IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 4, 2020, accepted February 27, 2020, date of publication March 2, 2020, date of current version March 16, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2977607

Analysis of Error Dependencies on Newhope

MINKI SONG[1], SEUNGHWAN LEE[1], DONG-JOON SHIN[1], (Senior Member, IEEE), EUNSANG LEE[2], YOUNG-SIK KIM[3], (Member, IEEE), AND JONG-SEON NO[2], (Fellow, IEEE)

[1]Department of Electronics and Computer Engineering, Hanyang University, Seoul 04763, South Korea
[2]Department of Electrical and Computer Engineering, Institute of New Media and Communications (INMC), Seoul National University, Seoul 08826, South Korea
[3]Department of Information and Communication Engineering, Chosun University, Gwangju 61452, South Korea

Corresponding author: Dong-Joon Shin (djshin@hanyang.ac.kr)

This work was supported by the Samsung Research Funding and Incubation Center of Samsung Electronics under Project SRFC-IT1801-08.

ABSTRACT Among many submissions to NIST post-quantum cryptography (PQC) project, NewHope is a promising key encapsulation mechanism (KEM) based on the Ring-Learning with errors (Ring-LWE) problem. Since NewHope is an indistinguishability (IND)-chosen ciphertext attack secure KEM by applying the Fujisaki-Okamoto transform to an IND-chosen plaintext attack secure public-key encryption, accurate calculation of decryption failure rate (DFR) is required to guarantee resilience against attacks that exploit decryption failures. However, the current upper bound (UB) on DFR of NewHope is rather loose because the compression noise, the effect of encoding/decoding of NewHope, and the approximation effect of centered binomial distribution are not fully considered. Furthermore, since NewHope is a Ring-LWE based cryptography, there is a problem of error dependency among error coefficients, which makes accurate DFR calculation difficult. In this paper, we derive much tighter UB on DFR than the current UB by using constraint relaxation and union bound. Especially, the above-mentioned factors are all considered in the derivation of new UB and the centered binomial distribution is not approximated. Since the error dependency is also considered, the new UB is much closer to the real DFR than the current UB. Furthermore, the new UB is parameterized by using Chernoff-Cramer bound to facilitate the calculation of new UB for the parameters of NewHope. Since the new UB is much lower than the DFR requirement of PQC, this DFR margin can be used to improve NewHope. As a result, the security level and bandwidth efficiency of NewHope are improved by 7.2 % and 5.9 %, respectively.

INDEX TERMS Bandwidth efficiency, Chernoff-Cramer bound, decryption failure rate, error dependency, key encapsulation mechanism, lattice-based cryptography, NewHope, NIST, post-quantum cryptography, relaxation, ring-learning with errors, security, union bound, upper bound.

I. INTRODUCTION

Current public-key algorithms based on integer factorization, discrete logarithm, and elliptic curve discrete logarithm problems (e.g, RSA and elliptic curve cryptography) have been unlikely to be broken by currently available technology. However, with the advent of quantum computing technology such as Shor's quantum algorithm for integer factorization, current public-key algorithms can be easily broken. For that reason, in order to avoid such a security problem of future systems, new public-key algorithms called post-quantum cryptography (PQC) should be developed to replace the existing public-key algorithms. Therefore, the National Institute of Standards and Technology (NIST) has recently begun a PQC project to identify and evaluate post-quantum public-key algorithms secure against quantum computing [1]. Among the various PQC candidates, lattice-based cryptography has become one of the most promising candidate algorithms for post-quantum key exchange. Lattice-based cryptography has been developed based on worst-case assumptions about lattice problems that are believed to be resistant to quantum computing.

Among various lattice problems, learning with errors (LWE) problem introduced by Regev in 2005 [2] has been widely analyzed and used. Furthermore, the Ring-LWE problem presented by Lynbashevsky, Peikert, and Regev in 2010 [3], which improves the computational and implementation efficiency of LWE, has also been widely used [4]–[8]. NewHope has been proposed by Alkim *et al.* [9], [10], which is one of the various cryptosystems based on Ring-LWE. NewHope has attracted a lot of attention [11]–[13] and it was

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

verified in an experiment of Google [14]. The key reasons that NewHope attracts so much attention are the use of simple and practical noise distribution, a centered binomial distribution, and a proper choice of ring parameters for better performance and security.

NewHope is an indistinguishability (IND)-chosen ciphertext attack (CCA) secure key encapsulation mechanism (KEM) that exchanges the shared secret key based on the IND-chosen plaintext attack (CPA) secure public-key encryption (PKE). Note that the IND-CPA secure PKE can be transformed into the IND-CCA secure KEM by using Fujisaki-Okamoto (FO) transform [15]. The IND-CCA secure KEM obtained by applying FO transform to IND-CPA secure PKE requires a very low decryption failure rate (DFR) because an attacker can exploit the decryption failure [15], [16]. Therefore, the DFR of NewHope should be lower than 2^{-128} to make sure of resilience against attacks that exploit decryption failures. Note that as in Frodo [5] and Kyber [6], this study aims to achieve the DFR lower than 2^{-140} to allow enough margin in NewHope. In [4], [9], an upper bound on DFR of NewHope is derived but this upper bound on DFR is rather loose because the compression noise, the effect of encoding/decoding of NewHope, and the approximation effect of centered binomial distribution are not fully considered. Furthermore, according to [20], [21], accurate calculation of DFR is very difficult because there is a problem of error dependency in Ring-LWE based cryptography. However, the DFR of IND-CCA secure KEM obtained by applying FO transform to IND-CPA secure PKE must be calculated as accurately as possible because DFR is closely related to the security.

In this paper, an upper bound on DFR of NewHope, which is much closer to the real DFR than the current upper bound on DFR derived in [4], [9], is derived by considering the above-ignored factors. Also, the centered binomial distribution is not approximated to the subgaussian distribution. Especially, the new upper bound on DFR considers the error dependency among error coefficients by using the constraint relaxation, which is an approximation of a difficult problem to a nearby problem that is easier to solve, and union bound. Furthermore, the new upper bound is parameterized by using Chernoff-Cramer (CC) bound in order to facilitate the calculation of the new upper bound for the parameters of NewHope. Since the new upper bound on DFR of NewHope is much lower than the DFR requirement of PQC, this DFR margin is used to improve the security and bandwidth efficiency where the improvement in bandwidth efficiency is realized by reducing the ciphertext size.

II. SUMMARY OF NEWHOPE

A. PARAMETERS

There are three important parameters in NewHope: n, q, and k.

- n: the dimension $n = 512$ or 1024 for NewHope guarantees the security properties of Ring-LWE and enables efficient number theoretic transform (NTT) [18].
- q: the modulus $q = 12289$ is determined to support security and efficient NTT and it is closely related with the bandwidth.
- k: the noise parameter $k = 8$ is the parameter of centered binomial distribution, which determines the noise strength and hence directly affects the security and DFR [4].

B. NOTATIONS

- $\mathcal{R}_q = \mathbb{Z}_q[x]/(X^n + 1)$: the ring of integer polynomials modulo $X^n + 1$ where each coefficient is reduced modulo q.
- $a \xleftarrow{\$} \chi$: the sampling of $a \in \mathcal{R}_q$ following the probability distribution χ over $\mathcal{R}_q$.
- ψ_k: the centered binomial distribution with parameter k, which is practically realized by $\sum_{i=0}^{k-1}(b_i - b'_i)$, where b_i and b'_i are uniformly and independently sampled from $\{0, 1\}$. The variance of ψ_k is $k/2$ [4].
- $a \circ b$: the coefficient-wise product of polynomials a and b.

C. NEWHOPE PROTOCOL

NewHope is a lattice-based KEM for Alice (Server) and Bob (Client) to share 256-bit secret key with each other. The protocol of NewHope is briefly explained based on Fig. 1 as follows, where the functions are the same ones as defined in [4].

Step	Alice (Server)		Bob (Client)
1	$\overset{\$}{seed} \leftarrow \{0,1,\ldots,255\}^{32}$ $z \leftarrow SHAKE256(64, seed)$ $\hat{a} \leftarrow GenA(z[0:31])$		
2	$\overset{\$}{s, e} \leftarrow \Psi_k^n$ $\hat{s} \leftarrow NTT(s)$ $\hat{e} \leftarrow NTT(e)$ $sk \leftarrow EncodePolynomial(\hat{s})$		$\overset{\$}{s', e', e''} \leftarrow \Psi_k^n$ $\hat{t} \leftarrow NTT(s')$
3	$\hat{b} \leftarrow \hat{a} \circ \hat{s} + \hat{e}$	$pk = EncodePK(\hat{b}, z[0:31])$ ⟶	$(\hat{b}, z[0:31]) = DecodePK(pk)$ $\hat{a} \leftarrow GenA(z[0:31])$
4			$\overset{\$}{\mu} \leftarrow \{0,1,\ldots,255\}^{32}$ $v \leftarrow Encode(\mu)$
5			$\hat{u} \leftarrow \hat{a} \circ \hat{t} + NTT(e')$ $v' \leftarrow NTT^{-1}(\hat{b} \circ \hat{t}) + e'' + v$
6	$(\bar{u}, h) \leftarrow DecodeC(c)$ $\hat{s} \leftarrow DecodePolynomial(sk)$ $v'_{decomp} \leftarrow Decompress(h)$ $v'' \leftarrow v'_{decomp} - NTT^{-1}(\bar{u} \circ \hat{s})$	$c = EncodeC(\bar{u}, h)$ ⟵	$h \leftarrow Compress(v')$
7	$\mu \leftarrow Decode(v'')$		

FIGURE 1. NewHope Protocol.

Step 1) $seed \xleftarrow{\$} \{0, 1, \ldots, 255\}^{32}$ denotes a uniform sampling of 32-byte arrays (corresponding to 256 bits) with 32 integer elements selected between 0 and 255 by using a random number generator. Then $SHAKE256(l, d)$, a strong hash function [19], takes an integer l that specifies the number of output bytes and a byte array d as its input. In NewHope, $z \leftarrow SHAKE256(64, seed)$ denotes that 32-byte arrays ($seed$) are hashed to generate 64 pseudorandom byte arrays (z) with 64 integer elements uniformly selected between 0 and 255. Then $GenA$ expands 32-pseudorandom-byte arrays $z[0:31]$

using *SHAKE*128 hash function [19] to generate the polynomial $\hat{a} \in \mathcal{R}_q$ where $z[0:31]$ is the first 32-byte arrays of z. Since $\hat{a}$ is generated from the *seed* sampled following a uniform distribution, the coefficients of $\hat{a}$ also follow a uniform distribution on $[0, q-1]$.

Step 2) Generate polynomials (s, s', e, e', $e'' \in \mathcal{R}_q$) whose coefficients are sampled following the centered binomial distribution ψ_k. The polynomials (s, s', e) are transformed to ($\hat{s}$, $\hat{t}$, $\hat{e}$), respectively, by applying NTT for efficient polynomial multiplication. Then Alice transforms the secret key ($\hat{s}$) into byte arrays using *EncodePolynomial*() which converts the polynomial ($\hat{s}$) into 2048-byte arrays.

Step 3) Alice creates a public key (pk) by converting $\hat{b} = \hat{a} \circ \hat{s} + \hat{e}$ and $z[0:31]$ into 1824-byte arrays by using *EncodePK*(), and transmits (pk) to Bob. Then Bob transforms the received public key (pk) into ($\hat{b}$, $z[0:31]$) using *DecodePK*(), and creates ($\hat{a}$) which is the same ($\hat{a}$) generated in Step 1.

Step 4) A 256-bit shared secret key (μ) is created and encoded by ATE encoder to generate a 1024-symbol codeword v.

Step 5) Generate a ciphertext ($\hat{u}$, v') by using the public key components $\hat{b}$, $\hat{a}$, the various errors $\hat{t}$, e', e'' and v.

Step 6) To efficiently reduce bandwidth, compression is performed on the coefficients of v' to generate the polynomial h, and then the ciphertext polynomials ($\hat{u}$, h) are transformed into the byte arrays c by using *EncodeC*(), and c is transmitted to Alice. Alice performs decompression on $\hat{h}$ to restore v'. However, this decompressed polynomial v'_{decomp} is different from v' generated in Step 5, due to the loss from compression and decompression. Alice creates v'' by using the received ciphertext c and sk generated in Step 2. Each coefficient of v'' is a sum of the corresponding coefficients of v and errors. Note that v'' is not a polynomial used in NewHope, but it is added in Fig. 1 for an easy explanation of the results in this paper.

Step 7) The 256-bit shared secret key (μ) is recovered (or decrypted) from the coefficients of v'' by performing the decoding of ATE.

