On the γ-Spreadness of Average-Case to Worst-Case Transformations

Hyun Ji Kwag* Jonghyun Kim† Changmin Lee‡ Jong Hwan Park§

May 11, 2026

Abstract

Achieving (at least) a worst-case correctness error is essential for an underlying public-key encryption (PKE) scheme to which the Fujisaki-Okamoto (FO) transformation is applied. There are three average-case to worst-case (ACWC) transformations—denoted as ACWC_0, ACWC_1 (PKC 2023), and ACWC_2 (TIFS 2023)-which generically convert a PKE scheme with an average-case correctness error into one with a worst-case correctness error. However, in these ACWC transformations the γ-*spreadness*, a critical factor in determining explicit rejection ($\mathsf{FO}^{\perp}$) or implicit rejection ($\mathsf{FO}^{\not\perp}$), has not been established with rigorous proofs. Existing analyses of γ-spreadness lack rigorous proofs, include analytical flaws, or fail to achieve the tightest possible bounds. In this work, we reprove the γ-spreadness of ACWC-transformed PKE schemes by leveraging two key facts: the random oracle is chosen at random and the encoding mechanism used in the ACWC framework is message-hiding. Our new proofs are applied to the previous NTRU-based PKE schemes, called NTRU-C, NTRU-B, and NTRU+, giving the corrected γ-spreadness for those PKE schemes with concrete parameters.

Keywords: γ-spreadness, ACWC transformation, Fujisaki-Okamoto transformation, NTRU

1 Introduction

A family of variants [3, 10] of the Fujisaki-Okamoto transformation [6, 7] has been developed to obtain a (post-quantum) key encapsulation mechanism (KEM) that is secure against chosen-ciphertext attacks (i.e., IND-CCA-secure) from any public-key encryption (PKE) scheme that satisfies chosen-plaintext security or one-wayness (i.e., $\{\mathsf{IND}, \mathsf{OW}\}$-$\mathsf{CPA}$-secure). A sequence of works [10, 2, 16, 4, 11, 8, 13, 9] has improved the security reduction for the PKE-to-KEM transformation (denoted FO) in the quantum random oracle model (QROM). Beyond the base $\{\mathsf{IND}, \mathsf{OW}\}$-$\mathsf{CPA}$ security, any PKE scheme (denoted PKE') used as the underlying scheme for FO must achieve (at least) a negligible *worst-case* correctness error. Roughly speaking, a PKE scheme is worst-case δ'-correct if, for any message and randomness drawn from a prescribed distribution, the maximum probability of decryption failure is bounded by δ'.

To systematically provide a negligible worst-case correctness error for an underlying PKE', three average-case to worst-case (ACWC) transformations-denoted ACWC_0 [5], ACWC_1 [5], and ACWC_2 [14] have been proposed. Let PKE be an underlying PKE scheme whose decryption error δ is negligible in the *average*

*Korea University, Seoul, Korea. Email: ijnuyh01@korea.ac.kr.
†Korea University, Seoul, Korea. Email: yoswuk@korea.ac.kr.
‡Korea University, Seoul, Korea. Email: changminlee@korea.ac.kr.
§Sangmyung University, Seoul, Korea. Email: jhpark@smu.ac.kr.

case, meaning that for any honestly sampled message and randomness (for prescribed distributions) the maximum probability of decryption failure is bounded by some negligible δ. Each ACWC transformation produces $\mathsf{PKE}' = \mathsf{ACWC}_i[\mathsf{PKE}]$ for $i = 0, 1, 2$, while preserving or improving the security of PKE. A benefit of these transformations is that the resulting worst-case correctness error δ' of PKE' remains essentially the same as the average-case correctness error δ of PKE, so that one only needs to analyze failures for honestly sampled inputs to control the worst-case correctness error of PKE'.

In the decapsulation algorithm of an FO-transformed KEM, there are two types of rejections in response to an invalid ciphertext: explicit rejection ($\mathsf{FO}^{\perp}$), which outputs the error symbol $\perp$, or implicit rejection ($\mathsf{FO}^{\not\perp}$), which proceeds to output a pseudorandom key. The choice between them depends on whether the underlying PKE scheme PKE' satisfies the γ-*spreadness*. Roughly speaking, the γ-spreadness means that for any fixed message m and ciphertext c, the maximum over randomnesses of the probability that $c = \mathsf{Enc}(pk, m; r)$ is less than $2^{-\gamma}$. In the standard spreadness-based analyses, if PKE' satisfies the γ-spreadness, the explicit rejection is permissible; otherwise, one must fall back to the implicit rejection. From an efficiency perspective, the explicit rejection is preferable, because the implicit rejection always needs to compute the pseudorandom key, regardless of whether a ciphertext is valid or not [1, 17]. In terms of security, [2, 12] show that the explicit rejection implies the implicit rejection, but the reverse direction incurs security loss and only holds if PKE' satisfies the γ-spreadness.

Security proofs for schemes obtained by applying the $\mathsf{FO}^{\perp}$-transformation to ACWC-transformed scheme ($\mathsf{PKE}' = \mathsf{ACWC}_i[\mathsf{PKE}]$) typically rely on the γ-spreadness of the underlying PKE'. Recently, [9] presented tighter security proofs for $\mathsf{FO}^{\perp}$-type KEMs, including a proof route that removes the separate γ-spreadness requirement for $\mathsf{FO}^{\perp} \circ \mathsf{ACWC}_0$, as well as a tighter QROM analysis for $\mathsf{FO}^{\perp} \circ \mathsf{ACWC}_1$ under γ-spreadness. These developments are complementary to our goal here: rather than replacing spreadness-based analyses, we focus on analyzing γ-spreadness more rigorously and establishing correct γ-spreadness bounds for ACWC-transformed encryption schemes. This remains important whenever one wants to justify explicit rejection through spreadness-based arguments and to derive concrete bounds for ACWC transformed schemes.

The three ACWC transformations present generic ways to provide for the γ-spreadness of PKE'. [5, 14] claim that if the underlying scheme PKE is γ-spread, then so is PKE', *without rigorous proofs*. Although the ACWC constructions successfully control worst-case correctness error, their internal structure complicates a direct application of the standard γ-spreadness analysis. Typically, one fixes a message m and ciphertext c (under a key pair (pk, sk)) and considers the maximum probability that is summed over all possible r such that $c = \mathsf{Enc}(pk, m; r)$. This typical analysis cannot be directly applied to the γ-spreadness of PKE'. For instance, during ACWC_2, a fixed message m (relative to PKE') is encoded as $M := \mathsf{Encode}(m, \mathsf{G}(r))$ using some encoding method 'Encode' and a hash function G. Then, M is encrypted as $c = \mathsf{Enc}(pk, M; r)$. Consequently, even for a fixed m, as r varies according to its distribution, the encoded plaintext M also changes, so M cannot be treated as fixed in the usual analysis. Analogous complications arise in ACWC_0 and ACWC_1, which require new rigorous proofs on the γ-spreadness of PKE' when applying those ACWC transformations.

1.1 Our result

Assuming that PKE is γ-spread, we revisit the γ'-spreadness in the (Q)ROM of PKE' obtained by applying the ACWC transformations to PKE. The previous proofs on the γ'-spreadness of PKE' under ACWC_0 and ACWC_1 were presented without sufficiently reflecting our argument mentioned above. In particular, the proof under ACWC_0 was incorrect, simply asserting that $\gamma' = \gamma$. Also, by considering our argument, [15] presented a proof on the γ'-spreadness of PKE' under ACWC_2, but the resulting bound on the γ'-spreadness can be further improved.

Since each ACWC-transformed scheme PKE' internally uses the random oracle G, we formulate the spreadness of PKE' in the (Q)ROM and use this notion throughout our analysis. We reprove the γ'-spreadness in the (Q)ROM of PKE' under ACWC_0, ACWC_1, and ACWC_2, respectively. All our proofs are based on some encoding method Encode and a hash function G modeled as a random oracle. Encode takes as input a message m (relative to PKE') and a hash value, and has a so-called *message-hiding* property that the output of Encode is distributed independently of m. Again, let (pk, sk) be a pair of public and private keys for PKE. Using Encode and G, all ciphertexts of PKE' share the following similarity: $c = (c_1, c_2) = (\mathsf{Enc}(pk, M; r), \mathsf{Encode}(m, \mathsf{G}(M)))$ under ACWC_0, $c = \mathsf{Enc}(pk, M_1||\mathsf{Encode}(m, \mathsf{G}(M_1)); r)$ under ACWC_1, and $c = \mathsf{Enc}(pk, \mathsf{Encode}(m, \mathsf{G}(r)); r)$ under ACWC_2. Given randomness R relative to PKE', R is used to sample (M, r) under ACWC_0, (M_1, r) under ACWC_1, and r under ACWC_2, following some distributions, respectively. Thus, we can see that each encrypted message (relative to PKE) also changes as a new randomness R is chosen. As mentioned above, this is the difficulty in directly analyzing the γ'-spreadness in the (Q)ROM of PKE'. Then, our proof strategy is as follows:

1. Given a ciphertext $c = (c_1, c_2) = (\mathsf{Enc}(pk, M; r), \mathsf{Encode}(m, \mathsf{G}(M)))$ under ACWC_0, the second component c_2 is distributed independently of m because of the message-hiding property of Encode. Next, using the fact that G is chosen at random in the random oracle model, c_2 can be viewed as random choice from the output space of Encode, indicating that the distributions of c_1 and c_2 are independent. Then, we can consider (M, r, c_2) as being sampled according to some distributions, in which case we adapt the Law of Total Probability to deal with all possible choices of (M, r, c_2).

2. Given a ciphertext $c = \mathsf{Enc}(pk, M_1||\mathsf{Encode}(m, \mathsf{G}(M_1)); r)$ under ACWC_1, the encoded partial message $M_2 := \mathsf{Encode}(m, \mathsf{G}(M_1))$ is distributed independently of m because of the message-hiding property of Encode. Additionally, the random choice of G allows for considering M_2 as being sampled from some distribution. Similarly to ACWC_0, we can then use the Law of Total Probability to address all possible choices of $(M_1||M_2, r)$.

3. Given a ciphertext $c = \mathsf{Enc}(pk, \mathsf{Encode}(m, \mathsf{G}(r)); r)$ under ACWC_2, the encoded message $M := \mathsf{Encode}(m, \mathsf{G}(r))$ is distributed independently of m because of the message-hiding property of Encode. Additionally, the random choice of G allows for considering M as being sampled according to some distribution. Similarly to ACWC_0 and ACWC_1, we can then use the Law of Total Probability to address all possible choices of (M, r).

All possible cases are rearranged into a group of encryptions, in which a fixed message M and all possible randomnesses $\{r\}$ are involved. For each group, we now apply the γ-spreadness of PKE to upper-bound the γ'-spreadness of PKE' in the (Q)ROM, when a specific ciphertext c of PKE' is given. In case of ACWC_0, we additionally consider the probability that a sampled c_2 becomes the second component of the given c. Then, our new proof shows that $\gamma' = \gamma + \lambda$, where the output space of Encode under ACWC_0 is instantiated with a set of λ-bit strings. In case of ACWC_1 and ACWC_2, we prove that $\gamma' = \gamma$. Although we follow a similar proof strategy [15], our result under ACWC_2 gives a tighter and more precise γ'-spreadness of PKE' in the (Q)ROM.

Finally, we recompute the γ'-spreadness in the (Q)ROM of three previous NTRU-based PKE's, which are NTRU-C [5], NTRU-B [5], and NTRU+ [14]. All are based on NTRU-based PKE schemes (as PKE) that are constructed over rings with cyclotomic trinomials. As noted in [15], it is easy to analyze the γ-spreadness of an NTRU-based PKE scheme in a statistical manner, given some distributions for sampling coefficients of a polynomial. By applying the three ACWC transformations to an NTRU-based PKE, we can have NTRU-C via ACWC_0, NTRU-B via ACWC_1, and NTRU+ via ACWC_2, respectively. During such

transformations, our new proofs give the corrected γ'-spreadness of the resultant NTRU-based PKE's in the (Q)ROM, as shown in Table 1.

2 Preliminaries

2.1 Notation

For a positive odd integer q, let $\mathbb{Z}_q := \{-(q-1)/2, \ldots, (q-1)/2\}$. For an integer $a \in \mathbb{Z}$, we write $a \bmod q$ for the unique element $y \in \mathbb{Z}_q$ such that $q \mid (y-a)$. Let $R_q := \mathbb{Z}_q[x]/\langle f(x)\rangle$ be the polynomial ring modulo $f(x)$; in the NTRU-based constructions considered in Section 5, q is an odd prime and $f(x)$ is a cyclotomic polynomial of degree n. For a polynomial $\mathbf{a} \in R_q$, the notation $\mathbf{a} \bmod q$ means that the above modular reduction is applied coefficient-wise to $\mathbf{a}$.

