IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 4 March 2025, accepted 2 April 2025, date of publication 11 April 2025, date of current version 22 April 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3560023

RESEARCH ARTICLE

Post-Quantum Wireless-Based Key Encapsulation Mechanism via CRYSTALS-Kyber for Resource-Constrained Devices

M. A. GONZÁLEZ DE LA TORRE[1], I. A. MORALES SANDOVAL[2], (Graduate Student Member, IEEE), G. T. FREITAS DE ABREU[2], (Senior Member, IEEE), AND L. HERNÁNDEZ ENCINAS[1]

[1]Institute of Physical and Information Technologies (ITEFI), Spanish National Research Council (CSIC), 28006 Madrid, Spain
[2]School of Computer Science and Engineering, Constructor University Bremen gGmbH, 28759 Bremen, Germany

Corresponding author: M. A. González de la Torre (ma.gonzalez@csic.es)

This work was supported in part by European Union (EU)-Japan European interest Group (EiG)-Concert Project Organically Resilient and Secure Wireless Networks for Next-Generation IoT Technologies to serve Future Connected Societies (ORACLE), Germany, under Grant 01DR21011; in part by EU-Japan EiG-Concert Project ORACLE, Spain, funded by MCIN/AEI/10.13039/501100011033 and EU "NextGenerationEU"/Plan de Recuperación, Transformación y Resiliencia (PRTR) under Grant PCI2020-120691-2; in part by Project P2QProMeTe funded by MCIN/AEI/10.13039/501100011033 under Grant PID2020-112586RBI00; and in part by Project Quantum-based Resistant Architectures and Techniques Integration QKD+PQC (QURSA) funded by MCIN/AEI/10.13039/501100011033 co-funded by EU "NextGenerationEU"/PRTR under Grant TED2021-130369B-C33.

ABSTRACT We consider the problem of adapting a Post-Quantum cryptosystem to be used in resource-constrained devices, such as those typically used in Device-to-Device and Internet of Things systems. In particular, we propose leveraging the characteristics of wireless communications channels to minimize the complexity of implementation of a Post-Quantum public key encryption scheme, without diminishing its security. To that end, we focus on the adaptation of a well-known cryptosystem, namely CRYSTALS-Kyber, so as to enable its direct integration into the lowest layer of the communication stack, the physical layer, defining two new transport schemes for CRYSTALS-Kyber to be used in Device-to-Device communications, both of which are modeled under a wireless channel subject to Additive White Gaussian Noise, using a 4 Quadrature Amplitude Modulation constellation and a BCH-code to communicate CRYSTALS-Kyber's polynomial coefficients. Simulation results demonstrate the viability of the adapted Kyber algorithm due to its low key error probability, while maintaining the security reductions of the original Kyber by considering the error distribution imposed by the channel on the cipher.

INDEX TERMS CRYSTALS-Kyber, physical layer security, post-quantum cryptography, wireless communications.

I. INTRODUCTION

Today's communication networks are characterized by an exponentially increasing number of wirelessly connected devices, which are expected to grow to up to 5 billion devices by the year 2025 [1], and which will be dominated by the deployment of Next-Generation (NG)-Internet of Things (IoT). A very important characteristic of this new development in wireless communications, is that the introduced devices will have a very diverse set of capabilities, ranging from computational, to power storage, to radio resources. This poses new challenges to security, authentication and data privacy, which need to be provided for these massive networks of heterogeneous devices [2], [3].

Concomitant with this trend, advances towards the widespread adoption of quantum computers are constantly being made [4], [5], [6], [7]. The use of Post-Quantum (PQ) Public Key Encryption (PKE) algorithms, and more generally post-quantum cryptography, is part of the strategy to build barriers against the threats of cryptanalytic attacks implemented on quantum computers [8]. In August 2024 the FIPS 203 was published by National Institute of Standards and Technology (NIST), establishing the first PQ Key Encapsulation Mechanism (KEM) standard, known as Module-Lattice-based Key Encapsulation Mechanism (ML-KEM) [9], which is based on the practically integral adaptation

The associate editor coordinating the review of this manuscript and approving it for publication was Fang Yang.

of CRYSTALS-Kyber [10], [11]. Kyber's status as standard and sets of parameters make it optimal, between the NIST lattice-based PQC KEM proposals, for our adaptation to the physical layer.

Despite the individual security guarantees provided by each individual component in a system, it is well-known [12], [13], [14] that their defenses can be compromised by targeting their weakest link. In the context of wireless networks, these typically are IoT devices with low power and computational capabilities which communicate in a Device-to-Device (D2D) fashion, which present strong challenge for the implementation of conventional PQ encryption schemes, due to their resource constraints and strong reliance on features from upper layers of communication [15]. In light of this, Physical Layer Security (PLS) is a technology that can help alleviating the computational requirements at upper layers of communications [16], [17], [18], [19].

In the context of this paper, PLS is referred to as the body of practical mechanisms which leverage the characteristics of wireless communications media to increase a system's security. This focus is distinct from the pioneering work of Wyner [20], where the concept of perfect information-theoretical secrecy is introduced. Instead, we address the integration of cryptography with features of PLS and propose, in particular, a mechanism to incorporate the well-known cryptographic Kyber KEM into a wireless communication system. Similar efforts to implement PQ security directly at the physical layer of communication systems have recently been published [21], [22]. However, these State-of-the-Art (SotA) approaches are not suitable for resource-constrained devices, as they require massive Multiple-Input Multiple-Output (MIMO) capabilities, and modulation schemes with large constellation sizes.

Kyber is a public key PQ algorithm, based on lattice problems that are currently considered hard, even against quantum attacks [23]. The design of Kyber constitutes a KEM, which is a public key algorithm specifically intended to perform key exchanges [24], and an underlying PKE that creates instances of the Modular Learning With Errors (MLWE) problem as both public keys and ciphertexts. Kyber encryption necessitates an error distribution to create instances of the MLWE problem. Consequently, a novel implementation of Kyber is proposed, incorporating an error by utilizing an Additive White Gaussian Noise (AWGN) channel and a 4 Quadrature Amplitude Modulation (4QAM) constellation [11].

The contributions of the article can be summarized as follows:

- A physical layer transport scheme for the polynomial coefficients of the CRYSTAL-Kyber cryptosystem is presented and modeled for a wireless channel subjected to AWGN, using a 4QAM constellation for symbol encoding and Bose-Chaudhuri-Hocquenghem (BCH) code for error correction.
- Two adaptations of Kyber to the defined physical layer transport scheme are introduced as Wireless Kyber (WKyber) V1 and V2. The first, WKyber V1, constitutes a PKE and a KEM, which reduces the reliance on the original scheme's Binomial Distribution Random Number Generator (RNG) which is used for error sampling. The second, WKyber V2, is a PKE scheme which further reduces the reliance on the aforementioned RNG reliance by eliminating its use in other parts of the cryptosystem. This is in contrast to the standard Kyber definition, which necessitates error-free information transport which usually can only be achieved by implementing the upper layers of a communication system.
- An analysis of the security of WKyber, in particular how the modifications affect the security of the original cryptosystem and how the security of WKyber can be estimated as a function of the parameters of the channel. This is achieved by considering the error distribution imposed by the transport scheme to the cipher's polynomial coefficients.

The remainder of this work is structured as follows. The main properties, characteristics and definitions of the original CRYSTALS-Kyber system are described in Section II. The physical layer transport scheme, channel model and encoding are described in Section III, together with the error probabilities for the transmitted polynomial coefficients. The proposal of the two versions of WKyber, along with the analysis of its security reductions, is presented in Section IV. This section also comprises an analysis and comparison of the proposed Kyber modification under different physical layer parameters. Additionally, the section provides an analysis of the implementation viability of the aforementioned modification. Finally, in Section V the conclusions are presented.

Notation: Column vectors and matrices are respectively denoted by lower- and upper-case bold face letters. The transpose operation is indicated by the superscript $^{\mathrm{T}}$. The operator $\leftarrow \mathcal{X}$ denotes sampling from a distribution $\mathcal{X}$, while, for any set C, $\leftarrow_R C$ denotes a uniformly random selection from C. The inner product between two vectors is denoted by $\langle \boldsymbol{x}, \boldsymbol{y} \rangle$. The $\lceil \cdot \rfloor$ operator denotes the rounding to the closest integer operation.

II. THE CRYSTALS-KYBER CRYPTOSYSTEM

CRYSTALS-Kyber is a latticed-based PQ cryptosystem proposed as the standard ML-KEM by NIST in the summer of 2024 [9]. Kyber consists of two algorithms 1) Kyber PKE, the Public Key Encryption algorithm, which provides the security, and 2) Kyber KEM, the Key Encapsulation Mechanism that defines the execution of the given PKE to exchange keys between users. The security features, key, ciphertext generation and plaintext recovery, of these algorithms all rely fundamentally on the Learning With Errors (LWE) problem [25], [26]. The rest of this section focuses on introducing these fundamental notions.