III. UNDERSTANDING NEWHOPE AS A DIGITAL COMMUNICATION SYSTEM

A. NEWHOPE AS A DIGITAL COMMUNICATION SYSTEM

In order to facilitate analysis of DFR of NewHope, it is much more convenient to understand the protocol of NewHope as a digital communication system. For NewHope, the mapping $\mathbb{Z}_2^{256} \rightarrow \mathbb{Z}_2^n$ ($\mu \rightarrow \mu_{enc}$) and the mapping $\mathbb{Z}^n \rightarrow \mathbb{Z}_2^{256}$ ($\mu'_{enc} \rightarrow \mu'$) through ATE, $n = 512$ or 1024, can be regarded as encoding and decoding of ECC, respectively. Also, the mapping $\mathbb{Z}_2^n \rightarrow \mathcal{R}_q$ ($\mu \rightarrow v$) and $\mathcal{R}_q \rightarrow \mathbb{Z}^n$ ($v'' \rightarrow \mu'_{enc}$) through ATE can be regarded as modulation and demodulation, respectively. Then NewHope can be understood as a digital communication system as follows.

Bob and Alice are transmitter and receiver, respectively, and the 256-bit shared secret key (μ) is a message bit stream. Also, the process of transmitting and receiving messages (steps 4, 5, 6, and 7) can be viewed as a digital communication channel. In more detail, the transmitter (Bob) generates a 256-bit message bit stream, encodes this message into a n-bit codeword, modulates each codeword bit to a symbol of $\mathbb{Z}_q$, and transmits the resulting signal (step 4). At the receiver (Alice), the received signal through the noisy channel is demodulated and decoded (step 7). For NewHope, a process of adding the compression noise and the difference noise generated in Steps 5 and 6 can be regarded as a noisy communication channel. This overall process in steps 4-7 can be described as a digital communication system shown in Fig. 2.

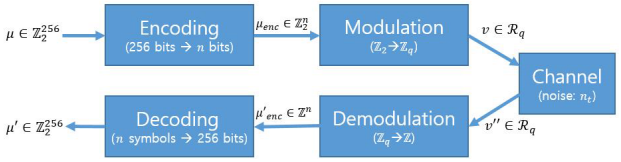


FIGURE 2. An interpretation of NewHope as a digital communication system ($n = 512$ or 1024).

In Fig. 2, μ_{enc} is the encoded signal of μ by applying an encoding of ATE, and n_t represents the overall noise generated in steps 5 and 6, which is called the total noise n_t. After interpreting NewHope as a digital communication system, the DFR in NewHope is equivalent to the block error rate $Pr(\mu \neq \mu')$ in a digital communication system. Therefore, in order to calculate the tight upper bound on DFR of NewHope, the exact analysis of encoding/modulation and decoding/demodulation of NewHope and the noisy channel is required. In the following subsection 3.2, each operation in Fig. 2 is explained in detail and analyzed.

B. ANALYSIS OF ENCODING/MODULATION AND DECODING/DEMODULATION AND CHANNEL NOISE OF NEWHOPE

1) ANALYSIS OF ENCODING/MODULATION AND DECODING/DEMODULATION OF NEWHOPE: ATE

In NewHope, ATE is used to encode and modulate a message bit μ_i, and decode and demodulate an erroneous message bit v''_i. Note that ATE performs both encoding/decoding as an ECC and modulation/demodulation. The encoding/modulation and decoding/demodulation procedures of ATE with the m-repetition are shown in Algorithms 1 and 2 where $m = 4$ for $n = 1024$ and $m = 2$ for $n = 512$ [17]. The encoding of ATE is performed such that one message bit μ_i is repeated m times and the modulation of ATE is a mapping of each bit to an element of $\mathbb{Z}_q$ (usually either 0 or $\lfloor \frac{q}{2} \rfloor$) as the coefficients of v where $\lfloor x \rfloor$ is a floor function that outputs the greatest integer less than or equal to x. Note that the m-repetition is the same operation as the encoding of an m-repetition code. The demodulation of ATE is to calculate the absolute value of the difference between the received erroneous symbol v''_i and $\lfloor q/2 \rfloor$ over integer domain $\mathbb{Z}$. The decoding of ATE is to sum up m absolute values corresponding to the same $\mu'_{enc,i+256l}, \forall l \in [0, m-1]$ to generate $\mu'_{s,i}$ and

Algorithm 1 Encoding of ATE

Input μ, m
Output v
1: **for** $i = 0$ to $\lfloor \frac{n}{m} \rfloor - 1$ **do**
2: **for** $j = 0$ to $m - 1$ **do**
3: $v_{i+\lfloor n/m \rfloor \cdot j} = \mu_i \cdot \lfloor \frac{q}{2} \rfloor$
4: **end for**
5: **end for**
6: **return** v

Algorithm 2 Decoding of ATE

Input v'', m
Output μ'
1: **for** $i = 0$ to $\lfloor \frac{n}{m} \rfloor - 1$ **do**
2: $\mu'_{s,i} = 0$
3: **for** $j = 0$ to $m - 1$ **do**
4: $\mu'_{s,i} = \mu'_{s,i} + |v''_{i+\lfloor n/m \rfloor \cdot j} - \lfloor \frac{q}{2} \rfloor|$
5: **end for**
6: **if** $\mu'_{s,i} < \frac{m \cdot q}{4}$ **then**
7: $\mu'_i = 1$
8: **else**
9: $\mu'_i = 0$
10: **end if**
11: **end for**
12: **return** μ'

compare it with the decision threshold $m \cdot q/4$ to determine if the estimate μ'_i of μ_i is 0 or 1 as follows.

$$\mu'_{s,i} \underset{\mu'_i=1}{\overset{\mu'_i=0}{\gtrless}} \frac{m \cdot q}{4} \tag{1}$$

2) ANALYSIS OF CHANNEL NOISE OF NEWHOPE

Total noise n_t, which is denoted as the channel noise of NewHope, is defined as the noise contained in the received signal v'' except the transmitted signal v. The i-th coefficient $n_{t,i}$ of the total noise polynomial n_t contained in the polynomial v'' in step 6 is expressed as follows.

$$\begin{aligned} n_{t,i} &= (v'' - v)_i \\ &= (v'_{decomp} - us - v)_i \\ &= (v' + n_c - us - v)_i \\ &= (bs' + e'' - ass' - e's)_i + n_{c,i} \\ &= (es' - e's + e'')_i + n_{c,i} \\ &= n_{d,i} + n_{c,i}, \end{aligned} \tag{2}$$

where $(\cdot)_i$ denotes the ith coefficient of the given polynomial, $n_c \in \mathcal{R}_q$ is the compression noise polynomial, $n_{c,i}$ is the ith coefficient of n_c, $n_d \in \mathcal{R}_q$ is the difference noise polynomial, and $n_{d,i}$ is the ith coefficient of n_d.

To analyze the compression noise $n_{c,i}$, we first need to investigate the coefficient of the polynomial $v' = ass' + es' + e''$ being compressed, where the coefficients of s, s', e, and e'' follow the predetermined centered binomial distribution. However, since the coefficients of polynomial a follow a uniform distribution, the coefficient of the compressed polynomial h will eventually follow a uniform distribution. A compression to v' is performed by applying $\lfloor v'_i \cdot r/q \rceil$ to the coefficients v'_i of v' to generate the coefficient h_i of h, where $\lfloor x \rceil$ is a rounding function that rounds x to the closest integer, r denotes the compression rate on v', and $r = 8$ for NewHope. Then the range of the compressed coefficients h_i of h is changed from $[0, q-1]$ to $[0, r-1]$ so that the number of bits required to store a coefficient is reduced from 14 bits ($= \lceil \log_2 q \rceil$) for v' to 3 bits ($= \lceil \log_2 r \rceil$) for NewHope with $r = 8$. Note that the smaller the value of r is, the more compression is performed. Decompression is performed by applying $\lfloor h_i \cdot q/r \rceil$ to each of the coefficients of h. Then the coefficient takes the value from 0, $\lfloor q/r \rceil$,$\lfloor 2q/r \rceil$ …, and $\lfloor (r-1) \cdot q/r \rceil$. This compression and decompression are illustrated in Fig. 3, where the coefficients v'_i of v' from different patterns (or ranges) are mapped to different $v_{decomp,i}$ values through compression and decompression. In the end, compression and decompression can be seen as a rounding operation. Therefore, the compression noise is inevitably generated with the maximum magnitude of $\lfloor q/2r \rfloor$ and the distribution $D_c(x)$ of the compression noise is derived as follows:

$$D_c(x) = \begin{cases} q/r, & 0 \le x \le \lceil \frac{q}{2r} \rceil - 1 \\ 0, & \text{otherwise} \\ q/r, & q - 2 - \lceil \frac{q}{2r} \rceil \le x \le q - 1. \end{cases} \tag{3}$$

To analyze the difference noise $n_{d,i} = (es' - e's + e'')_i$, we use the fact that the coefficients of e, e', e'', s, and s' are independent and identically distributed (*i.i.d.*) following the same centered binomial distribution. In order to derive the distribution of coefficient $n_{d,i}$ of n_d, a number of convolution operations are required because it is a sum of many *i.i.d.* random variables, each of which is obtained by multiplying two *i.i.d.* random variables following the centered binomial distribution. However, since it is difficult to calculate the multiple convolutions of the above distribution in closed form, the distribution of difference noise is numerically calculated [13].

Total noise is a sum of compression noise and difference noise which are independently generated. Thus, the distribution of total noise is obtained by performing a convolution of the distributions of compression noise and difference noise as shown in Fig. 4. Unfortunately, due to the error dependency among total noise coefficients $n_{t,i}$, the distribution of only one

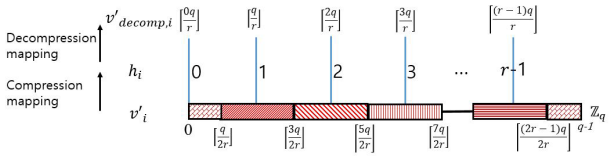


FIGURE 3. Compression and decompression mapping in NewHope.

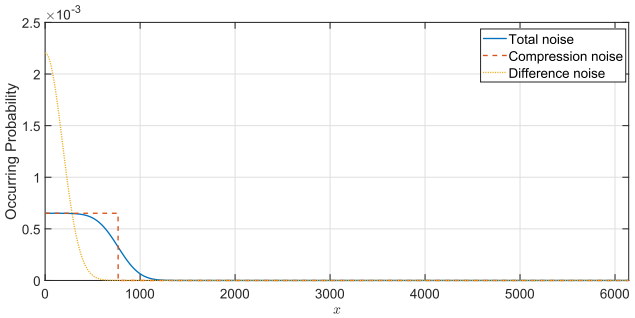


FIGURE 4. Distributions of total noise, compression noise, and difference noise of NewHope, where $0 \le x \le \lfloor \frac{q}{2} \rfloor$ (These distributions are symmetric with respect to $\lfloor \frac{q}{2} \rfloor$ where $q = 12289$).

total noise coefficient cannot be used to calculate the accurate DFR or derive a better upper bound on DFR [20], [21].

IV. DFR ANALYSIS OF NEWHOPE BY CONSIDERING ERROR DEPENDENCY

In this paper, a new upper bound on DFR of NewHope, which is much tighter than the upper bound given in [4], [9], is derived by considering the total noise in section 3 and the centered binomial distribution without doing subgaussian approximation. More importantly, the error dependency is considered in deriving an upper bound on DFR by using the constraint relaxation, which is an approximation of a difficult problem to a nearby problem that is easier to solve, and union bound.

A new upper bound on DFR of NewHope is derived by dividing the error dependency into two types as shown in Fig. 5. The first type of error dependency is analyzed for the output bit of one ATE decoder to derive an upper bound on the BER $\Pr(\mu_i \neq \mu_i')$. In this case, the error dependencies among m inputs are considered. Note that the analysis of one ATE decoder is good enough because all 256 ATE decoders are statistically identical. The analysis of the second type of error dependency is performed on 256 output bits μ_i' of ATE decoders to derive an upper bound on DFR $Pr(\mu \neq \mu')$ of NewHope. In this case, the error dependencies among 256 bits μ_i' are considered.