For sampling, if X is a finite set, then $a \leftarrow X$ means that a is sampled uniformly at random from X; if D is a distribution, then $a \leftarrow D$ means that a is sampled according to D. Additionally, for a polynomial $\mathbf{a}$, the notation $\mathbf{a} \leftarrow D$ means that its coefficients are sampled independently according to D; equivalently, when $\mathbf{a} \in R_q$, we write $\mathbf{a} \leftarrow D^n$. We denote $[\![B]\!]$ as 1 if the Boolean statement B is true, and 0 otherwise.

2.2 Definitions

Definition 2.1 (Public-Key Encryption). A public key encryption scheme $\mathsf{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}$, randomness space $\mathcal{R}$, and ciphertext space $\mathcal{C}$ consists of the following three algorithms:

- $\mathsf{Gen}(1^n)$: The key generation algorithm Gen is a probabilistic algorithm that takes a security parameter 1^n as input and outputs a pair of public and secret keys (pk, sk).
- $\mathsf{Enc}(pk, m; r)$: The encryption algorithm Enc is a probabilistic algorithm that takes a public key pk, a message $m \in \mathcal{M}$, and randomness $r \in \mathcal{R}$ as input and outputs a ciphertext $c \in \mathcal{C}$. If we write $\mathsf{Enc}(pk, m)$, it is to denote the encryption algorithm without explicitly mentioning the randomness.
- $\mathsf{Dec}(sk, c)$: The decryption algorithm Dec is a deterministic algorithm. Dec takes a secret key sk and a ciphertext $c \in \mathcal{C}$ as input and outputs either a message $m \in \mathcal{M}$ or a special symbol $\perp \notin \mathcal{M}$ to indicate that c is a invalid ciphertext.

Definition 2.2 (γ-spreadness [4]). PKE is γ-*spread* [4] if

$$\min_{m \in \mathcal{M}, (pk, sk)} \left(-\log \max_{c \in \mathcal{C}} \Pr_{r \leftarrow \psi_{\mathcal{R}}} [c = \mathsf{Enc}(pk, m; r)] \right) \geq \gamma,$$

where the probability is over the randomness $r \leftarrow \psi_{\mathcal{R}}$ and the minimum is over all key pairs (pk, sk) generated by Gen. This definition can be relaxed by considering an expectation over the choice of (pk, sk). PKE is *weakly* γ-*spread* [4] if

$$-\log \mathbb{E} \left[\max_{m \in \mathcal{M}, c \in \mathcal{C}} \Pr_{r \leftarrow \psi_{\mathcal{R}}} [c = \mathsf{Enc}(pk, m; r)] \right] \geq \gamma,$$

where the probability is over the randomness $r \leftarrow \psi_{\mathcal{R}}$ and the expectation is over $(pk, sk) \leftarrow \mathsf{Gen}(1^n)$.

Definition 2.3 ((Q)ROM γ-spreadness). Let $\mathsf{PKE}^{\mathsf{G}} = (\mathsf{Gen}, \mathsf{Enc}^{\mathsf{G}}, \mathsf{Dec}^{\mathsf{G}})$ be a public-key encryption scheme that may internally query a tuple G of random oracles. We say that $\mathsf{PKE}^{\mathsf{G}}$ is γ-spread in the (Q)ROM if

$$\min_{m\in\mathcal{M},(pk,sk)} \left(-\log \max_{c\in\mathcal{C}} \Pr_{\mathsf{G},r\leftarrow\psi_{\mathcal{R}}}[c = \mathsf{Enc}^{\mathsf{G}}(pk, m; r)] \right) \geq \gamma,$$

where the probability is over the randomness $r \leftarrow \psi_{\mathcal{R}}$ and the random oracle G, and the minimum is over all key pairs (pk, sk) generated by Gen.

$\mathsf{PKE}^{\mathsf{G}}$ is weakly γ-spread in the (Q)ROM if

$$-\log \mathbb{E}\left[\max_{m\in\mathcal{M},c\in\mathcal{C}} \Pr_{\mathsf{G},r\leftarrow\psi_{\mathcal{R}}}[c = \mathsf{Enc}^{\mathsf{G}}(pk, m; r)] \right] \geq \gamma,$$

where the probability is over the randomness $r \leftarrow \psi_{\mathcal{R}}$ and the random oracle G, and the expectation is over $(pk, sk) \leftarrow \mathsf{Gen}(1^n)$.

If the scheme does not use a random oracle, these definitions reduce to Definition 2.2

Definition 2.4 (Correctness [10]). PKE is worst-case correctness error δ [10] if

$$\mathbb{E}\left[\max_{m\in\mathcal{M}} \Pr_{r\leftarrow\psi_{\mathcal{R}}}[\mathsf{Dec}(sk, \mathsf{Enc}(pk, m; r)) \neq m] \right] \leq \delta,$$

where the expectation is over $(pk, sk) \leftarrow \mathsf{Gen}(1^n)$ and the choice of the random oracles (if any).
PKE is average-case correctness error δ if

$$\mathbb{E}\left[\Pr_{m\leftarrow\psi_{\mathcal{M}},r\leftarrow\psi_{\mathcal{R}}}[\mathsf{Dec}(sk, \mathsf{Enc}(pk, m; r)) \neq m] \right] \leq \delta,$$

where the expectation is over $(pk, sk) \leftarrow \mathsf{Gen}(1^n)$ and the choice of the random oracles (if any).

Definition 2.5 (Randomness Recoverability). PKE is defined as *randomness recoverable* (RR) if there exists an algorithm RRec such that for all key pairs $(pk, sk) \leftarrow \mathsf{Gen}(1^n)$, and for any message $m \in \mathcal{M}$ and ciphertext $c \in \mathcal{C}$, the following condition holds:

$$\text{if } r = \mathsf{RRec}(pk, m, c) \in \mathcal{R}, \text{ then } c = \mathsf{Enc}(pk, m; r).$$

3 ACWC Transformations

We describe three average-case to worst-case transformations, namely ACWC_0 [5], ACWC_1 [5] and ACWC_2 [14]. Each transformation takes an underlying PKE with average-case correctness error δ and produces a derived scheme PKE' with worst-case correctness error δ', satisfying $\delta' \approx \delta$.

3.1 ACWC_0

Figure 1 presents ACWC_0 and the instantiation $\mathsf{PKE}' = \mathsf{ACWC}_0[\mathsf{PKE}, \mathsf{G}]$ where $\mathsf{G} : \{0,1\}^* \to \mathcal{U}$ for the distribution $\psi_{\mathcal{U}}$. In particular, ACWC_0 assumes $\mathcal{U} = \{0,1\}^\lambda$ for a security parameter λ, and $\psi_{\mathcal{U}}$ is the uniform distribution over $\{0,1\}^\lambda$. The derived scheme $\mathsf{PKE}' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ has message space $\mathcal{M}' = \{0,1\}^\lambda$ and randomness space $\mathcal{R}'$, while the base scheme $\mathsf{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ has message space

$\mathcal{M}$ and randomness space $\mathcal{R}$ with respective distributions $\psi_{\mathcal{M}}$ and $\psi_{\mathcal{R}}$. In terms of security, [5] proves that PKE' is secure against chosen-plaintext attacks (i.e., IND-CPA secure) if PKE is one-way against chosen-plaintext attacks (i.e., OW-CPA secure), assuming G is modeled as a (quantum) random oracle. ACWC_0 is conceptually simple and transparent, but its instantiation increases ciphertext length by λ bits.

$\underline{\mathsf{Gen}'(1^n)}$
1: $(pk, sk) := \mathsf{Gen}(1^n)$
return (pk, sk)

$\underline{\mathsf{Enc}'(pk, m \in \mathcal{M}'; (R_1, R_2) \in \mathcal{R}')}$
1: $M \leftarrow \psi_{\mathcal{M}}$ using the randomness R_1
2: $r \leftarrow \psi_{\mathcal{R}}$ using the randomness R_2
3: $c_1 := \mathsf{Enc}(pk, M; r)$
4: $c_2 := \mathsf{G}(M) \oplus m$
5: $c := (c_1, c_2)$
return c

$\underline{\mathsf{Dec}'(sk, c)}$
1: $M := \mathsf{Dec}(sk, c_1)$
2: $m := \mathsf{G}(M) \oplus c_2$
return m

Figure 1: $\mathsf{ACWC}_0[\mathsf{PKE}, \mathsf{G}]$ transformation

3.2 ACWC_1

In addition to a hash function G modeled as a random oracle, the transformation ACWC_1 employs a supplementary primitive, the generalized one-time pad (GOTP) [5].

Definition 3.1. A generalized one-time pad $\mathsf{GOTP} = (\mathsf{Encode}, \mathsf{Inv})$ with a message space $\mathcal{X}$, a randomness space $\mathcal{U}$, and a code space $\mathcal{Y}$ (with distributions $\psi_{\mathcal{X}}, \psi_{\mathcal{U}}, \psi_{\mathcal{Y}}$) consists of the following deterministic algorithms:

- $\mathsf{Encode}(x, u)$: on input a message $x \in \mathcal{X}$ and random $u \in \mathcal{U}$ outputs a code $y \in \mathcal{Y}$.
- $\mathsf{Inv}(y, u)$: on input a code $y \in \mathcal{Y}$ and random $u \in \mathcal{U}$ recovers a message $x \in \mathcal{X}$.

It satisfies the following properties:

1. **Decoding:** $\mathsf{Inv}(\mathsf{Encode}(x, u), u) = x$ for all $x \in \mathcal{X}, u \in \mathcal{U}$.
2. **Message hiding:** For every $x \in \mathcal{X}$, the distribution of $\mathsf{Encode}(x, u)$ for $u \leftarrow \psi_{\mathcal{U}}$ equals $\psi_{\mathcal{Y}}$.
3. **Randomness hiding:** For every $u \in \mathcal{U}$, the distribution of $\mathsf{Encode}(x, u)$ for $x \leftarrow \psi_{\mathcal{X}}$ equals $\psi_{\mathcal{Y}}$.

For ACWC_1, the derived scheme $\mathsf{PKE}' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ has message space $\mathcal{M}'$ and randomness space $\mathcal{R}'$, while the base scheme $\mathsf{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ has message space $\mathcal{M} = \mathcal{M}_1 \times \mathcal{M}_2$ with distribution $\psi_{\mathcal{M}} = \psi_{\mathcal{M}_1} \times \psi_{\mathcal{M}_2}$, and randomness space $\mathcal{R}$ with distribution $\psi_{\mathcal{R}}$. Let $\mathsf{G} : \{0,1\}^* \to \mathcal{U}$ for the distribution $\psi_{\mathcal{U}}$, and let $\mathsf{Encode} : \mathcal{M}' \times \mathcal{U} \to \mathcal{M}_2$ and $\mathsf{Inv} : \mathcal{M}_2 \times \mathcal{U} \to \mathcal{M}'$ be the GOTP algorithms. Figure 2 illustrates ACWC_1 and the instantiation $\mathsf{PKE}' = \mathsf{ACWC}_1[\mathsf{PKE}, \mathsf{GOTP}, \mathsf{G}]$. By the message-hiding property of GOTP, the encoded component M_2 is distributed as $\psi_{\mathcal{M}_2}$ independently of the choice of $m \in \mathcal{M}'$. Regarding security, [5] establishes that, in the (Q)ROM with G as a random oracle, PKE' is one-way under chosen-plaintext attacks (i.e., OW-CPA secure) whenever PKE is so. Unlike ACWC_0, ACWC_1 does not require adding redundancy to ciphertexts.

