entropy

MDPI

Article

Quantum Misuse Attack on Frodo

Yaru Wang, Haodong Jiang * and Zhi Ma *

State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China
* Correspondence: hdjiang13@gmail.com (H.J.); ma.zhi@meac-skl.cn (Z.M.)

Abstract: Research on the security of lattice-based public-key encryption schemes against misuse attacks is an important part of the cryptographic assessment of the National Institute of Standards and Technology (NIST) post-quantum cryptography (PQC) standardization process. In particular, many NIST-PQC cryptosystems follow the same meta-cryptosystem. At EUROCRYPT 2019, Băetu et al. mounted a classical key recovery under plaintext checking attacks (KR-PCA) and a quantum key recovery under chosen ciphertext attacks (KR-CCA). They analyzed the security of the weak version of nine submissions to NIST. In this paper, we focus on learning with error (LWE)-based FrodoPKE, whose IND-CPA security is tightly related to the hardness of plain LWE problems. We first review the meta-cryptosystem and quantum algorithm for solving quantum LWE problems. Then, we consider the case where the noise follows a discrete Gaussian distribution and recompute the success probability for quantum LWE by using Hoeffding bound. Finally, we give a quantum key recovery algorithm based on LWE under CCA attack and analyze the security of Frodo. Compared with the existing work of Băetu et al., our method reduces the number of queries from 2^2 to 1 with the same success probability.

Keywords: learning with problem; lattice-based cryptography; quantum misuse attack; Frodo; quantum algorithm

Citation: Wang, Y.; Jiang, H.; Ma, Z. Quantum Misuse Attack on Frodo. *Entropy* **2022**, *24*, 1418. https://doi.org/10.3390/e24101418

Academic Editor: Guo-Hua Sun

Received: 6 September 2022
Accepted: 30 September 2022
Published: 4 October 2022

1. Introduction

Quantum computing exploits quantum mechanical properties to perform computations. It enables quantum parallelism and provides much more powerful data processing capabilities than classical computers [1]. In 1994, Peter Shor proposed an efficient quantum algorithm [2] that can break most of the current public-key cryptosystems, such as the Diffie–Hellman protocol [3] and RSA cryptosystem [4]. If large-scale quantum computers are realized, they would threaten the security of many public-key cryptosystems. In order to ensure the security of network information systems, NIST initiated a standardization process for post-quantum algorithms. In 2016, NIST called for proposals for post-quantum cryptosystems [5]. There are 69 candidates in the first round, based on a variety of hard problems considered to be intractable by quantum computers. After rigorous scrutiny by the cryptography community, 17 PKE and key encapsulation mechanisms (KEM) candidates were selected in the second round, where nine are lattice-based. In the third round, three of the four finalists are still lattice-based. In 2022, NIST has completed the third round of the PQC standardization process. A total of four candidate algorithms have been selected for standardization, and four additional algorithms will continue into the fourth round. The selected algorithms are mostly lattice-based cryptography [6]. Lattice-based cryptography is the use of conjectured hard problems on point lattices in R^n as the foundation for secure cryptographic systems. Attractive features of lattice cryptography include apparent resistance to quantum attacks, high asymptotic efficiency and parallelism, security under worst-case intractability assumptions, and solutions to long-standing open problems in cryptography. Lattice cryptography has some attractive features, including (1) conjectured security against quantum attacks, (2) algorithmic simplicity, efficiency, and parallelism, (3)

strong security guarantees from worst-case hardness, and (4) constructions of versatile and powerful cryptographic objects.

In general, most lattice-based NIST-chosen plaintext attack (CPA) secure candidates use the Fujisaki–Okamoto (FO) transformation [7] to achieve IND-CCA security. When the key is reused, the CPA-secure PKE is no security guarantee. Research on key reuse attacks against lattice-based CPA-secure schemes is an important topic in the post-quantum cryptography. Many key-recovery attacks have been proposed in [8–13]. In 1998, Bleichenbacher showed the security of IND-CPA secure public-key cryptosystems in the case of key reuse on RSA encryption standard PKCS#1 [14]. In 2010, Menezes et al. gave the key reuse attack on reusing ephemeral keys in Diffie–Hellman key agreement protocols [15]. In 2016, Fluhrer proposed a key reuse attack [16]. In 2017, Ding et al. expanded Fluhrer's attack to a class of key agreement protocols based on ring-LWE with signaling [17]. In 2019, Bauer et al. [18] gave a key-recovery attack on NewHope-CPA-PKE [19]. In 2021, Yue Qin et al. developed a systematic approach and analyzed key misuse attacks on lattice-based NIST candidates [20]. Although there have been a number of classical key misuse attacks on the lattice-based public key encryption schemes, quantum misuse attack algorithms are rarely studied. In 2019, Alagic et al. gave a quantum algorithm for learning rounding function and showed that this algorithm can recover the key of an IND-CPA-secure LWE-based encryption scheme with constant success probability [21]. At EUROCRYPT 2019, Băetu et al. analyzed the security of meta-cryptosystems under key reuse by mounting a quantum key recovery under the chosen-ciphertext attacks [22].