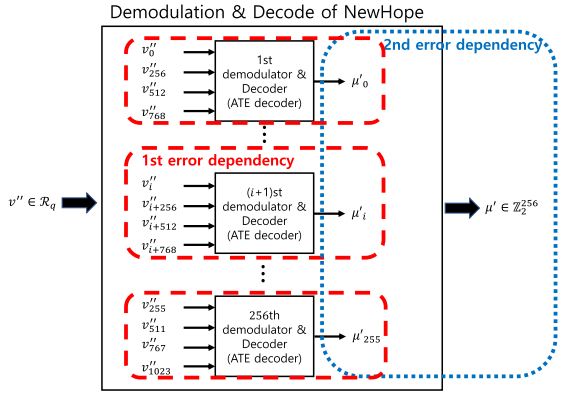


FIGURE 5. Two types of error dependency in the demodulation and decode of NewHope.

A. PROPOSE UPPER BOUND ON BER OF NEWHOPE

Suppose that $\Pr(\mu_i = 0) = \Pr(\mu_i = 1) = 1/2$, then the BER $\Pr(\mu_i \neq \mu_i')$ is average of two conditional probabilities depending on μ_i.

$$\begin{aligned}\Pr(\mu_i \neq \mu_i') &= \Pr\Big(\{\mu_i \neq \mu_i'\} \cap \{\mu_i = 0\}\Big) \\ &\quad + \Pr\Big(\{\mu_i \neq \mu_i'\} \cap \{\mu_i = 1\}\Big) \\ &= \frac{1}{2}\Big(\Pr(\mu_i \neq \mu_i' | \mu_i = 0) \\ &\quad + \Pr(\mu_i \neq \mu_i' | \mu_i = 1)\Big). \end{aligned} \tag{4}$$

Since $\Pr(\mu_i \neq \mu_i' | \mu_i = 0)$ and $\Pr(\mu_i \neq \mu_i' | \mu_i = 1)$ are statistically identical, we will analysis the BER given $\mu_i = 1$. Then the total noise given $\mu_i = 1$ is defined by $n_{t,i}^{\mu_i=1} = (n_{t,i} + \mu_{enc,i}\lfloor \frac{q}{2} \rfloor) \bmod q$ where $\mu_{enc,i} = 1$. The output $\mu_{s,i}'$ of decoding/demodulation of NewHope, which is defined in section 3.2, is determined by m dependent coefficients of v'' given $\mu_i = 1$ as follows:

$$\begin{aligned}\mu_{s,i}' &= \sum_{l=0}^{m-1} \left| n_{t,i+256l}^{\mu_i=1} - \left\lfloor \frac{q}{2} \right\rfloor \right|, \\ &= \sum_{l=0}^{m-1} \left| \left(n_{t,i+256l} + \left\lfloor \frac{q}{2} \right\rfloor \right) \bmod q - \left\lfloor \frac{q}{2} \right\rfloor \right| \end{aligned} \tag{5}$$

where $\mu_{s,i}' \in \mathbb{Z}$.

In NewHope, most operations are performed over $\mathcal{R}_q = \mathbb{Z}_q[x]/(X^n + 1)$, but for the convenience of analysis, we consider the two domains $\mathbb{Z}$ and $\mathbb{Z}_q$, and express the polynomials e, s, e', s', e'', and n_c in $\mathcal{R}_q = \mathbb{Z}_q[x]/(X^n + 1)$ by the vectors $\mathbf{e}$, $\mathbf{s}$, $\mathbf{e}'$, $\mathbf{s}'$, $\mathbf{e}''$, and $\mathbf{n}_c$ in $\mathbb{Z}^{n\times 1}$. Then, it is clear that $\mathbf{e}$, $\mathbf{s}$, $\mathbf{e}'$, $\mathbf{s}'$, $\mathbf{e}'' \in \mathbb{Z}^{n\times 1}$ are the random vectors following the centered binomial distribution with the parameter $k = 8$ and $n_c \in \mathbb{Z}^{n\times 1}$ is the random vector following the uniform distribution over the support $[-\lfloor \frac{q}{2r} \rfloor, \lfloor \frac{q}{2r} \rfloor]$. To express the product $\circ$ of two polynomials over $\mathcal{R}_q$ for the corresponding vectors over $\mathbb{Z}^{n\times 1}$, we define a new operation $\odot$, which is called cyclic shift product, as follows:

$$\begin{aligned}(e \circ s)_i &= (\mathbf{e} \odot \mathbf{s})_i \\ &= \sum_{j=0}^{n-1} \mathrm{sgn}(i-j) e_j s_{(i-j) \bmod n}, \end{aligned} \tag{6}$$

where $\mathrm{sgn}(x) = 1$ when $x \ge 0$, otherwise $\mathrm{sgn}(x) = -1$. For examples, if $n = 4$,

$$(\mathbf{e} \odot \mathbf{s})_0 = \begin{bmatrix} e_0 \\ e_1 \\ e_2 \\ e_3 \end{bmatrix}^T \begin{bmatrix} +s_0 \\ -s_3 \\ -s_2 \\ -s_1 \end{bmatrix}, \quad (\mathbf{e} \odot \mathbf{s})_1 = \begin{bmatrix} e_0 \\ e_1 \\ e_2 \\ e_3 \end{bmatrix}^T \begin{bmatrix} +s_1 \\ +s_0 \\ -s_3 \\ -s_2 \end{bmatrix},$$

$$(\mathbf{e} \odot \mathbf{s})_2 = \begin{bmatrix} e_0 \\ e_1 \\ e_2 \\ e_3 \end{bmatrix}^T \begin{bmatrix} +s_2 \\ +s_1 \\ +s_0 \\ -s_3 \end{bmatrix}, \quad (\mathbf{e} \odot \mathbf{s})_3 = \begin{bmatrix} e_0 \\ e_1 \\ e_2 \\ e_3 \end{bmatrix}^T \begin{bmatrix} +s_3 \\ +s_2 \\ +s_1 \\ +s_0 \end{bmatrix},$$

where $(\cdot)^T$ denotes the transpose of vector. Using the newly defined vectors $\mathbf{e}$, $\mathbf{s}$, $\mathbf{e}'$, $\mathbf{s}'$, $\mathbf{e}''$, $\mathbf{n}_c$ and operation $\odot$, $\mu'_{s,i}$ in (5) can be expressed as:

$$\begin{aligned}\mu'_{s,i} &= \sum_{l=0}^{m-1}\left|\left(n_{t,i+256l}+\left\lfloor\frac{q}{2}\right\rfloor\right) \bmod q-\left\lfloor\frac{q}{2}\right\rfloor\right| \\ &= \sum_{l=0}^{m-1}\left|n^*_{t,i+256l}-q\alpha_{i+256l}\right|, \end{aligned} \tag{7}$$

where $n^*_{t,i}=(\mathbf{e}\odot\mathbf{s}')_i-(\mathbf{e}'\odot\mathbf{s})_i+\mathbf{e}''_i+\mathbf{n}_{c,i}$ and α_i is an arbitrary integer making $n_{t,i}$ be in $[-\lfloor\frac{q}{2}\rfloor,\lfloor\frac{q}{2}\rfloor]$ where $n_{t,i}=n^*_{t,i} \bmod q-\lfloor q/2\rfloor$ and $|\alpha_i|\le\lfloor(2nk^2+k+(q-1)/r)/q\rfloor$. For example, if $|n^*_{t,i}|\le\lfloor\frac{q}{2}\rfloor$, then $\alpha_i=0$. Finally, under the assumption that an all-one message bit is transmitted, the event of bit error is equivalent to the following inequality.

$$T_m\le\sum_{l=0}^{m-1}|n^*_{t,i+256l}-q\alpha_{i+256l}|\le 2T_m, \tag{8}$$

where $T_m=\frac{m}{2}\lfloor\frac{q}{2}\rfloor$ is the decision threshold of ATE and $2T_m$ is a maximum value of $\sum_{l=0}^{m-1}|n^*_{t,i+256l}-q\alpha_{i+256l}|$.

In order to find the support satisfying (8), some sets and vector should be defined. Let Ω be the support of $\mathbf{e}$, $\mathbf{s}$, $\mathbf{e}'$, $\mathbf{s}'$, $\mathbf{e}''$, $\mathbf{n}_c$ where $\Omega=\text{supp}(\mathbf{e},\mathbf{s},\mathbf{e}',\mathbf{s}',\mathbf{e}'',\mathbf{n}_c)=\{\mathbf{e},\mathbf{s},\mathbf{e}',\mathbf{s}',\mathbf{e}'',\mathbf{n}_c|\mathbf{e},\mathbf{s},\mathbf{e}',\mathbf{s}',\mathbf{e}''\in[-k,k]^{n\times1},\mathbf{n}_c\in[-\lfloor\frac{q}{2r}\rfloor,\lfloor\frac{q}{2r}\rfloor]^{n\times1}\}$, supp$(\cdot)$ denotes the support of vector, k is parameter of the centered binomial distribution, and r is the compression rate. such that $\Pr(\Omega)=1$. Let E be the support of bit error, which is the same as the bit error event, where $E=\{\epsilon\in\Omega|T_m\le\sum_{l=0}^{m-1}|n^*_{t,i+256l}-q\alpha_{i+256l}|\le 2T_m\}$ such that $\Pr(\mu_i\neq\mu'_i)=\Pr(E)$.

Since (8) is the sum of m absolute values, it can be divided into 2^m cases. Such cases can be expressed by the following notation. Let $\mathcal{Y}=\{-1,1\}^{m\times1}$ be the set of vector whose elements are -1 or 1 so that $|\mathcal{Y}|=2^m$. Let $y^m_0,y^m_1,\ldots,y^m_{2^m-1}\in\mathcal{Y}$ be vectors included in $\mathcal{Y}$ and let $y^m_{k,l}$ denote the $(l+1)$-th element of $y^{m,k}$. For the convenience, y^m_0 is the all-one vector and the others $y^m_1,y^m_2,\ldots,y^m_{2^m-1}$ are corresponding to the remaining vectors in $\mathcal{Y}$. Then, the set Ω_k that satisfies each of 2^m cases of (8) can be defined as follows:

$$\Omega_k=\{\omega_k\in\Omega|(n^*_{t,i+256l}-q)y^m_{k,l}\ge 0,\ \forall l\in[0,m-1]\}, \tag{9}$$

where the details of Ω_k is shown in Table 1. The $\Omega_0,\Omega_1,\cdots$, and Ω_{2^m-1} are clearly disjoint set such that $\Omega=\cup_{i=0}^{2^m-1}\Omega_i$ and $\Omega_i\cap\Omega_j=\emptyset$ if $i\neq j$. If $\omega_k\in\Omega_k$, then absolute values in (8) can be replaced with y^m_k as follows:

$$\sum_{l=0}^{m-1}|n^*_{t,i+256l}-q\alpha_{i+256l}|=\sum_{l=0}^{m-1}(n^*_{t,i+256l}-q\alpha_{i+256l})y^m_{k,l}. \tag{10}$$

The support E of bit error can be partitioned into 2^m supports $E_0,E_1,\cdots$, and E_{2^m-1} by using the support Ω_k as follows:

$$E_k=\{\epsilon_k|\epsilon_k\in\Omega_k\cap E\}. \tag{11}$$

It is obvious that $E_k\subseteq\Omega_k$, $\forall j\in[0,2^m-1]$, $E_i\cap E_j=\emptyset$ if $i\neq j$, and $E=\cup_{i=0}^{2^m-1}E_i$. Also, E_k is expressed by using Ω_k as follows:

$$E_k=\left\{\epsilon_k\in\Omega_k\left|T_m\le\sum_{l=0}^{m-1}(n^*_{t,i+256l}-q\alpha_{i+256l})y^m_{k,l}\le 2T_m\right.\right\} \tag{12}$$

For the convenience of explanation, the inequality in (12) is expressed by using the new variable $\beta\in[T_m,2T_m]$ as follows:

$$\begin{aligned} T_m &\le \sum_{l=0}^{m-1}(n^*_{t,i+256l}-q\alpha_{i+256l})y^m_{k,l}\le 2T_m \\ &\Leftrightarrow \sum_{l=0}^{m-1}(n^*_{t,i+256l}-q\alpha_{i+256l})y^m_{k,l}=\beta \\ &\Leftrightarrow \sum_{l=0}^{m-1}n^*_{t,i+256l}y^m_{k,l}=q\left(\sum_{l=0}^{m-1}\alpha_{i+256l}y^m_{k,l}\right)+\beta \\ &\Leftrightarrow \sum_{l=0}^{m-1}n^*_{t,i+256l}y^m_{k,l}=qA_i+\beta, \end{aligned} \tag{13}$$

where $A_i=\sum_{l=0}^{m-1}\alpha_{i+256l}y^m_{k,l}$, A_i is fully determined by $n^*_{t,i}$, $n^*_{t,i+256}$, $n^*_{t,i+512}$, and $n^*_{t,i+768}$ for $n=1024$ or by $n^*_{t,i}$ and $n^*_{t,i+256}$ for $n=512$, and $|A_i|<m\alpha_{max}$ where $\alpha_{max}=\lfloor(2nk^2+k+(q-1)/r)/q\rfloor$. There are two constraints in (13) such that $\sum_{l=0}^{m-1}n^*_{t,i+256l}$ and β are congruent modulo q and A_i is a finite integer. Thus, E_k can be expressed as union of supports satisfying two constraints on $\sum_{l=0}^{m-1}n^*_{t,i+256l}$ and A_i as follows:

$$\begin{aligned} E_k &= \left\{\epsilon_k\in\Omega_k\left|T_m\le\sum_{l=0}^{m-1}(n^*_{t,i+256l}-q\alpha_{i+256l})y^m_{k,l}\le 2T_m\right.\right\} \\ &= \bigcup_{\beta}\left\{\epsilon_k\in\Omega_k\left|\sum_{l=0}^{m-1}n^*_{t,i+256l}y^m_{k,l}=qA_i+\beta\right.\right\} \\ &= \bigcup_{j=A_{min}}^{A_{max}}\left(\bigcup_{\beta}\left\{\epsilon_k\in\Omega_k\left|\sum_{l=0}^{m-1}n^*_{t,i+256l}y^m_{k,l}=jq+\beta\right.\right\}\right. \\ &\qquad \left.\cap\{\epsilon_k\in\Omega_k|A_i=j\}\right), \end{aligned} \tag{14}$$

where $A_{min}=-m\alpha_{max}$ and $A_{max}=m\alpha_{max}$.

