

Lattice Codes for Lattice-Based PKE

Shanxiang Lyu^{1*}, Ling Liu², Cong Ling³, Junzuo Lai¹
and Hao Chen¹

^{1*}College of Cyber Security, Jinan University, Guangzhou,
510632, China.

²College of Computer Science and Software Engineering,
Shenzhen University, Shenzhen, 518060, China.

³Department 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 naive modulation or its concatenation with error correction codes (ECC). This paper shows that lattice coding, as a joint ECC and modulation technique, can substitute the naive modulation in existing lattice-based PKEs to enjoy better correction performance. We begin by modeling the FrodoPKE protocol as a noisy point-to-point communication system, where the communication channel is similar to the additive white Gaussian noise (AWGN) channel. To employ lattice codes for this special channel that hinges on hypercube shaping, we propose an efficient labeling function that converts between binary information bits and lattice codewords. The parameter sets of FrodoPKE are improved towards either higher security levels or smaller ciphertext sizes. For example, the proposed Frodo-1344-E₈ has a 10-bit classical security gain 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 great challenge for modern public key cryptosystems. As Shor's quantum algorithm [1] can solve the prime factorization and discrete logarithm problems in polynomial time, conventional public-key cryptosystems based on these problems are no longer secure. Although making a prophesy for when we can build a large quantum computer is hard, we should start preparing the next generation quantum-safe cryptosystem as soon as possible, because historical experiences show that deploying modern public key cryptography infrastructures takes a long time.

Reacting to this urgency, the subject of post-quantum cryptography (PQC) has been systematically developed in the last decade [2, 3]. PQC aims to design cryptosystems secure against quantum attacks, while being able to run on a classic computer. From 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. The process revolves around public key encryption/key encapsulation mechanism (PKE/KEM) and digital signature proposals.

Recently NIST has announced four post-quantum cryptography standardization candidates [4]: CRYSTALS-Kyber for PKE/KEM, CRYSTALS-Dilithium, FALCON and SPHINCS+ for digital signatures. As the first three candidates are all based on lattices, it's a great victory of lattice-based cryptography (LBC), which enjoys the following prominent advantages. First, LBC enjoys very strong security proofs based on the hardness of worst-case problems. Second, LBC implementations are notable for their efficiency compared to other post quantum constructions, primarily due to their inherent linear algebra based matrix or vector operations on integers. Finally, LBC constructions offer extended functionality for advanced constructions such as identity-based encryption and fully-homomorphic encryption (FHE).

In lattice-based PKE/KEM, the decrypted messages may not be 100% correct. As the encryption-decryption process amounts to the transmission of messages through an additive noise channel, error correction techniques have been either implicitly or explicitly employed to reduce the decryption failure rate (DFR). Moreover, since the adversary may extract the secrets by taking advantages of high DFRs, the DFR of a PKE/KEM scheme has to be extremely small (e.g., smaller than 2^{-128} or 2^{-140}) [5, 6]. It is therefore worthwhile to improve the error correction mechanism in lattice-based PKE/KEM, with the hope of obtaining better trade-off parameters:

- **Security Strength:** If the error correction mechanism can increase the noise variance while maintaining a small DFR, then the PKE/KEM scheme has a higher security level.
- **Communication Bandwidth:** If the error correction mechanism can reduce the modulus while maintaining a small DFR, then the size of the ciphertext is reduced.

1.1 Related Works

KEMs can simultaneously output a session key together 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, see, e.g., [7–10]) and key exchanges (KEMs with reconciliation, see, e.g., [11–13]). As avoiding the error-reconciliation mechanism brings great simplicity, we focus on PKEs in this work.

Most lattice-based PKEs have implicitly employed an error correction mechanism which is referred to as “naive modulation”. It represents a mapping from a binary string to different positions in $\{0, 1, \dots, q - 1\}$. If the noise amplitude is smaller than the error correction radius, then the decryption is correct. Thus a larger q enables higher error correction capability. Specifically, Regev’s learning with errors (LWE) based PKE scheme [2] modulates 1-bit information $\{0, 1\}$ to $\{0, q/2\}$. Kawachi et. al. [14] extends the PKE scheme to multi-bit modulation.

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).

More importantly, using ECC and modulation in a concatenated manner confines the overall performance of the system, whose deficiencies include less flexible number of encoded bits, and the independent decoding nature of modulation and ECC. Fortunately, the joint design of ECC and modulation (referred to as “coded modulation”) has been studied in information theory and wireless communications for a few decades. Ungerboeck’s pioneering work [19] in the 1980s showed that coded modulation exhibits significant performance gains. Then, Forney [20, 21] systematically studied coded modulation schemes from coset codes/lattice codes. A breakthrough in information theory is that Erez and Zamir [22] show high dimensional random lattice codes can achieve the capacity of additive white Gaussian noise (AWGN) channels. Recent years have also witnessed the use of Polar lattices [23] and LDPC lattices [24] in achieving the capacity of AWGN channels. In the language of coset codes, lattice codes represent an *elegant combination* of linear codes and modulation: if points in the constellation are closed, they are protected by ECC; if points are far away, the information bits are directly mapped to them.

It is noteworthy that deploying lattice codes in lattice-based PKE is not straightforward, because previous lattice coding literature [25] was considering

lattice codes for the physical layer (the transmission power of the codes matters), while the modulo q arithmetic in LBC represents a higher layer. In the past few years, there have been some works that employ lattice codes in PKEs. In 2016 van Poppel designed a Leech lattice based PKE [9], while Saliba et. al. [10] designed an E_8 -lattice-based PKE in 2021. The use of E_8 and Leech parallels the celebrated breakthrough in mathematics in recent years: proving the E_8 and Leech lattices offer the best sphere packing density in dimensions 8 and 24 [26, 27]. Unfortunately, the labeling technique is missing in the Leech lattice based PKE [9], while the labeling technique for E_8 in [10] is nonlinear. In this regard, a general lattice-code based error correction formulation, along with efficient linear labeling, is needed for lattice-based PKEs.