Let L be a lattice, then the LWE problem can be stated as follows: given pairs $(\boldsymbol{a}_i, b_i)$, such that $\boldsymbol{a}_i \leftarrow_R L$ and $b_i =$

$\langle \boldsymbol{s}, \boldsymbol{a}_i \rangle + e_i$, where $e_i \leftarrow \mathcal{X}$ is an error, the goal is to find the secret vector $\boldsymbol{s} \in L$. If no algebraic structure is considered on the lattice, then $L = \mathbb{Z}_q^n$. The objective of the problem is to determine the vector $\boldsymbol{s}$ from several samples as follows

$$\boldsymbol{a}_1 \in \mathbb{Z}_q^n, \quad b_1 = \langle \boldsymbol{s}, \boldsymbol{a}_1 \rangle + e_1, \tag{1a}$$
$$\boldsymbol{a}_2 \in \mathbb{Z}_q^n, \quad b_2 = \langle \boldsymbol{s}, \boldsymbol{a}_2 \rangle + e_2, \tag{1b}$$
$$\vdots$$
$$\boldsymbol{a}_k \in \mathbb{Z}_q^n, \quad b_r = \langle \boldsymbol{s}, \boldsymbol{a}_k \rangle + e_k. \tag{1c}$$

In the case of Kyber the modular version of LWE is considered, i.e. the chosen lattice is also a module for a polynomial ring. Therefore, if $R_q := \mathbb{Z}_q[x]/(x^n + 1)$ is the finite ring of the polynomials of degree less than n with coefficients in $\mathbb{Z}_q$, the lattice considered in Kyber is $R_q^k = \left(\mathbb{Z}_q[x]/(x^n + 1)\right)^k$. The parameters q, n, and k define the lattice, R_q^k, where q denotes the modulus of the coefficients, n is the degree of the polynomials of the ring R_q, and k is the range of R_q^k as a module. Finally, parameters η_1 and η_2 define the range of the error distributions $\mathcal{X}_1 = \mathcal{B}_{\eta_1}$ and $\mathcal{X}_2 = \mathcal{B}_{\eta_2}$ respectively, where the binomial distribution $\mathcal{B}_{\eta_i}$ is centered at 0 and has range $[-\eta_i, \eta_i]$, $i \in \{1, 2\}$.

The Kyber cryptosystem defines two functions [10] that compress and decompress its inputs component-by-component, given respectively by

$$\text{Compress}_q(x, d) \triangleq \left\lceil \frac{2^d}{q} \cdot x \right\rfloor \left(\text{mod}^+ 2^d\right), \tag{2a}$$
$$\text{Decompress}_q(x, d) \triangleq \left\lceil \frac{q}{2^d} \cdot x \right\rfloor. \tag{2b}$$

These two functions apply a quantification of the polynomial coefficients belonging to the $[0, q-1]$ interval and approximate them to the closest value of the $[0, 2^d]$ interval. Applying the Compress$(\cdot)$ creates an instance of the Modular Learning With Rounding (MLWR) problem, which is a variant of MLWE where the small error terms are already determined rather than sampled, and this error is avoided by rounding from one modulus to a smaller one. It is specified in [10] that the error introduced by the compress function is not considered in the security analysis.

The structure of Kyber PKE is as follows:

1) The private and public keys are defined as $sk := \boldsymbol{s}$ and $pk := (\boldsymbol{A}, \boldsymbol{b})$ respectively; where $\boldsymbol{A} \in R_q^{k \times k}$ is a pseudorandom matrix and $\boldsymbol{b} := \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e}$; with $\boldsymbol{e}, \boldsymbol{s} \in R_q^k$, and $\boldsymbol{e}, \boldsymbol{s} \leftarrow \mathcal{X}_1$.
2) A binary message $m \leftarrow_R \{0, 1\}^n$ is selected, and errors are sampled such that $\boldsymbol{s}' \leftarrow \mathcal{X}_1$ and $\boldsymbol{e}', e'' \leftarrow \mathcal{X}_2$, where $\boldsymbol{s}', \boldsymbol{e}' \in R_q^k$ and $e'' \in R_q$.
3) The ciphertext c is defined as
$$c := \left(\text{Compress}_q(\boldsymbol{u}, d_u), \text{Compress}_q(v, d_v)\right), \tag{3}$$
with $\boldsymbol{u} = \boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}' + \boldsymbol{e}'$, $v = \boldsymbol{b}^{\mathrm{T}}\boldsymbol{s}' + e'' + \hat{m}$, and $\hat{m} = \text{Decompress}_q(m, 1)$.
4) The decryption of the message is then given by
$$\begin{aligned} v - \boldsymbol{s}^{\mathrm{T}}\boldsymbol{u} &= \boldsymbol{b}^{\mathrm{T}}\boldsymbol{s}' + e'' + \hat{m} - \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}' - \boldsymbol{s}^{T}\boldsymbol{e}' \\ &= \boldsymbol{e}^{\mathrm{T}}\boldsymbol{s}' + \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}' + e'' + \hat{m} - \boldsymbol{s}^{\mathrm{T}}\boldsymbol{A}^{T}\boldsymbol{s}' - \boldsymbol{s}^{\mathrm{T}}\boldsymbol{e}' \\ &= \hat{m} + \boldsymbol{e}^{\mathrm{T}}\boldsymbol{s}' - \boldsymbol{s}^{\mathrm{T}}\boldsymbol{e}' + e''. \end{aligned} \tag{4}$$
5) The original binary message can then be recovered:
$$m = \text{Compress}_q(\hat{m} + \boldsymbol{e}^{\mathrm{T}}\boldsymbol{s}' - \boldsymbol{s}^{\mathrm{T}}\boldsymbol{e}' + e'', 1). \tag{5}$$

In the absence of the secret $\boldsymbol{s}$, any party trying to access the message m must solve the LWE instance that presents any ciphertext or public key. The level of security provided by this problem depends on the set of parameters q, n, k, η_1, and η_2, which have previously been introduced in the description of the structure of the LWE-based PKE system.

TABLE 1. Sets of parameters for Kyber.

Parameters	NIST-level	q	n	k	η_1	η_2	(d_u, d_v)
Kyber512	1	3329	256	2	3	2	$(10, 4)$
Kyber768	3	3329	256	3	2	2	$(10, 4)$
Kyber1024	5	3329	256	4	2	2	$(11, 5)$

In its final release, three sets of parameters were defined for Kyber and can be found in Table 1. Kyber512, 768 and 1024 target security levels 1, 3, and 5 established by NIST. These security levels were defined as follows: Any attack that breaks a security definition, must require computational resources comparable to or greater than those required for a search on a blockcipher of Advanced Encryption Standard (AES) with either 128-, 192-, or 256-bit keys respectively (i.e. AES128, AES192 or AES256). In this work we focus in the parameter set for Kyber768, that corresponds to the security level 3.

Kyber is a cryptosystem with Indistinguishability under Chosen Ciphertext Attacks (IND-CCA) semantic security. In particular, Kyber PKE reaches Indistinguishability under Chosen Plaintext Attacks (IND-CPA) security, while Kyber KEM reduces the IND-CCA security to the IND-CPA of Kyber PKE. IND-CPA security is defined as the probability of success of an attacker that has to choose between two messages given the ciphertext of one of them, chosen randomly. If the adversary has access to a decryption oracle, then it is considered IND-CCA security [27].

III. WIRELESS CHANNEL PHYSICAL LAYER

A. SYSTEM MODEL

The public communication medium is modeled as a memoryless wireless communication channel with AWGN and no fading. The communication takes place between two independent devices, the complex baseband received signal is then described as [28]

$$\mathsf{y} = s + n, \tag{6}$$

where $s \in \mathbb{C}$ is the complex transmitted symbol, $n \in \mathbb{C} \sim \mathcal{N}(0, \sigma)$ is the circularly symmetric Gaussian noise added by the wireless channel, and $y \in \mathbb{C}$ is the received symbol.

The assumption of a Gaussian channel is made here only to simplify the error calculations used for security, without fundamentally compromising the security guarantees of the scheme, which hold also under fading channel

models. In particular, fading channels with perfect channel estimation at the receiver only affect the bit error rates in proportion to the fading rate, with a further degradation occurring under imperfect channel knowledge. In either of these cases, the higher Bit Error Rate (BER) needs merely be compensated, either by requiring a higher SNR, or by introducing diversity [29] or coding techniques for fading channels [30], so as to keep the key-agreement rates.

For the sake of illustration, the transmission of 4QAM symbols is considered, each representing a 2-bit word in a 4 symbol alphabet, with in-phase and quadrature components given by

$$A_i = \pm\sqrt{E_b}, \tag{7a}$$
$$A_q = \pm\sqrt{E_b}, \tag{7b}$$

where E_b is the energy per bit and each of the 4 transmitted symbols is described as

$$s_n = A_i\mathcal{I} + A_q\mathcal{Q}, \quad \forall n \in \{0, 1, 2, 3\}. \tag{7c}$$

It is also assumed that a Gray code is employed over the constellation, such that the Hamming distance between any two adjacent symbols is minimal and equal to one. Under this modulation scheme, a data block is mapped into a string of symbols to be transmitted over the wireless communication channel.