$\underline{\mathsf{Gen}'(1^n)}$
1: $(pk, sk) := \mathsf{Gen}(1^n)$
return (pk, sk)

$\underline{\mathsf{Enc}'(pk, m \in \mathcal{M}'; (R_1, R_2) \in \mathcal{R}')}$
1: $M_1 \leftarrow \psi_{\mathcal{M}_1}$ using the randomness R_1
2: $r \leftarrow \psi_{\mathcal{R}}$ using the randomness R_2
3: $M_2 := \mathsf{Encode}(m, \mathsf{G}(M_1))$
4: $c := \mathsf{Enc}(pk, M_1||M_2; r)$
return c

$\underline{\mathsf{Dec}'(sk, c)}$
1: $M_1||M_2 := \mathsf{Dec}(sk, c)$
2: $m := \mathsf{Inv}(M_2, \mathsf{G}(M_1))$
return m

Figure 2: $\mathsf{ACWC}_1[\mathsf{PKE}, \mathsf{GOTP}, \mathsf{G}]$ transformation

3.3 ACWC_2

Analogously to ACWC_1, ACWC_2 employs a semi-generalized one-time pad (SOTP) [14] together with a hash function G modeled as a (quantum) random oracle.

Definition 3.2. A semi-generalized one-time pad $\mathsf{SOTP} = (\mathsf{Encode}, \mathsf{Inv})$ with a message space $\mathcal{X}$, a randomness space $\mathcal{U}$, and a code space $\mathcal{Y}$ (with distributions $\psi_{\mathcal{X}}, \psi_{\mathcal{U}}, \psi_{\mathcal{Y}}$) comprises deterministic algorithms:

- $\mathsf{Encode}(x, u)$: on input a message $x \in \mathcal{X}$ and a randomness $u \in \mathcal{U}$ outputs a code $y \in \mathcal{Y}$.
- $\mathsf{Inv}(y, u)$: on input a code $y \in \mathcal{Y}$ and a randomness $u \in \mathcal{U}$ outputs either a message $x \in \mathcal{X}$ or $\perp$.

It satisfies:

1. **Decoding:** $\mathsf{Inv}(\mathsf{Encode}(x, u), u) = x$ for all $x \in \mathcal{X}, u \in \mathcal{U}$.
2. **Message hiding:** For every $x \in \mathcal{X}$, the distribution of $\mathsf{Encode}(x, u)$ with $u \leftarrow \psi_{\mathcal{U}}$ equals $\psi_{\mathcal{Y}}$.
3. **Rigidity:** For all $u \in \mathcal{U}$ and $y \in \mathcal{Y}$ with $\mathsf{Inv}(y, u) \neq \perp$, one has $\mathsf{Encode}(\mathsf{Inv}(y, u), u) = y$.

There are two differences between GOTP and SOTP: (1) Inv of SOTP outputs $\perp$ for an invalid input, which means that there is a process to determine whether the input (y, u) is valid or not, and (2) SOTP needs the rigidity, instead of the randomness-hiding property of GOTP.

For ACWC_2, the derived $\mathsf{PKE}' = (\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$[1] has message space $\mathcal{M}'$ and randomness space $\mathcal{R}'$, while the underlying $\mathsf{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{RRec})$ has message space $\mathcal{M}$ and randomness space $\mathcal{R}$ with distributions $\psi_{\mathcal{M}}$ and $\psi_{\mathcal{R}}$. The additional randomness-recovery algorithm RRec guarantees that given a ciphertext c and its decryption $M \in \mathcal{M}$, one can recover the associated randomness $r \in \mathcal{R}$ such that $c = \mathsf{Enc}(pk, M; r)$; if $r \notin \mathcal{R}$, RRec outputs $\perp$, implicitly checking validity. Let $\mathsf{G} : \{0,1\}^* \to \mathcal{U}$ for the distribution $\psi_{\mathcal{U}}$, and let $\mathsf{Encode} : \mathcal{M}' \times \mathcal{U} \to \mathcal{M}$ and $\mathsf{Inv} : \mathcal{M} \times \mathcal{U} \to \mathcal{M}'$ be the SOTP algorithms. Figure 3 illustrates ACWC_2 and the instantiation $\mathsf{PKE}' = \mathsf{ACWC}_2[\mathsf{PKE}, \mathsf{SOTP}, \mathsf{G}]$. By the message-hiding property

[1] In a standard PKE syntax, the public key is not used explicitly in decryption. However, the ACWC_2 transformation requires the public key in the decryption step because the randomness-recovery algorithm RRec takes (pk, M, c) as input. For this reason, we write the decryption algorithm as $\mathsf{Dec}'(pk, sk, c)$.

of SOTP, the encoded M is distributed as $\psi_{\mathcal{M}}$ regardless of the choice of $m \in \mathcal{M}'$. Regarding security, [14] shows that in the (Q)ROM, PKE′ is IND-CPA secure assuming PKE is OW-CPA secure[2].

$\underline{\mathsf{Gen}'(1^n)}$
1: $(pk, sk) := \mathsf{Gen}(1^n)$
return (pk, sk)

$\underline{\mathsf{Enc}'(pk, m \in \mathcal{M}'; R \in \mathcal{R}')}$
1: $r \leftarrow \psi_{\mathcal{R}}$ using the randomness R
2: $M := \mathsf{Encode}(m, \mathsf{G}(r))$
3: $c := \mathsf{Enc}(pk, M; r)$
return c

$\underline{\mathsf{Dec}'(pk, sk, c)}$
1: $M := \mathsf{Dec}(sk, c)$
2: $r := \mathsf{RRec}(pk, M, c)$
3: $m := \mathsf{Inv}(M, \mathsf{G}(r))$
4: **if** $r \notin \mathcal{R}$ or $m = \perp$
return $\perp$
return m

Figure 3: $\mathsf{ACWC}_2[\mathsf{PKE}, \mathsf{SOTP}, \mathsf{G}]$ transformation

4 Spreadness Proofs in ACWC Transformations

We show that an ACWC-transformed PKE′ is γ'-spread in the (Q)ROM, assuming that an underlying PKE is γ-spread and G is modeled as a random oracle. Our new rigorous analysis establishes $\gamma' = \gamma + \lambda$ for ACWC_0 and $\gamma' = \gamma$ for ACWC_1 and ACWC_2. That is, ACWC_0 preserves the spreadness of PKE up to an additive λ term, whereas ACWC_1 and ACWC_2 preserve it exactly in the (Q)ROM. By contrast, previous analyses [5, 14] roughly stated that γ-spreadness lifts to PKE′, neglecting the subtle dependency described below. Let $\{\mathcal{M}', \mathcal{C}', \mathcal{R}'\}$ be the {message, ciphertext, randomness} sets of PKE′, respectively. In analyzing the γ'-spreadness of PKE′, we fix $m \in \mathcal{M}'$ and consider the probability $\max_{c \in \mathcal{C}'} \Pr_{\mathsf{G}, R \leftarrow \psi_{\mathcal{R}'}}[c = \mathsf{Enc}'(pk, m; R)]$; the difficulty lies in the fact that, over random choices $R \leftarrow \psi_{\mathcal{R}'}$, a fixed message $m \in \mathcal{M}'$ of PKE′ does not lead to a fixed message $M \in \mathcal{M}$ of PKE, and rather through all the above-mentioned ACWC transformations, M of PKE is changed according to a chosen randomness $R \in \mathcal{R}'$ of PKE′. Therefore, in analyzing the above probability in the (Q)ROM, we need to consider all possible randomness-dependent messages $\{M\}$ over random choices $R \leftarrow \psi_{\mathcal{R}'}$ and random oracle G.

Although the three ACWC transformations require separate analyses, the proofs of (weak) γ-spreadness in the (Q)ROM follow the same general pattern. We first use the random-oracle-induced distribution and the message-hiding property of the encoded component to rewrite the transformed-scheme encryption probability as a weighted sum over base-scheme encryptions with a fixed underlying message. We then apply the γ-spreadness of the base PKE to each such fixed-message slice. For the weak γ-spreadness in the (Q)ROM, the same fixed-key derivation is followed by taking expectation over key generation.

4.1 New Proof on the γ' -Spreadness of $\mathsf{ACWC}_0[\mathsf{PKE}, \mathsf{G}]$

Let $m \in \mathcal{M}' = \{0,1\}^\lambda$ be fixed. The γ'-spreadness of PKE′ in the (Q)ROM is defined as the maximum probability that $\mathsf{Enc}'(pk, m; R)$ equals a given ciphertext $c \in \mathcal{C}'$, where the probability is taken over the encryption randomness $R \leftarrow \psi_{\mathcal{R}'}$ and the random choice of the oracle G. Under ACWC_0, $c = (c_1, c_2)$ with $c_1 = \mathsf{Enc}(pk, M; r)$ and $c_2 = \mathsf{G}(M) \oplus m$, where (M, r) are sampled from $R = (R_1, R_2)$, respectively. Hence although m of PKE′ is fixed, the underlying message $M \in \mathcal{M}$ of PKE varies with R. To reduce γ' to

[2]Their analysis in [14] additionally requires the base PKE to be message-recoverable and (computationally) injective; we omit those auxiliary assumptions here to focus on ACWC_2 and γ-spreadness.

the γ-spreadness of PKE, we need to fix a message $M \in \mathcal{M}$ of PKE. To relate γ' to the γ-spreadness of PKE, we use the Law of Total Probability to consider all possible cases generated by all sampling messages $\{M_j\}$ and randomnesses $\{r_i\}$. Next, we leverage the random oracle property to ensure that $c_1 = \mathsf{Enc}(pk, M_j; r_i)$ and $c_2 = \mathsf{G}(M_j) \oplus m$ are probabilistically independent. Assuming that G is modeled as a random oracle and *chosen at random*, evaluating $\mathsf{G}(M_j)$ is identical to sampling a random u from $\{0,1\}^\lambda$, and by the message-hiding property of the One-Time Pad $c_2 = u \oplus m$ is also uniformly random in $\{0,1\}^\lambda$. Therefore, by replacing $c_2 = \mathsf{G}(M_j) \oplus m$ with a uniformly sampled $\tilde{c} \leftarrow \{0,1\}^\lambda$, we can eliminate any dependence of c_2 on M_j, allowing us to treat c_1 and c_2 as independent in terms of their probability distributions. Lastly, we define two indicator functions $\mathbf{I}(pk, M_j, r_i, c_1)$ and $\mathbf{I}'(\tilde{c}, c_2)$ that output 0 or 1, reflecting the probability that $c_1 \stackrel{?}{=} \mathsf{Enc}(pk, M_j; r_i)$ for a given (c_1, M_j, r_i) and the probability that $c_2 \stackrel{?}{=} \tilde{c}$ for a given $(c_2, \tilde{c})$. Using these functions, we can scan all possible combinations of (M_j, r_i) and $\tilde{c}$ that match a specific $c = (c_1, c_2)$. Especially, the sum of the indicator function $\mathbf{I}(pk, M_j, r_i, c_1)$ for all sampled $\{r_i\}$ is related to the γ-spreadness of PKE in case when M_j of PKE is fixed, because the function accounts only for the probability of sampling r_i such that $c_1 = \mathsf{Enc}(pk, M_j; r_i)$. Using this property, we can upper-bound the sum of $\mathbf{I}(pk, M_j, r_i, c_1)$ for all sampled $\{r_i\}$ by the probability $2^{-\gamma}$ for each message M_j and a specific c_1.

Theorem 4.1. If PKE is γ-spread and G is modeled as a random oracle, then $\mathsf{PKE}' = \mathsf{ACWC}_0[\mathsf{PKE}, \mathsf{G}]$ is γ'-spread in the (Q)ROM with

$$\gamma' = \gamma + \lambda,$$

where λ is the message length of PKE'.