1.2 Contributions

This paper contributes in the following ways, suggesting the naive modulation in lattice based PKE should be replaced with coded modulation.

- We consider the plain-LWE scheme Frodo [7] and model it as a communication system, over which the communication channel is akin to the AWGN channel. We show that the error correction performance can be easily improved by replacing the naive modulation with lattice-based coded modulation. In a similar vein, the ring-based or module-based schemes such as NewHope-Simple [8] and Kyber [28], can also resort to lattice-based coded modulation.
- We present a universal and efficient labeling technique for cubic-shaping based lattice codes. Due to the modulo q arithmetic, lattice codes in LBC have to use hypercube shaping, which means the coarse lattice should be a simple integer lattice $q\mathbb{Z}^n$. Although the number of lattice codewords can be easily identified in hypercube shaping, there seems to be no efficient labeling function available in the literature. In response, we propose a labeling function to establish a one-to-one map between the binary information bits and the set of lattice vectors. For a fine lattice whose Hermite parameter is large, we first rewrite its lattice basis to a rectangular form (the product of a unimodular matrix and a diagonal matrix). The proposed labeling is feasible for a wide range of lattices, such as D_4 , E_8 , BW_{16} , Λ_{24} , etc.
- A unified DFR formula over AWGN channels is derived to analyze the DFR of lattice-code based FrodoPKE. Only the Hermite parameter and the kissing number of lattices are needed in the DFR formula. Previously the DFRs were calculated by a computationally intensive case-by-case analysis. Via the DFR formula, better parameter sets for FrodoPKE are derived, where the E_8 or BW_{16} based implementations are particularly attractive: their encoding and decoding procedures are simple, and the modified PKE enjoys either higher security levels or smaller ciphertext sizes.

The rest of this paper is organized as follows. Background about lattice codes and PKE are reviewed in Section II. The proposed labeling is introduced and analyzed in Section III. Section IV presents a coset-based lattice decoding

formulation, along with the pseudocode of decoding BW_{16} . Section V presents the improved parameter sets for FrodoPKE. The last section concludes this paper.

2 Preliminaries

2.1 Lattice Codes and Hypercube Shaping

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

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

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 (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 nearest neighbor quantizer $Q_\Lambda(\cdot)$ denotes a function that solves CVP, i.e.,

$$Q_\Lambda(\mathbf{t}) = \arg \min_{\mathbf{v} \in \Lambda} \|\mathbf{t} - \mathbf{v}\|. \quad (2)$$

In case of a tie, (2) outputs the candidate with the smallest Euclidean norm.

Definition 3 (Fundamental region). A fundamental region \mathcal{R}_Λ of a lattice Λ includes one and only one point of Λ , and when shifting it to any lattice point, the whole \mathbb{R}^n space is tiled.

The Voronoi region \mathcal{V}_Λ is a special case of the fundamental region \mathcal{R}_Λ . It denotes the set of points in \mathbb{R}^n that are closer to the origin than any other lattice points in Λ , i.e.,

$$\mathcal{V}_\Lambda = \{\mathbf{y} \in \mathbb{R}^n \mid \|\mathbf{y}\| \leq \|\mathbf{y} - \mathbf{w}\|, \forall \mathbf{w} \in \Lambda\}. \quad (3)$$

Definition 4 (Modulo lattice). $[\mathbf{x}] \bmod \Lambda$ denotes the quantization error of \mathbf{x} with respect to Λ :

$$[\mathbf{x}] \bmod \Lambda = \mathbf{x} - Q_\Lambda(\mathbf{x}). \quad (4)$$

Definition 5 (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,

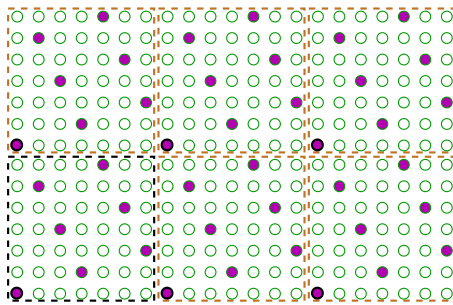


Fig. 1: Demonstration of the lattice code $\mathcal{C}(\Lambda_f, 7\mathbb{Z}^2) = \{(0, 0), (1, 5), (2, 3), (3, 1), (4, 6), (5, 4), (6, 2)\}$ cut from hypercube shaping.

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 6 (Lattice code). A lattice code $\mathcal{C}(\Lambda_f, \Lambda_c)$ is the finite set of points in Λ_f that lie within \mathcal{R}_{Λ_c} :

$$\mathcal{C}(\Lambda_f, \Lambda_c) = \Lambda_f \cap \mathcal{R}_{\Lambda_c}. \quad (5)$$

If $\Lambda_c = p\mathbb{Z}^n$, then (5) is called *hypercube shaping*. A 2-dimensional example is shown in Fig. 1. The purple points denote Λ_f , and those points enclosed with black circles denote Λ_c . The nesting relation is $\Lambda_c = 7\mathbb{Z}^2 \subset \Lambda_f \subset \mathbb{Z}^2$. The fundamental region \mathcal{R}_{Λ_c} in the example, enclosed by dashed black lines, is the shifted version of \mathcal{V}_{Λ_c} , i.e., $\mathcal{R}_{\Lambda_c} = \mathcal{V}_{\Lambda_c} + (3, 3)$.