Finally, the received baseband symbols, s, are decoded back into data by observing in which one of the four quadrants they lie. Using this decoding scheme, the BER approximation for a Gray-coded 4QAM constellation transmitted over an AWGN channel [28] is given by the bit error probability

$$P_b \approx \mathcal{Q}\left(\sqrt{2\frac{E_b}{N_0}}\right), \tag{8}$$

where E_b/N_0 is the ratio of energy per bit to the noise power spectra density given in linear form, and $\mathcal{Q}(x)$ is the Q-function given by [31]

$$\mathcal{Q}(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty \exp\left(-\frac{t^2}{2}\right)dt. \tag{9}$$

The behavior of the error probability[1] is described by Eq. (9), where x is a Signal to Noise Ratio (SNR), which in turn can be also represented in terms of energy-per-bit over noise (E_b/N_0) via the relation

$$\text{SNR} = 10\log_{10}(E_b/N_0). \tag{10}$$

B. WKyber TRANSPORT PROTOCOL

The objective of the physical layer employed in this scheme is to bring the exchanges required to run CRYSTALS-Kyber down to the signal level of information exchange, without the use of upper layer protocols. For the sake of clarity, we describe in the sequel how the information is transported down to the symbol level during an exchange. It is important to note that under the assumption of AWGN, the error probability of each transmitted symbol/bit is independent and identically distributed, which allows us to more easily calculate the error distribution for the encoded transmitted words.

From the beginning, it was clear that naively encoding the coefficients of the polynomials as single symbols is not viable, as the constellation size required is that of $q = 3329$ elements. It is known [28] that the bit error probability for an MPSK (M-ary Phase Shift Keying) constellation is

$$P_b \approx \frac{2}{\log_2 M}\mathcal{Q}\left(\sqrt{2\frac{E_b}{N_0}\log_2 M}\sin\left(\frac{\pi}{M}\right)\right), \tag{11}$$

where M is the number of elements in the constellation.

In other words, prohibitively large transmit signal powers would be necessary to achieve the low error rates required to make this transmission scheme viable.

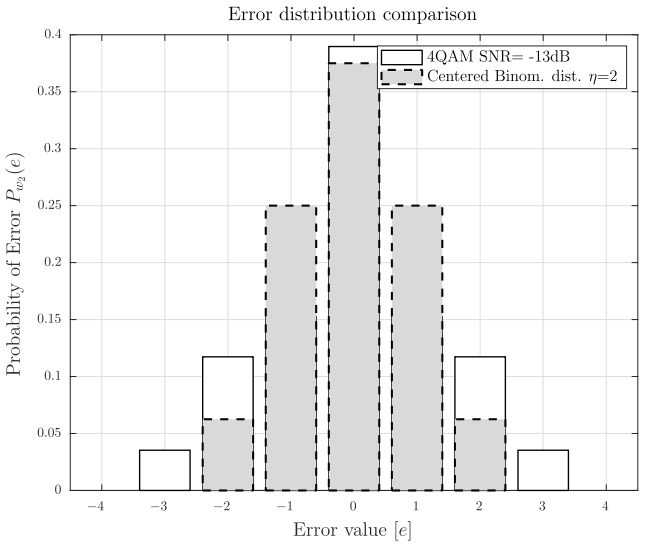

FIGURE 1. 2 Bit error probability for −13 dB SNR.

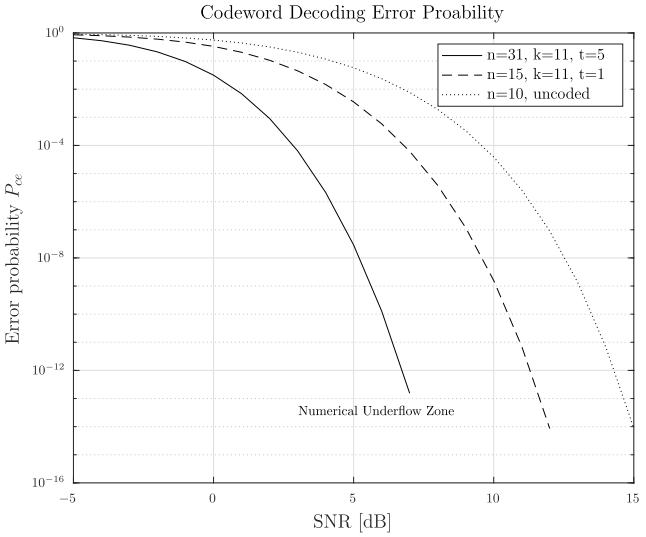

FIGURE 2. Codeword error decoding probability against SNR.

In order to circumvent this challenge, the symbol constellation presented in Section III-A was used. However, this now

[1]This formulation is only valid at high signal to noise ratios.

requires to encode the polynomial coefficients in $\mathbb{Z}_{3329}$ into a string of 2-bit symbols before transmission, thus fitting into a 6-symbol/12-bit word. In the original Kyber scheme, the u and v values are mapped from $\mathbb{Z}_q$ to $\mathbb{Z}_{2^d}$ values, followed by a bit packing step which moved the coefficients into d bit words. However, we instead skip the compression step for all coefficients and separate each 12 bit word into the 10 most significant bits, and the 2 least significant bits

$$w = \underbrace{b_{11}b_{10}b_9b_8b_7b_6b_5b_4b_3b_2}_{w_{10}}\,\underbrace{b_1b_0}_{w_2}. \tag{12}$$

This packing is specially problematic as all symbols experience the same bit error probability regardless of their significance within the word, resulting on equal likelihoods for a coefficient to have a shift of ± 2048 units as that of ± 1 unit in value.

To protect against this scenario, the upper word w_{10} is encoded using a BCH code, and the lower word w_2 is then mapped into a single 4QAM symbol. For now, assuming a sufficiently high protection to the most significant bits of the coefficient from the BCH code, the worst case scenario for the difference in magnitude between transmitted and received coefficients is equal to 3. These transitions are represented by

$$(11)_2 \rightarrow (00)_2, \text{ with } e = -3, \tag{13}$$

and

$$(00)_2 \rightarrow (11)_2, \text{ with } e = 3. \tag{14}$$

Taking into account all potential error transitions in the last two bits w_2, the error distribution on each of the $[0, 3328]$ information chunks representing each of the polynomial coefficients in $\mathbb{Z}_{3329}$ is independent and identically distributed and is approximately given by

$$P_{w_2}(e) = \begin{cases} 0, & \text{if } |e| \geq 4 \\ \frac{1}{4}P_b^2, & \text{if } |e| = 3 \\ \frac{1}{2}P_b \cdot (1 - P_b), & \text{if } |e| = 2 \\ \frac{1}{2}P_b \cdot (1 - P_b) + P_b^2, & \text{if } |e| = 1 \\ \frac{1}{4}(1 - P_b)^2, & \text{if } e = 0 \end{cases} \tag{15}$$

where P_b is calculated as a function of the SNR as in Eq. (8).

This distribution is compared against the Kyber768's error distribution in Figure 1. In order to ensure the correctness of the approximation in Eq. (15), the probability of error of the upper 10-bits, w_{10}, must be sufficiently small, which can be achieved using a binary BCH code to encode the 10 most relevant bits (w_{10}). BCH codes [32], [33] are a class of cyclic error-correcting codes which are constructed using polynomials over a Galois field [34] with the following parameters[2] for the binary case

$$\begin{aligned} &\text{Block length:} \quad n = 2^m - 1, \\ &\text{Parity check bits} \quad n - k \leq mt, \\ &\text{Minimum distance:} \quad d_{min} \geq 2t + 1, \end{aligned}$$

where m is the degree of the generator polynomial, k is the number of information bits to encode, t is the error correction capability of the code, and d_{min} is the minimum distance between any two codewords.

A validly constructed BCH code will always be able to correct any pattern of t or fewer errors in a block of n digits [34], as well as coming in a wide range of values for n and k. The aforementioned versatility in these well-known codes is why a BCH code of length $n = 31$ bits, error correction capability of $t = 5$ bits over a message of at most $k = 11$ bits has been chosen to protect the upper 10 bits, w_{10}, of the polynomial coefficient during transmission.

One could have potentially used a longer code to further minimize the error probability; however, this was not deemed necessary for an initial analysis due to the already minimal codeword decoding error probability shown in Figure 2.