In order to calculate the BER, the occurring probability $\Pr(E)$ of the bit error support E should be calculated. As above mentioned, since the support E of bit error can be disjointly partitioned, $\Pr(E)=\sum_{i=0}^{2^m-1}\Pr(E_i)$. For the description of simplicity, we first consider the support E_0 of bit error, and it can be expressed as the union of different supports on $j=0$ and $j\neq0$ as follows:

$$E_0=E_{0,j\neq0}\cup E_{0,j=0}, \tag{15}$$

where $E_{0,j\neq0}=\bigcup_{j:j\neq0}\left(\bigcup_{\beta}\{\epsilon_0\in\Omega_0|\sum_{l=0}^{m-1}n^*_{t,i+256l}=jq+\beta\}\cap\{\epsilon_0\in\Omega_0|A_i=j\}\right)$ and $E_{0,j=0}=\bigcup_{\beta}\{\epsilon_0\in$

TABLE 1. The details of support Ω_k for $m = 4$.

Support	Support condition
Ω_0	$\{\omega_0 \in \Omega \mid n^*_{t,i} - \alpha_i q \geq 0, n^*_{t,i+256} - \alpha_{i+256} q \geq 0, n^*_{t,i+512} - \alpha_{i+512} q \geq 0, n^*_{t,i+768} - \alpha_{i+768} q \geq 0\}$
Ω_1	$\{\omega_1 \in \Omega \mid n^*_{t,i} - \alpha_i q \geq 0, n^*_{t,i+256} - \alpha_{i+256} q \geq 0, n^*_{t,i+512} - \alpha_{i+512} q \geq 0, n^*_{t,i+768} - \alpha_{i+768} q < 0\}$
Ω_2	$\{\omega_2 \in \Omega \mid n^*_{t,i} - \alpha_i q \geq 0, n^*_{t,i+256} - \alpha_{i+256} q \geq 0, n^*_{t,i+512} - \alpha_{i+512} q < 0, n^*_{t,i+768} - \alpha_{i+768} q \geq 0\}$
Ω_3	$\{\omega_3 \in \Omega \mid n^*_{t,i} - \alpha_i q \geq 0, n^*_{t,i+256} - \alpha_{i+256} q \geq 0, n^*_{t,i+512} - \alpha_{i+512} q < 0, n^*_{t,i+768} - \alpha_{i+768} q < 0\}$
Ω_4	$\{\omega_4 \in \Omega \mid n^*_{t,i} - \alpha_i q \geq 0, n^*_{t,i+256} - \alpha_{i+256} q < 0, n^*_{t,i+512} - \alpha_{i+512} q \geq 0, n^*_{t,i+768} - \alpha_{i+768} q \geq 0\}$
Ω_5	$\{\omega_5 \in \Omega \mid n^*_{t,i} - \alpha_i q \geq 0, n^*_{t,i+256} - \alpha_{i+256} q < 0, n^*_{t,i+512} - \alpha_{i+512} q \geq 0, n^*_{t,i+768} - \alpha_{i+768} q < 0\}$
Ω_6	$\{\omega_6 \in \Omega \mid n^*_{t,i} - \alpha_i q \geq 0, n^*_{t,i+256} - \alpha_{i+256} q < 0, n^*_{t,i+512} - \alpha_{i+512} q < 0, n^*_{t,i+768} - \alpha_{i+768} q \geq 0\}$
Ω_7	$\{\omega_7 \in \Omega \mid n^*_{t,i} - \alpha_i q \geq 0, n^*_{t,i+256} - \alpha_{i+256} q < 0, n^*_{t,i+512} - \alpha_{i+512} q < 0, n^*_{t,i+768} - \alpha_{i+768} q < 0\}$
Ω_8	$\{\omega_8 \in \Omega \mid n^*_{t,i} - \alpha_i q < 0, n^*_{t,i+256} - \alpha_{i+256} q \geq 0, n^*_{t,i+512} - \alpha_{i+512} q \geq 0, n^*_{t,i+768} - \alpha_{i+768} q \geq 0\}$
Ω_9	$\{\omega_9 \in \Omega \mid n^*_{t,i} - \alpha_i q < 0, n^*_{t,i+256} - \alpha_{i+256} q \geq 0, n^*_{t,i+512} - \alpha_{i+512} q \geq 0, n^*_{t,i+768} - \alpha_{i+768} q < 0\}$
Ω_{10}	$\{\omega_{10} \in \Omega \mid n^*_{t,i} - \alpha_i q < 0, n^*_{t,i+256} - \alpha_{i+256} q \geq 0, n^*_{t,i+512} - \alpha_{i+512} q < 0, n^*_{t,i+768} - \alpha_{i+768} q \geq 0\}$
Ω_{11}	$\{\omega_{11} \in \Omega \mid n^*_{t,i} - \alpha_i q < 0, n^*_{t,i+256} - \alpha_{i+256} q \geq 0, n^*_{t,i+512} - \alpha_{i+512} q < 0, n^*_{t,i+768} - \alpha_{i+768} q < 0\}$
Ω_{12}	$\{\omega_{12} \in \Omega \mid n^*_{t,i} - \alpha_i q < 0, n^*_{t,i+256} - \alpha_{i+256} q < 0, n^*_{t,i+512} - \alpha_{i+512} q \geq 0, n^*_{t,i+768} - \alpha_{i+768} q \geq 0\}$
Ω_{13}	$\{\omega_{13} \in \Omega \mid n^*_{t,i} - \alpha_i q < 0, n^*_{t,i+256} - \alpha_{i+256} q < 0, n^*_{t,i+512} - \alpha_{i+512} q \geq 0, n^*_{t,i+768} - \alpha_{i+768} q < 0\}$
Ω_{14}	$\{\omega_{14} \in \Omega \mid n^*_{t,i} - \alpha_i q < 0, n^*_{t,i+256} - \alpha_{i+256} q < 0, n^*_{t,i+512} - \alpha_{i+512} q < 0, n^*_{t,i+768} - \alpha_{i+768} q \geq 0\}$
Ω_{15}	$\{\omega_{15} \in \Omega \mid n^*_{t,i} - \alpha_i q < 0, n^*_{t,i+256} - \alpha_{i+256} q < 0, n^*_{t,i+512} - \alpha_{i+512} q < 0, n^*_{t,i+768} - \alpha_{i+768} q < 0\}$

TABLE 2. The details of support Ω_k for $m = 2$.

Support	Support condition
Ω_0	$\{\omega_0 \in \Omega \mid n^*_{t,i} - \alpha_i q \geq 0, n^*_{t,i+256} - \alpha_{i+256} q \geq 0\}$
Ω_1	$\{\omega_1 \in \Omega \mid n^*_{t,i} - \alpha_i q \geq 0, n^*_{t,i+256} - \alpha_{i+256} q < 0\}$
Ω_2	$\{\omega_2 \in \Omega \mid n^*_{t,i} - \alpha_i q < 0, n^*_{t,i+256} - \alpha_{i+256} q \geq 0\}$
Ω_3	$\{\omega_3 \in \Omega \mid n^*_{t,i} - \alpha_i q < 0, n^*_{t,i+256} - \alpha_{i+256} q < 0\}$

$\Omega_0 | \sum_{l=0}^{m-1} n^*_{t,i+256l} = \beta\} \cap \{\epsilon_0 \in \Omega_0 | A_i = 0\}$. Unfortunately, it is difficult to know the exact supports of $E_{0,j\neq 0}$ and $E_{0,j=0}$, and even if they are exactly known, it is very difficult to calculate the exact occurring probabilities. Therefore, we derive the upper bounds on the occurring probabilities of each support $E_{0,j\neq 0}$ and $E_{0,j=0}$ through Theorems 1 and 2, and by using such upper bounds on $\Pr(E_{0,j\neq 0})$ and $\Pr(E_{0,j=0})$, the occurring probability $\Pr(E_0)$ can be upper bounded.

Theorem 1: The occurring probability $\Pr(E_{0,j\neq 0})$ *of* $E_{0,j\neq 0}$ *in* (15) *is at most* $m\Pr(|n^*_{t,i}| > \lfloor \frac{q}{2} \rfloor)$.

Proof: If $A_i \neq 0$, then at least one of α_i, α_{i+256}, α_{i+512}, and α_{i+768} is not zero for $n = 1024$. Similarly, for $n = 512$, if $A_i \neq 0$, then at least one of α_i and α_{i+256} is not zero. In the equation $n_{t,i} = n^*_{t,i} - \alpha_i q + \lfloor \frac{q}{2} \rfloor$, since α_i makes $n_{t,i}$ be in $[-\lfloor \frac{q}{2} \rfloor, \lfloor \frac{q}{2} \rfloor]$, $\alpha_i = 0$ if and only if $|n^*_{t,i}| \leq \lfloor \frac{q}{2} \rfloor$. Conversely, $\alpha_i \neq 0$ if and only if $|n^*_{t,i}| > \lfloor \frac{q}{2} \rfloor$. Therefore, at least one among $|n^*_{t,i}|$, $|n^*_{t,i+256}|$, $|n^*_{t,i+512}|$, and $|n^*_{t,i+768}|$ is greater than $\lfloor \frac{q}{2} \rfloor$ for $n = 1024$. Similarly, at least one among $|n^*_{t,i}|$ and $|n^*_{t,i+256}|$ is greater than $\lfloor \frac{q}{2} \rfloor$ for $n = 512$. Then, we can relax the constraint $\bigcup_\beta \{\epsilon_0 \in \Omega_0 | \sum_{l=0}^{m-1} n^*_{t,i+256l} = jq + \beta\}$ and make the superset whose occurring probability is greater than or equal to set $E_{0,j\neq 0}$ as follows:

$$
\begin{aligned}
E_{0,j\neq 0} &= \bigcup_{j:j\neq 0} \left(\bigcup_{\beta} \left\{ \epsilon_0 \in \Omega_0 \left| \sum_{l=0}^{m-1} n^*_{t,i+256l} = jq + \beta \right. \right\} \right. \\
&\qquad \left. \cap \{\epsilon_0 \in \Omega_0 | A_i = j\} \right) \\
&\subseteq \bigcup_{j:j\neq 0} \{\epsilon_0 \in \Omega_0 | A_i = j\} \\
&\subseteq \bigcup_{l=0}^{m-1} \left\{ \epsilon_0 \in \Omega_0 \left| |n^*_{t,i+256l}| > \frac{q}{2} \right. \right\}
\end{aligned}
$$

The occurring probability of $E_{0,j\neq 0}$ is bounded by using the union bound and the fact that the distributions of $n^*_{t,i}$, $\forall i \in [0, n-1]$ are identical.

$$
\begin{aligned}
\Pr(E_{0,j\neq 0}) &\leq \Pr\left(\bigcup_{l=0}^{m-1} \left\{ \epsilon_0 \in \Omega_0 \left| |n^*_{t,i+256l}| > \frac{q}{2} \right. \right\} \right) \\
&\leq \sum_{l=0}^{m-1} \Pr\left(|n^*_{t,i+256l}| > \frac{q}{2} \right) \\
&\leq m \Pr\left(|n^*_{t,i}| > \frac{q}{2} \right).
\end{aligned}
$$

□

The distribution of $n^*_{t,i}$ can be numerically calculated as shown in Fig. 6. By using the distribution of $n^*_{t,i}$, we can calculate $\Pr(E_{0,j\neq 0}) \leq 2^{-564}$ for $n = 1024$ and $\Pr(E_{0,j\neq 0}) \leq 2^{-908}$ for $n = 512$.