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

$$B = \frac{1}{n} \log_2 \left(\frac{\text{Vol}(\Lambda_c)}{\text{Vol}(\Lambda_f)} \right). \quad (6)$$

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

$$\gamma(\Lambda) = \lambda_1(\Lambda)^2 / \text{Vol}(\Lambda)^{2/n} \quad (7)$$

where $\lambda_1(\Lambda)$ denotes the length of a shortest non-zero vector in Λ , and $\text{Vol}(\Lambda) = |\det(\mathbf{B})|$ 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 $\lambda_1(\Lambda)^2 / \text{Vol}(\Lambda)^{2/n}$ over all n -dimensional lattices is known as Hermite's constant.

2.2 PKE/KEM in LBC

FrodoKEM [7] is a simple and conservative KEM from generic lattices, and it is one of two post-quantum algorithms recommended by the German Federal Office for Information Security (BSI) as cryptographically suitable for

long-term confidentiality [29]. The core of FrodoKEM is a public-key encryption scheme called FrodoPKE, whose IND-CPA security is tightly related to the hardness of a corresponding learning with errors problem. Due to the lack of algebraic structure, the security estimates of FrodoPKE rely on fewer assumptions than other PKE/KEM schemes based on ring or module LWE.

A public key encryption scheme PKE is a tuple of algorithms (KeyGen, Enc, Dec) along with a message space \mathcal{M} .

In the key generation algorithm, by sampling $\mathbf{S}, \mathbf{E} \sim \chi_{\sigma}^{n' \times \bar{n}}$, with χ_{σ} being a (truncated) discrete Gaussian distribution with width σ , and sampling \mathbf{A} from a uniform distribution in $\mathbb{Z}_q^{n' \times n'}$, it computes

$$\mathbf{B} = \mathbf{A}\mathbf{S} + \mathbf{E} \in \mathbb{Z}_q^{n' \times \bar{n}}. \quad (8)$$

The public key is $pk = (\mathbf{B}, \mathbf{A})$, and the secret key is $sk = \mathbf{S}$.

In the part of public key encryption, it samples $\mathbf{S}', \mathbf{E}' \sim \chi_{\sigma}^{\bar{m} \times n'}$, $\mathbf{E}'' \sim \chi_{\sigma}^{\bar{m} \times \bar{n}}$, and computes

$$\mathbf{C}_1 = \mathbf{S}'\mathbf{A} + \mathbf{E}' \quad (9)$$

$$\mathbf{V} = \mathbf{S}'\mathbf{B} + \mathbf{E}'' \quad (10)$$

To encrypt a message $\mu \in \mathcal{M} = \{0, 1\}^{\bar{m}\bar{n}B}$, the ciphertext is generated by

$$c = (\mathbf{C}_1, \mathbf{C}_2 = \mathbf{V} + \text{Frodo.EncodeM}(\mu)). \quad (11)$$

The function `Frodo.EncodeM` represents a matrix encoding function of bit strings. In an element-wise manner, each B -bit value is transformed into the B most significant bits of the corresponding entry modulo q . We refer to `Frodo.EncodeM` as “naive modulation”, as it amounts to a special case of the lattice code based encoding that employs hypercube shaping, with $\Lambda_f = q/(2^B)\mathbb{Z}^{64}$, $\Lambda_c = q\mathbb{Z}^{64}$.

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

$$\hat{\mu} = \text{Frodo.DecodeM}(\mathbf{C}_2 - \mathbf{C}_1\mathbf{S}), \quad (12)$$

where `Frodo.DecodeM` stands 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 (matching or exceeding the brute-force security of AES-128, AES-192, AES-256), the recommended parameters are

$$\text{Frodo-640} : n' = 640, \bar{n} = 8, \bar{m} = 8, q = 2^{15}, \sigma = 2.75, \mathcal{M} = \{0, 1\}^{128}$$

$$\text{Frodo-976} : n' = 976, \bar{n} = 8, \bar{m} = 8, q = 2^{16}, \sigma = 2.3, \mathcal{M} = \{0, 1\}^{192}$$

$$\text{Frodo-1344} : n' = 1344, \bar{n} = 8, \bar{m} = 8, q = 2^{16}, \sigma = 1.4, \mathcal{M} = \{0, 1\}^{256}.$$

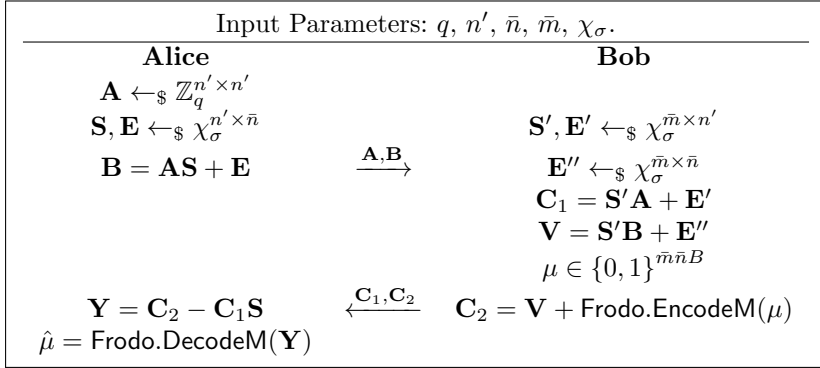


Fig. 2: The FrodoPKE protocol.