Proof. c is composed of (c_1, c_2), and thus we need to consider the spreadness of both c_1 and c_2 in analyzing the spreadness of c. For a fixed key pair (pk, sk) and a fixed m in PKE', we consider the probability $\Pr_{R \leftarrow \mathcal{R}', \mathsf{G}}[c = \mathsf{Enc}'(pk, m; R)]$ for every possible ciphertext c where $R = (R_1, R_2)$. Since M and r are sampled according to $\psi_\mathcal{M}$ and $\psi_\mathcal{R}$ using the randomness (R_1, R_2), respectively, the probability is taken over random choices of M and r. When assuming G is chosen at random, the probability can be expressed as

$$\Pr_{R \leftarrow \mathcal{R}', \mathsf{G}}[c = \mathsf{Enc}'(pk, m; R)] = \Pr_{r \leftarrow \psi_\mathcal{R}, M \leftarrow \psi_\mathcal{M}, \mathsf{G}}[c_1 = \mathsf{Enc}(pk, M; r) \wedge c_2 = \mathsf{G}(M) \oplus m].$$

Using the Law of Total Probability, we consider all possible values of $r_i \in \mathcal{R}$ and $M_j \in \mathcal{M}$ into conditions:

$$\begin{aligned}
&\Pr_{r \leftarrow \psi_\mathcal{R}, M \leftarrow \psi_\mathcal{M}, \mathsf{G}}[c_1 = \mathsf{Enc}(pk, M; r) \wedge c_2 = \mathsf{G}(M) \oplus m] \\
&= \sum_{r_i \in \mathcal{R}} \Pr_{M \leftarrow \psi_\mathcal{M}, \mathsf{G}}[c_1 = \mathsf{Enc}(pk, M; r) \wedge c_2 = \mathsf{G}(M) \oplus m \mid r = r_i] \cdot \Pr_{r \leftarrow \psi_\mathcal{R}}[r = r_i] \\
&= \sum_{r_i \in \mathcal{R}} \Pr_{M \leftarrow \psi_\mathcal{M}, \mathsf{G}}[c_1 = \mathsf{Enc}(pk, M; r_i) \wedge c_2 = \mathsf{G}(M) \oplus m] \cdot \Pr_{r \leftarrow \psi_\mathcal{R}}[r = r_i] \\
&= \sum_{r_i \in \mathcal{R}} \sum_{M_j \in \mathcal{M}} \Pr_{\mathsf{G}}[c_1 = \mathsf{Enc}(pk, M_j; r_i) \wedge c_2 = \mathsf{G}(M_j) \oplus m] \cdot \Pr_{M \leftarrow \psi_\mathcal{M}}[M = M_j] \cdot \Pr_{r \leftarrow \psi_\mathcal{R}}[r = r_i].
\end{aligned}$$

By the random oracle assumption, $\mathsf{G}(M_j)$ is uniform and the distribution of $\mathsf{G}(M_j) \oplus m$ is identical to

that of a uniformly random $\tilde{c} \leftarrow \{0,1\}^\lambda$.

$$\begin{aligned}
&\sum_{r_i \in \mathcal{R}} \sum_{M_j \in \mathcal{M}} \Pr_{\mathsf{G}}[c_1 = \mathsf{Enc}(pk, M_j; r_i) \wedge c_2 = \mathsf{G}(M_j) \oplus m] \cdot \Pr_{M \leftarrow \psi_{\mathcal{M}}}[M = M_j] \cdot \Pr_{r \leftarrow \psi_{\mathcal{R}}}[r = r_i] \\
&= \sum_{r_i \in \mathcal{R}} \sum_{M_j \in \mathcal{M}} \Pr_{u \leftarrow \{0,1\}^\lambda}[c_1 = \mathsf{Enc}(pk, M_j; r_i) \wedge c_2 = u \oplus m] \cdot \Pr_{M \leftarrow \psi_{\mathcal{M}}}[M = M_j] \cdot \Pr_{r \leftarrow \psi_{\mathcal{R}}}[r = r_i] \\
&= \sum_{r_i \in \mathcal{R}} \sum_{M_j \in \mathcal{M}} \Pr_{\tilde{c} \leftarrow \{0,1\}^\lambda}[c_1 = \mathsf{Enc}(pk, M_j; r_i) \wedge c_2 = \tilde{c}] \cdot \Pr_{M \leftarrow \psi_{\mathcal{M}}}[M = M_j] \cdot \Pr_{r \leftarrow \psi_{\mathcal{R}}}[r = r_i].
\end{aligned}$$

Now, we leverage independence of $c_1 = \mathsf{Enc}(pk, M_j; r_i)$ and $c_2 = \tilde{c}$. To facilitate our analysis, we define two indicator functions $\mathbf{I}(pk, M, r, c_1) = [\![c_1 == \mathsf{Enc}(pk, M; r)]\!]$ and $\mathbf{I}'(\tilde{c}, c_2) = [\![c_2 == \tilde{c}]\!]$. Then,

$$\begin{aligned}
&\sum_{r_i \in \mathcal{R}} \sum_{M_j \in \mathcal{M}} \Pr_{\tilde{c} \leftarrow \{0,1\}^\lambda}[c_1 = \mathsf{Enc}(pk, M_j; r_i) \wedge c_2 = \tilde{c}] \cdot \Pr_{M \leftarrow \psi_{\mathcal{M}}}[M = M_j] \cdot \Pr_{r \leftarrow \psi_{\mathcal{R}}}[r = r_i] \\
&= \sum_{r_i \in \mathcal{R}} \sum_{M_j \in \mathcal{M}} \sum_{\tilde{c}_k \in \{0,1\}^\lambda} \left(\mathbf{I}(pk, M_j, r_i, c_1) \cdot \mathbf{I}'(\tilde{c}_k, c_2) \cdot \Pr_{\tilde{c} \leftarrow \{0,1\}^\lambda}[\tilde{c} = \tilde{c}_k] \right) \cdot \\
&\qquad \Pr_{M \leftarrow \psi_{\mathcal{M}}}[M = M_j] \cdot \Pr_{r \leftarrow \psi_{\mathcal{R}}}[r = r_i] \\
&= \left(\sum_{\tilde{c}_k \in \{0,1\}^\lambda} \mathbf{I}'(\tilde{c}_k, c_2) \cdot \Pr_{\tilde{c} \leftarrow \{0,1\}^\lambda}[\tilde{c} = \tilde{c}_k] \right) \cdot \sum_{M_j \in \mathcal{M}} \sum_{r_i \in \mathcal{R}} \mathbf{I}(pk, M_j, r_i, c_1) \cdot \\
&\qquad \Pr_{r \leftarrow \psi_{\mathcal{R}}}[r = r_i] \cdot \Pr_{M \leftarrow \psi_{\mathcal{M}}}[M = M_j] \\
&= \left(\sum_{\tilde{c}_k \in \{0,1\}^\lambda} \mathbf{I}'(\tilde{c}_k, c_2) \cdot \Pr_{\tilde{c} \leftarrow \{0,1\}^\lambda}[\tilde{c} = \tilde{c}_k] \right) \cdot \sum_{M_j \in \mathcal{M}} \Pr_{r \leftarrow \psi_{\mathcal{R}}}[c_1 = \mathsf{Enc}(pk, M_j; r)] \cdot \Pr_{M \leftarrow \psi_{\mathcal{M}}}[M = M_j].
\end{aligned}$$

Since $\sum_{\tilde{c}_k \in \{0,1\}^\lambda} \mathbf{I}'(\tilde{c}_k, c_2) = 1$ holds for exactly one $\tilde{c}_k \in \{0,1\}^\lambda$, the probability $\Pr_{\tilde{c} \leftarrow \{0,1\}^\lambda}[\tilde{c} = \tilde{c}_k]$ is counted only once. Considering $\Pr_{r \leftarrow \psi_{\mathcal{R}}}[c_1 = \mathsf{Enc}(pk, M_j; r)]$ as the γ-spreadness of PKE for a message M_j, we use the fact that $\Pr_{r \leftarrow \psi_{\mathcal{R}}}[c_1 = \mathsf{Enc}(pk, M_j; r)] \leq 2^{-\gamma}$ for a specific c_1 and each M_j. Therefore, the value $2^{-\gamma}$ can be treated as a constant, and the sum of the probabilities satisfies $\sum_{M_j \in \mathcal{M}} \Pr_{M \leftarrow \psi_{\mathcal{M}}}[M = M_j] = 1$. Consequently, the γ'-spreadness of PKE' in the (Q)ROM is derived as follows:

$$\begin{aligned}
&\Pr_{R \leftarrow \mathcal{R}', \mathsf{G}}[c = \mathsf{Enc}'(pk, m; R)] \\
&= \Pr_{\tilde{c} \leftarrow \{0,1\}^\lambda}[\tilde{c} = \tilde{c}_k] \cdot \sum_{M_j \in \mathcal{M}} \Pr_{r \leftarrow \psi_{\mathcal{R}}}[c_1 = \mathsf{Enc}(pk, M_j; r)] \cdot \Pr_{M \leftarrow \psi_{\mathcal{M}}}[M = M_j] \\
&\leq \Pr_{\tilde{c} \leftarrow \{0,1\}^\lambda}[\tilde{c} = \tilde{c}_k] \cdot \sum_{M_j \in \mathcal{M}} 2^{-\gamma} \cdot \Pr_{M \leftarrow \psi_{\mathcal{M}}}[M = M_j] \\
&= 2^{-\lambda} \cdot 2^{-\gamma} \cdot \sum_{M_j \in \mathcal{M}} \Pr_{M \leftarrow \psi_{\mathcal{M}}}[M = M_j] \\
&= 2^{-\lambda - \gamma}.
\end{aligned}$$

Since the above analysis holds for any (pk, sk) and any $m \in \mathcal{M}'$, the γ'-spreadness of PKE' in the (Q)ROM is obtained as $\gamma' = \gamma + \lambda$ as required. □

Corollary 4.2. If PKE is weakly γ-spread and G is modeled as a random oracle, then $\mathsf{PKE}' = \mathsf{ACWC}_0[\mathsf{PKE}, \mathsf{G}]$ is weakly $(\gamma + \lambda)$-spread in the (Q)ROM, where λ is the message length of PKE'.

Proof. For each public key $pk \in \mathcal{PK}$, where $\mathcal{PK}$ denotes the set of all possible public keys, define

$$A_{pk} := \max_{M \in \mathcal{M}, c_1 \in \mathcal{C}} \Pr_{r \leftarrow \psi_{\mathcal{R}}} [\, c_1 = \mathsf{Enc}(pk, M; r) \,]$$

and

$$A'_{pk} := \max_{\substack{m \in \mathcal{M}', \\ (c_1, c_2) \in \mathcal{C}'}} \Pr_{\mathsf{G},\, R \leftarrow \mathcal{R}'} [\, (c_1, c_2) = \mathsf{Enc}'(pk, m; R) \,].$$

By the definition of weak γ-spreadness in Definition 2.2, $\mathbb{E}_{(pk,sk)}[A_{pk}] \leq 2^{-\gamma}$. For each fixed pk, $m \in \mathcal{M}'$, and $(c_1, c_2) \in \mathcal{C}'$, by the same fixed-key derivation as in the proof of Theorem 4.1, we have

$$\begin{aligned}
\Pr_{\mathsf{G},\, R \leftarrow \mathcal{R}'} [\, c = \mathsf{Enc}'(pk, m; R) \,] &= \Pr_{\widetilde{c} \leftarrow \{0,1\}^\lambda} [\, \widetilde{c} = c_2 \,] \cdot \sum_{M_j \in \mathcal{M}} \Pr_{r \leftarrow \psi_{\mathcal{R}}} [\, c_1 = \mathsf{Enc}(pk, M_j; r) \,] \cdot \Pr_{M \leftarrow \psi_{\mathcal{M}}} [\, M = M_j \,] \\
&\leq 2^{-\lambda} \sum_{M_j \in \mathcal{M}} A_{pk} \cdot \Pr_{M \leftarrow \psi_{\mathcal{M}}} [\, M = M_j \,] \\
&= 2^{-\lambda} A_{pk} \sum_{M_j \in \mathcal{M}} \Pr_{M \leftarrow \psi_{\mathcal{M}}} [\, M = M_j \,] \\
&= 2^{-\lambda} A_{pk},
\end{aligned}$$

where $\widetilde{c} := \mathsf{G}(M) \oplus m$. Since ACWC_0 uses $\mathsf{G} : \{0,1\}^* \to \{0,1\}^\lambda$ with uniform output, $\widetilde{c}$ is uniformly distributed over $\{0,1\}^\lambda$. Since this holds for every $m \in \mathcal{M}'$ and $(c_1, c_2) \in \mathcal{C}'$, it follows that

$$A'_{pk} \leq 2^{-\lambda} A_{pk}.$$

Taking expectation over $(pk, sk) \leftarrow \mathsf{Gen}(1^n)$ [3], we obtain

$$\mathbb{E}_{(pk,sk)}[A'_{pk}] \leq 2^{-\lambda} \mathbb{E}_{(pk,sk)}[A_{pk}] \leq 2^{-(\gamma+\lambda)}.$$

□

4.2 New Proof on the γ' -Spreadness of $\mathsf{ACWC}_1[\mathsf{PKE}, \mathsf{GOTP}, \mathsf{G}]$

A ciphertext c generated by ACWC_1 is $c = \mathsf{Enc}'(pk, m; (R_1, R_2)) = \mathsf{Enc}(pk, M_1 \| \mathsf{Encode}(m, \mathsf{G}(M_1)); r)$, where M_1 and r are sampled from $\psi_{\mathcal{M}_1}$ and $\psi_{\mathcal{R}}$ using randomness R_1 and R_2, respectively. As in ACWC_0, for a fixed message $m \in \mathcal{M}'$, the message $M_1 \| \mathsf{Encode}(m, \mathsf{G}(M_1))$ of PKE is changed depending on the choice of M_1. Under the assumption that G is a random oracle and GOTP satisfies message-hiding, the encoded component $M_2 := \mathsf{Encode}(m, \mathsf{G}(M_1))$ is distributed according to $\psi_{\mathcal{M}_2}$, since $\mathsf{G}(M_1)$ can be viewed as sampled from $\psi_{\mathcal{U}}$ and the message-hiding property renders M_2 independent of m. We then apply the law of total probability over all choices of $M_1 \| M_2$ and r. In this context, the γ'-spreadness of PKE' in the (Q)ROM is analyzed as the maximum probability $\Pr[c = \mathsf{Enc}(pk, M_1 \| M_2; r)]$, based on the sampling probabilities of $M_1 \leftarrow \psi_{\mathcal{M}_1}$, $M_2 \leftarrow \psi_{\mathcal{M}_2}$, and $r \leftarrow \psi_{\mathcal{R}}$ in PKE. To organize the contribution of all tuples (M_1, M_2, r) that produce c, we introduce an indicator function for matching, and then, when summing over r, the resulting quantity is upper-bounded by the γ-spreadness of the base PKE in the same manner as in ACWC_0.