Theorem 2: The occurring probability of $E_{0,j=0}$ *is at most* $\Pr(T_m \leq \sum_{l=0}^{m-1} n^*_{t,i+256l} \leq 2T_m)$.

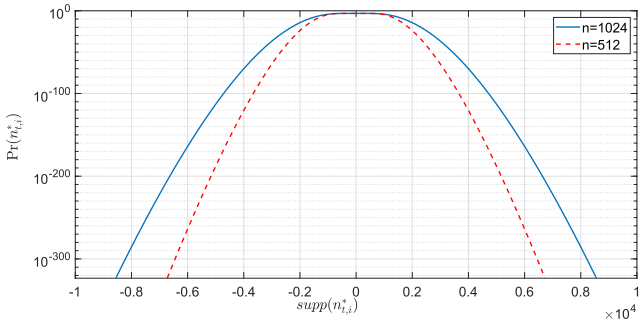


FIGURE 6. The distributions of $n^*_{t,i}$ for $n = 1024$ ($m = 4$) and $n = 512$ ($m = 2$).

Proof: If $A_i = 0$, then the superset of support of $E_{0,j=0}$ can be found by relaxing the constraints $\{\epsilon_0 \in \Omega_0 | A_i = 0\}$ as follows:

$$\begin{aligned} E_{0,j=0} &= \bigcup_{\beta} \left\{ \epsilon_0 \in \Omega_0 \left| \sum_{l=0}^{m-1} n^*_{t,i+256l} = \beta \right. \right\} \\ &\quad \cap \{\epsilon_0 \in \Omega_0 | A_i = 0\} \\ &\subseteq \bigcup_{\beta} \left\{ \epsilon_0 \in \Omega_0 \left| \sum_{l=0}^{m-1} n^*_{t,i+256l} = \beta \right. \right\}. \end{aligned}$$

The occurring probability of $E_{0,j=0}$ can be upper bounded through the union bound as follows:

$$\begin{aligned} \Pr(E_{0,j=0}) &= \Pr\left(\bigcup_{\beta} \left\{ \epsilon_0 \in \Omega_0 \left| \sum_{l=0}^{m-1} n^*_{t,i+256l} = \beta \right. \right\} \right) \\ &\leq \Pr\left(T_m \leq \sum_{l=0}^{m-1} n^*_{t,i+256l} \leq 2T_m \right). \end{aligned}$$

□

To calculate the upper bound of occurring probability $\Pr(E_0)$ through Theorems 1 and 2, the distributions of $\sum_{l=0}^{m-1} n^*_{t,i+256l}$ are required. However, since $n^*_{t,i}$, $n^*_{t,i+256}$, $n^*_{t,i+512}$, and $n^*_{t,i+768}$ for $n = 1024$ or $n^*_{t,i}$ and $n^*_{t,i+256}$ for $n = 512$ are statistically dependent to each other, it is difficult to analytically calculate the occurring probability $\Pr(E_{0,j=0})$. Also, it is not possible to numerically compute because the $\sum_{l=0}^{m-1} n^*_{t,i+256l}$ consists of the products and sums of $4n + 2m$ independent random variables. However, in this paper, the distribution of $\sum_{l=0}^{m-1} n^*_{t,i+256l}$ can be numerically computable by using the trick that decomposes $\sum_{l=0}^{m-1} n^*_{t,i+256l}$ into the sum of $2n/m + 2m$ independent random variables, which is the following Theorem 3.

Theorem 3: $\sum_{l=0}^{m-1} n^*_{t,i+256l}$ *is decomposed into the sum of* $2n/m+2m$ *independent random variables.*

Proof: We know that $n^*_{t,i} = (\mathbf{e} \odot \mathbf{s}')_i - (\mathbf{e}' \odot \mathbf{s})_i + \mathbf{e}''_i + \mathbf{n}_{c,i}$. Then,

$$\begin{aligned} \sum_{l=0}^{m-1} n^*_{t,i+256l} &= \sum_{l=0}^{m-1} (\mathbf{e} \odot \mathbf{s}')_{i+256l} - \sum_{l=0}^{m-1} (\mathbf{e}' \odot \mathbf{s})_{i+256l} \\ &\quad + \sum_{l=0}^{m-1} \mathbf{e}''_{i+256l} + \sum_{l=0}^{m-1} \mathbf{n}_{c,i+256l}. \end{aligned} \tag{16}$$

If $\sum_{l=0}^{m-1} (\mathbf{e} \odot \mathbf{s})_{i+256l}$ is decomposed into the sum of independent random vectors, $\sum_{l=0}^{m-1} n^*_{t,i+256l}$ can be also decomposed into the sum of independent random variables. An inner product of two vectors can be decomposed into the sum of inner products of sub vectors. Thus, $\sum_{l=0}^{m-1} (\mathbf{e} \odot \mathbf{s})_{i+256l}$ can be decomposed into the sum of inner products of sub vectors as follows for $n = 1024$ and $m = 4$:

$$\begin{aligned} &\sum_{l=0}^{3} (\mathbf{e} \odot \mathbf{s})_{i+256l} \\ &= \begin{bmatrix} e_0 \\ \vdots \\ e_{256} \\ \vdots \\ e_{512} \\ \vdots \\ e_{768} \\ \vdots \end{bmatrix}^T \left(\begin{bmatrix} s_0 \\ \vdots \\ -s_{768} \\ \vdots \\ -s_{512} \\ \vdots \\ -s_{256} \\ \vdots \end{bmatrix} + \begin{bmatrix} s_{256} \\ \vdots \\ s_0 \\ \vdots \\ -s_{768} \\ \vdots \\ -s_{512} \\ \vdots \end{bmatrix} + \begin{bmatrix} s_{512} \\ \vdots \\ s_{256} \\ \vdots \\ s_0 \\ \vdots \\ -s_{768} \\ \vdots \end{bmatrix} + \begin{bmatrix} s_{768} \\ \vdots \\ s_{512} \\ \vdots \\ s_{256} \\ \vdots \\ s_0 \\ \vdots \end{bmatrix} \right) \\ &= \begin{bmatrix} e_0 \\ e_{256} \\ e_{512} \\ e_{768} \end{bmatrix}^T \left(\begin{bmatrix} s_0 \\ -s_{768} \\ -s_{512} \\ -s_{256} \end{bmatrix} + \begin{bmatrix} s_{256} \\ s_0 \\ -s_{768} \\ -s_{512} \end{bmatrix} + \begin{bmatrix} s_{512} \\ s_{256} \\ s_0 \\ -s_{768} \end{bmatrix} + \begin{bmatrix} s_{768} \\ s_{512} \\ s_{256} \\ s_0 \end{bmatrix} \right) \\ &\quad + \begin{bmatrix} e_1 \\ e_{257} \\ e_{513} \\ e_{769} \end{bmatrix}^T \left(\begin{bmatrix} s_1 \\ -s_{769} \\ -s_{513} \\ -s_{257} \end{bmatrix} + \begin{bmatrix} s_{257} \\ s_1 \\ -s_{769} \\ -s_{513} \end{bmatrix} + \begin{bmatrix} s_{513} \\ s_{257} \\ s_1 \\ -s_{769} \end{bmatrix} + \begin{bmatrix} s_{769} \\ s_{513} \\ s_{257} \\ s_1 \end{bmatrix} \right) \\ &\quad \vdots \\ &\quad + \begin{bmatrix} e_{255} \\ e_{511} \\ e_{767} \\ e_{1023} \end{bmatrix}^T \left(\begin{bmatrix} s_{255} \\ -s_{1023} \\ -s_{767} \\ -s_{511} \end{bmatrix} + \begin{bmatrix} s_{511} \\ s_{255} \\ -s_{1023} \\ -s_{767} \end{bmatrix} + \begin{bmatrix} s_{767} \\ s_{511} \\ s_{255} \\ -s_{1023} \end{bmatrix} + \begin{bmatrix} s_{1023} \\ s_{767} \\ s_{511} \\ s_{255} \end{bmatrix} \right). \end{aligned}$$

It is clear that each inner product of sub vectors is a similar structure, and hence we define new random variable W_j for $n = 1024$ and $m = 4$,

$$\begin{aligned} W_j = \begin{bmatrix} e_j \\ e_{j+256} \\ e_{j+512} \\ e_{j+768} \end{bmatrix}^T \left(\begin{bmatrix} s_j \\ s_{j+768} \\ -s_{j+512} \\ -s_{j+256} \end{bmatrix} + \begin{bmatrix} s_{j+256} \\ s_j \\ -s_{j+768} \\ -s_{j+512} \end{bmatrix} \right. \\ \left. + \begin{bmatrix} s_{j+512} \\ s_{j+256} \\ s_j \\ -s_{j+768} \end{bmatrix} + \begin{bmatrix} s_{j+768} \\ s_{j+512} \\ s_{j+256} \\ s_j \end{bmatrix} \right), \end{aligned} \tag{17}$$

and for $n = 512$ and $m = 2$,

$$W_j = \begin{bmatrix} e_j \\ e_{j+256} \end{bmatrix}^T \left(\begin{bmatrix} s_j \\ -s_{j+256} \end{bmatrix} + \begin{bmatrix} s_{j+256} \\ s_j \end{bmatrix} \right). \tag{18}$$

Since W_j and $W_{j'}$ for $j \neq j'$ consist of different random variables, W_j's are clearly independent to each other. By using new random variable W_j, $\sum_{l=0}^{m-1} (\mathbf{e} \odot \mathbf{s})_{i+256l}$ can be expressed

by the sum of the independent random variables such that $\sum_{l=0}^{m-1}(\mathbf{e}\odot\mathbf{s})_{i+256l}=\sum_{j=0}^{n/m}W_j$. Thus,

$$\begin{aligned}\sum_{l=0}^{m-1}n^*_{t,i+256l}&=\sum_{l=0}^{m-1}\Big((\mathbf{e}'\odot\mathbf{s})_{i+256l}-(\mathbf{e}\odot\mathbf{s}')_{i+256l}\\&\quad+\mathbf{e}''_{i+256l}+\mathbf{n}_{c,i+256l}\Big)\\&=\sum_{j=0}^{2n/m}W_j+\sum_{l=0}^{m-1}\left(\mathbf{e}''_{i+256l}+\mathrm{n}_{c,i+256l}\right).\end{aligned}$$

Note that $(\mathbf{e}'\odot\mathbf{s})$ and $(\mathbf{e}\odot\mathbf{s}')$ are decomposed into the sum of n/m independent random variables W_j, respectively. Therefore, $n^*_{t,i}$ can be decomposed into the sum of $2n/m$ independent random variables W_j and $2m$ independent random variables of e''_i and $n_{c,i}$. □

In conclusion, by using Theorems 1, 2, and the union bound, the occurring probability $\Pr(E_0)$ of E_0 is upper bounded as follows:

$$\begin{aligned}\Pr(E_0)&=\Pr(E_{0,j\neq0}\cup E_{0,j=0})\\&\le\Pr(E_{0,j\neq0})+\Pr(E_{0,j=0})\\&\le m\Pr\left(|n^*_{t,i}|>\frac{q}{2}\right)\\&\quad+\Pr\left(T_m\le\sum_{l=0}^{m-1}n^*_{t,i+256l}\le2T_m\right).\end{aligned}$$

Next, in order to calculate the BER, $\Pr(E_1)$, $\Pr(E_2)$, $\cdots$, and $\Pr(E_{2^m-1})$ are also calculated, and they can be calculated by using following Theorem 4.

Theorem 4: The occurring probabilities $\Pr(E_k)$, $\forall k\in[0,2^m-1]$ *are at most* $m\Pr(|n^*_{t,i}|>\frac{q}{2})+\Pr(T_m\le\sum_{l=0}^{m-1}n^*_{t,i+256l}\le2T_m)$.