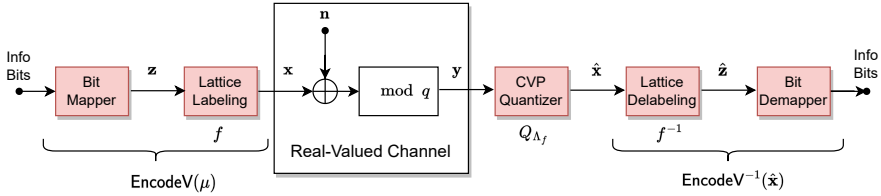


Fig. 3: The equivalent communication system model.

3 The Proposed Scheme

3.1 Equivalent Communication Model

Recall that the decryption algorithm of FrodoPKE computes

$$\begin{aligned} \mathbf{Y} &= \mathbf{C}_2 - \mathbf{C}_1\mathbf{S} \\ &= \text{Frodo.EncodeM}(\mu) + \mathbf{S}'\mathbf{E} + \mathbf{E}'' - \mathbf{E}'\mathbf{S}, \end{aligned} \quad (13)$$

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. (13) can be formulated as

$$\mathbf{y} = \mathbf{x} + \mathbf{n} \pmod{q}, \quad (14)$$

where $\mathbf{x} = \text{EncodeV}(\mu) \in \mathbb{R}^{\bar{m}\bar{n}}$ 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 modulo a lattice $q\mathbb{Z}^{\bar{m}\bar{n}}$, 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. The later 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 Quantizer*: 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.

While the conventional Frodo.EncodeM employs $\Lambda_f = q/(2^B)\mathbb{Z}^{\bar{m}\bar{n}}$ that leads to simple labeling functions and CVP quantization, our work seeks to employ a better Λ_f for error correction performance. Thus the associated labeling function and CVP quantization are more involved.

3.2 Lattice Labeling and Delabeling

This section will show that for any fine lattice with a basis in a rectangular form, a linear labeling from certain index sets to lattice codewords can be generically defined.

Definition 7 (Rectangular Form). A lattice basis \mathbf{B} is in a rectangular form if

$$\mathbf{B} = \mathbf{U} \cdot \text{diag}(\pi_1, \pi_2, \dots, \pi_n), \quad (15)$$

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

For any lattice with a rational basis, it has a rectangular form. Specifically, consider the Smith Normal Form factorization of a lattice basis $\mathbf{B}^* \in \mathbb{Q}^{n \times n}$, then we have

$$\mathbf{B}^* = \mathbf{U} \cdot \text{diag}(\pi_1, \pi_2, \dots, \pi_n) \cdot \mathbf{U}', \quad (16)$$

where $\mathbf{U}, \mathbf{U}' \in \text{GL}_n(\mathbb{Z})$ ¹. As lattice bases are equivalent up to unimodular transforms, the term \mathbf{U}' can be canceled out, and the rectangular form is derived.

For a lattice that features a rectangular form, an efficient labeling scheme can be constructed. The idea is that the combination of rectangular form and non-uniform labeling amounts to hypercube shaping. Specifically, let the fine lattice be

$$\Lambda_f = \mathcal{L}(\mathbf{B}_f) = \mathcal{L}(\mathbf{U} \cdot \text{diag}(\pi_1, \pi_2, \dots, \pi_n)). \quad (17)$$

Let $p \in \mathbb{Z}^+$ be a common multiplier of $\pi_1, \pi_2, \dots, \pi_n$, and define

$$p_1 = p/\pi_1, p_2 = p/\pi_2, \dots, p_n = p/\pi_n. \quad (18)$$

If $\mathbf{B}_c = \mathbf{B}_f \text{diag}(p_1, p_2, \dots, p_n)$, we have

$$\Lambda_c = \mathcal{L}(\mathbf{U} \cdot \text{diag}(\pi_1, \pi_2, \dots, \pi_n) \cdot \text{diag}(p_1, p_2, \dots, p_n))$$

¹The determinants of \mathbf{U} and \mathbf{U}' are 1 or -1 by incorporating the necessarily rational factors into $\text{diag}(\pi_1, \pi_2, \dots, \pi_n)$.

$$\begin{aligned}
&= \mathcal{L}(p\mathbf{U}) \\
&= p\mathbb{Z}^n.
\end{aligned} \tag{19}$$

The last equality is due to the fact that a unimodular matrix can be regarded as a lattice basis of \mathbb{Z}^n . Hence modulo Λ_c becomes equivalent to modulo p . Then we arrive at the following theorem.

Theorem 8 (Labeling Function). *Let the message space be*

$$\mathcal{I} = \{0, 1, \dots, p_1 - 1\} \times \dots \times \{0, 1, \dots, p_n - 1\}, \tag{20}$$

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

$$f(\mathbf{z}) = [\mathbf{B}_f \mathbf{z}] \pmod{p} \tag{21}$$

is bijective.

Proof It suffices to prove that f is both injective and surjective. ‘‘Injective’’ means no two elements in the domain of the function gets mapped to the same image, i.e., for $\mathbf{z}_1, \mathbf{z}_2 \in \mathcal{I}$,

$$\mathbf{z}_1 \neq \mathbf{z}_2 \rightarrow f(\mathbf{z}_1) \neq f(\mathbf{z}_2). \tag{22}$$

We prove this by contradiction, showing $\mathbf{z}_1 \neq \mathbf{z}_2 \rightarrow f(\mathbf{z}_1) = f(\mathbf{z}_2)$ does not hold. If $f(\mathbf{z}_1) = f(\mathbf{z}_2)$, it implies that we can find $\mathbf{z}_1, \mathbf{z}_2 \in \mathcal{I}$, $\mathbf{z}_3 \in \mathbb{Z}^n$ such that

$$\begin{aligned}
\mathbf{B}_f(\mathbf{z}_1 - \mathbf{z}_2) &= \mathbf{B}_f \cdot \text{diag}(p_1, p_2, \dots, p_n) \cdot \mathbf{z}_3 \\
\rightarrow \mathbf{z}_1 - \mathbf{z}_2 &= \text{diag}(p_1, p_2, \dots, p_n) \cdot \mathbf{z}_3.
\end{aligned} \tag{23}$$

Then (23) has a solution only when $\mathbf{z}_3 = \mathbf{0}$, which leads to $\mathbf{z}_1 = \mathbf{z}_2$.

