Tight Analysis of Decrypton Failure Probability of Kyber in Reality

Boyue Fang[1], Weize Wang[2], and Yunlei Zhao[1]

[1] Fudan University, China
[2] Sun Yat-sen University, China

Abstract. Kyber is a candidate in the third round of the National Institute of Standards and Technology (NIST) Post-Quantum Cryptography (PQC) Standardization. However, because of the protocol's independence assumption, the bound on the decapsulation failure probability resulting from the original analysis is not tight. In this work, we give a rigorous mathematical analysis of the actual failure probability calculation, and provides the Kyber security estimation in reality rather than only in a statistical sense. Our analysis does not make independency assumptions on errors, and is with respect to concrete public keys in reality. Through sample test and experiments, we also illustrate the difference between the actual failure probability and the result given in the proposal of Kyber. The experiments show that, for Kyber-512 and 768, the failure probability resulting from the original paper is relatively conservative, but for Kyber-1024, the failure probability of some public keys is worse than claimed. This failure probability calculation for concrete public keys can also guide the selection of public keys in the actual application scenarios. What's more, we measure the gap between the upper bound of the failure probability and the actual failure probability, then give a tight estimate. Our work can also re-evaluate the traditional $1-\delta$ correctness in the literature, which will help re-evaluate some candidates' security in NIST post-quantum cryptographic standardization.

Keywords: Post-Quantum Cryptography · Learning with Errors · Key Encapsulation Mechanism · Decryption Failure.

1 Introduction

Cryptographic systems based on learning with errors (LWE) and related problems are the central topics of recent cryptographic research. Factorization and discrete logarithm problems have always been the basis of modern cryptography, but due to the development of quantum computing, cryptographic schemes based on these problems are no longer secure in the post-quantum era. Lattice-based cryptography makes it possible to implement a rich set of cryptographic primitives, including key exchange, key encapsulation, encryption, and digital signatures, and more advanced structures such as fully homomorphic encryption.

Therefore, post-quantum cryptography (PQC) should be developed to avoid security problems in future systems to replace the existing public-key algorithms. The National Institute of Standards and Technology(NIST) is running a PQC standardization project. One type of candidate is designed based on learning with errors (LWE) and related problems such as Module-LWE. Unlike traditional public-key schemes, LWE-based schemes have the possibility of decryption failures. Last year, the third round of the NIST PQC project began, and only 15 candidates remained. Seven of them are finalists, and eight alternative algorithms also moved to the third round of the process. Kyber is a promising candidate for the key encapsulation mechanism (KEM), which is based on module-LWE (MLWE). For the recommended parameter sets, the failures of the Kyber decryption procedure are pretty small. For Kyber-512/768/1024 according to the NIST security categories I, III and V, the decryption failures claimed are about $2^{-139}, 2^{-164}, 2^{-174}$ respectively [2]. These upper bounds are low enough to discourage reaction attacks. However, in the current estimation technology of decryption failure probability for KEM schemes based on LWE and its variants, it assumes the failure independence in individual bits of the transmitted message. It then calculates the overall failure probability of the scheme. However, it is difficult to estimate the gap between this assumption and the actual situation, and it may cause unpredictable consequences when applying this type of encryption scheme. Therefore, this paper considers the upper bound of the actual decryption failure probability of this type of encryption scheme. This paper takes the Kyber scheme as an example to provide an analysis more in line with the actual situation. The failure probability estimation method proposed in this paper will also impact the effect of failure-boosting technology based on the independence of failure probability assumption.

Contribution. Our main contribution is to give a rigorous mathematical analysis of the actual failure probability for Kyber in reality, and then discuss the traditional $1-\delta$ correctness analysis. Our analysis of the Kyber decryption failure probability mainly focuses on the impact of the non-independence of the random vectors, and shows that the independence assumption in the traditional $1-\delta$ correctness analysis may affect the security of the encryption schemes in reality. This impact is not only related to Kyber. In the failure probability analysis, we need to consider the probability of $||e_1s_1 + e_2s_2 + e_3||_\infty < t$, where e_1, s_1, e_2, s_2, e_3 obey certain distributions, and t is some threshold. This formula is the cornerstone of error rate analysis. The rigorous mathematical analysis of this basic problem is worthy of in-depth study, which also greatly eliminates the gap between theoretical error rate and the error rate in actual applications for KEM schemes based on LWE and its variants. For the samples we selected, the difference between the upper and lower bounds in the power of 2 is usually less than 40, which means that the upper bound of the error given in this work can approximately represent its actual error rate.