Although NIST did not select Frodo as the initial post-quantum algorithm in the process of post-quantum cryptography standardization, Frodo remains a post-quantum recommendation of Germany's Bundesamt für Sicherheit in der Informationstechnik (BSI) [23]. The FrodoPKE scheme is an instantiation and implementation of the Lindner–Peikert scheme [24] with some modifications, for example, more balanced key and ciphertext sizes and new LWE parameters. The IND-CPA security of FrodoPKE is tightly related to the hardness of a corresponding learning with errors problem. In 2005, Regev [25] defined the LWE problem, proved the hardness of LWE assuming the hardness of various worst-case lattice problems against quantum algorithms, and defined a PKE scheme whose IND-CPA security is based on the hardness of LWE. The LWE problem is a generalization of the learning parity with a noise problem [26] into large moduli q.

In this paper, we give an improved quantum algorithm for recovering the key of IND-CPA version of Frodo by using a quantum CCA attack. The security of Frodo's proposal is based on a plain LWE problem. In lattice-based cryptography, the plain LWE problem [25] is to solve a noisy linear system modulo as a known integer.

The main contributions of this paper are as follows:

(1) Based on the improved quantum algorithm for solving the quantum LWE problem, we first recalculate the success probability when the error follows a discrete Gaussian distribution. Using Hoeffding bound, we give the success probability for solving quantum LWE by computing the expectation and variance of the error.

(2) Then, we present a quantum KR-CCA attack which is inspired by the quantum LWE solving algorithm. Based on the existing quantum LWE solving algorithm, we recompute the success probability by using a different method. We analyze the security of Frodo640, Frodo976 and Frodo1344. By computing the expectation and variance of the error term, we can recover the full key with fewer oracle queries. Compared with the work of Băetu et al. [22], our algorithm can reduce the number of oracle calls to 1 and meanwhile keep the same success probability as the AJOP-based quantum KR-CCA algorithm; see Table 1.

Table 1. Three types of attacks on several lattice-based cryptosystems. P denotes the success probability, and O denotes the total number of oracle calls required to recover the full key with probability 1 by iterating the attack.

	GKZ-Based Quantum KR-CCA Attack [22]		**AJOP-Based Quantum KR-CCA Attack [22]**		**Improved Quantum KR-CCA Attack**	
	P	O	P	O	P	O
Frodo	2^{-13}	2^{17}	2^{-2}	2^{2}	2^{-2}	1

The organization of our paper is as follows. In Section 2, we give basic definitions and the meta-cryptosystem defined in the algorithm. In Section 3, we review the quantum algorithm for solving quantum LWE. Then, we recalculate the success probability for solving quantum LWE problems when the noise follows a discrete Gaussian distribution. In Section 4, we propose an improved quantum key-recovery attack on LWE-based IND-CPA schemes and analyze the security of Frodo. We conclude the paper in Section 5. In addition, we give a table with the acronyms and their meaning in Abbreviations.

2. Preliminaries

2.1. Notation and Definitions

For an integer $q \geq 1$, let Z_q be the residue class group modulo q such that $Z_q = \{0, 1, \cdots, q-1\}$. Let $x \to X$ denote an element x is chosen according to uniform distribution from a finite set X. $x \xrightarrow{\chi} X$ denotes an element x is chosen according to χ distribution from a finite set X. For a random variable y, $E[y]$ denotes the expectation value of y, $Var[y]$ denotes the variance of y. Given a matrix A, A^T will denote the transpose of A.