‘‘Surjective’’ means that any element in the range of the function is hit by the function. Recall that the number of coset representatives of Λ_f/Λ_c is

$$|\det(\mathbf{B}_c)| / |\det(\mathbf{B}_f)| = p_1 p_2 \dots p_n. \tag{24}$$

As $|\mathcal{I}| = p_1 p_2 \dots p_n$, it follows from the injective property that all the coset representatives have been hit distinctively. So the surjection is proved. \square

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

$$\mathbf{z} = f^{-1}(\mathbf{x}) \triangleq \mathbf{B}_f^{-1} \mathbf{x} \pmod{(p_1, \dots, p_n)}, \tag{25}$$

which stands for $z_i = \left(\mathbf{B}_f^{-1} \mathbf{x}\right)_i \pmod{p_i}$, $i = 1, \dots, n$. 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 9 (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

$$Q_{\Lambda_f}(\mathbf{x} + \mathbf{n}) = \mathbf{x} + Q_{\Lambda_f}(\mathbf{n}), \quad (26)$$

then we have

$$f^{-1}(Q_{\Lambda_f}(\mathbf{x} + \mathbf{n})) = \mathbf{B}_f^{-1}\mathbf{x} + \mathbf{B}_f^{-1}Q_{\Lambda_f}(\mathbf{n}) \pmod{(p_1, \dots, p_n)} \quad (27)$$

The condition of $Q_{\Lambda_f}(\mathbf{n}) \in \Lambda_c$ implies that this vector of the coarse lattice can be written as $\mathbf{B}_f \text{diag}(p_1, p_2, \dots, p_n)\mathbf{k}$ for a $\mathbf{k} \in \mathbb{Z}^n$. This yields $Q_{\Lambda_f}(\mathbf{n}) \pmod{(p_1, \dots, p_n)} = \mathbf{0}$ and the theorem is proved. \square

We summarize three cases for the correct recovery of messages. i) Noiseless: $\mathbf{n} = \mathbf{0}$. ii) Noise is small: $Q_{\Lambda_f}(\mathbf{n}) = \mathbf{0}$. iii) Noise is large but still in the coarse lattice: $Q_{\Lambda_f}(\mathbf{n}) \in \Lambda_c$.

An example of using labeling and delabeling is given below.

Example: Consider the D_4 lattice, whose lattice basis and its inverse are respectively given by

$$\mathbf{B}_{D_4} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} \cdot \text{diag}(1, 1, 1, 2), \quad (28)$$

$$\mathbf{B}_{D_4}^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -0.5 & -0.5 & -0.5 & 0.5 \end{bmatrix}. \quad (29)$$

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

$$\mathcal{I} = \{0, 1, 2, 3\}^3 \times \{0, 1\}. \quad (30)$$

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. (21), we have

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

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

$$f^{-1}(\mathbf{x}) = f^{-1}([1, 2, 3, 0]^\top) \quad (31)$$

$$= [1, 2, 3, -3]^\top \pmod{(4, 4, 4, 2)} \quad (32)$$

$$= [1, 2, 3, 1]^\top. \quad (33)$$

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

$$f^{-1}(Q_{\Lambda_f}(\mathbf{x} + \mathbf{n})) = f^{-1}([5, 6, 7, 4]^\top) \quad (34)$$

$$= [9, 10, 11, -7]^\top \pmod{(4, 4, 4, 2)} \quad (35)$$

$$= [1, 2, 3, 1]^\top. \quad (36)$$

Finally, the ‘‘Bit Demapper’’ transforms the information integers to bits, which equal to the original input.

3.3 Rectangular Forms of Code-Based Lattices

The proposed labeling is feasible for a wide range of lattices, such as low-dimensional optimal lattices D_2 , D_4 , E_8 , Λ_{24} , and the general Construction-A and Construction-D lattices. Construction A and Construction D are popular techniques of lifting linear codes to lattices, based on which many remarkable lattices with large coding gains have been constructed, 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 10 (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

$$\Lambda_A = \mathcal{L} \left(\begin{bmatrix} \phi(\mathbf{I}) & \mathbf{0} \\ \phi(\mathbf{A}) & 2\mathbf{I} \end{bmatrix} \right). \quad (37)$$

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

$$V(\Lambda_A) = 2^{n-k}. \quad (38)$$

Definition 11 (Construction D [33]). Let $C_0 \subset C_1 \subset \dots \subset C_a = \mathbb{F}_2^n$ 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, \dots, C_a) if and only if \mathbf{y} is congruent (modulo 2^a) to a vector in $C_0 + 2C_1 + \dots + 2^{a-1}C_{a-1}$.