Through the analysis method proposed in this paper, the failure probability of Kyber512 and Kyber768 can be considered as an overestimation of the actual situation, while Kyber1024 has a certain underestimation. The number of public

keys that make the corresponding failure probability higher than the probability claimed in [2] is not negligible, which means that the security level of Kyber-1024 under certain public keys will be reduced after using technologies such as directional failure boosting.

Our analysis method can estimate the gap between the theoretical error rate and the actual error rate, quantitatively analyzes the error rate of a given public key, and provides the Kyber security estimation in actual applications rather than only in a statistical sense. Our work can also re-evaluate the traditional $1-\delta$ correctness in the literature, which will help re-evaluate some candidates' security in the third round of NIST post-quantum cryptographic standardization.

Related Work. D'Anvers et al. rejected the assumption that the failure independence in individual bits of the transmitted message theoretically and practically [7]. They provided a method to estimate the probability of decryption failure, taking the correlation of bit failures into account. Therefore, Kyber, as a KEM scheme based on the MLWE problem, the deviation between its actual decryption failure rate and the theoretical decryption failure rate given in the NIST proposal is also worthy of attention. This paper proposes an estimation method to calculate the tight failure probability upper bound of Kyber, which does not make the assumption of independence of errors. It effectively avoids the problem that the gap (between the theoretical failure probability and the actual failure probability) caused by the independence assumption is difficult to measure.

The impact of the failure probability on the encryption scheme is also reflected in the security of it. Guo et al. proposed a key recovery attack against LWE-based KEM schemes that use error correction codes to lower error probabilities. When their method is applied to LAC256-v2, the pre-computation complexity is 2^{-171}, and the success probability is 2^{-64} [8]. Bindel et al. showed that the adversary could use the first successful decryption information to increase the probability of getting the subsequent successful decryption. They also re-evaluated some candidates' security for the NIST PQC standardization [1]. When the side information about decryption failure is available, Dachman-Soled et al. proposed a cryptanalysis framework for lattice-based schemes [4]. This framework summarizes the primitive reduction attack, and allows for the gradual integration of prompts before running the final reduction step. This technique includes the sparsity of the grid, projection onto the hyperplane, and the distribution of the vector corresponding to the secret key that intersects the hyperplane. Their main contribution is to propose a toolbox and a method that can integrate this information into grid reduction attacks and can use side information to predict these grid reduction attacks' performance. They provided several end-to-end applications, such as the improvement of Frodo's single-track attack proposed by Bos et al. [3]. In particular, even with little side information, this study can also perform security loss estimation, bringing a smooth calculation trade-off for side-channel attacks. D'Anvers et al. studied the effect of decryption failure on the security of lattice-based encryption schemes, and attacked some NIST candidate encryption schemes [6]. The results show that the attack will

significantly reduce the security of the lattice-based encryption schemes with a relatively high failure rate. After applying their model to some NIST candidate cryptographic schemes, they believe that the actual security level is lower than their declared security level. Therefore, it is essential to give a failure rate analysis method that the deviation can be estimated and the theoretical bound is tight. Especially in the actual application scenarios, the public key is fixed once and for all rather than randomly selected each time, which means the failure rate in the sense of mathematical expectation cannot precisely indicate the error rate of a given public key. The failure probability estimation method proposed in this paper will provide the upper bound of the actual error rate, and conducts simulation experiments for concrete public keys. The analysis of the number of public keys corresponding to different error rates will be able to provide guidance for the public key selection.

