation. IACR Cryptol. ePrint Arch. (2016)

[9] van Poppelen, A.: Cryptographic decoding of the Leech lattice. IACR Cryptol. ePrint Arch. (2016)

[10] Saliba, C., Luzzi, L., Ling, C.: Error correction for FrodoKEM using the Gosset lattice. In: International Zurich Seminar on Information and Communication (IZS 2022), Zurich, Switzerland. ETH, Zurich (2022). https://doi.org/10.3929/ethz-b-000535279

[11] Ding, J.: A simple provably secure key exchange scheme based on the learning with errors problem. IACR Cryptol. ePrint Arch. (2012)

[12] Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P.: Post-quantum key exchange - A new hope. In: Holz, T., Savage, S. (eds.) 25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, pp. 327–343. USENIX Association, Berkeley, California (2016)

[13] Jin, Z., Shen, S., Zhao, Y.: Compact and flexible KEM from ideal lattice. IEEE Trans. Inf. Theory **68**(6), 3829–3840 (2022). https://doi.org/10.1109/TIT.2022.3148586

[14] Kawachi, A., Tanaka, K., Xagawa, K.: Multi-bit cryptosystems based on lattice problems. In: Okamoto, T., Wang, X. (eds.) Public Key Cryptography - PKC 2007, 10th International Conference on Practice and Theory in Public-Key Cryptography, Beijing, China. Lecture Notes in Computer Science, vol. 4450, pp. 315–329. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-71677-8_21

[15] Lu, X., Liu, Y., Zhang, Z., Jia, D., Xue, H., He, J., Li, B.: LAC: practical ring-lwe based public-key encryption with byte-level modulus. IACR Cryptol. ePrint Arch. (2018)

[16] Saarinen, M.O.: HILA5: on reliability, reconciliation, and error correction for ring-lwe encryption. In: Adams, C., Camenisch, J. (eds.) Selected Areas in Cryptography - SAC 2017 - 24th International Conference, Ottawa, ON, Canada. Lecture Notes in Computer Science, vol. 10719, pp. 192–212. Springer, Heidelberg (2017). https://doi.org/10.1007/978-3-319-72565-9_10

[17] Wang, J., Ling, C.: How to construct polar codes for ring-LWE-based public key encryption. Entropy **23**(8), 938 (2021). https://doi.org/10.3390/e23080938

[18] D'Anvers, J., Tiepelt, M., Vercauteren, F., Verbauwhede, I.: Timing attacks on error correcting codes in post-quantum schemes. In: Bilgin, B., Petkova-Nikova, S., Rijmen, V. (eds.) Proceedings of ACM Workshop on Theory of Implementation Security, CCS 2019, London, UK, pp. 2–9. ACM, New York (2019). https://doi.org/10.1145/3338467.3358948

[19] Ungerboeck, G.: Channel coding with multilevel/phase signals. IEEE Trans. Inf. Theory **28**(1), 55–66 (1982). https://doi.org/10.1109/TIT.1982.1056454

[20] Forney, G.D.: Coset codes-I: Introduction and geometrical classification. IEEE Trans. Inf. Theory **34**(5), 1123–1151 (1988). https://doi.org/10.1109/18.21245

[21] Forney, G.D.: Coset codes-II: Binary lattices and related codes. IEEE Trans. Inf. Theory **34**(5), 1152–1187 (1988). https://doi.org/10.1109/18.21246

[22] Erez, U., Zamir, R.: Achieving 1/2 log (1+SNR) on the AWGN channel with lattice encoding and decoding. IEEE Trans. Inf. Theory **50**(10), 2293–2314 (2004). https://doi.org/10.1109/TIT.2004.834787

[23] Liu, L., Yan, Y., Ling, C., Wu, X.: Construction of capacity-achieving lattice codes: Polar lattices. IEEE Trans. Commun. **67**(2), 915–928 (2019). https://doi.org/10.1109/TCOMM.2018.2876113

[24] Silva, P.R.B., Silva, D.: Multilevel LDPC lattices with efficient encoding and decoding and a generalization of Construction D. IEEE Trans. Inf. Theory **65**(5), 3246–3260 (2019). https://doi.org/10.1109/TIT.2018.2883119

[25] Zamir, R.: Lattice Coding for Signals and Networks. Cambridge University Press, Cambridge, UK (2014)

[26] Viazovska, M.S.: The sphere packing problem in dimension 8. Annals of Mathematics, 991–1015 (2017). https://doi.org/10.4007/annals.2017.185.3.7

[27] Cohn, H., Kumar, A., Miller, S., Radchenko, D., Viazovska, M.: The sphere packing problem in dimension 24. Annals of Mathematics **185**(3), 1017–1033 (2017). https://doi.org/10.4007/annals.2017.185.3.8

[28] Bos, J.W., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Seiler, G., Stehlé, D.: CRYSTALS - Kyber: A CCA-secure module-lattice-based KEM. In: 2018 IEEE European Symposium on Security and Privacy, EuroS&P 2018, London, United Kingdom, pp. 353–367. IEEE, New York (2018). https://doi.org/10.1109/EuroSP.2018.00032