[3] Since ACWC transformation preserves the key-generation algorithm, we identify $\mathsf{Gen}' = \mathsf{Gen}$ and write $(pk, sk) \leftarrow \mathsf{Gen}(1^n)$ throughout. In particular, A_{pk} and A'_{pk} are quantities associated with the same public key pk.

Theorem 4.3. If PKE is γ-spread, GOTP satisfies message-hiding, and G is modeled as a random oracle, then the transformed scheme $\mathsf{PKE}' = \mathsf{ACWC}_1[\mathsf{PKE}, \mathsf{GOTP}, \mathsf{G}]$ is γ'-spread in the (Q)ROM, where $\gamma' = \gamma$.

Proof. For a fixed key (pk, sk) and a fixed message m in PKE', we consider the probability $\Pr_{R\leftarrow\mathcal{R}',\mathsf{G}}[c = \mathsf{Enc}'(pk, m; R)]$ for every possible ciphertext c where $R = (R_1, R_2)$. By the fact that M_1 and r are sampled according to $\psi_{\mathcal{M}_1}$ and $\psi_{\mathcal{R}}$ with the randomness R_1 and R_2 respectively, the probability is taken over random choice of M_1 and r. When assuming G is a random oracle, the probability can be expressed as

$$\Pr_{R\leftarrow\mathcal{R}',\mathsf{G}}[c = \mathsf{Enc}'(pk, m; R)] = \Pr_{M_1\leftarrow\psi_{\mathcal{M}_1}, r\leftarrow\psi_{\mathcal{R}},\mathsf{G}}[c = \mathsf{Enc}(pk, M_1||\mathsf{Encode}(m, \mathsf{G}(M_1)); r)].$$

We leverage the Law of Total Probability to consider all possible values of $r_i \in \mathcal{R}$ and $M_{1,i} \in \mathcal{M}_1$ as conditions:

$$\begin{aligned}
&\Pr_{M_1\leftarrow\psi_{\mathcal{M}_1}, r\leftarrow\psi_{\mathcal{R}},\mathsf{G}}[c = \mathsf{Enc}(pk, M_1||\mathsf{Encode}(m, \mathsf{G}(M_1)); r)] \\
&= \sum_{r_i\in\mathcal{R}} \Pr_{M_1\leftarrow\psi_{\mathcal{M}_1},\mathsf{G}}[c = \mathsf{Enc}(pk, M_1||\mathsf{Encode}(m, \mathsf{G}(M_1)); r) \mid r = r_i] \cdot \Pr_{r\leftarrow\psi_{\mathcal{R}}}[r = r_i] \\
&= \sum_{r_i\in\mathcal{R}} \Pr_{M_1\leftarrow\psi_{\mathcal{M}_1},\mathsf{G}}[c = \mathsf{Enc}(pk, M_1||\mathsf{Encode}(m, \mathsf{G}(M_1)); r_i)] \cdot \Pr_{r\leftarrow\psi_{\mathcal{R}}}[r = r_i] \\
&= \sum_{r_i\in\mathcal{R}} \sum_{M_{1,j}\in\mathcal{M}_1} \Pr_{\mathsf{G}}[c = \mathsf{Enc}(pk, M_{1,j}||\mathsf{Encode}(m, \mathsf{G}(M_{1,j})); r_i)] \cdot \Pr_{M_1\leftarrow\psi_{\mathcal{M}_1}}[M_1 = M_{1,j}] \cdot \Pr_{r\leftarrow\psi_{\mathcal{R}}}[r = r_i].
\end{aligned}$$

By the fact that $\mathsf{G}(M_{1,j})$ is $\psi_{\mathcal{U}}$-distributed and the message hiding property of GOTP holds for $\mathsf{G}(M_{1,j})$, the output $M_2 = \mathsf{Encode}(m, \mathsf{G}(M_{1,j}))$ is $\psi_{\mathcal{M}_2}$-distributed over random choice of G.

$$\begin{aligned}
&\sum_{r_i\in\mathcal{R}} \sum_{M_{1,j}\in\mathcal{M}_1} \Pr_{\mathsf{G}}[c = \mathsf{Enc}(pk, M_{1,j}||\mathsf{Encode}(m, \mathsf{G}(M_{1,j})); r_i)] \cdot \\
&\qquad\qquad \Pr_{M_1\leftarrow\psi_{\mathcal{M}_1}}[M_1 = M_{1,j}] \cdot \Pr_{r\leftarrow\psi_{\mathcal{R}}}[r = r_i] \\
&= \sum_{r_i\in\mathcal{R}} \sum_{M_{1,j}\in\mathcal{M}_1} \Pr_{u\leftarrow\psi_{\mathcal{U}}}[c = \mathsf{Enc}(pk, M_{1,j}||\mathsf{Encode}(m, u); r_i)] \cdot \\
&\qquad\qquad \Pr_{M_1\leftarrow\psi_{\mathcal{M}_1}}[M_1 = M_{1,j}] \cdot \Pr_{r\leftarrow\psi_{\mathcal{R}}}[r = r_i] \\
&= \sum_{r_i\in\mathcal{R}} \sum_{M_{1,j}\in\mathcal{M}_1} \Pr_{M_2\leftarrow\psi_{\mathcal{M}_2}}[c = \mathsf{Enc}(pk, M_{1,j}||M_2; r_i)] \cdot \Pr_{M_1\leftarrow\psi_{\mathcal{M}_1}}[M_1 = M_{1,j}] \cdot \Pr_{r\leftarrow\psi_{\mathcal{R}}}[r = r_i].
\end{aligned}$$

Next, we consider all possible combinations of (r, M_1, M_2) which is mapped to a specific c. Introducing an indicator $\mathbf{I}(pk, M_1, M_2, r, c) = [\![c == \mathsf{Enc}(pk, M_1||M_2; r)]\!]$, the sum can be rewritten as follows :

$$\sum_{r_i\in\mathcal{R}}\sum_{M_{1,j}\in\mathcal{M}_1}\Pr_{M_2\leftarrow\psi_{\mathcal{M}_2}}[c=\mathsf{Enc}(pk,M_{1,j}||M_2;r_i)]\cdot\Pr_{M_1\leftarrow\psi_{\mathcal{M}_1}}[M_1=M_{1,j}]\cdot\Pr_{r\leftarrow\psi_{\mathcal{R}}}[r=r_i]$$

$$=\sum_{r_i\in\mathcal{R}}\sum_{M_{1,j}\in\mathcal{M}_1}\left(\sum_{M_{2,k}\in\mathcal{M}_2}\mathbf{I}(pk,M_{1,j},M_{2,k},r_i,c)\cdot\Pr_{M_2\leftarrow\psi_{\mathcal{M}_2}}[M_2=M_{2,k}]\right)\cdot$$
$$\Pr_{M_1\leftarrow\psi_{\mathcal{M}_1}}[M_1=M_{1,j}]\cdot\Pr_{r\leftarrow\psi_{\mathcal{R}}}[r=r_i]$$

$$=\sum_{M_{2,k}\in\mathcal{M}_2}\sum_{M_{1,j}\in\mathcal{M}_1}\left(\sum_{r_i\in\mathcal{R}}\mathbf{I}(pk,M_{1,j},M_{2,k},r_i,c)\cdot\Pr_{r\leftarrow\psi_{\mathcal{R}}}[r=r_i]\right)\cdot$$
$$\Pr_{M_1\leftarrow\psi_{\mathcal{M}_1}}[M_1=M_{1,j}]\cdot\Pr_{M_2\leftarrow\psi_{\mathcal{M}_2}}[M_2=M_{2,k}]$$

$$=\sum_{M_{2,k}\in\mathcal{M}_2}\sum_{M_{1,j}\in\mathcal{M}_1}\Pr_{r\leftarrow\psi_{\mathcal{R}}}[c=\mathsf{Enc}(pk,M_{1,j}||M_{2,k};r)]\cdot$$
$$\Pr_{M_1\leftarrow\psi_{\mathcal{M}_1}}[M_1=M_{1,j}]\cdot\Pr_{M_2\leftarrow\psi_{\mathcal{M}_2}}[M_2=M_{2,k}].$$

Considering $\Pr_{r\leftarrow\psi_{\mathcal{R}}}[c=\mathsf{Enc}(pk,M_{1,j}||M_{2,k};r)]$ over all messages $M_{1,j}||M_{2,k}$, the maximum probability is upper-bounded by $2^{-\gamma}$ by the γ-spreadness of PKE. Since $2^{-\gamma}$ is treated as a constant, the sum of the probabilities of M_1 and M_2 becomes 1, respectively. Then, the γ'-spreadness of PKE' in the (Q)ROM is upper-bounded as:

$$\Pr_{R\leftarrow\mathcal{R}',\mathsf{G}}[c=\mathsf{Enc}'(pk,m;R)]$$
$$=\sum_{M_{2,k}\in\mathcal{M}_2}\sum_{M_{1,j}\in\mathcal{M}_1}\Pr_{r\leftarrow\psi_{\mathcal{R}}}[c=\mathsf{Enc}(pk,M_{1,j}||M_{2,k};r)]\cdot\Pr_{M_1\leftarrow\psi_{\mathcal{M}_1}}[M_1=M_{1,j}]\cdot\Pr_{M_2\leftarrow\psi_{\mathcal{M}_2}}[M_2=M_{2,k}]$$
$$\leq\sum_{M_{2,k}\in\mathcal{M}_2}\sum_{M_{1,j}\in\mathcal{M}_1}2^{-\gamma}\cdot\Pr_{M_1\leftarrow\psi_{\mathcal{M}_1}}[M_1=M_{1,j}]\cdot\Pr_{M_2\leftarrow\psi_{\mathcal{M}_2}}[M_2=M_{2,k}]$$
$$=2^{-\gamma}\cdot\sum_{M_{2,k}\in\mathcal{M}_2}\sum_{M_{1,j}\in\mathcal{M}_1}\Pr_{M_1\leftarrow\psi_{\mathcal{M}_1}}[M_1=M_{1,j}]\cdot\Pr_{M_2\leftarrow\psi_{\mathcal{M}_2}}[M_2=M_{2,k}]$$
$$=2^{-\gamma}.$$

Since this holds for any (pk,sk) and any $m\in\mathcal{M}'$, the γ'-spreadness of PKE' in the (Q)ROM is obtained as $\gamma'=\gamma$ as required. □

Corollary 4.4. If PKE is weakly γ-spread, GOTP satisfies message-hiding, and G is modeled as a random oracle, then $\mathsf{PKE}'=\mathsf{ACWC}_1[\mathsf{PKE},\mathrm{GOTP},\mathsf{G}]$ is weakly γ-spread in the (Q)ROM.