The probability that a transmitted codeword cannot be decoded can be easily calculated starting from the fact that the probability of error of each individual bit is known, independent and identically distributed. Therefore, each number of errors is characterized by a binomial distribution per its definition, and the probability of seeing between 0 and t errors is described by the Cumulative Distribution Function (CDF) $F(k; n, p)$ of a binomial distribution given by

$$F(k; n, p) = I_{1-p}(n - k, k + 1), \tag{16a}$$

$$I_x(a, b) = \frac{B(x; a, b)}{B(a, b)}, \tag{16b}$$

$$B(x; a, b) = \int_0^x t^{a-1}(1 - t)^{b-1}dt, \tag{16c}$$

where, for our case, we want the complement of this CDF, finally yielding the probability to fail to recover a coded word

$$P_{ce} = 1 - I_{1-P_b}(n - t, t + 1), \tag{17}$$

where P_b is the bit error probability of the underlying transmission scheme.

IV. WIRELESS KYBER

This section presents Wireless Kyber (WKyber), our work's primary contribution, which adapts CRYSTALS-Kyber's algorithms and message exchange protocols to maximize the usage of a wireless channel's physical layer security properties. Depending on the degree of embedding of WKyber into the physical layer of communications it can be separated into two different schemes, or "Versions". Their high-level differences are summarized in Table 2 and are differentiated by how many of Kyber's LWE error instances are replaced by the AWGN introduced by the wireless propagation media during the encryption procedure, i.e. Kyber PKE.

In addition to the novel source of errors for the LWE problem, changes to the compression scheme, ciphertext and

[2] A BCH code will exist for any case where $m \geq 3$, $t < 2^{m-1}$ and $m, t \in \mathbb{Z}$.

public key (in the case of WKyber V2) definitions were also required. Furthermore, it is crucial to ensure that the proposed scheme is secure, and for this reason a security and error probability analysis has been conducted.

A. WKyber PKE

In this subsection two proposals to adapt Kyber PKE for the wireless channel are introduced as WKyber V1 and V2. They are key exchange algorithms capable of leveraging the properties of the AWGN channel, designed to be analogous to the original Kyber PKE system, to ensure that the Fujisaki-Okamoto (FO) transformation [27] can still be applied to the first version. This results in an adapted yet recognizable KEM scheme, where the distinction between two versions of the precursor PKE depends on the depth of integration of the the public key into the physical layer of communication.

TABLE 2. Proposed versions of WKyber.

Version	Channel use	Scheme	Security
V1	ciphertext	PKE and KEM	IND-CCA
V2	ciphertext and public key	PKE	IND-CPA

TABLE 3. WKyber PKE V1: KeyGen, Encryption, and Decryption.

WKyber PKE V1	
KeyGeneration()	
Get $seed_A$ if not given	
$\boldsymbol{A} = GenMatrix(seed_A)$	
$\boldsymbol{s} \leftarrow \mathcal{B}_{\eta_1}$	
$\boldsymbol{e} \leftarrow \mathcal{B}_{\eta_1}$	
$\boldsymbol{b} = \boldsymbol{As} + \boldsymbol{e}$	
$sk := \boldsymbol{s}$	
$pk := (seed_A, \boldsymbol{b})$	
return (pk, sk)	
$\xrightarrow{\text{AWGN}(pk,10,10)}$	
	Encrypt$(pk, m; r)$
	$\boldsymbol{A} = GenMatrix(seed_A)$
	$\boldsymbol{s}' \leftarrow \mathcal{B}_{\eta_1}$
	$\boldsymbol{u} = \boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}'$
	$v = \boldsymbol{b}^{\mathrm{T}}\boldsymbol{s}' + \hat{m}$
	return $c := (\boldsymbol{u}, v)$
$\xleftarrow{\text{AWGN}(c,10,-10)}$	
Decrypt(sk, c)	
$m = \text{Compress}_q(v - \boldsymbol{s}^{\mathrm{T}}\boldsymbol{u}, 1)$	
return m	

PKE V1 is presented in Table 3; this scheme limits its use of the AWGN channel as a source of errors for ciphertext generation, while the public key generation and transmission is identical to the original Kyber. The original Kyber submission used the FO$^{\not\perp}$ transformation to build Kyber KEM from Kyber PKE because in [35] it was proven that as long as Kyber PKE is IND-CPA secure, then Kyber KEM will be IND-CCA secure. To reach this level of security, the FO$^{\not\perp}$ transformation requires a re-encryption step inside the decapsulation algorithm, i.e. after the ciphertext is decrypted the resulting plaintext is encrypted again to verify if the new ciphertext matches one. Utilizing WKyber PKE V1 allows for re-encryption, since the public key ($seed_A$, $\boldsymbol{b} = \boldsymbol{As} + \boldsymbol{e}$) does not depend on the uncontrollable conditions originating from the channel's effects. Therefore, if the security of WKyber PKE V1 is equivalent to that of the original Kyber, it is possible to apply the FO$^{\not\perp}$ transformation and thus construct a KEM, denoted as WKyber KEM V1, of the same form.

TABLE 4. WKyber PKE V2: KeyGen, Encryption, and Decryption.

WKyber PKE V2	
KeyGeneration()	
Get $seed_A$ if not given	
$\boldsymbol{A} = GenMatrix(seed_A)$	
$\boldsymbol{s} \leftarrow \mathcal{B}_{\eta_1}$	
$\boldsymbol{b} = \boldsymbol{As}$	
$sk := \boldsymbol{s}$	
$pk := (seed_A, \boldsymbol{b})$	
return (pk, sk)	
$\xrightarrow{\text{AWGN}(As,10,-10)}$	
	Encrypt$(pk, m; r)$
	$\boldsymbol{A} = GenMatrix(seed_A)$
	$\boldsymbol{s}' \leftarrow \mathcal{B}_{\eta_1}$
	$\boldsymbol{u} = \boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}'$
	$v = \boldsymbol{b}^{\mathrm{T}}\boldsymbol{s}' + \hat{m}$
	return $c := (\boldsymbol{u}, v)$
$\xleftarrow{\text{AWGN}(c,10,-10)}$	
Decrypt(sk, c)	
$m = \text{Compress}_q(v - \boldsymbol{s}^{\mathrm{T}}\boldsymbol{u}, 1)$	
return m	

When both the public key and ciphertexts are under the influence of AWGN noise from the wireless channel, as it is for WKyber PKE V2, the original Kyber scheme requires further modifications than the ones needed for WKyber PKE V1. Specifically, the LWE instance of public key is redefined to be $A \cdot s$ and the receiver gets $pk = (seed_A, A \cdot s + e_{AWGN})$, where it and the ciphertext observe a low SNR of -10 dB. Therefore, the FO transformation is not applicable anymore, as the sender of a public key of WKyber PKE V2 does not acquire a copy of it; and by definition is unable to replicate the encryption process. The NIST asserts that if a cryptosystem is IND-CPA secure, its utilization with ephemeral keys, i.e. the generation of a new key pair at the beginning of each communication, becomes a viable proposition. Under this setup, WKyber PKE V2 is recommended as KEM without re-encryption and utilizing ephemeral keys.

The proposed schemes are viable adaptations of the original Kyber system, each with its respective tradeoffs in the context of resource constrained devices. WKyber KEM V1 has the advantage that it reaches the higher level of IND-CCA security, and thus allows the sender to re-use its public key. However, this comes at the cost of an usage of additional error correction. While WKyber PKE V2 relaxes both of these requirements by 1) leveraging the AWGN channel to introduce errors into the public key and 2) removing the need to provide error correction for the least significant bits of the public key.

Both versions of the construction of Wireless Kyber are compatible with all three Kyber parameters sets presented in Table 1. These parameter sets differentiate only in the value of $k \in \{2, 3, 4\}$, and k remains unaffected by the changes on the error distribution. The primary focus is on

the Kyber768 parameter set, as it is labeled as *recommended*, while Kyber512 is labeled as *light* and Kyber1024 as *paranoid*.

B. OTHER MODIFICATIONS

Equations (2a) and (2b) show the compression and decompression functions employed in the Kyber cryptosystem. During the execution of a key exchange of Kyber, the Compress_q function is utilized to compress the ciphertext during encapsulation. This function is also used during decryption to transform the plaintext from a polynomial back to a bit string, and to erase the error added during the whole key exchange process. It is important to differentiate between these two applications. While the utilization of Compress_q during the decryption is required for this process to work, the compression of the ciphertext is only considered to enhance the performance. The adaptations introduced in WKyber have an negative impact on the applicability of Compress_q.

A ciphertext of Kyber is conformed of a vector of polynomials u and a polynomial v, with coefficients in the finite field $\mathbb{Z}_q$ with $q = 3329$. The Compress_q function reduces the size of each coefficient from module q to the parameters $(d_u, d_v) = (10, 4)$ (see Table 1). The bit reduction applied by the compression function includes a few steps described as follows. If $d_u = 10$, the interval $[0, q-1]$ is quantified into 2^{10} sub-intervals, and subsequently, each integer in $[0, q-1]$ is rounded to the nearest division. Given that the alphabet left has 2^{10} total words, it can be expressed as 10-bits words, ordered by size.