Besides, the failure-boosting attack showed that the first decryption failure requires special attention. For example, D'Anvers et al. expanded their technology proposed in 2019 [6] and called it the "directional failure boosting" technology [5], which can speed up the search for the next decryption error. They also made an in-depth discussion on the quotient ring of the polynomial ring modulus $\langle x^N + 1 \rangle$ over the finite field, and used the Kyber/Saber schemes based on module lattices to test the technology. They showed that after the decryption fails once, it can speed up the finding of the subsequent failed decryption. They proved that for such a single-target key model, the cryptographic algorithm design needs to make the first decryption failure difficult, while for the multi-target key model, the attack method is more effective. We noticed that the error analysis of D'Anvers et al.[5] is based on the analysis results given in the Kyber proposal where the independence of errors is assumed.

2 Preliminaries

2.1 Kyber

The complete description of CRYSTALS-Kyber can be found in [1]. Here we mainly focus on the failure probability analysis part of it. The system parameters are a ring R, positive integer k, d_t, d_u, d_v, and n=256. The ciphertexts are of the form $(\mathbf{u}, v) \in \{0,1\}^{256 \cdot k d_u} \times \{0,1\}^{256 \cdot d_v}$. The public-key encryption scheme Kyber.CPA=KeyGen, Enc, Dec as described in Algorithms 1 to 3.

Algorithm 1 Kyber.CPA.KeyGen(): key generation

1: $\rho, \sigma \leftarrow \{0,1\}^{256}$
2: $\mathbf{A} \sim R_q^{k \times k} := Sam(\rho)$
3: $(s, e) \sim \beta_\eta^k \times \beta_\eta^k := Sam(\rho)$
4: $\mathbf{t} := Compress_q(\mathbf{As} + \mathbf{e}, d_t)$
5: **return** $(pk := (\mathbf{t}, \rho), sk := s)$

Algorithm 2 Kyber.CPA.Enc($pk = (\mathbf{t}, \rho), m \in \mathcal{M}$): encryption

$r \leftarrow \{0,1\}^{256}$
$t \coloneqq Decompress_q(\mathbf{t}, d_t)$
$\mathbf{A} \sim R_q^{k \times k} \coloneqq Sam(\rho)$
$(\mathbf{r}, \mathbf{e_1}, e_2) \sim \beta_\eta^k \times \beta_\eta^k \times \beta_\eta \coloneqq Sam(\tau)$
$\mathbf{u} \coloneqq Compress_q(\mathbf{A^T r} + \mathbf{e_1}, d_u)$
$v \coloneqq Compress_q(\mathbf{t^T r} + e_2 + \lfloor \frac{q}{2} \rceil \cdot m, d_v)$
return $c \coloneqq (\mathbf{u}, v)$

Algorithm 3 Kyber.CPA.Dec($sk = s, c = (\mathbf{u}, v)$): decryption

$u \coloneqq Decompress_q(\mathbf{u}, d_u)$
$v \coloneqq Decompress_q(v, d_v)$
return $Compress_q(v - s^T\mathbf{u}, 1)$

The compression and decompression function are defined as:

$$Compress_q(x, d) = \lfloor \frac{2^d}{q} \cdot x \rceil \mod^+ 2^d,$$

$$Decompress_q(x, d) = \lfloor \frac{q}{2^d} \cdot x \rceil.$$

2.2 Distributions on R

Notation. For a finite set S, $|S|$ denotes its cardinality, and we write $s \leftarrow S$ to say that s is sampled uniformly from S. Denote with $\mathbb{Z}_q$ the ring of integers modulo q, represented in $(-\frac{q}{2}, \frac{q}{2}]$. Let R_q be the ring $\mathbb{Z}_q(X)/(X^N + 1)$, with N a power of two. For a vector V (or matrix A), we denote by v^T (or A^T) its transpose.