Proof: E_k can be expressed as a union of $E_{k,j\neq0}$ and $E_{k,j=0}$ by using y^m_k, similar to (15). First, the superset of $E_{k,j\neq0}$ can be found likewise the proof of Theorem 1. If $\sum_{l=0}^{m-1}\alpha_{i+256l}y^m_{k,l}\neq0$, then at least one among α_i, α_{i+256}, α_{i+512}, and α_{i+768} is not zero for $n=1024$. Similarly, for $n=512$, if $\sum_{l=0}^{m-1}\alpha_{i+256l}y^m_{k,l}\neq0$, then at least one among α_i and α_{i+256} is not zero. The fact implies at least one among $|n^*_{t,i}|$, $|n^*_{t,i+256}|$, $|n^*_{t,i+512}|$, and $|n^*_{t,i+768}|$ is greater than $\lfloor q/2\rfloor$. Then, we can relax the constraint $\bigcup_\beta\{\epsilon\in\Omega_k|\sum_{l=0}^{m-1}n^*_{t,i+256l}y^m_{k,l}=jq+\beta\}$ and make the superset whose occurring probability is greater than or equal to the set $E_{k,j\neq0}$ like $E_{0,j\neq0}$ as follows:

$$\begin{aligned}E_{k,j\neq0}&=\bigcup_{j:j\neq0}\left(\bigcup_\beta\left\{\epsilon_k\in\Omega_k\left|\sum_{l=0}^{m-1}n^*_{t,i+256l}y^m_{k,l}=jq+\beta\right.\right\}\right.\\&\quad\left.\cap\{\epsilon_k\in\Omega_k|A_i=j\}\right)\\&\subseteq\bigcup_{j:j\neq0}\{\epsilon_k\in\Omega_k|A_i=j\}\\&=\bigcup_{j:j\neq0}\left\{\epsilon_k\in\Omega_k\left|\sum_{l=0}^{m-1}\alpha_{i+256l}y^m_{k,l}=j\right.\right\}\\&\subseteq\bigcup_{l=0}^{m-1}\left\{\epsilon_k\in\Omega_k\left||n^*_{t,i+256l}|>\frac{q}{2}\right.\right\}\end{aligned}$$

Clearly, $\Pr(E_{k,j\neq0})$, $\forall k\in[1,2^m-1]$ is upper bonded as same as $\Pr(E_{0,j\neq0})$ by using the union bound as follows:

$$\begin{aligned}\Pr(E_{k,j\neq0})&\le\Pr\left(\bigcup_{l=0}^{m-1}\left\{\epsilon_k\in\Omega_k\left||n^*_{t,i+256l}|>\frac{q}{2}\right.\right\}\right)\\&\le\sum_{l=0}^{m-1}\Pr\left(|n^*_{t,i+256l}|>\frac{q}{2}\right)\\&\le m\Pr\left(|n^*_{t,i}|>\frac{q}{2}\right).\end{aligned}$$

Also, Theorem 2 is applied to $E_{k,j=0}$, $\forall k\in[1,2^m-1]$ as follows:

$$\begin{aligned}E_{k,j=0}&=\left(\bigcup_\beta\left\{\epsilon_k\in\Omega_k\left|\sum_{l=0}^{m-1}n^*_{t,i+256l}y^m_{k,l}=\beta\right.\right\}\right.\\&\quad\left.\cap\{\epsilon_k\in\Omega_k|A_i=0\}\right)\\&\subseteq\bigcup_\beta\left\{\epsilon_k\in\Omega_k\left|\sum_{l=0}^{m-1}n^*_{t,i+256l}y^m_{k,l}=\beta\right.\right\}.\end{aligned}$$

Therefore, we can calculate the upper bound on $\Pr(E_{k,j=0})$, $\forall k\in[1,2^m-1]$ as follows:

$$\Pr(E_{k,j=0})\le\Pr\left(T_m\le\sum_{l=0}^{m-1}n^*_{t,i+256l}y^m_{k,l}\le2T_m\right).$$

Since expectation of W_j, $\forall j\in[0,2n/m-1]$ in (17) is sum of product of *i.i.d.* random variables e_i, e'_i, s_i, s'_i, and s''_i whose means are zero, the expectation of W_j is zero. Also, since the distributions of e_i, e'_i, s_i, s'_i, and s''_i are symmetric, the distribution of W_j is also symmetric. These facts guarantee that for any y^m_k, the distributions of $\sum_{l=0}^{m-1}n^*_{t,i+256l}y^m_{k,l}$, $\forall k\in[0,2^m-1]$ are statistically identical and hence the upper bounds on $\Pr(E_1)$, $\Pr(E_2)$, $\cdots$, and $\Pr(E_{2^m-1})$ are same as $\Pr(E_0)$. □

In summary, the occurring probabilities $\Pr(E_k)$, $\forall k\in[0,2^m-1]$ are upper bounded through Theorems 1, 2, 3, and 4, and then they are used to derive the upper bound on BER $\Pr(E)$ of NewHope by using the union bound as follows:

$$\begin{aligned}\Pr(E)&=\Pr\left(\bigcup_{k=0}^{2^m-1}E_k\right)\\&\le\sum_{k=0}^{2^m-1}\Pr(E_k)\\&\le2^m\left(m\Pr\left(|n^*_{t,i}|>\frac{q}{2}\right)\right.\\&\quad\left.+\Pr\left(T_m\le\sum_{l=0}^{m-1}n^*_{t,i+256l}\le2T_m\right)\right).\end{aligned}\tag{19}$$

B. DERIVATION OF UPPER BOUND ON DFR OF NEWHOPE

Since decryption fails at $\{\mu\neq\mu'\}$, there must not be any bit in which an error occurs in order to succeed in the decryption.

Conversely, the union of all the bit errors supports is the decryption failure support, so the DFR $\Pr(\mu \neq \mu')$ is easily upper bounded by using the union bound and BER $\Pr(E)$.

Theorem 5: The DFR $\Pr(\mu \neq \mu')$ *of NewHope is at most* $\frac{n}{m}Pr(E)$.

Proof: Since the support of decryption failure is the union of the supports of bit error and the occurring probabilities of the supports of bit error are identical, the DFR is upper bounded by the sum of BERs by using the union bound as follows:

$$\begin{aligned} DFR &= \Pr\left(\bigcup_{i=0}^{n/m-1}(\mu_i \neq \mu_i')\right) \\ &\leq \sum_{i=0}^{n/m-1}\Pr(\mu_i \neq \mu_i') \\ &= \frac{n}{m}Pr(E). \end{aligned}$$

□

Finally, the upper bound on DFR of NewHope is upper bounded through Theorems 1, 2, 4, and 5 as follows:

$$DFR \leq \frac{n2^m}{m}\left(m\Pr\left(|n_{t,i}^*| > \frac{q}{2}\right) + \Pr\left(T_m \leq \sum_{l=0}^{m-1} n_{t,i+256l}^* \leq 2T_m\right)\right). \quad (20)$$

V. PARAMETRIZATION OF THE PROPOSED UPPER BOUND ON DFR OF NEWHOPE

The computational complexity of deriving the distribution of $\sum_{l=0}^{m-1} n_{t,i+256l}^*$ is $O(k^{2m})$ since k^{2m} operations are required to calculate the distribution of W_j. Therefore, as k increases, the proposed upper bound on DFR of NewHope cannot be computed. For this reason, the derivation of the proposed upper bound on DFR is required to be parametrized in spite of losing some tightness. In this paper, by using CC bound, the proposed upper bound on DFR is parameterized by the parameter of NewHope.

Theorem 6 (Chernoff-Cramer bound): Let Φ *be a distribution over* $\mathbb{R}$ *and let* $\chi_0, \ldots, \chi_{n-1}$ *be i.i.d. random variable of* Φ*, with average* μ*. Then, for any* t *such that* $M_{\Phi_\chi}(t) = E_\chi[\exp(\chi t)] < \infty$ *it holds that*

$$\Pr\left(\sum_{i=0}^{n-1}\chi_i > n\mu + \beta\right) \leq \inf_t \exp(\beta t + n\ln[M_{\Phi_\chi}(t)]). \quad (21)$$

The proposed upper bound on DFR is the sum of two occurring probabilities $\Pr(|n_{t,i}^*| > \frac{q}{2})$ and $\Pr(T_m \leq \sum_{l=0}^{m-1} n_{t,i+256l}^* \leq 2T_m)$ in (20) and these probabilities can be parameterized with CC bound, respectively. In order to apply CC bound to $\Pr(|n_{t,i}^*| > \frac{q}{2})$, we need to calculate the moment generating function (MGF) of product of two random variables following the centered binomial distribution. Suppose that X and Y follow the binomial distribution with parameter $2k$, and X_c and Y_c follow the centered binomial distribution with parameter k. Then, $X_c = X - k$ and $Y_c = Y - k$ and the MGF $M_{\Phi_{X_c \cdot Y_c}}(t)$ of $X_c \cdot Y_c$ is calculated as follows:

$$\begin{aligned} M_{\Phi_{X_c\cdot Y_c}}(t) &= E_{X,Y}\left[e^{(x-k)(y-k)t}\right] \\ &= E_Y\left[E_X[e^{(x-k)(y-k)t}]\right] \\ &= E_Y\left[e^{-kt(Y-k)}\left(\frac{1}{2}(e^{t(y-k)}+1)\right)^{2k}\right] \\ &= E_Y\left[\cosh^{2K}\left(\frac{t(y-k)}{2}\right)\right] \\ &= E_{Y_c}\left[\cosh^{2K}\left(\frac{ty_c}{2}\right)\right]. \end{aligned} \quad (22)$$

Since $n_{t,i}^*$ consists of $(\mathbf{e}\odot\mathbf{s}')_i$ and $(\mathbf{e}'\odot\mathbf{s})_i$, which are products of *i.i.d.* random variables drawn from the centered binomial distribution, and the independent random variables of $\mathbf{e}_i''$ and $\mathbf{n}_{c,i}$, CC bound can be applied as follows:

$$\begin{aligned} &\Pr\left(|n_{t,i}^*| > \frac{q}{2}\right) \\ &= \Pr\left(n_{t,i}^* > \frac{q}{2}\right) + \Pr\left(n_{t,i}^* < -\frac{q}{2}\right) \\ &= 2\Pr\left((\mathbf{e}\odot\mathbf{s}')_i - (\mathbf{e}'\odot\mathbf{s})_i > \frac{q}{2} - (\mathbf{e}_i'' - \mathbf{n}_{c,i})\right) \\ &\leq 2\Pr\left((\mathbf{e}\odot\mathbf{s}')_i - (\mathbf{e}'\odot\mathbf{s})_i > \frac{q}{2} - \left(k + \frac{q-1}{2r}\right)\right) \\ &\leq \inf_t 2\exp\left(C_1(t) + 2n\ln E_Y\left[\cosh^{2K}\left(\frac{ty_c}{2}\right)\right]\right), \end{aligned}$$

where $C_1(t) = (q/2 - (k + (q-1)/2r))t$. Although the MGF of $\sum_{l=0}^{m-1} n_{t,i+256l}^*$ is very complicated, Theorem 3 guarantees that $\sum_{l=0}^{m-1} n_{t,i+256l}^*$ is decomposed into $2n/m + 2m$ independent random variables such that $\sum_{l=0}^{m-1} n_{t,i+256l}^* = \sum_{j=0}^{2n/m-1} W_j + \sum_{l=0}^{m-1}(e_{i+256l}'' + n_{c,i+256l})$, where W_j is in (17). For the convenience of analysis, the new random variable W is defined as:

$$W = \begin{bmatrix} e_0 \\ e_1 \\ e_2 \\ e_3 \end{bmatrix}^T \cdot \left(\begin{bmatrix} +s_0 \\ -s_3 \\ -s_2 \\ -s_1 \end{bmatrix} + \begin{bmatrix} +s_1 \\ +s_0 \\ -s_3 \\ -s_2 \end{bmatrix} + \begin{bmatrix} +s_2 \\ +s_1 \\ +s_0 \\ -s_3 \end{bmatrix} + \begin{bmatrix} +s_3 \\ +s_2 \\ +s_1 \\ +s_0 \end{bmatrix}\right).$$