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

$$\mathbf{G}_0 = \begin{bmatrix} | & | & \cdots & | \\ \mathbf{g}_1 & \mathbf{g}_2 & \cdots & \mathbf{g}_{k_0} \\ | & | & \cdots & | \end{bmatrix} \quad (39)$$

$$\mathbf{G}_i = \begin{bmatrix} | & | & & | & & | \\ \mathbf{g}_1 & \mathbf{g}_2 & \cdots & \mathbf{g}_{k_0} & \cdots & \mathbf{g}_{k_i} \\ | & | & & | & & | \end{bmatrix} \quad (40)$$

$$\mathbf{G}_a = \begin{bmatrix} | & | & & | & & | & & | \\ \mathbf{g}_1 & \mathbf{g}_2 & \cdots & \mathbf{g}_{k_0} & \cdots & \mathbf{g}_{k_i} & \cdots & \mathbf{g}_{k_a} \\ | & | & & | & & | & & | \end{bmatrix}, \quad (41)$$

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

$$\Lambda_D = \bigcup_{\mathbf{u}_i \in \{0,1\}^{k_i}} \left(\sum_{i=0}^{a-1} 2^i \phi(\mathbf{G}_i) \mathbf{u}_i \right) + 2^a \mathbb{Z}^n \quad (42)$$

$$= \mathcal{L}(\phi(\mathbf{G}_a) \cdot \text{diag}(2^0 \mathbf{1}_{k_0}, \dots, 2^a \mathbf{1}_{k_a - k_{a-1}})), \quad (43)$$

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

$$V(\Lambda_D) = 2^{an - \sum_{i=0}^{a-1} k_i}. \quad (44)$$

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

$$BW_8 = (8, 4, 4) + 2\mathbb{Z}^8 \cong E_8 \quad (45)$$

$$BW_{16} = (16, 5, 8) + 2(16, 15, 2) + 4\mathbb{Z}^{16} \cong \Lambda_{16} \quad (46)$$

$$BW_{32} = (32, 6, 16) + 2(36, 26, 4) + 4\mathbb{Z}^{32} \quad (47)$$

$$BW_{64} = (64, 7, 32) + 2(64, 42, 8) + 4(64, 63, 2) + 8\mathbb{Z}^{64}, \quad (48)$$

where \cong denotes equality up to rotations. The rectangular-form lattice basis in (43) can be derived by considering the Kronecker product based construction of Reed-Muller codes [35, Section I-D]. With explicit rectangular forms, the lattice bases of E_8 , BW_8 and BW_{16} are shown in Appendix A.

3.4 CVP Decoding

Enumeration and sieving are two popular types of CVP algorithms for decoding random lattices [36, 37]. For the code-based lattices used in error correction, they feature strong structures, thus algorithms should exploit the structures to improve the decoding efficiency. While there exist bounded distance decoding (BDD) for the considered Barnes–Wall lattices [34, 38], BDD fails to reach the DFR of CVP decoding. Exploiting the structure of cosets, efficient CVP algorithms of E_8 and D_n can be found in [39]. In a similar vein, this section examines the CVP decoding of BW_{16} , BW_{32} and BW_{64} .

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

3.4.1 Lattice Partition as Cosets

A natural and efficient way to design CVP algorithms for Construction-D lattices is to partition the lattice as the union of cosets. If Λ equals to the union of Λ' cosets, the CVP of Λ can resort to that of Λ' :

$$\begin{aligned} Q_{\Lambda}(\mathbf{t}) &= Q_{\Lambda'+\mathbf{g}'}(\mathbf{t}), \\ \mathbf{g}' &= \operatorname{argmin}_{\mathbf{g} \in \Lambda/\Lambda'} \|\mathbf{t} - Q_{\Lambda'+\mathbf{g}}(\mathbf{t})\|, \end{aligned} \quad (49)$$

where $Q_{\Lambda'+\mathbf{g}}(\mathbf{t}) = \mathbf{g} + Q_{\Lambda'}(\mathbf{t} - \mathbf{g})$. Denote the number of cosets as $|\Lambda/\Lambda'|$. Then the computational complexity of Q_{Λ} is $|\Lambda/\Lambda'|$ times larger than $Q_{\Lambda'}$.

All the Construction-D lattices admit a \mathbb{Z}^n based coset partition, but such partition has a huge number of cosets in general. Whenever possible, partitioning the lattice as D_n based cosets helps to decode faster. For example, the magic behind the CVP algorithm of E_8 [39] is to treat E_8 as two D_8 cosets while D_8 amounts to two \mathbb{Z}^8 cosets.

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:

$$BW_{16} = (16, 5, 8) + 2D_{16}, \quad (50)$$

$$BW_{64} = (64, 7, 32) + 2(64, 42, 8) + 4D_{64}. \quad (51)$$

Their number of cosets are $|BW_{16}/2D_{16}| = 2^5$, $|BW_{64}/4D_{64}| = 2^{49}$, contrary to $|BW_{16}/4\mathbb{Z}^{16}| = 2^{20}$, $|BW_{64}/8\mathbb{Z}^{64}| = 2^{112}$. In addition, $|BW_{32}/4\mathbb{Z}^{32}| = 2^{32}$.

Summarizing the above, the decoding complexity of BW_{16} seems more affordable than those of BW_{32} and BW_{64} . With reference to Eqs. (49) and (50), we have

$$\begin{aligned} Q_{BW_{16}}(\mathbf{t}) &= Q_{2D_{16}+\mathbf{g}'}(\mathbf{t}), \\ \mathbf{g}' &= \operatorname{argmin}_{\mathbf{g} \in (16,5,8)} \|\mathbf{t} - Q_{2D_{16}+\mathbf{g}}(\mathbf{t})\|. \end{aligned} \quad (52)$$

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

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 $\mathcal{N}(0, \sigma^2)$.

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} .