Denote with $\langle ., . \rangle$ the Eulidean inner product, and with $\lfloor x \rceil$ the nearest integer function. Let $|\cdot|$ denote taking the absolute value. These notations can be natually extended to vectors, matrices and polynomials element wise. For an element $x \in \mathbb{Z}_q$, we write $||x||_\infty$ to mean $|x \mod \pm q|$ and $||x||_2$ to mean $|x|$. Elements of $R = \mathbb{Z}[x]/(x^n + 1)$ can be viewed as vectors in $\mathbb{R}^n$ by identifying the power basis $\{1, x, x^2, \ldots, x^{n-1}\}$ of R as an orthonormal basis of $\mathbb{R}^n$, so for $\mathbf{x} = (x_0, \ldots, x_{n-1})$, we define l_∞ norm and l_2 norm as following:

$$||\mathbf{x}||_\infty = \max_i ||x_i||_\infty$$

$$||\mathbf{x}||_2 = \sqrt{\sum_{i=0}^{n-1} ||x_i||_2}.$$

Denote with $\mathbb{P}[E]$ the probability of an event E, with $\mathbb{E}[\varepsilon]$ the expectation of the random variable ε.

The centered binomial distribution B_η are defined as follows:

Sample $\{(a_i, b_i)\}_{i=1}^{\eta} \leftarrow (\{0,1\}^2)^\eta$ and output $\sum_{i=1}^{\eta}(a_i - b_i)$.

If v is an element of R, we write $v \leftarrow \beta_\eta$ to mean that $v \in R$ is generated from a distribution where each of its coefficients is generated according to B_η. Similarly, a k-dimensional vector of polynomials $v \in R^k$ can be generated according to the distrbution β_η^k.

3 Analysis of Decryption Failure Probability

Decryption failure refers to an event in which the correct ciphertext cannot be successfully restored during decryption after the decryption steps described in the algorithm are performed. The probability of decryption failure usually depends on the functions of the secret terms, denoted as s_1, s_2, e_1, e_2, e_3. Take Kyber as an example, when

$$|| \langle e + c_t, r\rangle - \langle s, e_1 + c_u\rangle + e_2 + c_v||_\infty \leq B = \lfloor \frac{q}{4} \rceil,$$

the ciphertext can be decrypted successfully. And in the theorem of $1 - \delta$ correctness,

$$|| \langle e + c_t, r\rangle - \langle s, e_1 + c_u\rangle + e_2 + c_v||_\infty \geq B = \lfloor \frac{q}{4} \rceil$$

is usually defined as the error rate of decryption failure. In general, the error rate analysis mainly discusses the probability that

$$|| \left\langle e^{'}, s^{''} \right\rangle + \left\langle e^{''}, s^{'} \right\rangle + e^{'''}|| \leq B,$$

where $e^{'}, e^{''}, e^{'''}, s^{'}, s^{''}$ obey a certain distribution, B is the threshold.

In the work of Kyber et al.[2], after expressing the failure probability problem in the above form, they adopted the independence assumption, that is, $e^{'}, e^{''}, e^{'''}, s^{'}, s^{''}$ are regarded as independent distributions for error rate calculation. However, it will bring deviations that are difficult to evaluate in the error rate calculation. Here we give a simple example to explain. It does not mean that the central binomial distribution and parameters used by Kyber are consistent with the parameters' distribution in the example. This example is to show that the independence assumption will bring massive deviations. Assume $\varepsilon_1, \varepsilon_2, \varepsilon_3$ are independent, $\varepsilon_1, \varepsilon_2$ obeys the Gaussian distribution $\varepsilon_1, \varepsilon_2 \sim \mathcal{N}(0, 4)$, then define $c_1 = \frac{\varepsilon_1 + \varepsilon_2}{2}, c_2 = \frac{\varepsilon_2 - \varepsilon_1}{2}$, so c_1, c_2 also obey the Gaussian distribution $c_1, c_2 \sim \mathcal{N}(0, 4)$. Consider the probability of

$$||\varepsilon_1 c_1 + \varepsilon_2 c_2 + \varepsilon_3|| \leq B,$$

Since we are mainly concerned with the influence of the independence assumption here, we might as well set ε_3 to 0. At this time, we consider the difference in

probability calculated before and after adopting the assumption of independence. When the independence assumption is not taken, the probability is

$$\mathbb{P}(||\varepsilon_1^2 + \varepsilon_2^2|| \leq 2B),$$

and $\varepsilon_1^2 + \varepsilon_2^2 \sim \chi^2(2)$, where $\chi^2(2)$ is the chi-square distribution with 2 degrees of freedom. The probability density function is