[29] BSI—Technical Guideline: Cryptographic mechanisms: Recommendations and key lengths. BSI TR-02102-1 (2021)

[30] Salomon, A.J., Amrani, O.: Augmented product codes and lattices: Reed-Muller codes and Barnes-Wall lattices. IEEE Trans. Inf. Theory **51**(11), 3918–3930 (2005). https://doi.org/10.1109/TIT.2005.856937

[31] Salomon, A.J., Amrani, O.: Reed-Muller codes and Barnes-Wall lattices: Generalized multilevel constructions and representation over GF(2^q). Des. Codes Cryptogr. **42**(2), 167–180 (2007). https://doi.org/10.1007/s10623-006-9028-3

[32] Liu, L., Shi, J., Ling, C.: Polar lattices for lossy compression. IEEE Trans. Inf. Theory **67**(9), 6140–6163 (2021). https://doi.org/10.1109/TIT.2021.3097965

[33] Conway, J.H., Sloane, N.J.A.: Sphere Packings, Lattices and Groups, 3rd edn. Springer, New York (1999). https://doi.org/10.1007/978-1-4757-6568-7

[34] Grigorescu, E., Peikert, C.: List-decoding Barnes-Wall lattices. Comput. Complex. **26**(2), 365–392 (2017). https://doi.org/10.1007/s00037-016-0151-x

[35] Arikan, E.: Channel polarization: a method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. IEEE Trans. Inf. Theory **55**(7), 3051–3073 (2009). https://doi.org/10.1109/TIT.2009.2021379

[36] Hanrot, G., Pujol, X., Stehlé, D.: Algorithms for the shortest and closest lattice vector problems. In: Chee, Y.M., Guo, Z., Ling, S., Shao, F., Tang, Y., Wang, H., Xing, C. (eds.) Coding and Cryptology - Third International Workshop, IWCC 2011, Qingdao, China. Lecture Notes in Computer Science, vol. 6639, pp. 159–190. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-20901-7_10

[37] Voulgaris, P.: Algorithms for the closest and shortest vector problems on general lattices. PhD thesis, University of California, San Diego, USA (2011). http://www.escholarship.org/uc/item/4zt7x45z

[38] Micciancio, D., Nicolosi, A.: Efficient bounded distance decoders for Barnes-Wall lattices. In: Kschischang, F.R., Yang, E. (eds.) 2008 IEEE International Symposium on Information Theory, ISIT 2008, Toronto, ON, Canada, pp. 2484–2488. IEEE, New York (2008). https://doi.org/10.1109/ISIT.2008.4595438

[39] Conway, J.H., Sloane, N.J.A.: Fast quantizing and decoding and algorithms for lattice quantizers and codes. IEEE Trans. Inf. Theory **28**(2), 227–231 (1982). https://doi.org/10.1109/TIT.1982.1056484

[40] Prest, T.: Sharper bounds in lattice-based cryptography using the Rényi divergence. In: Takagi, T., Peyrin, T. (eds.) Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China. Lecture Notes in Computer Science, vol. 10624, pp. 347–374. Springer, Heidelberg (2017). https://doi.org/10.1007/978-3-319-70694-8_13

[41] Cover, T.M.: Elements of Information Theory. John Wiley & Sons, Hoboken, New Jersey (1999)

[42] Boutros, J., Viterbo, E., Rastello, C., Belfiore, J.: Good lattice constellations for both Rayleigh fading and Gaussian channels. IEEE Trans. Inf. Theory **42**(2), 502–518 (1996). https://doi.org/10.1109/18.485720

[43] Classical, Quantum, and Plausible (conservative) Quantum Cost Estimates. https://github.com/lwe-frodo/parameter-selection/blob/master/pqsec.py

[44] Thakor, V.A., Razzaque, M.A., Khandaker, M.R.A.: Lightweight cryptography algorithms for resource-constrained iot devices: A review, comparison and research opportunities. IEEE Access **9**, 28177–28193 (2021). https://doi.org/10.1109/ACCESS.2021.3052867

[45] Fujisaki, E., Okamoto, T.: Secure integration of asymmetric and symmetric encryption schemes. In: Wiener, M.J. (ed.) Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa

Barbara, California, USA, August 15-19, 1999, Proceedings. Lecture Notes in Computer Science, vol. 1666, pp. 537–554. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48405-1_34

[46] Hofheinz, D., Hövelmanns, K., Kiltz, E.: A modular analysis of the fujisaki-okamoto transformation. In: Kalai, Y., Reyzin, L. (eds.) Theory of Cryptography - 15th International Conference, TCC 2017, Baltimore, MD, USA, November 12-15, 2017, Proceedings, Part I. Lecture Notes in Computer Science, vol. 10677, pp. 341–371. Springer, Heidelberg (2017). https://doi.org/10.1007/978-3-319-70500-2_12

[47] Annex on FrodoKEM Updates, April 18, 2023 Version (PDF). https://frodokem.org/files/FrodoKEM-annex-20230418.pdf