- 1: Define the codewords of $(16, 5, 8)$ as $\mathbf{d}_1, \dots, \mathbf{d}_{32}$
 - 2: **for** $t = 1, \dots, 32$ **do**
 - 3: $\mathbf{y}_t = (\mathbf{y} - \mathbf{d}_t)/2$
 - 4: $\hat{\mathbf{v}}_t = 2Q_{D_n}(\mathbf{y}_t) + \mathbf{d}_t$
 - 5: $\text{Dist}_t = \mathbf{y} - \hat{\mathbf{v}}_t$
 - 6: **end for**
 - 7: $t^* = \min_t \text{Dist}_t$
 - 8: $\hat{\mathbf{v}} = \hat{\mathbf{v}}_{t^*}$.
-

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 .

- 1: $\mathbf{u} = \lfloor \mathbf{y} \rfloor$
 - 2: $\delta = |\mathbf{y} - \mathbf{u}|$
 - 3: $t^* = \max_t |y_t - u_t|$
 - 4: $\mathbf{v} = \mathbf{u}$
 - 5: **if** $y_{t^*} - u_{t^*} > 0$ **then**
 - 6: $v_{t^*} \leftarrow v_{t^*} + 1$
 - 7: **else**
 - 8: $v_{t^*} \leftarrow v_{t^*} - 1$
 - 9: **end if**
 - 10: **if** $u_1 + \dots + u_n \pmod 2 = 0$ **then**
 - 11: $\hat{\mathbf{v}} = \mathbf{u}$
 - 12: **else**
 - 13: $\hat{\mathbf{v}} = \mathbf{v}$
 - 14: **end if**
-

Recall that Section 3.1 has formulated an $\bar{m}\bar{n}$ -dimensional modulo lattice additive noise channel “ $\mathbf{y} = \mathbf{x} + \mathbf{n} \pmod q$ ”. 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

$$\mathbb{E}(\mathbf{s}'\mathbf{e} + e'' - \mathbf{e}'\mathbf{s}) = 0 \quad (53)$$

$$\mathbb{E}\left(\|\mathbf{s}'\mathbf{e} + e'' - \mathbf{e}'\mathbf{s}\|^2\right) = 2n'\sigma^4 + \sigma^2. \quad (54)$$

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.

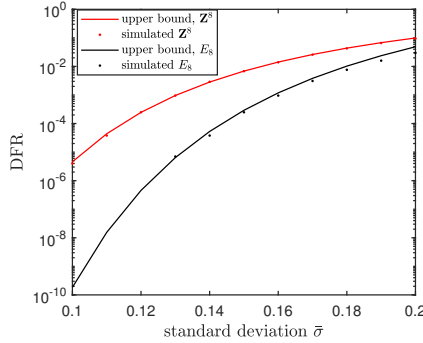


Fig. 4: The DFRs of naive modulation and E_8 based coded modulation.

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

$$\text{Vol}(\Lambda_f) = \frac{\text{Vol}(\Lambda_c)}{2^{nB}}. \quad (55)$$

Based on Theorem 9, the DFR can be evaluated as

$$P_e \triangleq \Pr(\hat{\mu} \neq \mu) = \Pr(Q_{\Lambda_f}(\mathbf{n}) \notin \Lambda_c) \leq \Pr(Q_{\Lambda_f}(\mathbf{n}) \neq \mathbf{0}). \quad (56)$$

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

$$\Pr(Q_{\Lambda_f}(\mathbf{n}) \neq \mathbf{0}) \lesssim \frac{\tau}{2} \text{erfc}\left(\frac{\lambda_1/2}{\sqrt{2}\bar{\sigma}}\right) \quad (57)$$

$$= \frac{\tau}{2} \text{erfc}\left(\frac{\sqrt{\gamma}q}{2^{B+3/2}\bar{\sigma}}\right), \quad (58)$$

where the second equality is obtained by substituting $\lambda_1 = \sqrt{\gamma}(q^n/2^{nB})^{1/n}$, which is based on the definition of Hermite parameter γ and $\text{Vol}(\Lambda_c) = q^n$. 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 (57) is tight.

The DFR formula is determined by a few factors: (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 that measure the number of facets in the Voronoi region of a lattice. (iii) The modulus q in

LBC. (iv) The averaged number of encoded bits B . (v) The standard deviation $\bar{\sigma}$ of the effective noise.

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 $r = 1, 2, 3, \dots$, the kissing number is

$$\tau = (2 + 2)(2 + 2^2) \cdots (2 + 2^r), \quad (59)$$

and the Hermite parameter is

$$\gamma_r = 2^{(r-1)/2}, \quad (60)$$

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

$$\tau(\Lambda') = k\tau(\Lambda) \quad (61)$$

$$\gamma_r(\Lambda') = \gamma_r(\Lambda). \quad (62)$$

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

Table 1: The properties of some popular lattices.

	\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 $\text{Vol}(\Lambda_t)$	1	2	1	2^{12}	1	2^{32}	2^{80}

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

$$\Lambda_f = 2^\Delta \Lambda_t \times \cdots \times \Lambda_t. \quad (63)$$

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

$$B = \frac{1}{n} \log_2 \left(\frac{\text{Vol}(\Lambda_c)}{\text{Vol}(\Lambda_f)} \right) = \frac{1}{t} \log_2 \frac{p^t}{\text{Vol}(\Lambda_t)}. \quad (64)$$

For a Construction-A or Construction-D lattice, one always has

$$p\mathbb{Z}^t \subset 2^a\mathbb{Z}^t \subset \Lambda_t. \quad (65)$$

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 $64B$.

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

4.3 Improved Frodo Parameters

Frodo-640, Frodo-976 and Frodo-1344 target security levels 1, 3 and 5 in the NIST PQC Standardization, respectively. To resist the attack exploiting DFRs [6], the DFRs at levels 1, 3 and 5 should be no larger than 2^{-128} , 2^{-192} and 2^{-256} , respectively.