$$f_1(x) = \frac{1}{2}e^{-\frac{x}{2}}, x \geq 0.$$

Then consider to adopt the independence assumption, the distribution can be regarded as the sum of two independent and identically distributed random variables, each of which is the product of two normally distributed variables. The probability density function of the product is $f(u) = \frac{B(0,\frac{\sqrt{u^2}}{4})}{4\pi}$, where B is the second kind of modified Bessel function, $B(0,x) = \int_0^\infty cos(x\sinh t)dt$. In this case, the probability density function is

$$f_2(x) = \int_{\mathbb{R}} f(x-u)f(u)du = \frac{1}{16\pi^2}\int_{\mathbb{R}}(\int_0^\infty cos((x-u)\sinh t)dt \int_0^\infty cos(u\sinh t)dt)du.$$

By comparing $f_1(x)$ and $f_2(x)$, it can be seen that the distribution of the corresponding random variables before and after the independence assumption is very different. Therefore, it is very important to consider the distribution of the real situation.

3.1 Decryption Failures

The Kyber key generation procedure involves ring elements s, e and matrix A. Key encapsulation involves ring elements r, e_1, e_2. The condition that decryption failure probability is less than δ is the following formula holds:

$$\mathbb{P}(||\langle e + c_t, r\rangle - \langle s, e_1 + c_u\rangle + e_2 + c_v||_\infty \leq B) \leq \delta,$$

where

$$c_u = \lfloor \frac{q}{2^{d_u}}(\lfloor \frac{2^{d_u}}{q}(A^T r + e_1)\rceil) \mod {}^+ 2^{d_u}\rceil - (A^T r + e_1)$$

$$c_t = \lfloor \frac{q}{2^{d_t}}(\lfloor \frac{2^{d_t}}{q}(As + e)\rceil) \mod {}^+ 2^{d_t}\rceil - (As + e)$$

$$c_v = \lfloor \frac{q}{2^{d_v}}(\lfloor \frac{2^{d_v}}{q}(t^T r + e_2 + \lfloor \frac{q}{2}\rceil m)\rceil) \mod {}^+ 2^{d_v}\rceil - (t^T r + e_2 + \lfloor \frac{q}{2}\rceil m)$$

and $t = As + e + c_t$. The distribution of s, e, r, e_1, e_2, A is introduced in section 3.1.

3.2 Formula Derivation

Define $a_i = \frac{2^{d_i}}{q}$, $f(i,x) = x - \lfloor \frac{1}{a_i} \lfloor a_i x \rceil \rceil$.

Then

$$|| \langle e + c_t, r \rangle - \langle s, e_1 + c_u \rangle + e_2 + c_v ||_\infty \leq B = \lfloor \frac{q}{4} \rceil$$

can be written as

$$|| \langle e, r \rangle - \left\langle \lfloor \frac{1}{a_t} \lfloor a_t(As + e) \rceil \rceil, r \right\rangle - \langle s, e_1 \rangle + \left\langle s, \lfloor \frac{1}{a_u} \lfloor a_u(A^T r + e_1) \rceil \rceil \right\rangle + e_2 - \lfloor \frac{1}{a_v} (\lfloor a_v((As + e + c_t)^T r + e_2) \rceil ||_\infty \leq B$$

Which is equal to

$$|| \langle e, r \rangle - \langle As + e, r \rangle + \langle f(t, As + e), r \rangle - \langle s, e_1 \rangle + \left\langle s, A^T r + e_1 \right\rangle - \left\langle s, f(u, A^T r + e_1) \right\rangle + e_2 - \langle f(t, As + e), r \rangle - e_2 + f(v, \langle f(t, As + e), r \rangle + e_2) ||_\infty \leq B$$

It's equal to

$$|| f(v, \langle f(t, As + e), r \rangle + e_2) - \left\langle f(u, A^T r + e_1), s \right\rangle ||_\infty \leq B.$$

We found that

$$||f(i,x)||_\infty \leq \frac{1}{2a_i} + \frac{1}{2},$$

Consider the triangular inequality of the norm, a sufficient condition is

$$|| \left\langle f(u, A^T r + e_1), s \right\rangle ||_\infty \leq B' = \lfloor \frac{q}{4} \rceil - \frac{1}{2a_v} - \frac{1}{2}.$$

Now we discuss about $|| \left\langle f(u, A^T r + e_1), s \right\rangle ||_\infty$.