Proof. For each public key $pk\in\mathcal{PK}$ generated by $\mathsf{Gen}(1^n)$, define

$$A_{pk}:=\max_{M\in\mathcal{M},\,c\in\mathcal{C}}\Pr_{r\leftarrow\psi_{\mathcal{R}}}[\,c=\mathsf{Enc}(pk,M;r)\,]$$

and

$$A'_{pk}:=\max_{m\in\mathcal{M}',\,c\in\mathcal{C}'}\Pr_{\mathsf{G},\,R\leftarrow\mathcal{R}'}[\,c=\mathsf{Enc}'(pk,m;R)\,].$$

By the definition of weak γ-spreadness of PKE, $\mathbb{E}_{(pk,sk)}[A_{pk}] \leq 2^{-\gamma}$. By the same fixed-key derivation as in the proof of Theorem 4.3, we have

$$\begin{aligned}
\Pr_{\mathsf{G},\, R\leftarrow\mathcal{R}'}[\, c = \mathsf{Enc}'(pk, m; R)\,] &= \sum_{M_{2,k}\in\mathcal{M}_2}\sum_{M_{1,j}\in\mathcal{M}_1} \Pr_{r\leftarrow\psi_{\mathcal{R}}}[\, c = \mathsf{Enc}(pk, M_{1,j}\|M_{2,k}; r)\,] \\
&\qquad \cdot \Pr_{M_1\leftarrow\psi_{\mathcal{M}_1}}[\, M_1 = M_{1,j}\,] \cdot \Pr_{M_2\leftarrow\psi_{\mathcal{M}_2}}[\, M_2 = M_{2,k}\,] \\
&\leq \sum_{M_{2,k}\in\mathcal{M}_2}\sum_{M_{1,j}\in\mathcal{M}_1} A_{pk} \cdot \Pr_{M_1\leftarrow\psi_{\mathcal{M}_1}}[\, M_1 = M_{1,j}\,] \cdot \Pr_{M_2\leftarrow\psi_{\mathcal{M}_2}}[\, M_2 = M_{2,k}\,] \\
&= A_{pk}\left(\sum_{M_{1,j}\in\mathcal{M}_1} \Pr_{M_1\leftarrow\psi_{\mathcal{M}_1}}[\, M_1 = M_{1,j}\,]\right)\left(\sum_{M_{2,k}\in\mathcal{M}_2} \Pr_{M_2\leftarrow\psi_{\mathcal{M}_2}}[\, M_2 = M_{2,k}\,]\right) \\
&= A_{pk},
\end{aligned}$$

where $M_2 := \mathsf{Encode}(m, \mathsf{G}(M_1))$. By the message-hiding property of GOTP and the fact that G is modeled as a random oracle, the induced distribution of M_2 is exactly $\psi_{\mathcal{M}_2}$, independently of the choice of m, while M_1 is distributed according to $\psi_{\mathcal{M}_1}$. Since this holds for every $m \in \mathcal{M}'$ and every $c \in \mathcal{C}'$, it follows that

$$A'_{pk} \leq A_{pk}.$$

Taking expectation over $(pk, sk) \leftarrow \mathsf{Gen}(1^n)$, $\mathbb{E}_{(pk,sk)}[A'_{pk}] \leq \mathbb{E}_{(pk,sk)}[A_{pk}] \leq 2^{-\gamma}$. □

4.3 New Proof on the γ' -Spreadness of $\mathsf{ACWC}_2[\mathsf{PKE}, \mathsf{SOTP}, \mathsf{G}]$

Building on the framework of [15], we retain its high-level structure but derive a refined and tighter upper bound on the γ'-spreadness of PKE' in the (Q)ROM in Theorem 4.5.

A ciphertext in ACWC_2 is of the form $c = \mathsf{Enc}'(pk, m; R) = \mathsf{Enc}(pk, \mathsf{Encode}(m, \mathsf{G}(r)); r)$, where r is sampled from $\psi_{\mathcal{R}}$ according to R. For a fixed $m \in \mathcal{M}'$, the encoded message $M = \mathsf{Encode}(m, \mathsf{G}(r))$ for PKE is changed depending on the choice of r. Under the random oracle model for G and assuming SOTP satisfies message-hiding, M is distributed as $\psi_{\mathcal{M}}$. To consider all possible cases of M and r, we also leverage the Law of Total Probability. Accordingly, to analyze the above (Q)ROM quantity for PKE', we rewrite it using the induced distributions $M \leftarrow \psi_{\mathcal{M}}$ and $r \leftarrow \psi_{\mathcal{R}}$, and then bound it through the event $c = \mathsf{Enc}(pk, M; r)$. We define an indicator function to account for the probabilities of all possible combinations (M, r) that match a specific ciphertext c. Over the randomness sampled according to $r \leftarrow \psi_{\mathcal{R}}$, the sum of the probabilities regarding the indicator function can be upper-bounded by the γ-spreadness of PKE.

Theorem 4.5. If PKE is γ-spread, SOTP has the message hiding property, and G is modeled as a random oracle, then $\mathsf{PKE}' = \mathsf{ACWC}_2[\mathsf{PKE}, \mathsf{SOTP}, \mathsf{G}]$ is γ'-spread in the (Q)ROM, where $\gamma' = \gamma$.

Proof. For a fixed key (pk, sk) and a fixed message m in PKE', we consider the probability $\Pr_{R\leftarrow\mathcal{R}',\mathsf{G}}[c = \mathsf{Enc}'(pk, m; R)]$ for every possible ciphertext c. The probability is taken over a random choice of r, assuming G is a random oracle. When r is sampled as $r \leftarrow \psi_{\mathcal{R}}$ with the randomness $R \leftarrow \mathcal{R}'$, the probability can be expressed as

$$\Pr_{R\leftarrow\mathcal{R}',\mathsf{G}}[c = \mathsf{Enc}'(pk, m; R)] = \Pr_{r\leftarrow\psi_{\mathcal{R}},\mathsf{G}}[c = \mathsf{Enc}(pk, \mathsf{Encode}(m, \mathsf{G}(r)); r)].$$

We leverage the Law of Total Probability to consider all possible values of $r_i \in \mathcal{R}$ as conditions:

$$\begin{aligned}
&\Pr_{r\leftarrow\psi_{\mathcal{R}},\mathsf{G}}[c = \mathsf{Enc}(pk, \mathsf{Encode}(m, \mathsf{G}(r)); r)] \\
&= \sum_{r_i\in\mathcal{R}} \Pr_{\mathsf{G}}[c = \mathsf{Enc}(pk, \mathsf{Encode}(m, \mathsf{G}(r)); r) \mid r = r_i] \cdot \Pr_{r\leftarrow\psi_{\mathcal{R}}}[r = r_i] \\
&= \sum_{r_i\in\mathcal{R}} \Pr_{\mathsf{G}}[c = \mathsf{Enc}(pk, \mathsf{Encode}(m, \mathsf{G}(r_i)); r_i)] \cdot \Pr_{r\leftarrow\psi_{\mathcal{R}}}[r = r_i].
\end{aligned}$$

By the fact that $\mathsf{G}(r_i)$ is $\psi_{\mathcal{U}}$-distributed and the message hiding property of SOTP holds, the output $M = \mathsf{Encode}(m, \mathsf{G}(r_i))$ is $\psi_{\mathcal{M}}$-distributed over random choice of G.

$$\begin{aligned}
&\sum_{r_i\in\mathcal{R}} \Pr_{\mathsf{G}}[c = \mathsf{Enc}(pk, \mathsf{Encode}(m, \mathsf{G}(r_i)); r_i)] \cdot \Pr_{r\leftarrow\psi_{\mathcal{R}}}[r = r_i] \\
&= \sum_{r_i\in\mathcal{R}} \Pr_{u\leftarrow\psi_{\mathcal{U}}}[c = \mathsf{Enc}(pk, \mathsf{Encode}(m, u); r_i)] \cdot \Pr_{r\leftarrow\psi_{\mathcal{R}}}[r = r_i] \\
&= \sum_{r_i\in\mathcal{R}} \Pr_{M\leftarrow\psi_{\mathcal{M}}}[c = \mathsf{Enc}(pk, M; r_i)] \cdot \Pr_{r\leftarrow\psi_{\mathcal{R}}}[r = r_i].
\end{aligned}$$

Next, we consider all possible combinations of (r, M) which is mapped to a specific c. To facilitate our analysis, we define an indicator function $\mathbf{I}(pk, M, r, c) = [\![c == \mathsf{Enc}(pk, M; r)]\!]$. Then,

$$\begin{aligned}
&\sum_{r_i\in\mathcal{R}} \Pr_{M\leftarrow\psi_{\mathcal{M}}}[c = \mathsf{Enc}(pk, M; r_i)] \cdot \Pr_{r\leftarrow\psi_{\mathcal{R}}}[r = r_i] \\
&= \sum_{r_i\in\mathcal{R}} \Big(\sum_{M_j\in\mathcal{M}} \mathbf{I}(pk, M_j, r_i, c) \cdot \Pr_{M\leftarrow\psi_{\mathcal{M}}}[M = M_j] \Big) \cdot \Pr_{r\leftarrow\psi_{\mathcal{R}}}[r = r_i] \\
&= \sum_{M_j\in\mathcal{M}} \Big(\sum_{r_i\in\mathcal{R}} \mathbf{I}(pk, M_j, r_i, c) \cdot \Pr_{r\leftarrow\psi_{\mathcal{R}}}[r = r_i] \Big) \cdot \Pr_{M\leftarrow\psi_{\mathcal{M}}}[M = M_j] \\
&= \sum_{M_j\in\mathcal{M}} \Pr_{r\leftarrow\psi_{\mathcal{R}}}[c = \mathsf{Enc}(pk, M_j; r)] \cdot \Pr_{M\leftarrow\psi_{\mathcal{M}}}[M = M_j].
\end{aligned}$$

By the γ-spreadness of PKE, for each fixed ciphertext c and message M_j, the maximum probability $\Pr_{r\leftarrow\psi_{\mathcal{R}}}\big[c = \mathsf{Enc}(pk, M_j; r)\big] \leq 2^{-\gamma}$. Treating $2^{-\gamma}$ as a constant and summing over $M_j \leftarrow \psi_{\mathcal{M}}$ yields $\sum_{M_j} \Pr_M[M = M_j] = 1$. Hence the γ'-spreadness of PKE' in the (Q)ROM is bounded by :

$$\begin{aligned}
\Pr_{R\leftarrow\mathcal{R}',\mathsf{G}}[c = \mathsf{Enc}'(pk, m; R)] &= \sum_{M_j\in\mathcal{M}} \Pr_{r\leftarrow\psi_{\mathcal{R}}}[c = \mathsf{Enc}(pk, M_j; r)] \cdot \Pr_{M\leftarrow\psi_{\mathcal{M}}}[M = M_j] \\
&\leq \sum_{M_j\in\mathcal{M}} 2^{-\gamma} \cdot \Pr_{M\leftarrow\psi_{\mathcal{M}}}[M = M_j] \\
&= 2^{-\gamma} \cdot \sum_{M_j\in\mathcal{M}} \cdot \Pr_{M\leftarrow\psi_{\mathcal{M}}}[M = M_j] \\
&= 2^{-\gamma}.
\end{aligned}$$

Since the above analysis holds for any (pk, sk) and any $m \in \mathcal{M}'$, the γ'-spreadness of PKE' in the (Q)ROM, as required. □

Corollary 4.6. If PKE is weakly γ-spread, SOTP satisfies message-hiding, and G is modeled as a random oracle, then $\mathsf{PKE}' = \mathsf{ACWC}_2[\mathsf{PKE}, \mathrm{SOTP}, \mathsf{G}]$ is weakly γ-spread in the (Q)ROM.