The compression of Kyber supposes adding an error to each coefficient of any ciphertext. This approach is deemed feasible due to the fact that the errors introduced are eliminated at the conclusion of the decryption process. In the case of WKyber PKE, none of the proposed versions is compatible with this function, since its design relies on the transmission of the whole 12 bits of each coefficient of the ciphertext. In order to apply the BCH code and recover the initial 10 bits as well as to send the last two bits with a lower SNR, and add the error in this way, it is necessary to send 12 bits in total. Consequently, the Compress_q function does not work with the introduced modifications.

The error added by the Compress_q function is not considered in the security analysis, therefore not using this function does not affect the assumption that the WKyber scheme as a whole resembles a standard Kyber instance with a different error distribution. However, it is acknowledged that the error generated by the compression function is considered in the calculation of the error probability of the cryptosystem. Thus, if this error is eliminated, the probability error during a key exchange is reduced.

The adaptation of Kyber to this wireless implementation requires a new definition of the ciphertext, using the noise of the wireless communications channel to generate the errors. In the case of WKyber PKE V1, $\boldsymbol{e}'$ and e'' are generated by the channel, as well as the error e in the key generation algorithm for WKyber PKE V2. Instead of sending the ciphertext composed of $(\mathbf{u}, v)$ where

$$\boldsymbol{u} = \text{Compress}_q\left(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}' + \boldsymbol{e}', d_u\right), \tag{18a}$$

$$v = \text{Compress}_q\left(\boldsymbol{b}^{\mathrm{T}}\boldsymbol{s}' + e'' + \text{Decompress}_q(m, 1), d_v\right), \tag{18b}$$

the ciphertext is sent without adding an error sampled from the $\mathcal{B}_{\eta_i}$ distribution.

Consequently, the ciphertext in both WKyber versions consists in the pair $(\mathbf{u}_{WK}, w_{WK})$, where

$$\boldsymbol{u}_{\text{WK}} = \boldsymbol{A}^{\mathrm{T}}\boldsymbol{s}', \tag{19a}$$

$$v_{\text{WK}} = \boldsymbol{b}^{T}\boldsymbol{s}' + \text{Decompress}_q(m, 1). \tag{19b}$$

In the case of WKyber V2, a similar modification is also applied to the public key. In previous versions of the standard Kyber, the public key had a compression, but this is removed in the final draft of the cryptosystem [36], and in the final NIST standard draft of ML-KEM [9]. The public key of Kyber is defined as $pk_{Kyber} = (seed_A, \boldsymbol{b} := \boldsymbol{As} + \boldsymbol{e})$. In the case of WKyber V2 the error is also added through the channel, hence the information sent is $pk_{WKyberV2} = (seed_A, \boldsymbol{As})$.

C. SECURITY AND ERROR DISTRIBUTION

In this section, a detailed analysis of the security of both versions of the WKyber cryptosystem is presented. The fundamental argument supporting the security of WKyber is based on the premise that Kyber is regarded as a secure cryptosystem and that the modifications introduced do not compromise the original security.

The evaluation of Post-Quantum Cryptography (PQC) cryptosystems is typically conducted considering three primary aspects: semantic security, the underlying hardness of the mathematical problem, and the security of the implementations. CRYSTALS Kyber

The $\text{FO}^{\not\perp}$ transformation applied in the original scheme is also considered for WKyber KEM V1, thereby ensuring that semantic security remains unaltered. Consequently, the focus is directed towards proving that the PKE of both versions of WKyber are IND-CPA secure. The security of Kyber's mathematical foundation derives from the fact that Kyber PKE generates keys and ciphertexts that are instances of the LWE problem, meaning that its security is based on the computational difficulty of solving these instances. Kyber PKE's security reduction can be also be considered for the two versions of WKyber PKE, but only if the hardness of the LWE problem is equivalent for the AWGN channel error distribution.

The LWE and MLWE problems are stated with parameters q, n, k and (η_1, η_2), and the additional hidden parameter m. The η_i parameters denote the range of the error distributions used in the cryptosystem. In the ML-KEM documentation [9], the error distribution is defined as a discrete binomial distribution centered at the origin, with values

in the interval $[-\eta_i, \eta_i]$. However, the general formulation of the LWE problem models, the error distribution as a centered Gaussian distribution. The first version of Kyber submitted to NIST followed this convention, but in the second round of the NIST PQC call, the authors proposed to use a centered binomial distribution to sample the LWE errors, as its implementation is much easier and does not harm the security of the cryptosystem. In the third round submission of Kyber [10], it is stated that the execution of the best attacks against the cryptosystem does not depend on the nature of the error distribution, but on its standard deviation. Before Kyber, another lattice-based cryptosystem called NewHope proposed the change of error distribution, from a Gaussian to a binomial in [37]. The literature further presents examples of works changing the model of the error distribution, like FrodoKEM [38] that defines a specific error distribution for this cryptosystem. As stated in Lemma 5.5 of the FrodoKEM documentation, the alteration in error distribution requires an additional security reduction.

To solve the LWE problem, two attacks are considered to be viable strategies 1) the dual and 2) the primal attack, where in the case of Kyber, the authors considered two estimation strategies. First, the Core-Shortest Vector Problem (SVP) [37] primal attack strategy was included as a cost measurement in Kyber's security analysis, which consists in only taking into account the cost of a single call to an SVP oracle in a fixed dimension. Therefore, it is seen as a pessimistic estimation.

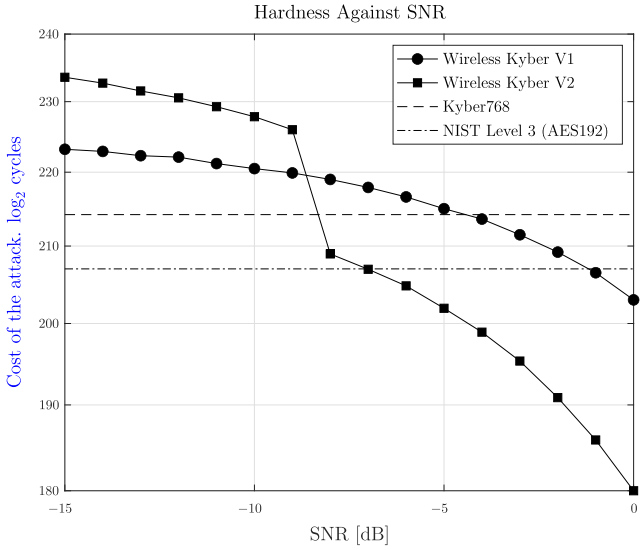

FIGURE 3. Cost of the dual attack against LWE samples of WKyber PKE V1 and V2 in comparison to standard Kyber and NIST level 3 security bound (AES192).

The dual attack [39], [40] is the second main strategy to solve a LWE instance, in particular the LWE decision problem. The cost of the dual attack gives an estimation that fits better the comparison with the NIST security levels. In contrast, the estimations for the original Kyber with the CoreSVP methodology do not reach the corresponding target level of security on any parameter set. Both Kyber and ML-KEM estimate the security level of each parameter set as the

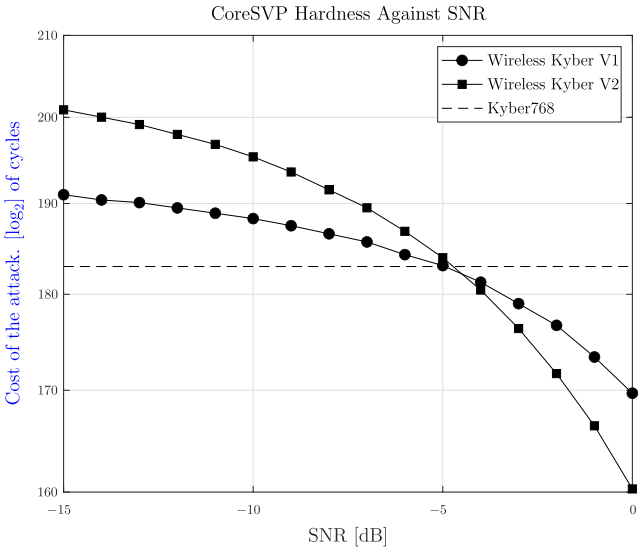

FIGURE 4. Cost of using the primal CoreSVP strategy against LWE samples of WKyber PKE V1 and V2 in comparison to standard Kyber.

hardness associated with such parameters against the dual attack, i.e. cost of running the attack.

To obtain an equivalent security evaluation for WKyber, the open source lattice estimator presented in [39] and [41] was used. It provides various estimations of the complexity of solving a designated LWE instance, based on diverse strategies, criteria, and publications. This tool facilitates the selection of a LWE parameter set, with the option to define distinct distributions of error. In particular, the cost of the dual or primal attacks can be estimated for any given LWE parameter set. Additionally, the calculus of the cost of other attacks, based on more recent publications, is included in the estimator. The hybrid attack, proposed in [42], is relevant due to its better performance in some cases, hence it is included in the security analysis.