The MGF $M_{\Phi_W}(t)$ of W is

$$\begin{aligned} M_{\Phi_W}(t) = E_{s_{0:3}}\Big[&E_{e_0}\left[\exp(e_0(s_0+s_1+s_2+s_3)t)\right] \\ &\cdot E_{e_1}\left[\exp(e_1(s_0+s_1+s_2-s_3)t)\right] \\ &\cdot E_{e_2}\left[\exp(e_2(s_0+s_1-s_2-s_3)t)\right] \\ &\cdot E_{e_3}\left[\exp(e_3(s_0-s_1-s_2-s_3)t)\right]\Big], \end{aligned} \quad (23)$$

and by using $M_{\Phi_{X_c\cdot Y_c}}(t) = E_{Y_c}[\cosh^{2K}(\frac{ty_c}{2})]$ in (22),

$$\begin{aligned} M_{\Phi_W}(t) = E_{s_{0:3}}\Big[&\cosh^{2k}\left(\frac{t}{2}(s_0+s_1+s_2+s_3)\right) \\ &\cdot \cosh^{2k}\left(\frac{t}{2}(s_0+s_1+s_2-s_3)\right) \end{aligned}$$

$$\cdot \cosh^{2k}\left(\frac{t}{2}(s_0+s_1-s_2-s_3)\right)$$
$$\cdot \cosh^{2k}\left(\frac{t}{2}(s_0-s_1-s_2-s_3)\right)\Big]. \quad (24)$$

Even if the computational complexity of M_{Φ_W} is $O(k^{2m})$, by using $\cosh^{2k}(t) \le e^{-kt^2}$ and new random variable $Z = (s_0+s_1+s_2+s_3)^2+(s_0+s_1+s_2-s_3)^2+(s_0+s_1-s_2-s_3)^2+(s_0-s_1-s_2-s_3)^2$, the upper bound on M_{Φ_W} can be derived, which has the computational complexity $O(k^m)$ as follows:

$$M_{\Phi_W}(t) \le E_Z\Big[\exp\left(\frac{zkt^2}{4}\right)\Big]. \quad (25)$$

Then, by using CC bound and (25), $\Pr(T_m \le \sum_{l=0}^{m-1} n^*_{t,i+256l} \le 2T_m)$ is upper bounded as follows:

$$\begin{aligned}
&\Pr\left(T_m \le \sum_{l=0}^{m-1} n^*_{t,i+256l} \le 2T_m\right)\\
&\le \Pr\left(\sum_{i=0}^{2n/m-1} W_i + \sum_{j=0}^{m-1}(e''_j + n_{c,j}) > T_m\right)\\
&\le \Pr\left(\sum_{i=0}^{2n/m-1} W_i \ge T_m - m\Big(k+\frac{q-1}{2r}\Big)\right)\\
&\le \inf_t \exp\left\{C_2(t) + \frac{2n}{m}\ln M_{\Phi_W}(t)\right\}\\
&\le \inf_t \exp\left\{C_2(t) + \frac{2n}{m}\ln E_Z\Big[\exp\left(\frac{zkt^2}{4}\right)\Big]\right\},
\end{aligned}$$

where $C_2(t) = (T_m - m\Big(k+q-1/(2r)\Big))t$. Finally, a simplified upper bound on DFR of NewHope is derived as follows:

$$DFR \le \frac{n2^m}{m}\left(\inf_t \exp\left\{C_2(t) + \frac{2n}{m}\ln E_Z\Big[\exp\left(\frac{zkt^2}{4}\right)\Big]\right\} + m\inf_t \exp\left\{C_1(t) + 2n\ln E_Y\Big[\cosh^{2k}\left(\frac{ty}{2}\right)\Big]\right\}\right). \quad (26)$$

VI. IMPROVEMENT IN NEWHOPE BASED ON THE PROPOSED UPPER BOUNDS ON DFR

A. VERIFICATION OF THE PROPOSED UPPER BOUNDS ON DFR OF NEWHOPE

We compare the proposed upper bound in (20) and the simplified upper bound using CC bound in (26) with the current upper bound on DFR of NewHope [4], [9] for various k. Note that the current upper bound on DFR of NewHope [4], [9] is only provided at $k = 8$. Additionally, we compare the proposed upper bounds with the DFR derived by assuming no error dependency as in [13]. For convenience of expression, we will use "Proposed upper bound" to denote the upper bound derived in (20), "CC upper bound" to denote the simplified upper bound using CC bound in (26), "Current upper bound" to denote the current upper bound on DFR of NewHope [4], [9], "Independence assumption" to denote the DFR values calculated under assumption that there is no error dependency among error coefficients as in [13], and "Monte Carlo" to denote the DFR values obtained by performing Monte Carlo simulation of NewHope protocol.

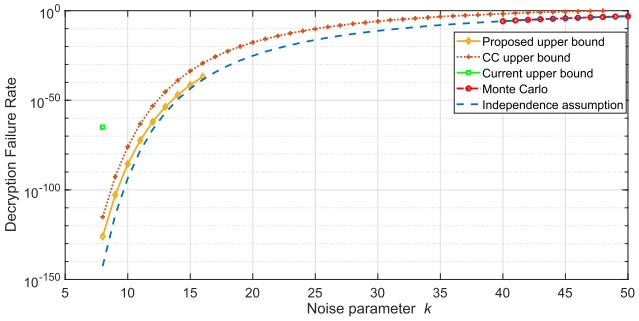


FIGURE 7. Comparison of various upper bounds for various k ($n = 1024$).

Fig. 7 compares the various upper bounds on DFR of NewHope for various noise parameter k for $n = 1024$. First of all, it is confirmed that the proposed upper bound and CC upper bound are improved more than fifty orders of magnitude compared to the current upper bound at $k = 8$. Note that the proposed upper bound on DFR of NewHope is less than 10^{-126}, the CC upper bound is less than 10^{-115}, and the current upper bound is less than 10^{-64}. Also, it is confirmed that the CC upper bound is looser than the proposed upper bound as expected. Nevertheless, since the computational complexity of the proposed upper bound substantially increases as k increases, the proposed upper bound is difficult to calculate when k is large. However, CC upper bound can be calculated for most k because CC upper bound is parameterized for easy calculation. In Fig. 7, Monte Carlo is the DFR value obtained by performing Monte Carlo simulation of NewHope protocol. Therefore, this DFR value reflects the error dependency, but this simulation is only possible for higher noise case (i.e., larger k values). Comparing the Monte Carlo with the independence assumption, it is shown that Monte Carlo DFR values are slightly larger than the independence assumption. The reason for this is that NewHope uses an ECC called ATE [20], and therefore the DFR performance is degraded due to error dependency. Also, according to the argument in [20], since NewHope uses ATE as an ECC, the independence assumption becomes too positive. Fig. 7 shows that as k increases, the proposed upper bound and independence assumption become almost identical. It is revealed that the independence assumption is referred to as the lower bound on the DFR of Ring-LWE-based cryptography with an error dependency [20]. Therefore, it is guaranteed that the proposed upper bound is a fairly tight upper bound, especially for large k.

Fig. 8 compares the various upper bounds on DFR of NewHope for various noise parameter k for $n = 512$. It is confirmed that the proposed upper bound and CC upper bound are improved more than forty orders of magnitude compared to the current upper bound for $k = 8$. Note that the proposed upper bound on DFR of NewHope is less

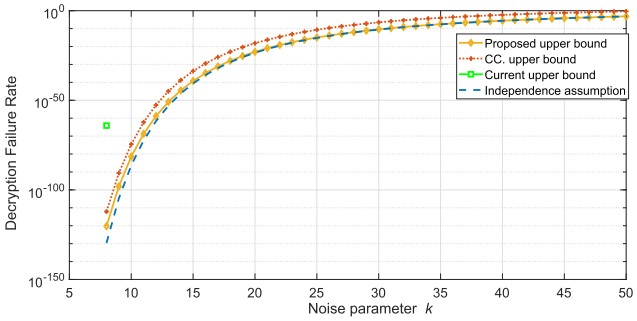


FIGURE 8. Comparison of various upper bounds for various k ($n = 512$).

than 10^{-120}, the CC upper bound is less than 10^{-111}, and the current upper bound is less than 10^{-63}. Unlike the case of $n = 1024$, the proposed upper bound can be calculated for most k when $n = 512$. Thus, when $n = 512$, we can calculate tight upper bound values for most k. It is shown that there is almost no difference between the proposed upper bound and independence assumption, which is the lower bound of DFR of Ring-LWE based cryptography for most k. Therefore, it is guaranteed that the proposed upper bound is a fairly tight upper bound for most k.

In conclusion, when $n = 1024$ and $n = 512$, it is confirmed that the proposed upper bound is fairly tight. Furthermore, Figs. 7 and 8 show that when the noise parameter k is 8, the proposed upper bound on DFR of NewHope is much smaller than the DFR requirement of PQC. Therefore, by utilizing this new DFR margin, the security and bandwidth efficiency of NewHope can be improved, which will be verified in the next section.

B. IMPROVEMENT IN SECURITY LEVEL OF NEWHOPE

Since there exists a trade-off relation between the security level and the DFR, it is necessary to properly select the noise parameter k of centered binomial distribution such that the security level and the DFR are appropriately determined to meet the requirements. Since it is confirmed by the new upper bound on DFR that NewHope is designed to have unnecessarily low DFR, the security level can be more improved by using the new DFR margin which is the difference between the new upper bound and the required DFR.

Table 3 shows the improved security levels which are calculated as the cost of the primal attack and the cost of dual attack [22] to NewHope. It is possible to improve the security level by 7.2 % ($n = 1024$, $k = 14$) and 8.9 % ($n = 512$, $k = 14$) while guaranteeing the required DFR of 2^{-140} compared with the current NewHope. The improvement in the security level can easily be reflected in NewHope because it is required to only change of the noise parameter k without any additional procedure.

C. IMPROVEMENT IN BANDWIDTH EFFICIENCY OF NEWHOPE

The bandwidth efficiency of NewHope can also be improved by utilizing the new DFR margin. An improvement in bandwidth efficiency is achieved by reducing (or more compressing) the ciphertext size which, however, increases the compression noise resulting in the DFR degradation. Even with such increased compression noise, both the improvement of bandwidth efficiency and the required DFR of 2^{-140} can be achieved by utilizing a new DFR margin.

Table 4 shows the improved bandwidth efficiency of NewHope achieved by doing the additional compression to ciphertext. It is possible to improve the bandwidth efficiency by 5.9 % by changing the compression rate on v' from 8 (3 bits per coefficient) to 4 (2 bits per coefficient) and the security level by 2.5 % by changing the noise parameter from 8 to 10 for $n = 1024$. Similarly, it is possible to improve the bandwidth efficiency by 5.9 % and the security level by 1.9 % by changing the noise parameter from 8 to 9 for $n = 512$. The improvement of the security and bandwidth efficiency requires little change in the protocol of NewHope so that this improvement can be easily reflected in NewHope.

D. CLOSENESS OF CENTERED BINOMIAL DISTRIBUTION AND THE CORRESPONDING ROUNDED GAUSSIAN DISTRIBUTION FOR VARIOUS K

The properties of rounded Gaussian distribution ξ are a key factor to the worst-case to average-case reduction for Ring-LWE. However, since a very high-precision and

TABLE 3. Improved security level of NewHope based on new DFR margin and the required DFR is 2^{-140} (The noise parameter of current NewHope is $k = 8$).

n	k	DFR	Cost of primal attack Classical/Quantum [bits]	Cost of dual attack Classical/Quantum [bits]
1024	8	$\leq 2^{-418}$	259/235	257/233
	9	$\leq 2^{-341}$	262/238	261/237
	10	$\leq 2^{-284}$	266/241	265/240
	11	$\leq 2^{-240}$	269/244	268/243
	12	$\leq 2^{-205}$	272/247	271/246
	13	$\leq 2^{-178}$	275/249	274/248
	14	$\leq 2^{-156}$	278/252	276/250
	15	$\leq 2^{-137}$	280/254	279/253
512	8	$\leq 2^{-399}$	112/101	112/101
	9	$\leq 2^{-325}$	114/103	113/103
	10	$\leq 2^{-270}$	115/105	115/104
	11	$\leq 2^{-228}$	117/106	117/106
	12	$\leq 2^{-195}$	119/107	118/107
	13	$\leq 2^{-169}$	120/109	119/108
	14	$\leq 2^{-147}$	121/110	121/110
	15	$\leq 2^{-130}$	122/111	122/111

TABLE 4. Improved bandwidth efficiency of NewHope based on new DFR margin and the required DFR is 2^{-140} (The noise parameter and compression rate of current NewHope are $k = 8$ and $r = 8$, respectively).

n	r	k	Ciphertext reduction (%)	DFR
1024	8	8	0 (Current NewHope)	$\leq 2^{-418}$
	4	8	5.9	$\leq 2^{-212}$
		9	5.9	$\leq 2^{-173}$
		10	5.9	$\leq 2^{-144}$
512	8	8	0 (Current NewHope)	$\leq 2^{-399}$
	4	8	5.9	$\leq 2^{-199}$
		9	5.9	$\leq 2^{-161}$

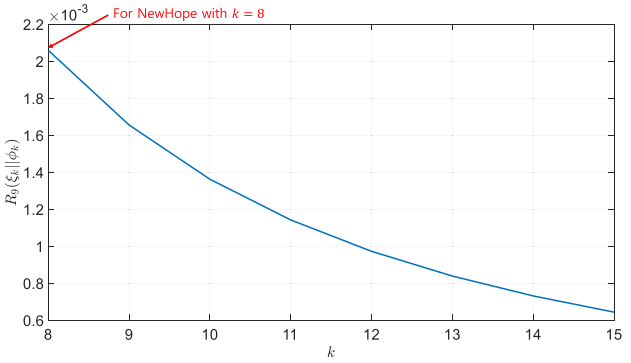


FIGURE 9. Rényi divergence of the centered binomial distribution ψ_k and the rounded Gaussian distribution ξ_k with the same variance $k/2$ according to k ($a = 9$).

high-complexity sampling is required for the rounded Gaussian distribution, NewHope uses the centered binomial distribution ψ_k for practical sampling without having rigorous security proof. It is generally accepted that as the centered binomial distribution and the rounded Gaussian distribution are closer to each other, NewHope is regarded as more secure. The closeness of two distributions can be measured through many methods. Among them, Rényi divergence is a well-known method, which is parameterized by a real $a > 1$ and defined for two distributions P and Q as follows [23], [24].

$$R_a(P||Q) = \left(\sum_{x \in \mathrm{supp}(P)} \frac{P(x)^a}{Q(x)^{a-1}} \right)^{\frac{1}{a-1}}, \tag{27}$$

where $\mathrm{supp}(P)$ represents the support of P and $Q(x) \neq 0$ for $x \in \mathrm{supp}(P)$.