Proof. For each public key $pk \in \mathcal{PK}$ generated by $\mathsf{Gen}(1^n)$, define

$$A_{pk} := \max_{M \in \mathcal{M},\, c \in \mathcal{C}} \Pr_{r \leftarrow \psi_{\mathcal{R}}} [\, c = \mathsf{Enc}(pk, M; r)\,]$$

and

$$A'_{pk} := \max_{m \in \mathcal{M}',\, c \in \mathcal{C}'} \Pr_{\mathsf{G},\, R \leftarrow \mathcal{R}'} [\, c = \mathsf{Enc}'(pk, m; R)\,].$$

By the definition of weak γ-spreadness of PKE, $\mathbb{E}_{(pk,sk)}[A_{pk}] \le 2^{-\gamma}$. By the same fixed-key derivation as in the proof of Theorem 4.5, for a fixed public key pk, we have

$$\begin{aligned}
\Pr_{\mathsf{G},\, R \leftarrow \mathcal{R}'} [\, c = \mathsf{Enc}'(pk, m; R)\,] &= \sum_{M_j \in \mathcal{M}} \Pr_{r \leftarrow \psi_{\mathcal{R}}} [c = \mathsf{Enc}(pk, M_j; r)] \cdot \Pr_{M \leftarrow \psi_{\mathcal{M}}} [M = M_j] \\
&\le \sum_{M_j \in \mathcal{M}} A_{pk} \cdot \Pr_{M \leftarrow \psi_{\mathcal{M}}} [M = M_j] \\
&= A_{pk} \cdot \sum_{M_j \in \mathcal{M}} \Pr_{M \leftarrow \psi_{\mathcal{M}}} [M = M_j] \\
&= A_{pk},
\end{aligned}$$

where $M = \mathsf{Encode}(m, \mathsf{G}(r))$; by the message-hiding property of SOTP and the fact that G is modeled as a random oracle, this induced distribution of M is $\psi_{\mathcal{M}}$. Since this holds for every $m \in \mathcal{M}'$ and $c \in \mathcal{C}'$, it follows that

$$A'_{pk} \le A_{pk}.$$

Taking expectation over $(pk, sk) \leftarrow \mathsf{Gen}(1^n)$, $\mathbb{E}_{(pk,sk)}[A'_{pk}] \le \mathbb{E}_{(pk,sk)}[A_{pk}] \le 2^{-\gamma}$. □

5 Applications to NTRU-Based PKE Schemes

5.1 $\mathsf{GenNTRU}[D^n]$ as PKE

We assume that R_q is defined for an appropriate cyclotomic polynomial $f(x)$ with degree n. Then, Figure 4 shows $\mathsf{GenNTRU}[D^n] = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{RRec})$ as an underlying PKE, where D is a distribution. $\mathsf{GenNTRU}[D^n]$ is randomness-recoverable under the condition that $\mathbf{h}$ is invertible, and RRec is a randomness-recovery algorithm. We notice that RRec is necessary for only ACWC_2.

$\underline{\mathsf{Gen}(1^n)}$
1: $\mathbf{f}', \mathbf{g} \leftarrow D^n$
2: $\mathbf{f} = 3\mathbf{f}' + 1$
3: **if** $\mathbf{f}, \mathbf{g}$ are not invertible in R_q, restart
4: $\mathbf{h} = 3\mathbf{g}\mathbf{f}^{-1} \bmod q$
return $(pk, sk) = (\mathbf{h}, \mathbf{f})$

$\underline{\mathsf{Enc}(\mathbf{h}, M \leftarrow D^n;\ \mathbf{r} \leftarrow D^n)}$
1: **return** $\mathbf{c} = \mathbf{h}\mathbf{r} + M \bmod q$

$\underline{\mathsf{Dec}(\mathbf{f}, \mathbf{c})}$
1: **return** $M = \big(\mathbf{c}\mathbf{f} \bmod q\big) \bmod 3$

$\underline{\mathsf{RRec}(\mathbf{h}, M, \mathbf{c})}$
1: **return** $\mathbf{r} = (\mathbf{c} - M)\mathbf{h}^{-1} \bmod q$

Figure 4: Generic $\mathsf{GenNTRU}[D^n]$ construction

A desirable feature of $\mathsf{GenNTRU}[D^n]$ is that its γ-spreadness admits a straightforward statistical characterization: for any fixed key pair (pk, sk) and message M, there is exactly one randomness $\mathbf{r}$ satisfying $\mathbf{c} = \mathsf{Enc}(\mathbf{h}, M; \mathbf{r})$ for a given ciphertext $\mathbf{c} \in \mathcal{C}$ [15]. Consequently, to maximize the probability that M meets $\mathbf{c}$, we can simply consider the maximum probability $\hat{p}$ of sampling a randomness $\mathbf{r}$ over a distribution D. Since this holds for any key pair (pk, sk) and any message M (sampled from its message space $\mathcal{M}$), the γ-spreadness of $\mathsf{GenNTRU}[D^n]$ becomes $\gamma = -\log \hat{p}$.

5.2 NTRU-C := $\mathsf{ACWC_0}[\mathsf{GenNTRU}[\overline{\psi}_2^n], \mathsf{G}]$

Let $\overline{\psi}_2$ be the distribution that is obtained by computing $(b_0 + b_1 - b_2 - b_3) \mod 3$ for uniformly random bits $\{b_i\}_{i=0}^3$. Notice that $\overline{\psi}_2$ samples $-1, 0, 1$ with probabilities $5/16, 6/16, 5/16$, respectively. For a hash function $\mathsf{G} : \{0,1\}^* \to \{0,1\}^\lambda$, NTRU-C [5] is obtained by applying $\mathsf{ACWC_0}$ to $\mathsf{GenNTRU}[\overline{\psi}_2^n]$, which is shown in Figure 5.

$\underline{\mathsf{Gen}'(1^n)}$

1: $\mathbf{f}', \mathbf{g} \leftarrow \overline{\psi}_2^n$
2: $\mathbf{f} = 3\mathbf{f}' + 1$
3: **if** $\mathbf{f}$, $\mathbf{g}$ are not invertible in R_q, restart
4: $\mathbf{h} = 3\mathbf{g}\mathbf{f}^{-1} \bmod q$
return $(pk, sk) = (\mathbf{h}, \mathbf{f})$

$\underline{\mathsf{Enc}'(\mathbf{h}, \mathbf{m} \in \{0,1\}^\lambda; (R_1, R_2) \in \mathcal{R}')}$

1: $M \leftarrow \overline{\psi}_2^n$ using the randomness R_1
2: $\mathbf{r} \leftarrow \overline{\psi}_2^n$ using the randomness R_2
3: $\mathbf{c_1} = \mathbf{h}\mathbf{r} + M \bmod q$
4: $\mathbf{c_2} = \mathbf{m} \oplus \mathsf{G}(M)$
return $\mathbf{c} = (\mathbf{c_1}, \mathbf{c_2})$

$\underline{\mathsf{Dec}'(\mathbf{f}, \mathbf{c})}$

1: $M = (\mathbf{c_1}\mathbf{f} \mod q) \mod 3$
2: $\mathbf{m} = \mathbf{c_2} \oplus \mathsf{G}(M)$
return $\mathbf{m}$

Figure 5: Construction of NTRU-C

Lemma 5.1. (Spreadness) $\mathsf{GenNTRU}[\overline{\psi}_2^n]$ is $n \log\left(\frac{8}{3}\right)$-spread.

Proof. Since the maximum probability of sampling $\mathbf{r}$ over $\overline{\psi}_2^n$ is $\left(\frac{3}{8}\right)^n$, we see that $\mathsf{GenNTRU}$ $[\overline{\psi}_2^n]$ is $n \log\left(\frac{8}{3}\right)$-spread. □

Lemma 5.2. (Weak spreadness) $\mathsf{GenNTRU}[\overline{\psi}_2^n]$ is weakly $n \log\left(\frac{8}{3}\right)$-spread.

Proof. The γ-spreadness of $\mathsf{GenNTRU}[\overline{\psi}_2^n]$ only depends on the maximum probability of sampling $\mathbf{r}$ from $\overline{\psi}_2^n$, and thus the maximum probability remains the same across all generated (pk, sk). Based on this, the expected maximum probability over (pk, sk) is given as follows:

$$
\begin{aligned}
&\mathbb{E}\left[\max_{M\in\mathcal{M},\mathbf{c}\in\mathcal{C}} \Pr_{\mathbf{r}\leftarrow\overline{\psi}_2^n}[\mathbf{c}=\mathsf{Enc}(pk,M;\mathbf{r})]\right] \\
&= \sum_{pk_i\in\mathcal{PK}} \max_{\substack{M\in\mathcal{M}\\ \mathbf{c}\in\mathcal{C}}} \Pr_{\mathbf{r}\leftarrow\overline{\psi}_2^n}[\mathbf{c}=\mathsf{Enc}(pk_i,M;\mathbf{r})] \cdot \Pr_{pk\leftarrow\mathsf{Gen}(1^n)}[pk=pk_i] \\
&\leq \sum_{pk_i\in\mathcal{PK}} 2^{-\gamma} \cdot \Pr_{pk\leftarrow\mathsf{Gen}(1^n)}[pk=pk_i] \\
&= \left(\frac{3}{8}\right)^n \cdot \sum_{pk_i\in\mathcal{PK}} \Pr_{pk\leftarrow\mathsf{Gen}(1^n)}[pk=pk_i] \\
&= \left(\frac{3}{8}\right)^n .
\end{aligned}
$$

This concludes that $\mathsf{GenNTRU}[\overline{\psi}_2^n]$ is weakly $n\log\left(\frac{8}{3}\right)$-spread. □

Lemma 5.3. NTRU-C is (weakly) $(n\log\left(\frac{8}{3}\right)+\lambda)$-spread in the (Q)ROM.

Proof. Based on the above result that $\mathsf{GenNTRU}[\overline{\psi}_2^n]$ is (weakly) $n\log\left(\frac{8}{3}\right)$-spread, Theorem 4.1 and Corollary 4.2 imply that $\mathsf{NTRU\text{-}C} = \mathsf{ACWC_0}[\mathsf{GenNTRU}[\overline{\psi}_2^n],\mathsf{G}]$ is (weakly) γ'-spread in the sense of Definition 2.3, with $\gamma' = n\log\left(\frac{8}{3}\right)+\lambda$. □

5.3 NTRU-B := $\mathsf{ACWC_1}[\mathsf{GenNTRU}[U_3^n],\mathsf{GOTP},\mathsf{G}]$

Denote by U_3 the uniform distribution on $\{-1,0,1\}$, and instantiate the hash function $\mathsf{G}:\{0,1\}^*\to\{-1,0,1\}^\lambda$ so that its outputs follow U_3^λ. The concrete instantiation of GOTP is given in Figure 6, where message-hiding is immediate from sampling $u\leftarrow U_3^\lambda$. Moreover, GOTP requires the randomness-hiding, i.e., each $x\in\mathcal{M}'=\{-1,0,1\}^\lambda$ must be sampled according to U_3^λ. Applying $\mathsf{ACWC_1}$ to $\mathsf{GenNTRU}[U_3^n]$ with these primitives yields NTRU-B [5], as illustrated in Figure 7.

$\underline{\mathsf{Encode}(x\in\mathcal{M}'=\{-1,0,1\}^\lambda, u\leftarrow U_3^\lambda)}$	$\underline{\mathsf{Inv}(y\in\mathcal{M}_2=\{-1,0,1\}^\lambda, u\leftarrow U_3^\lambda)}$
1: $y=x+u \mod 3$	1: $x=y-u \mod 3$
return y	**return** x

Figure 6: GOTP instantiation

$\underline{\mathsf{Gen}'(1^n)}$

1: $\mathbf{f}', \mathbf{g} \leftarrow U_3^n$
2: $\mathbf{f} = 3\mathbf{f}' + 1$
3: **if** $\mathbf{f}$, $\mathbf{g}$ are not invertible in R_q, restart
4: $\mathbf{h} = 3\mathbf{g}\mathbf{f}^{-1} \bmod q$
5: **return** $(pk, sk) = (\mathbf{h}, \mathbf{f})$

$\underline{\mathsf{Enc}'(\mathbf{h}, \mathbf{m} \leftarrow U_3^\lambda; (R_1, R_2) \in \mathcal{R}')}$

1: $\mathbf{r} \leftarrow U_3^n$ using the randomness R_1
2: $M_1 \leftarrow U_3^{n-\lambda}$ using randomness R_2
3: $M_2 = \mathsf{Encode}(\mathbf{m}, \mathsf{G}(M_1))$:
– $\mathbf{u} = \mathsf{G}(M_1)$
– $M_2 = \mathbf{m} + \mathbf{u} \mod 3$
4: $M = M_1 || M_2$
5: $\mathbf{c} = \mathbf{h}\mathbf{r} + M \bmod q$
6: **return** $\mathbf{c}$

$\underline{\mathsf{Dec}'(\mathbf{f}, \mathbf{c})}$

1: $M_1 || M_2 = (\mathbf{c}\mathbf{f} \mod q) \mod 3$
2: $\mathbf{m} = \mathsf{Inv}(M_2, \mathsf{G}(M_1))$:
– $\mathbf{u} = \mathsf{G}(M_1)$
– $\mathbf{m} = M_2 - \mathbf{u} \mod 3$
3: **return** $\mathbf{m}$

Figure 7: Construction of NTRU-B

Lemma 5.4. (Spreadness) $\mathsf{GenNTRU}[U_3^n]$ is $n \log 3$-spread.

Proof. Since the distribution of $\mathbf{r}$ is uniform over $\{-1, 0, 1\}$, the maximum probability of sampling $\mathbf{r}$ over U_3^n is $\left(\frac{1}{3}\right)^n$. Therefore, we see that $\mathsf{GenNTRU}\ [U_3^n]$ is $n \log 3$-spread. □

Lemma 5.5. (Weak spreadness) $\mathsf{GenNTRU}[U_3^n]$ is weakly $n \log 3$-spread.