The AWGN channel distribution considered in WKyber was introduced in the lattice estimator [39] as a LWE error distribution that generates $\boldsymbol{e}$, $\boldsymbol{e}'$ and e''. The cost of the dual, primal and hybrid attack was calculated using the estimator, creating LWE parameters corresponding to WKyber PKE V1, WKyber PKE V2 and Kyber PKE. Tables 5 and 6 show the results of the estimator, including between brackets, the cost of the attacks against Kyber presented in the reference documentation.

To analyze the effect of the change of error distribution, Table 5 compares the computational cost of solving the LWE problem using the attacks previously presented against the instances of Kyber PKE and WKyber PKE V1, the latter transmitted with a SNR of -10 dB. Although this particular SNR was chosen for analysis, it is important to note that other values could also be selected. This can be observed in Figures 3 and 4, which illustrate that the change in the error distribution does not compromise the hardness of LWE instances up to SNR of -5 dB. The cost of the attacks is evaluated in terms of CPU cycles; also, some specific algorithms have also a exponential cost of memory.

When the error distribution of the PQ-cryptosystems Kyber or NewHope was modified [10], [37], it was argued that the security was unaffected as long as the standard deviation remained the same. This argument is reinforced in the estimator presented in [39], since only the standard deviation is used in the calculus of the cost of solving LWE. Therefore, if the distribution is changed to a different one with higher standard deviation, the cost of solving the problem also rises. The binomial distribution presented in the original parameter sets has a standard deviation of 1. The standard deviation of the channel error distribution is determined by Eq. (15), depending upon the SNR. Consequently, the estimations of the cost of solving WKyber instances vary according to the SNR utilized to transmit the two least significant bits. A lower standard deviation corresponds to a lower cost of attacks, and conversely, a higher SNR is associated with a lower security estimation. The SNR considered for the results presented in Figures 3 and 4 ranges from -15 dB to 0 dB.

These results demonstrate that under optimal SNR conditions the security of WKyber is equivalent to that of standard Kyber. The cost of the dual attack as a function of the SNR is presented in Figure 3. WKyber PKE V1 and V2 achieve a higher degree of security than Kyber for an SNR in the ranges [-15 dB, -5 dB], and [-15 dB, -9 dB] respectively. Furthermore, a comparison between the hardness of WKyber LWE instances and the computational cost of solving AES192 is presented, revealing a wider range of secure SNR values.

TABLE 5. Hardness ($\log_2$ of cycles) of the instances presented by SotA Kyber and proposed WKyber PKE V2 at -10dB[3].

	Kyber512	WKyber V1 $k=2$
CoreSVP classical	115(118)	119.4
Dual attack	146.2(151.5)	150.9
Dual hybrid attack	135.3	140
	Kyber768	WKyber V1 $k=3$
CoreSVP classical	182.2	188
Dual attack	214.2(215.1)	220.5
Dual hybrid attack	196.1	190.3
	Kyber1024	WKyber V1 $k=4$
CoreSVP classical	255.2(256)	263.1
Dual attack	288.6(287.3)	296.9
Dual hybrid attack	262.4	268.5

Figure 4 shows the cost of the primal attack against WKyber PKE and the standard Kyber, assuming the CoreSVP strategy. As can be appreciated, the results for SNR lower than -5 dB are, again, better than the respective results of Kyber, thereby ensuring a consistent level of security.

The analysis indicates that the standard deviation significantly impacts the performance of cryptanalysis against LWE. As previously explained and further elaborated in the Kyber submission, the performance of the cryptanalysis with respect to the error distribution is primarily influenced by the standard deviation. The binomial distribution employed

TABLE 6. Hardness ($\log_2$ of cycles) of the instances presented by SotA Kyber and proposed WKyber PKE V2 at -10dB[3].

	Kyber512	WKyber V2 $k=2$
CoreSVP classical	115(118)	120
Dual attack	146.2(151.5)	151.5
Dual hybrid attack	135.3	140.8
	Kyber768	WKyber V2 $k=2$
CoreSVP classical	182.2	195.3
Dual attack	214.2(215.1)	227.8
Dual hybrid attack	196.1	208.9
	Kyber1024	WKyber V2 $k=2$
CoreSVP classical	255.2(256)	272.7
Dual attack	288.6(287.3)	306.5
Dual hybrid attack	262.4	279.3

in Kyber768 has a standard deviation of 1, and for SNR ≥ -5 dB, the standard deviation of the error distribution of the channel exceeds 1.

D. ERROR PROBABILITY

Kyber/ML-KEM are probabilistic cryptosystems, a characteristic shared by the majority of LWE-based cryptosystems, this implies an inherent probability of error in the exchange of information and data, which has a significant impact on the final error probability of the cryptosystem. Therefore, this section is dedicated on analyzing the error probability of the WKyber cryptosystem.

TABLE 7. Error probability of Kyber and WKyber PKE V1/V2 (SNR$=-10$dB).

	Error probability ($\log_2$)
Kyber512	-139
WKyber V1 $k=2$	-219.1
WKyber V2 $k=2$	-198.7
Kyber768	-164
WKyber V1 $k=3$	-227.2
WKyber V2 $k=3$	-138.5
Kyber1024	-175
WKyber V1 $k=4$	-174
WKyber V2 $k=4$	-105.2

The designers of Kyber present a Python script to calculate the error probability of the cryptosystem. This script was adapted to include the change in error distribution and the absence of compression. The change in the error distribution increases the probability of error; however, not applying the compression significantly mitigates this effect. As expected, the error probability of WKyber is higher than the one from the original cryptosystem. This is due to the fact that the range of the binomial distribution used in Kyber is $[-2, 2]$, while the channel error distribution range varies with the SNR. The security analysis in Subsection IV-C shows that if the error distribution has a wider range, the complexity of the LWE instances is enhanced. In the case of WKyber, the security in

terms of cost of attacks is higher than the same of Kyber, but also the error probability is higher. Not using the Compress_q function on ciphertexts means a loss in performance, given the necessity to transmit longer bit strings. However, from a security standpoint the absence of compression results in a reduction in the error probability.

The error probability of Kyber derives from the following expression

$$\text{Decompress}_q(m, 1) + \boldsymbol{e}^{\mathrm{T}}\boldsymbol{s}' - \boldsymbol{s}^{\mathrm{T}}\boldsymbol{e}' + e'' + e_u + e_v, \quad (20)$$

where the coefficients of $\boldsymbol{e}$, $\boldsymbol{e}'$, $\boldsymbol{s}$, $\boldsymbol{s}'$, and e'' are sampled using the error distribution of the cryptosystem, and e_u and e_v represent the error introduced during the compression. In the case of WKyber, as discussed in section IV-B, it is important to note that the compression is not applied, hence this error is not considered. Since the error of compression is not considered in the security analysis of the original submission of Kyber [10], the omission of this function does not affect the security of WKyber. Table 7 shows the probability of error in a key exchange for both, the original Kyber and the proposed WKyber versions. It can be appreciated that the version 1 of WKyber exhibits a lower error probability than the original scheme. On the other hand, the version 2 of WKyber presents a higher error probability than Kyber, however this can be mitigated using a higher SNR still in the secure range between -10 dB and -5 dB.

Despite the inclusion of the BCH code for error correction, there is still a chance that will not be able to correct all errors. As presented in IV-B, the first 10 bits of each polynomial coefficient are coded before their transmission, adding redundant bits which add the capacity to correct up to 5 errors. The probability of a codeword not being correctly decoded was defined in Eq. (17), while Figure 5 represents the errors of the key exchange vs. the SNR.

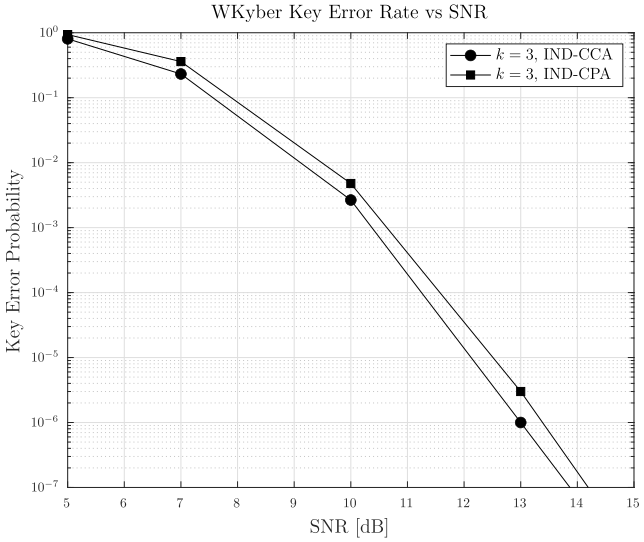

FIGURE 5. KER for the WKyber 768 V1/V2 system under various SNRs and values of k.