Definition 1 ((LWE) [25])**.** *Let n, q be positive integers, χ be a probability distribution on Z and s be a secret element in Z_q^n. We denote by L the probability distribution on $Z_q^n \times Z_q$ obtained by choosing $a \in Z_q^n$ uniformly at random, choosing $e \in Z_q$ by sampling each of its coefficients according to χ, and returning $(a, b) = (a, a \cdot s + e) \in Z_q^n \times Z_q$. Decision-LWE is the problem of deciding whether pairs $(a, b) \in Z_q^n \times Z_q$ are sampled according to L or the uniform distribution on $Z_q^n \times Z_q$. Search-LWE is the problem of recovering s from $(a, b) = (a, a \cdot s + e) \in Z_q^n \times Z_q$ sampled according to L.*

Definition 2 ((Quantum LWE) [27])**.** *The samples are given in the form of a uniform quantum superposition state $\frac{1}{\sqrt{q^n}} \sum_{a \in Z_q^n} |a\rangle |a \cdot s + e_a (\mathrm{mod}\ q)\rangle$ by querying a quantum oracle, where e_a are independent identical distribution random variables from some distribution χ. The goal is to output s.*

Definition 3 (Public key encryption)**.** *A public key encryption scheme is a triple of randomized algorithms as follows:*

(1) The key generator: given the security parameter, it outputs a public key and secret key.

(2) The encryption algorithm: takes a public key and a message (from some known set of valid messages) and outputs a ciphertext.

(3) The decryption algorithm takes a secret key and a ciphertext and outputs either a message or a distinguished "failure" symbol.

The scheme is said to be correct if generating a key pair, then encrypting a valid message using the public key, and then decrypting the resulting ciphertext using the secret key yields the original message (perhaps with all but negligible probability).

Definition 4 (Quantum Fourier transform)**.** *For any positive integer q, the quantum Fourier transform over Z_q is defined by the operation*

$$QFT_{Z_q}|x\rangle = \frac{1}{\sqrt{q}} \sum_{y \in Z_q} \omega_q^{x \cdot y} |y\rangle \tag{1}$$

where $\omega_q = e^{\frac{2\pi i}{q}}$.

Definition 5 (Hoeffding's bound)**.** *Consider a set of k independent random variables X_i, such that $a_i \leq X_i \leq b_i$. Let $c_i = b_i - a_i$, $X = \sum_{i \in [n]} X_i$. The expectation value of X is $\mu = E[X]$. Then, it follows that for any $\delta > 0$,*

$$Pr[X - \mu \leq -\delta n] \leq e^{\frac{-2n^2\delta^2}{(b_i - a_i)^2}} \tag{2}$$

2.2. The Meta-Cryptosystem Defined on the Algebra

The meta-cryptosystem defined on the algebra was given by Băetu et al. [22] in 2019. Băetu et al. considered six additive Abelian groups $S_{sk}, S_A, S_B, S_t, S_U, S_V$ and its four bilinear mappings: $S_A \times S_{sk} \to S_B$, $S_U \times S_{sk} \to S_V$, $S_t \times S_A \to S_U$, $S_t \times S_B \to S_V$. The operation satisfies the associative law for bilinear mappings $\times$, that is $(t \times A) \times sk = t \times (A \times sk)$ for all $t \in S_t, A \in S_A, sk \in S_{sk}$.

For any plaintext $pt \in M$, we first define two functions: encode function $M \to S_V$ and decode function $S_V \to M$ such that encode function is injective. As shown in Table 2, we have

$$\begin{aligned} W &= V - U \times sk \\ &= t \times B + f + encode(pt) - t \times A \times sk - e \times sk \\ &= t \times (A \times sk) + t \times d + f + encode(pt) - t \times A \times sk - e \times sk \\ &= t \times d - e \times sk + f + encode(pt), \end{aligned} \tag{3}$$

then $W = \delta + encode(pt)$ with $\delta = t \times d - e \times sk + f$, where δ denotes the error introduced by encoding/decoding.

In fact, in many cryptosystems, the encode and decode functions are different. In particular, we give the encode and decode functions on Frodo in Section 4.2.

Table 2. The meta-cryptosystem defined on the algebra.

Algorithm setup(1^λ)**:**	**Algorithm enc**$(pp, pk, pt; coinB)$**:**
1: set up the algebra and define pp	1: parse $pk = (A, B)$
2: return pp	2: pick random sparse $t \in S_t, e \in S_U$ and $f \in S_V$ by using coinB
Algorithm gen$(pp; coinA)$**:**	3: $U = t \times A + e$
1: pick a random $A \in S_A$ and random sparse $sk \in S_{sk}$ and $d \in S_B$ by using coinA	4: $V = t \times B + f + encode(pt)$
2: $B = A \times sk + d$	5: return $ct = (U, V)$
3: $pk = (A, B)$	**Algorithm dec**(pp, sk, ct)**:**
4: return (sk, pk)	1: parse $ct = (U, V)$
	2: $W = V - U \times sk$
	3: $pt' = decode(W)$
	4: return pt'

3. New Method for Solving Quantum LWE Problem

3.1. Quantum Algorithm for Solving Quantum LWE Problem

In 2019, Grilo et al. gave an efficient quantum-solving algorithm for the quantum LWE problem [28]. After, Wang et al. presented an improved quantum algorithm [27] based on the work of Grilo et al. In their algorithm, the noise e_u is a random variable with the absolute value at most k. In the following, we first give the algorithm of Wang et al. Then,

we consider the case where the noise follows a discrete Gaussian distribution and propose a new method of computing the success probability.