We define ξ_k to be the rounded Gaussian distribution with the variance $\sigma^2 = k/2$, which is the distribution of $\lfloor \sqrt{k/2} \cdot x \rceil$ where x follows the standard normal distribution.

Fig. 9 shows that the Rényi divergence ($a = 9$ is used as in [4]) of the centered binomial distribution ψ_k and the rounded Gaussian distribution ξ_k with the same variance $k/2$. It is clear that the Rényi divergence decreases as k increases. Therefore, an increase in the noise parameter k can quantitatively and qualitatively improve the security of NewHope although the time complexity increases a little bit due to the complexity increase of calculating $\sum_{i=0}^{k-1}(b_i - b'_i)$.

VII. CONCLUSION

Since NewHope is an IND-CCA secure KEM by applying the FO transform to an IND-CPA secure PKE, accurate DFR calculation is required to guarantee resilience against attacks that exploit decryption failures. However, the upper bound on DFR of NewHope derived in [4], [9] is rather loose because the compression noise and effect of encoding/decoding of ATE in NewHope are not fully considered. Also, the centered binomial distribution is approximated by subgaussian distribution. Furthermore, since NewHope is a Ring-LWE based cryptography, there is a problem of error dependency among error coefficients, which makes accurate DFR calculation difficult.

In this paper, an upper bound on DFR, which is much closer to the real DFR than the previous upper bound on DFR derived in [4], [9], is derived by considering the above-ignored factors. Also, the centered binomial distribution is not approximated by the subgaussian distribution. Especially, the new upper bound on DFR considers the error dependency among error coefficients by using the constraint relaxation and union bound. Furthermore, the new upper bound on DFR is parameterized by using CC bound in order to facilitate the calculation of new upper bound on DFR for the parameters of NewHope.

According to the new upper bound on DFR of NewHope, since it is much lower than the DFR requirement of PQC, this DFR margin can be used to improve the security and bandwidth efficiency. As a result, the security level of NewHope is improved by 7.2%, or the bandwidth efficiency is improved by 5.9%. This improvement in the security and bandwidth efficiency can be easily achieved in NewHope because it is required to little change in the protocol of NewHope.

ACKNOWLEDGMENT

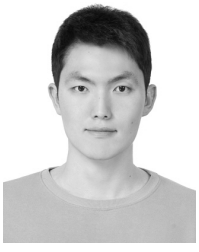
(Minki Song and Seunghwan Lee contributed equally to this work.)

REFERENCES

[1] L. Chen, "Report on post-quantum cryptography," NIST, Gaithersburg, MD, USA, Tech. Rep. 8105, 2016.
[2] R. Lindner and C. Peikert, "Better key sizes (and attacks) for LWE-based encryption," in *Proc. Cryptograph. Track RSA Conf.* (Lecture Notes in Computer Science), vol. 6558. 2011, pp. 319–339.
[3] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *J. ACM*, vol. 56, no. 6, pp. 1–37, 2009.
[4] T. Pöppelmann, E. Alkim, R. Avanzi, J. Bos, L. Ducas, A. Piedra, P. Schwabe, and D. Stebila. *NewHope*. Accessed: Dec. 13, 2019. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions
[5] M. Naehrig, E. Alkim, J. Bos, L. Ducas, K. Easterbrook, B. LaMacchia, P. Longa, I. Mironov, V. Nikolaenko, C. Peikert, A. Raghunathan, and D. Stebila. *FrodoKEM*. Accessed: Dec. 13, 2019. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions
[6] P. Schwabe, R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, G. Seiler, and D. Stehle. *CRYSTALS-KYBER*. Accessed: Dec. 31, 2019. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions
[7] X. Lu, Y. Liu, D. Jia, H. Xue, J. He, Z. Zhang, Z. Liu, H. Yang, B. Li, and K. Wang. *LAC*, Accessed: Dec. 13, 2019. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions
[8] M. O. Saarinen, "HILA5: On reliability, reconciliation, and error correction for Ring-LWE encryption," in *Proc. Int. Conf. Sel. Areas Cryptogr.* (Lecture Notes in Computer Science), vol. 10719. Berlin, Germany: Springer, 2017, pp. 192–212.
[9] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, "Post-quantum key exchange—A new hope," in *Proc. 25th USENIX Secur. Symp.*, Santa Clara, CA, USA, 2016, pp. 327–343.
[10] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, *Newhope Without Reconciliation*. Accessed: Jun. 18, 2018. [Online]. Available: https://eprint.iacr.org/2016/1157
[11] J.-C. Deneuville, P. Gaborit, Q. Guo, and T. Johansson, "Ouroboros-E: An efficient lattice-based key-exchange protocol," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Vail, CO, USA, Jun. 2018, pp. 1450–1454.
[12] S. Streit and F. De Santis, "Post-quantum key exchange on ARMv8-A: A new hope for NEON made simple," *IEEE Trans. Comput.*, vol. 67, no. 11, pp. 1651–1662, Nov. 2018.

[13] T. Fritzmann, T. Pöppelmann, and J. Sepulveda, "Analysis of error-correcting codes for lattice-based key exchange," in *Proc. Int. Conf. Sel. Areas Cryptogr.* (Leture Notes in Computer Science). Berlin, Germany: Springer, vol. 2018, pp. 369–390.
[14] Google. (Jul. 2016). *CECPQ1 in BoringSSL, Google Security Blog*. Accessed: Jan. 31, 2019. [Online]. Available: https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html
[15] E. E. Targhi and D. Unruh, "Post-quantum security of the Fujisaki-Okamoto and OAEP transforms," in *Proc. Int. Conf. Sel. Areas Cryptogr.* (Leture Notes in Computer Science). Heidelberg, Germany: Springer, 2016, pp. 192–216.
[16] S. Fluhrer, "Cryptanalysis of ring-LWE based key exchange with key share reuse," *IACR Cryptol. ePrint Arch.*, vol. 2016, pp. 85–91, Jan. 2016.
[17] T. Pöppelmann and T. Güneysu, "Towards practical lattice-based public-key encryption on reconfigurable hardware," in *Proc. Int. Conf. Sel. Areas Cryptogr.*, Burnaby, BC, Canada, Aug. 2013, pp. 68–85.
[18] J. M. Pollard, "The fast Fourier transform in a finite field" *Math. Comput.*, vol. 25, no. 114, pp. 365–374, 1971.
[19] P. Q. Nguyen and B. Vallée, *The LLL Algorithm: Survey and Applications*. New York, NY, USA: Springer-Verlag, 2010.
[20] J. P. D'Anvers, F. Vercauteren, and I. Verbauwhede, "The impact of error dependencies on Ring/Mod-LWE/LWR based schemes," in *Proc. Int. Conf. Post-Quantum Cryptogr.* (Lecture Notes in Computer Science). Berlin, Germany: Springer, 2019, pp. 246–255.
[21] J. P. D'Anvers, F. Vercauteren, and I. Verbauwhede, "On the impact of decryption failures on the security of LWE/LWR based schemes," IACR, Lyno, France, Tech. Rep. 2018/1089, 2018. Accessed: Nov. 11, 2019. [Online]. Available: https://eprint.iacr.org/2018/1089/
[22] 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, 2015.
[23] A. Rényi, "On measures of entropy and information," in *Proc. 4th Berkeley Symp. Math. Stat. Probab.*, 1961, pp. 547–561.
[24] S. Bai, A. Langlois, T. Lepoint, D. Stehlé, and R. Steinfeld, "Improved security proofs in lattice-based cryptography: Using the Rényi divergence rather than the statistical distance," in *Proc. 21st Int. Conf. Adv. Cryptol. (ASIACRYPT)*, 2015, pp. 3–24.

MINKI SONG received the B.S. degree in electronics and communication engineering and the M.S. degree in electronics and computer engineering from Hanyang University, Seoul, South Korea, in 2013 and 2015, respectively, where he is currently pursuing the Ph.D. degree in electronics and computer engineering. His research interests include signal processing, error-correcting codes, and cryptography.



SEUNGHWAN LEE received the B.S. degree in electronics engineering from Hanyang University, Seoul, South Korea, in 2019, where he is currently pursuing the Ph.D. degree in electronics and computer engineering. His research interests include cryptography, signal processing, and error-correcting codes.

DONG-JOON SHIN (Senior Member, IEEE) received the B.S. degree in electronics engineering from Seoul National University, Seoul, South Korea, the M.S. degree in electrical engineering from Northwestern University, Evanston, IL, USA, and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, CA, USA. From 1999 to 2000, he was a Member of Technical Staff with the Wireless Network Division and Satellite Network Division, Hughes Network Systems, Germantown, MD, USA. Since September 2000, he has been with the Department of Electronic Engineering, Hanyang University, Seoul, South Korea. His current research interests include signal processing, error-correcting codes, sequences, discrete mathematics, and cryptography.

EUNSANG LEE received the B.S. degree in electrical and computer engineering from Seoul National University, Seoul, South Korea, in 2014, where he is currently pursuing the Ph.D. degree in electrical engineering and computer science. His current research interests include cryptography and error-correcting codes.

YOUNG-SIK KIM (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electrical engineering and computer science from Seoul National University, in 2001, 2003, and 2007, respectively. He joined the Semiconductor Division, Samsung Electronics, where he carried out research and development of security hardware IPs for various embedded systems, including modular exponentiation hardware accelerator (called *Tornado 2MX2*) for RSA and elliptic curve cryptography in smart card products and mobile application processors of Samsung Electronics, until 2010. He is currently an Associate Professor with Chosun University, Gwangju, South Korea. He is also a Submitter for two candidate algorithms (McNie and pqsigRM) in the first round for the NIST Post Quantum Cryptography Standardization. His research interests include post-quantum cryptography, the IoT security, physical layer security, data hiding, channel coding, and signal design. He was selected as one of the 2025's 100 Best Technology Leaders (for Crypto-Systems) by the National Academy of Engineering of Korea.

JONG-SEON NO (Fellow, IEEE) received the B.S. and M.S.E.E. degrees in electronics engineering from Seoul National University, Seoul, South Korea, in 1981 and 1984, respectively, and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, CA, USA, in 1988. From 1988 to 1990, he was a Senior MTS with Hughes Network Systems. From 1990 to 1999, he was an Associate Professor with the Department of Electronic Engineering, Konkuk University, Seoul. He joined the Faculty of the Department of Electrical and Computer Engineering, Seoul National University, in 1999, where he is currently a Professor. His current research interests include error-correcting codes, sequences, cryptography, LDPC codes, interference alignment, and wireless communication systems. He became a Fellow of the IEEE through the IEEE Information Theory Society, in 2012. He was a recipient of the IEEE Information Theory Society Chapter of the Year Award, in 2007. From 1996 to 2008, he served as the Founding Chair for the Seoul Chapter of the IEEE Information Theory Society. He was the General Chair of Sequence and Their Applications, Seoul, in 2004. He also served as the General Co-Chair for the International Symposium on Information Theory and Its Applications, in 2006, and the International Symposium on Information Theory, Seoul, in 2009.