The schemes presented in Tables 3 and 4 define two SNR values on each communication, one for the ten most significant bits of each coefficient, which controls the decoding error probability, and one for the two least significant bits, which control the hardness of the system. As demonstrated in Figure 5, utilizing higher SNR results in a reduced error probability. It is notable that, for SNR $=$ 15 dB, the error function falls in Figure 5 under the numerical underflow. In summary, managing the power profile utilized during a WKyber is imperative avoid errors and maintain security, as the SNR achieved for the BCH words must be greater than 10 dB, and the one for the last two bits of each coefficient are transmitted to be below -5 dB to avoid security losses, and keep negligible the error probability of the scheme.

E. A NOTE ON IMPLEMENTATION REQUIREMENTS

In this subsection the feasibility of the proposed WKyber schemes is analyzed. The first requirement to implement WKyber is the adaptation of the underlying mathematical functions, like Number Theoretical Transform (NTT) multiplication and other lattice arithmetics, to a physical/hardware implementation; ideally, an implementation contained in a hardware security module. This is, however, a well known reality for the adoption of post-quantum cryptography, specially in IoT. As hardware implementations of cryptographic primitives generally perform better, those are currently demanded for some implementation of Kyber. In this regard, therefore, it can be said that WKyber demands no additional cryptographic requirements compared to currently used methods.

Next, in order to address the overhead associated with implementing WKyber in comparison to standard Kyber, one can look into the efficiency of both approaches with respect to requirements in terms of transmitted information. Considering an implementation over Bluetooth 5.0 as an example, the efficiency of the WKyber scheme can be estimated at $\frac{12}{16+2} \approx 67\%$, which follows from the encoding scheme employed, namely, BCH coding of 10 bit codewords into 15 bits, rounded up to 16 due to the 4QAM modulation, plus the lower 2-bit word. In comparison, it is known [43], [44], [45] that under 1 MBit/s and 2 Mbit/s raw transmission, Bluetooth Low Energy (BLE) achieves efficiencies of 23%–48% bits, and 19%–68% bits, respectively. In other words, the spectral efficiency of WKyber can be said to be comparable to the highest achievable by the most recent and advanced version of BLE, which is one of the key wireless technologies for IoT applications.

The standard Kyber scheme requires the implementation of an auxiliary error function in order to generate the errors added to the messages and keys. In contrast, under WKyber V1, the call to the binomial distribution for the error of the ciphertext is not required, while under WKyber V2 the equivalent call is also not needed during the execution of the key generation algorithm, which implicates that WKyber is more efficient and can run faster than standard Kyber.

Finally, it should be noted that issues such as added latency by using a PQ scheme are also mitigated due to the efficiency of communication mentioned earlier, meaning that standard Kyber requires error-free channel, while WKyber does not. As for the latency associated with key establishment, this is inevitable when adopting PQ schemes [9], as it is already well known that keys, signatures and the messages needed to exchange them are longer than those in pre-quantum cryptography [46], [47]. In other words, by limiting the overhead at the transport layer, the overall impact is lowered, and latency gains/losses due to computational complexity of the WKyber algorithm are not relevant, since the highest complexity operations are the generation of the public key matrix A and its multiplication with the generated secret.

V. CONCLUSION

The field of crypto-security is currently at a compromised and convulsive moment. Various authorities and standardization bodies are calling for a transition to post-quantum cryptography and the adoption of hybrid systems. Following this trend, we propose a combination of the first standard adopted by NIST, CRYSTALS-Kyber, and the use of the physical security layer. Public key encryption is among the subjects most affected by the quantum threat and algorithms such as ElGamal, RSA and those based on elliptic curves will no longer be secure. The proposal of Wireless Kyber can be seen as a step in the post-quantum transition with the possibility of replacing those algorithms in wireless IoT devices. A viable adaptation makes use of BCH codes in the error correction section, and of signal strength manipulation to introduce an error in each coefficient, very similar to that of the Kyber cryptosystem. Finally, the security and error probability of WKyber have been analyzed to assess the feasibility of the cryptosystem, with the conclusion that if the SNR difference is sufficiently high, a secure exchange, analogous to the original Kyber key exchange, can be maintained. Future work includes implementing WKyber in hardware and researching possible vulnerabilities. In particular, to investigate whether the use of the Gaussian channel in a hardware implementation can compromise the original Kyber security, and if new side-channel attacks on this implementation are feasible.

Generated by IEEEtran.bst, version: 1.14 (2015/08/26)

ACKNOWLEDGMENT

M. A. González de la Torre would like to thank CSIC Project EFiDiP for its support.

REFERENCES

[1] Ericsson. (2019). *Ericsson Mobility Report*. [Online]. Available: https://www.ericsson.com/4acd7e/assets/local/reports-papers/mobility-report/documents/2019/emr-november-2019.pdf

[2] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G mobile wireless networks," *IEEE Access*, vol. 6, pp. 4850–4874, 2018, doi: 10.1109/ACCESS.2017.2779146.

[3] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3682–3722, 2019, doi: 10.1109/COMST.2019.2916180.

[4] D. Deutsch, "Quantum theory, the Church–Turing principle and the universal quantum computer," *Proc. Roy. Soc. London. A. Math. Phys. Sci.*, vol. 400, no. 1818, pp. 97–117, Jul. 1985, doi: 10.1098/rspa.1985.0070.

[5] A. W. Cross, L. S. Bishop, S. Sheldon, P. D. Nation, and J. M. Gambetta, "Validating quantum computers using randomized model circuits," *Phys. Rev. A, Gen. Phys.*, vol. 100, no. 3, Sep. 2019, Art. no. 032328, doi: 10.1103/physreva.100.032328.

[6] R. Cumming and T. Thomas, "Using a quantum computer to solve a real-world problem - what can be achieved today?" 2022, *arXiv:2211.13080*.

[7] T. Ichikawa et al., "A comprehensive survey on quantum computer usage: How many qubits are employed for what purposes?" 2023, *arXiv:2307.16130*.

[8] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Rev.*, vol. 41, no. 2, pp. 303–332, Jan. 1999, doi: 10.1137/s0036144598347011.

[9] *Module-Lattice-Based Key-Encapsulation Mechanism Standard*, document FIPS 203, 2024.

[10] R. Avanzi, J. Bos, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé. (2020). *CRYSTALS-Kyber*. [Online]. Available: https://pq-crystals.org

[11] G. Maringer, S. Puchinger, and A. Wachter-Zeh, "Information- and coding-theoretic analysis of the RLWE/MLWE channel," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 549–564, 2023, doi: 10.1109/TIFS.2022.3226907.

[12] M. Wang and Z. Yan, "Security in D2D communications: A review," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, vol. 1, Aug. 2015, pp. 1199–1204, doi: 10.1109/TRUSTCOM.2015.505.

[13] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jul. 2015, pp. 180–187, doi: 10.1109/ISCC.2015.7405513.

[14] J. Jung, B. Kim, J. Cho, and B. Lee, "A secure platform model based on ARM platform security architecture for IoT devices," *IEEE Internet Things J.*, vol. 9, no. 7, pp. 5548–5560, Apr. 2022, doi: 10.1109/JIOT.2021.3109299.

[15] J. Huang, H. Zhao, J. Zhang, W. Dai, L. Zhou, R. C. C. Cheung, Ç. K. Koç, and D. Chen, "Yet another improvement of plantard arithmetic for faster kyber on low-end 32-bit IoT devices," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 3800–3813, 2024, doi: 10.1109/TIFS.2024.3371369.

[16] P. Porambage, G. Gür, D. P. Moya Osorio, M. Livanage, and M. Ylianttila, "6G security challenges and potential solutions," in *Proc. Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit)*, Jun. 2021, pp. 622–627, doi: 10.1109/EuCNC/6GSummit51104.2021.9482609.

[17] L. Mucchi, S. Jayousi, S. Caputo, E. Panayirci, S. Shahabuddin, J. Bechtold, I. Morales, R.-A. Stoica, G. Abreu, and H. Haas, "Physical-layer security in 6G networks," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1901–1914, 2021, doi: 10.1109/OJCOMS.2021.3103735.

[18] P. Angueira, I. Val, J. Montalbán, Ó. Seijo, E. Iradier, P. S. Fontaneda, L. Fanari, and A. Arriola, "A survey of physical layer techniques for secure wireless communications in industry," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 810–838, 2nd Quart., 2022, doi: 10.1109/COMST.2022.3148857.

[19] Y. Katsuki, G. T. F. D. Abreu, K. Ishibashi, and N. Ishikawa, "Noncoherent massive MIMO with embedded one-way function physical layer security," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 3158–3170, 2023, doi: 10.1109/TIFS.2023.3277255.

[20] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975, doi: 10.1002/j.1538-7305.1975.tb02040.x.

[21] S. Liu, T. Gao, Y. Liu, and X. Lu, "Physical-layer public key encryption through massive MIMO," in *Proc. 19th ACM Asia Conf. Comput. Commun. Secur.* New York, NY, USA: Association for Computing Machinery, Jul. 2024, pp. 353–365, doi: 10.1145/3634737.3656284.