Proof. The γ-spreadness of $\mathsf{GenNTRU}[U_3^n]$ is determined solely by the maximum probability of sampling $\mathbf{r}$ from U_3^n, which remains invariant across all key pairs (pk, sk). An argument similar to Lemma 5.2 can be made. □

Lemma 5.6. NTRU-B is (weakly) $n \log 3$-spread in the (Q)ROM.

Proof. Based on the above result that $\mathsf{GenNTRU}[U_3^n]$ is (weakly) $n \log 3$-spread, Theorem 4.3 and Corollary 4.4 imply that $\mathsf{NTRU\text{-}B} = \mathsf{ACWC}_1[\mathsf{GenNTRU}[U_3^n], \mathsf{GOTP}, \mathsf{G}]$ is (weakly) γ'-spread in the sense of Definition 2.3, with $\gamma' = n \log 3$. □

5.4 $\mathsf{NTRU}+ := \mathsf{ACWC}_2[\mathsf{GenNTRU}[\psi_1^n], \mathsf{SOTP}, \mathsf{G}]$

Let ψ_1 denote the centered binomial distribution that is obtained by computing $(b_0 - b_1)$ for two uniformly random bits b_0 and b_1. Notice that ψ_1 samples $-1, 0, 1$ with the probabilities $1/4, 1/2, 1/4$, respectively. Let G be a hash function $\mathsf{G} : \{0,1\}^* \to \{0,1\}^{2n}$ whose output is uniform over $\{0,1\}^{2n}$. The instantiation of SOTP is specified in Figure 8. The message-hiding property follows from the one-time pad $x \oplus u_1$ with $u_1 \leftarrow \{0,1\}^n$. Also, for another uniformly-random n-bit u_2, the rigidity of SOTP comes from the fact that $x = (y + u_2) \oplus u_1$ implies $y = (x \oplus u_1) - u_2$, as long as $y + u_2 \in \{0,1\}^n$. Figure 9 shows $\mathsf{NTRU}+$ [14] that is obtained by applying ACWC_2 to $\mathsf{GenNTRU}[\psi_1^n]$.

$\underline{\mathsf{Encode}(x \in \mathcal{M}' = \{0,1\}^n, u \leftarrow U^{2n})}$

1: $u = (u_1, u_2) \in \{0,1\}^n \times \{0,1\}^n$
2: $y = (x \oplus u_1) - u_2 \in \{-1,0,1\}^n$
3: **return** y

$\underline{\mathsf{Inv}(y \in \mathcal{M} = \{-1,0,1\}^n, u \in \{0,1\}^{2n})}$

1: $u = (u_1, u_2) \in \{0,1\}^n \times \{0,1\}^n$
2: **if** $y + u_2 \notin \{0,1\}^n$, **return** $\perp$
3: **Else** $x = (y + u_2) \oplus u_1 \in \{0,1\}^n$
4: **return** x

Figure 8: SOTP instantiation

$\underline{\mathsf{Gen}'(1^n)}$

1: $\mathbf{f}', \mathbf{g} \leftarrow \psi_1^n$
2: $\mathbf{f} = 3\mathbf{f}' + 1$
3: **if** $\mathbf{f}$, $\mathbf{g}$ are not invertible in R_q, restart
4: $\mathbf{h} = 3\mathbf{g}\mathbf{f}^{-1} \bmod q$
5: **return** $(pk, sk) = (\mathbf{h}, \mathbf{f})$

$\underline{\mathsf{Enc}'(pk, \mathbf{m} \in \{0,1\}^n; R \in \mathcal{R}')}$

1: $\mathbf{r} \leftarrow \psi_1^n$ using randomness R
2: $M = \mathsf{Encode}(\mathbf{m}, \mathsf{G}(\mathbf{r}))$:
– $\mathsf{G}(\mathbf{r}) = (u_1, u_2)$
– $M = (\mathbf{m} \oplus u_1) - u_2$
3: $\mathbf{c} = \mathbf{h}\mathbf{r} + M \bmod q$
4: **return** $\mathbf{c}$

$\underline{\mathsf{Dec}'(pk, sk, \mathbf{c})}$

1: $M = (\mathbf{c}\mathbf{f} \bmod q) \bmod 3$
2: $\mathbf{r} = (\mathbf{c} - M)\mathbf{h}^{-1} \bmod q$
3: $\mathbf{m} = \mathsf{Inv}(M, \mathsf{G}(\mathbf{r}))$:
– $\mathsf{G}(\mathbf{r}) = (u_1, u_2)$
– **if** $M + u_2 \notin \{0,1\}^n$, **return** $\perp$
– $\mathbf{m} = (M + u_2) \oplus u_1$
4: **return** $\mathbf{m}$

Figure 9: Construction of NTRU+

Lemma 5.7. (Spreadness) $\mathsf{GenNTRU}[\psi_1^n]$ is n-spread.

Proof. Since sampling $\mathbf{r}$ from ψ_1^n yields a maximum probability of $(\frac{1}{2})^n$, it follows that $\mathsf{GenNTRU}[\psi_1^n]$ achieves n-spreadness. □

Lemma 5.8. (Weak spreadness) $\mathsf{GenNTRU}[\psi_1^n]$ is weakly n-spread.

Proof. The γ-spreadness of $\mathsf{GenNTRU}[\psi_1^n]$ is determined by the maximum probability of sampling $\mathbf{r}$ from ψ_1^n, which remains invariant across all key pairs (pk, sk). Therefore, an argument similar to Lemma 5.2 can be made. □

Lemma 5.9. NTRU+ is (weakly) n-spread in the (Q)ROM.

Proof. Based on the above result that $\mathsf{GenNTRU}[\psi_1^n]$ is (weakly) n-spread, Theorem 4.5 and Corollary 4.6 imply that NTRU+ $= \mathsf{ACWC}_2[\mathsf{GenNTRU}[\psi_1^n], \mathsf{SOTP}, \mathsf{G}]$ is (weakly) γ'-spread in the sense of Definition 2.3, with $\gamma' = n$. □

5.5 (Weak) Spreadness on Concrete Parameters

All the (weak) γ'-spreadness of $\{$NTRU-C, NTRU-B, NTRU+$\}$ are determined by the choice of n and λ in NTRU-C. We choose $n = 576, 768, 864, 1152$ as the degree of cyclotomic trinomials such as $x^n - x^{n/2} + 1$,

and we set $\lambda = 256$ as the bit-length of a message only for NTRU-C. Table 1 shows the (weak) γ-spreadness of each GenNTRU$[\cdot]$ and γ'-spreadness of each NTRU-based scheme in the (Q)ROM, as obtained from our refined analysis.[4]

Table 1: (Weak) spreadness in the (Q)ROM calculated from our new spreadness proofs

Scheme	**(Weak) $\star$-spreadness**	$\lambda = 256$			
		$n = 576$	$n = 768$	$n = 864$	$n = 1152$
GenNTRU$[\overline{\psi}_2^n]$	$n \log\left(\frac{8}{3}\right)$	815.1	1086.8	1222.6	1630.1
NTRU-C [5]	$n \log\left(\frac{8}{3}\right) + \lambda$	1071.1	1342.8	1478.6	1886.1
GenNTRU$[U_3^n]$ NTRU-B [5]	$n \log 3$	912.9	1217.2	1369.4	1825.9
GenNTRU$[\psi_1^n]$ NTRU+ [14]	n	576	768	864	1152

6 Conclusion

We revisited the γ-spreadness of the three ACWC transformations. Our rigorous analysis in the (Q)ROM shows that, if the underlying PKE scheme is γ-spread, then $\mathsf{ACWC}_0[\mathsf{PKE}, \mathsf{G}]$ is $(\gamma + \lambda)$-spread, whereas $\mathsf{ACWC}_1[\mathsf{PKE}, \mathsf{GOTP}, \mathsf{G}]$ and $\mathsf{ACWC}_2[\mathsf{PKE}, \mathsf{SOTP}, \mathsf{G}]$ are γ-spread.

Applying these corrected bounds to the NTRU-based instantiations considered in this paper yields $\gamma' = n \log(8/3) + \lambda$ for NTRU-C, $\gamma' = n \log 3$ for NTRU-B, and $\gamma' = n$ for NTRU+. These results clarify the exact spreadness available after ACWC preprocessing when FO-transformed schemes are instantiated with explicit rejection: ACWC_1 and ACWC_2 preserve the underlying spreadness parameter exactly, while ACWC_0 yields an additional λ-bit through its independent masking component. Because this parameter plays an important role as a security-loss term in CCA security proofs, our refined analysis is meaningful both in providing a more rigorous and accurate proof framework than previous analyses and in updating the resulting concrete bounds.

[4]For the numerical evaluation in Table 1, we use base-2 logarithms and display the constants up to the fifth decimal place, namely $\log_2(8/3) = 1.41504$ and $\log_2(3) = 1.58496$. After substitution into the corresponding formulas, the final numerical values are reported rounded to one decimal place.

References

[1] Daniel J Bernstein and Edoardo Persichetti. Towards kem unification. *Cryptology ePrint Archive*, 2018.

[2] Nina Bindel, Mike Hamburg, Kathrin Hövelmanns, Andreas Hülsing, and Edoardo Persichetti. Tighter proofs of cca security in the quantum random oracle model. In *Theory of Cryptography Conference*, pages 61–90. Springer, 2019.

[3] Alexander W. Dent. A designer's guide to KEMs. Cryptology ePrint Archive, Paper 2002/174, 2002.

[4] Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner. Online-extractability in the quantum random-oracle model. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 677–706. Springer, 2022.

[5] Julien Duman, Kathrin Hövelmanns, Eike Kiltz, Vadim Lyubashevsky, Gregor Seiler, and Dominique Unruh. A thorough treatment of highly-efficient ntru instantiations. In *IACR International Conference on Public-Key Cryptography*, pages 65–94. Springer, 2023.

[6] Eiichiro Fujisaki and Tatsuaki Okamoto. How to enhance the security of public-key encryption at minimum cost. In *International workshop on public key cryptography*, pages 53–68. Springer, 1999.

[7] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. *Journal of cryptology*, 26:80–101, 2013.

[8] Jiangxia Ge, Tianshu Shan, and Rui Xue. Tighter QCCA-secure key encapsulation mechanism with explicit rejection in the quantum random oracle model. Cryptology ePrint Archive, Paper 2023/862, 2023.

[9] Jiangxia Ge, Kang Yang, Yang Yu, and Yu Yu. Fujisaki-okamoto transformation under average-case decryption error: Tighter and more general proofs with applications to PQC. Cryptology ePrint Archive, Paper 2025/1641, 2025.

[10] Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz. A modular analysis of the fujisaki-okamoto transformation. In *Theory of Cryptography Conference*, pages 341–371. Springer, 2017.

[11] Kathrin Hövelmanns, Andreas Hülsing, and Christian Majenz. Failing gracefully: Decryption failures and the fujisaki-okamoto transform. page 414–443, Berlin, Heidelberg, 2023. Springer-Verlag.

[12] Kathrin Hövelmanns and Mikhail Kudinov. Treating dishonest ciphertexts in post-quantum kems–explicit vs. implicit rejection in the fo transform. *Cryptology ePrint Archive*, 2025.

[13] Kathrin Hövelmanns and Christian Majenz. A note on failing gracefully: Completing the picture for explicitly rejecting fujisaki-okamoto transforms using worst-case correctness. Cryptology ePrint Archive, Paper 2023/1811, 2023.

[14] Jonghyun Kim and Jong Hwan Park. Ntru+: Compact construction of ntru using simple encoding method. *IEEE Transactions on Information Forensics and Security*, 2023.

[15] Jonghyun Kim and Jong Hwan Park. Ntru+ pke: Efficient public-key encryption schemes from the ntru problem. *Cryptology ePrint Archive*, 2024.

[16] Veronika Kuchta, Amin Sakzad, Damien Stehlé, Ron Steinfeld, and Shi-Feng Sun. Measure-rewind-measure: Tighter quantum random oracle model proofs for one-way to hiding and cca security. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology – EUROCRYPT 2020*, pages 703–728, Cham, 2020. Springer International Publishing.

[17] Gina M Raimondo and Laurie E Locascio. Fips 203 federal information processing standards publication module-lattice-based key-encapsulation mechanism standard. *Nist Natl. Inst. Stand. Technol*, 47, 2024.