Firstly,

$$A \leftarrow R_q^{k \times k}, r \leftarrow \beta_\eta^k, e_1 \leftarrow \beta_\eta^k, s \leftarrow \beta_\eta^k$$

If we write A, r, e_1, s as $A = (a^{(ij)})_{1 \leq i,j \leq k}, e_1 = (e^{(i)})_{i=1}^k, r_1 = (r^{(i)})_{i=1}^k, s_1 = (s^{(i)})_{i=1}^k$, Then the formula can be written as

$$|| \sum_{j=1}^{k} (s_j (\sum_{i=1}^{k} a^{(ji)} r^{(i)} + e^{(j)} - \lfloor \frac{1}{a_u} \lfloor a_u (\sum_{i=1}^{k} a^{(ji)} r^{(i)} + e^{(j)}) \rceil \rceil)) ||_\infty \leq B',$$

where $a^{(ji)} = \sum_{m=0}^{n-1} a_m^{(ji)} x^m, r^{(i)} = \sum_{m=0}^{n-1} r_m^{(i)} x^m, e^{(j)} = \sum_{m=0}^{n-1} e_m^{(j)} x^m$.

Consider to define

$$a^{(ji)} r^{(i)} = \sum_{m=0}^{n-1} b_m x^m$$

Then

$$b_{n-1} = \sum_{k=0}^{n-1} a_k^{(ji)} r_{n-1-k}^{(i)}$$

and for $m < n-1$,

$$b_m = \sum_{k=0}^{m} a_k^{(ji)} r_{m-k}^{(i)} - \sum_{k=m+1}^{n-1} a_k^{(ji)} r_{m+n-k}^{(i)}$$

3.3 The deviation between the theoretical failure probability and the actual failure probability

Consider the following theorem in Kyber [2]

Theorem 1. Let k be a positive integer parameter. Let s, e, r, e_1, e_2 be random variables that have the same distribution. Also, let $c_t \leftarrow \varphi_{d_t}^k, c_u \leftarrow \varphi_{d_u}^k, c_v \leftarrow \varphi_{d_v}$ be distributed according to the distribution φ defined as follows:

Let φ_d^k be the following distribution over R:

- Choose uniformly-random $y \leftarrow R^k$
- **return** $(y - Decompress_q(Compress_q(y, d), d)) \mod^{\pm} q$.

Denote

$$\delta = Pr[||\langle e, r\rangle + e_2 + c_v - \langle s, e_1\rangle + \langle c_t, r\rangle - \langle s, c_u\rangle||_\infty \geq \lfloor \frac{q}{4} \rceil].$$

Then Kyber.CPA is $(1-\delta)$- correct.

Review our previous analysis, i.e.

$$||f(v, \langle f(t, As+e), r\rangle + e_2) - \langle f(u, A^T r + e_1), s\rangle||_\infty \leq B.$$

Because

$$|f(i, x)| \leq \frac{1}{2a_i} + \frac{1}{2},$$

The bound of the actual failure probability can be restricted between the sufficient condition and the necessary condition.

The sufficient condition can be writen as:

$$||\langle f(u, A^T r + e_1), s\rangle||_\infty \geq B^{'} = \lfloor \frac{q}{4} \rceil - \frac{1}{2a_v} - \frac{1}{2},$$

which is the upper bound of the failure probability. And the necessary condition is:

$$||\langle f(u, A^T r + e_1), s\rangle||_\infty \geq B^{''} = \lfloor \frac{q}{4} \rceil + \frac{1}{2a_v} + \frac{1}{2},$$

which can be seen as the lower bound of the failure probability.