Compared to the standard Frodo protocol, our scheme only modifies the labeling function, the corresponding CVP algorithm, and the choice of parameters σ, B, 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

We increase σ while keeping n', q unchanged in Frodo-640/976/1344. As shown in Table 2, error correction via E_8 , BW_{16} and BW_{32} can improve the security level of the original Frodo-640/976/1344 by 6 to 16 bits. While \mathbb{Z}^{64} , E_8^8 and BW_{32}^2 can naturally encode 128, 192 and 256 bits per instance, BW_{16}^4 only supports 144, 208, and 272 bits. The BW_{32} based parameter set offers the highest security enhancement in the table, but its CVP decoding complexity of $O(2^{32})$ makes it less attractive.

We recommend the E_8 and BW_{16} based parameter sets. The information rate of Frodo-640/976/1344- E_8 matches well with that of the original Frodo-640/976/1344, and the classical security level has been increased by 7 or 8 bits, respectively. Frodo-640/976/1344- BW_{16} maintains basically the same security level as that of Frodo-640/976/1344- E_8 , while the information rate is slightly higher, either $B = 2.25, 3.25$ or 4.25 .

Parameter set 2: Reduced size of ciphertext

Recall that the size of ciphertext is $(\bar{m}n' + \bar{m}\bar{n}) \log_2(q)/8$ bytes, so we reduce q to achieve higher bandwidth efficiency. To keep the DFR small, we also reduce σ to various degrees, as long as the security level is no smaller.

As shown in Table 3, by reducing q from 2^{15} to 2^{14} , the ciphertext size c can be reduced from 9720 bytes to 9072 bytes in Frodo-640, from 15744 bytes to 14760 bytes in Frodo-976, and from 21632 bytes to 20280 bytes in Frodo-1344. Again, the E_8 and BW_{16} based parameter sets are recommended.

It is interesting to note that the lattice-code based FrodoPKE can also be extended to a KEM for symmetric lightweight cryptography algorithms. For instance, via setting $\Lambda_f = 2^\Delta \cdot BW_{16}^4$, $\Lambda_c = 2^\Delta \cdot 4\mathbb{Z}^{64}$, it is possible to tightly exchange 80 bits for the PRESENT algorithm [44].

4.4 IND-CCA Security

The lattice codes based PKE/KEM also features chosen ciphertext secure (IND-CCA) security. Similarly to the argument in [7], the IND-CPA security of FrodoPKE is upper bounded by the advantage of the decision-LWE problem for the same parameters and error distribution. To endow an IND-CPA encryption scheme with IND-CCA security, the post-quantum secure version of the Fujisaki-Okamoto transform [45, 46] can be applied. When bounding the probability that an attacker can undermine a given cryptographic scheme in the quantum random-oracle model, security proofs use the number of decryption queries submitted by the CCA adversary. [47, Theorem 4.3] shows that the impact of decryption failure is given by $4q_G P_e$ where q_G is the number of quantum oracle queries and P_e is the DFR. Then, using bounds on decryption failure established above, one can argue that such queries pose no danger.

5 Conclusions

While the cryptography community is more familiar with random lattices for security, this paper shows that low-dimensional structure lattices can improve the error correction performance in FrodoPKE. The rationale is that lattice codes represent coded modulation, the elegant combination of ECC and modulation. The bridge that connects lattice codes and FrodoPKE (and more generally lattice-based PKEs) is the modulo q operation, which induces hypercube shaping. By presenting an efficient lattice labeling function, as well as a general formula to estimate the DFR, lattice based coded modulation becomes practical in LBC. By using some low-dimensional optimal lattices, a few improved parameter sets for FrodoPKE have been achieved, with either

Table 2: The recommended parameter sets with higher security.

	Structure of lattice code		n', \bar{n}, \bar{m}	q	σ	B	DFR	c size (bytes)	Security		
	Λ_f	Λ_c							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 size (bytes)	Security		
	Λ_f	Λ_c							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	2¹⁴	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	2¹⁴	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	2¹⁴	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	2¹⁵	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	2¹⁵	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	2¹⁵	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	2¹⁵	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	2¹⁵	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	2¹⁵	1.39	4	2^{-290}	20280	302	275	217

higher security or smaller ciphertext sizes. The lattice coding techniques in this work can be similarly applied to Ring/Module LWE-based PKEs.

Appendix A

The lattice bases of E_8 , BW_8 and BW_{16} can be respectively chosen as

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

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)
- [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)
- [3] Peikert, C.: A decade of lattice cryptography. *Found. Trends Theor. Comput. Sci.* **10**(4), 283–424 (2016)

- [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)
- [6] 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 Poppel, 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)
- [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)
- [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)

- [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)
- [17] Wang, J., Ling, C.: How to construct polar codes for ring-LWE-based public key encryption. *Entropy* **23**(8), 938 (2021)
- [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)
- [19] Ungerboeck, G.: Channel coding with multilevel/phase signals. *IEEE Trans. Inf. Theory* **28**(1), 55–66 (1982)
- [20] Jr., G.D.F.: 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)
- [22] Erez, U., Zamir, R.: Achieving $1/2 \log(1+\text{SNR})$ on the AWGN channel with lattice encoding and decoding. *IEEE Trans. Inf. Theory* **50**(10), 2293–2314 (2004)
- [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)
- [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)
- [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)
- [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)
- [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)
- [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 $\text{gf}(2^q)$. *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)
- [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., Nicosi, 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)
- [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)
- [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)
- [47] Annex on FrodoKEM Updates, April 18, 2023 Version (PDF). <https://>

frodokem.org/files/FrodoKEM-annex-20230418.pdf