[22] W. Abdallah, "A physical layer security scheme for 6G wireless networks using post-quantum cryptography," *Comput. Commun.*, vol. 218, pp. 176–187, Mar. 2024, doi: 10.1016/j.comcom.2024.02.019.

[23] T. Tosun and E. Savas, "Zero-value filtering for accelerating non-profiled side-channel attack on incomplete NTT-based implementations of lattice-based cryptography," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 3353–3365, 2024, doi: 10.1109/TIFS.2024.3359890.

[24] M. R. Nosouhi, S. W. Shah, L. Pan, Y. Zolotavkin, A. Nanda, P. Gauravaram, and R. Doss, "Weak-key analysis for BIKE post-quantum key encapsulation mechanism," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 2160–2174, 2023, doi: 10.1109/TIFS.2023.3264153.

[25] C. Peikert, "Public-key cryptosystems from the worst-case shortest vector problem: Extended abstract," in *Proc. 41st Annu. ACM Symp. Theory Comput.*, May 2009, pp. 333–342, doi: 10.1145/1536414.1536461.
[26] P. Ravi, S. Bhasin, S. S. Roy, and A. Chattopadhyay, "On exploiting message leakage in (Few) NIST PQC candidates for practical message recovery attacks," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 684–699, 2022, doi: 10.1109/TIFS.2021.3139268.
[27] H. Jiang, Z. Zhang, L. Chen, H. Wang, and Z. Ma, "IND-CCA-secure key encapsulation mechanism in the quantum random Oracle model, revisited," in *Proc. Annu. Int. Cryptol. Conf.*, vol. 10993, Jan. 2018, pp. 96–125, doi: 10.1007/978-3-319-96878-0_4.
[28] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2008.
[29] T. M. Duman and A. Ghrayeb, *Fading Channels and Diversity Techniques*. Chichester, U.K.: Wiley, 2007, pp. 7–42, doi: 10.1002/9780470724347.ch2.
[30] E. Biglieri, G. Caire, and G. Taricco, "Coding for the fading channel: A survey," *Signal Process.*, vol. 80, no. 7, pp. 1135–1148, Jul. 2000, doi: 10.1016/s0165-1684(00)00027-x.
[31] J. G. Proakis and M. Salehi, *Digital Communications*, 5th ed., New York, NY, USA: McGraw-Hill, 2007. [Online]. Available: https://daskalakispiros.com/files/Ebooks/digital-communication-proakis-salehi-5th-edition.pdf
[32] R. C. Bose and D. K. Ray-Chaudhuri, "On a class of error correcting binary group codes," *Inf. Control*, vol. 3, no. 1, pp. 68–79, Mar. 1960, doi: 10.1016/s0019-9958(60)90287-4.
[33] A. Hocquenghem, "Codes correcteurs d'erreurs," *Chiffres*, vol. 2, pp. 147–156, Sep. 1959.
[34] S. Lin and D. J. Costello, *Error Control Coding*. Upper Saddle River, NJ, USA: Prentice-Hall, 2004.
[35] D. Hofheinz, K. Hövelmanns, and E. Kiltz, "A modular analysis of the Fujisaki-Okamoto transformation," in *Proc. 15th Int. Conf. Theory Cryptography (TCC)*, vol. 10677, Jan. 2017, pp. 341–371, doi: 10.1007/978-3-319-70500-2_12.
[36] *Module-Lattice-Based Key Encapsulation Mechanism Standard*, Standard FIPS 203, IPD, NIST, National Institute of Standards and Tecnology, 2023, doi: 10.6028/NIST.FIPS.203.ipd.
[37] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, "Post-quantum key exchange—A new hope," in *Proc. 25th USENIX Secur. Symp.*, Jan. 2015, p. 1092.
[38] E. Alkim, J. W. Bos, L. Ducas, P. Longa, I. Mironov, M. Naehrig, V. Nikolaenko, C. Peikert, A. Raghunathan, and D. Stebila. (2021). *FrodoKEM Learning With Errors Key Encapsulation (Round 3 Submission)*. [Online]. Available: https://frodokem.org/spec
[39] M. R. Albrecht, R. Player, and S. Scott, "On the concrete hardness of learning with errors," *J. Math. Cryptol.*, vol. 9, no. 3, pp. 169–203, Oct. 2015, doi: 10.1515/jmc-2015-0016.
[40] M. R. Albrecht and Y. Shen, "Quantum augmented dual attack," Cryptol. ePrint Arch., Int. Assoc. Cryptologic Res. (IACR), Tech. Rep. 2002/656, 2022. [Online]. Available: https://eprint.iacr.org/2022/656
[41] M. R. Albrecht. (2024). *Lattice-Estimator*. [Online]. Available: https://github.com/malb/lattice-estimator/tree/main
[42] T. Espitau, A. Joux, and N. Kharchenko, "On a dual/hybrid approach to small secret LWE—A dual/enumeration technique for learning with errors and application to security estimates of FHE schemes," in *Proc. Int. Conf. Cryptol. India*, 2020, pp. 440–462. [Online]. Available: https://api.semanticscholar.org/CorpusID:219332962
[43] M. Afaneh. (Apr. 2023). *Bluetooth 5 Speed: How to Achieve Maximum Throughput for Your BLE Application*. [Online]. Available: https://novelbits.io/bluetooth-5-speed-maximum-throughput/
[44] H. Xu, Z. Yan, B. Li, and M. Yang, "Modeling and analysis of the performance for Bluetooth low energy," *IEEE Commun. Lett.*, vol. 28, no. 3, pp. 732–736, Mar. 2024, doi: 10.1109/LCOMM.2024.3352545.
[45] M. Woolley, "Bluetooth core 5.0 feature enhancements," Version 1.1.1, Bluetoot SIG, INC., Tech. Rep., Jan. 2025. [Online]. Available: https://www.bluetooth.com/bluetooth-resources/bluetooth-core-5-0-go-faster-go-further/
[46] *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography*, document FIPS 800-56A, National Institute of Standard and Technology, NIST, 2018, doi: 10.6028/NIST.SP.800-56Ar3.
[47] *Digital Signature Standard (DSS)*, FIPS 186-5, NIST, Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography, Feb. 2023, doi: 10.6028/NIST.FIPS.186-5.

M. A. GONZÁLEZ DE LA TORRE received the Graduate degree in mathematics from the University of Salamanca, in 2019, and the master's degree in teaching and in mathematics from the University of Granada. He is currently pursuing the Ph.D. degree with the GiCSI Group. He is currently working under contract with Consejo Superior de Investigaciones Científicas (CSIC), has been being part of the GiCSI Group, since 2021. His research interest includes post-quantum cryptography, in particular lattice-based cryptosystems.

I. A. MORALES SANDOVAL (Graduate Student Member, IEEE) received the B.Sc. degree in electrical and computer engineering from Constructor University, Bremen, Germany, in 2018, where he is currently pursuing the Ph.D. degree in electrical engineering. His research interests include signal processing, wireless physical layer key generation for resource constrained devices, and wireless physical layer secrecy maximization and authentication schemes.

G. T. FREITAS DE ABREU (Senior Member, IEEE) received the D.Eng. degree in physics, electrical, and computer engineering from Yokohama National University, Japan, in March 2004. He was a Postdoctoral Fellow and later an Adjunct Professor (Docent) in statistical signal processing and communications theory with the Department of Electrical and Information Engineering, University of Oulu, Finland, from 2004 to 2006 and from 2006 to 2011, respectively. Since 2011, he has been a Professor in electrical engineering with Constructor University, Bremen, Germany. From April 2015 to August 2018, he simultaneously held a full professorship with the Department of Computer and Electrical Engineering, Ritsumeikan University, Japan. His research interests include communications and signal processing, including communications theory, estimation theory, statistical modeling, wireless localization, cognitive radio, wireless security, MIMO systems, ultrawideband and millimeter wave communications, full-duplex and cognitive radio, compressive sensing, energy harvesting networks, random networks, and connected vehicles networks.

L. HERNÁNDEZ ENCINAS is currently pursuing the Ph.D. degree in mathematics with the University of Salamanca, Spain. He is currently a Research Professor with the Institute of Physical and Information Technologies "Leonardo Torres Quevedo" of Spanish National Research Council, Madrid. He has participated in many research projects and is the author of several books and patents, more than 70 articles in JCR-listed journals, and more than 150 contributions to workshops and conferences. He has supervised several doctoral theses. He is a member of various national and international committees on security and cybersecurity and is a Cryptological Adviser for Spanish national security agencies. His research interest includes pre- and post-quantum cryptology. He received the National Prize "CCN-2021 for Professional Career in Favor of Cybersecurity" from Spanish Ministry of Defense, and the "Cross of Police Merit with White Badge" Award by the Spanish Ministry of Home Office, in 2022.