For a given public key A, the actual failure probability is between these two, and the bound is tight. We draw the graph with the upper and lower bounds corresponding to the selected range of random variables to illustrate:

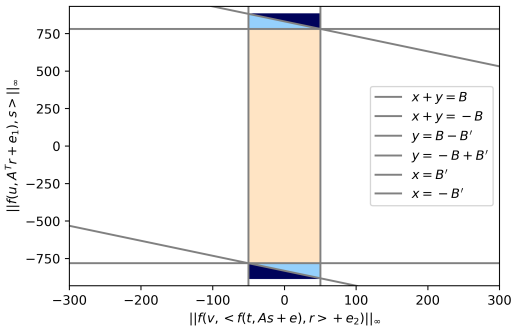

Fig. 1. The orange part corresponds to the sufficient condition we gave. The light blue part is the gap between the actual failure probability and the sufficient condition. The dark blue part is the gap between the necessary condition and the actual failure probability.

For the 900 samples we selected, the difference between the upper and lower bounds in the power of 2 is usually less than 40, which means that the upper bound of the error given can approximately represent its actual error rate. The deviation is 12 orders of magnitude.

4 Experiment and Sample Test

The paremeter set for KYBER can be seen in the following table.

	n	k	q	η_1	η_2	d_u, d_v	δ
KYBER512	256	2	3329	3	2	(10,4)	2^{-139}
KYBER768	256	3	3329	2	2	(10,4)	2^{-164}
KYBER1024	256	4	3329	2	2	(11,5)	2^{-174}

Table 1. Paremeter Set for KYBER

In practical applications, the public key is usually fixed rather than randomly selected every time. The error rate of the mathematical expectation given in the traditional analysis cannot give the actual decryption failure probability of the fixed public key. Therefore, we give the error rate analysis for a given public key, consider the number of public keys corresponding to different error rates, and guide public key selection. The failure probability corresponding to the public key can be further discussed. This paper studies more about the probability distribution of the decryption failure. This paper uses the non-parametric estimation method proposed by Rosenblatt [10] and Parzen [9] to estimate the

probability density function. This method calculates the probability density of the corresponding parameter by calculating the number of samples in a given area. For the Parzen window method, the estimated area volume used in different areas is fixed. The window function is

$$\phi(x) = \begin{cases} 1, & |x_i| \leq \frac{1}{2}; i = 1, \ldots, d \\ 0, & otherwise \end{cases}$$

By calculating $p_n(x) = \frac{1}{n} \sum_{i=1}^{n} \frac{1}{h^d} \phi(\frac{x - x_i}{h_n})$. Where $h^d = V_n$, the density function is obtained. Through kernel density estimation, it is able to give the probability that a given public key's failure probability is greater than the threshold. Therefore, this method will help the higher-order moment analysis of the failure probability, and thus have a deeper understanding of the moment characteristics of the public keys. The corresponding kernel density estimation curve is shown in Figure 2, 3, 4.

The calculation process is quite time-consuming. It takes several hours to calculate the decryption failure probability for a given public key. As a consequence, we only testes 300 samples for each parameter set. The differences in the decryption failure probability before and after the independence assumption are given in Figure 2, 3, 4, respectively.

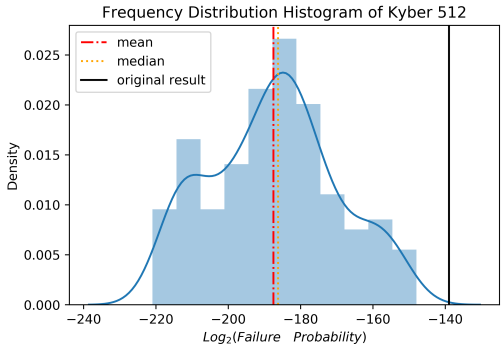

Fig. 2. Frequency histograms of $Kyber512$. The red line is the mean of all samples, the orange line is the median of all samples, and the black line is the failure probability provided in the original paper. The blue line is the kernel density estimation curve.

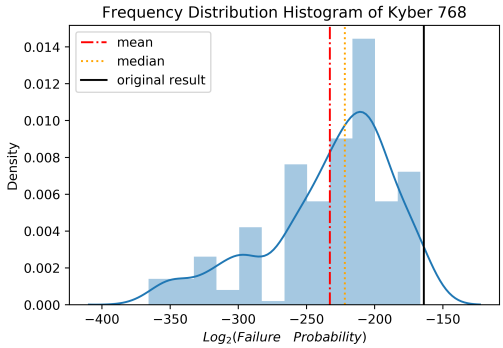

Fig. 3. Frequency histograms of $Kyber768$. The red line is the mean of all samples, the orange line is the median of all samples, and the black line is the failure probability provided in the original paper. The blue line is the kernel density estimation curve.

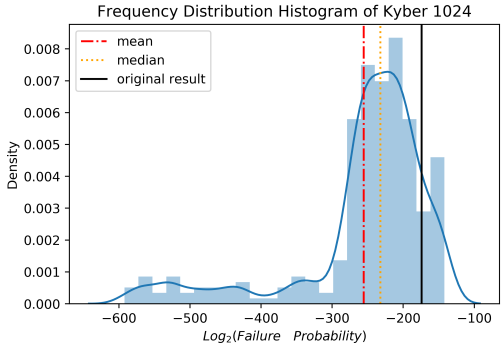

Fig. 4. Frequency histograms of $Kyber1024$. The red line is the mean of all samples, the orange line is the median of all samples, and the black line is the failure probability provided in the original paper. The blue line is the kernel density estimation curve.

We select 300 random matrices A for each Kyber parameter set for testing and then draw their corresponding frequency histograms. It can be seen that the failure probability of most samples is lower than the probability given in the original paper, and the mean of the sample is less than the median of the sample.

	original [2]	mean	median	max	min
KYBER512	2^{-139}	2^{-188}	2^{-186}	2^{-148}	2^{-221}
KYBER768	2^{-164}	2^{-233}	2^{-222}	2^{-166}	2^{-366}
KYBER1024	2^{-174}	2^{-255}	2^{-232}	2^{-142}	2^{-592}

Table 2. Comparison of failure probabilities before and after adopting the assumption of independence.

References

1. Bindel N, Schanck J M. Decryption failure is more likely after success. *International Conference on Post-Quantum Cryptography,* pages 206-225. Springer, Cham, 2020.
2. Bos J, Ducas L, Kiltz E, et al. CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM. *2018 IEEE European Symposium on Security and Privacy (EuroS&P).* pages 353-367. IEEE, 2018.
3. Bos J W, Friedberger S, Martinoli M, et al. Assessing the feasibility of single trace power analysis of frodo. *International Conference on Selected Areas in Cryptography.* pages 216-234. Springer, Cham, 2018.
4. Dachman-Soled D, Ducas L, Gong H, et al. LWE with Side Information: Attacks and Concrete Security Estimation. *IACR Cryptol.* pages ePrint Arch., 2020:292. 2020.
5. D'Anvers J P, Rossi M, Virdia F. (One) Failure Is Not an Option: Bootstrapping the Search for Failures in Lattice-Based Encryption Schemes. *Annual International Conference on the Theory and Applications of Cryptographic Techniques.* pages 3-33. Springer, Cham, 2020.
6. D'Anvers J P, Guo Q, Johansson T, et al. Decryption failure attacks on IND-CCA secure lattice-based schemes. *IACR International Workshop on Public Key Cryptography.* pages 565-598. Springer, Cham, 2019.
7. D'Anvers J P, Vercauteren F, Verbauwhede I. The impact of error dependencies on Ring/Mod-LWE/LWR based schemes. *International Conference on Post-Quantum Cryptography.* pages 103-115. Springer, Cham, 2019.
8. Guo Q, Johansson T, Yang J. A novel CCA attack using decryption errors against LAC. *International Conference on the Theory and Application of Cryptology and Information Security.* pages 82-111. Springer, Cham, 2019.
9. Parzen, E. On estimation of a probability density function and mode. *The annals of mathematical statistics.* pages 1065-1076. 33(3), 1962.
10. Rosenblatt, M. Remarks on Some Nonparametric Estimates of a Density Function. *The Annals of Mathematical Statistics.* pages 832–837. 27(3), 1956.
11. Wishart J, Bartlett M S. The distribution of second order moment statistics in a normal system. *Mathematical Proceedings of the Cambridge Philosophical Society.* pages 455-459. Cambridge University Press, 1932, 28(4).