Lemma 1 ([27]). *Let* $\mathbf{u}, \mathbf{sk} \in Z_q^n$, $e_\mathbf{u} \in [-k, k]$, $k < \frac{q}{4}$, q *be subexponential in the dimension* n. *The algorithm can recover the secret key* **sk** *with the probability of at least* $\frac{1}{q^{2n}} || \sum_{\mathbf{u} \in Z_q^n} \cos \frac{2\pi e_\mathbf{u}}{q} ||^2$.

From the algorithm process in Algorithm 1, the probability of outputting the key **sk** is

$$\begin{aligned} Pr[\mathbf{sk}] &= \frac{1}{q^{2n}} || \sum_{\mathbf{u} \in Z_q^n} \omega^{-e_u} ||^2 \\ &= \frac{1}{q^{2n}} [(\sum_{\mathbf{u} \in Z_q^n} \mathrm{Re}(\omega^{-e_u}))^2 + (\sum_{\mathbf{u} \in Z_q^n} \mathrm{Im}(\omega^{-e_u}))^2] \\ &\geq \frac{1}{q^{2n}} (\sum_{\mathbf{u} \in Z_q^n} \mathrm{Re}(\omega^{-e_u}))^2 \\ &= \frac{1}{q^{2n}} || \sum_{\mathbf{u} \in Z_q^n} \cos \frac{2\pi e_u}{q} ||^2 \end{aligned} \tag{4}$$

Since $E(\sum_{\mathbf{u} \in Z_q^n} \sin \frac{-2\pi e_\mathbf{u}}{q}) \to 0$, the first inequality holds.

Algorithm 1: Improved quantum algorithm for solving the quantum LWE problem.

Quantum oracle: $|\mathbf{u}\rangle|y\rangle \to |\mathbf{u}\rangle|\mathbf{u} \cdot \mathbf{sk} + e_\mathbf{u} + y\rangle$
1: Set the initial state to $|0\rangle^{\otimes n}|1\rangle$
2: Apply a quantum Fourier transform on the all registers
and obtain $\frac{1}{\sqrt{q^n}} \sum_{\mathbf{u} \in Z_q^n} |\mathbf{u}\rangle \frac{1}{\sqrt{q}} \sum_{x \in Z_q} \omega^x |x\rangle$
3: Apply a quantum oracle query and obtain
$\frac{1}{\sqrt{q^n}} \sum_{\mathbf{u} \in Z_q^n} \omega^{-\mathbf{u} \cdot \mathbf{sk} - e_\mathbf{u}} |\mathbf{u}\rangle \frac{1}{\sqrt{q}} \sum_{x \in Z_q} \omega^x |x\rangle$
4: Apply a quantum Fourier transform on the first register
and obtain $\frac{1}{q^n} \sum_{\mathbf{u},\mathbf{y} \in Z_q^n} \omega^{-e_\mathbf{u}} |\mathbf{y}\rangle \frac{1}{\sqrt{q}} \sum_{x \in Z_q} \omega^x |x\rangle$
5: Discard the second register and measure the first register
6: Output **sk**

3.2. New Method

As shown in Equation (4), Wang et al. can obtain the success probability for solving the quantum LWE problem by using the method of enlarging and reducing, where the error $e_u \in [-k, k]$. In some lattice-based cryptosystems, the noise follows a discrete Gaussian distribution, such as Frodo. In this subsection, we recompute the success probability that the noise follows a discrete Gaussian distribution. The new method is explained as follows: by using Hoeffding bound in Equation (4), we can obtain the success probability with expectation value and variance. Then, we consider the case where the error e_u follows the discrete Gaussian distribution and compute the expectation value and variance of e_u. The details are listed as follows.

Let e_u follow the discrete Gaussian distribution $\mathcal{N}(0, \sigma^2)$, $e_\mathbf{u} \in [-\frac{q}{2}, \frac{q}{2}]$. The expectation of $e_\mathbf{u}$ is $\mathrm{E}(e_\mathbf{u}) = 0$, the variance of $e_\mathbf{u}$ is $\mathrm{Var}(e_\mathbf{u}) = \sigma^2$, then $\mathrm{E}(e_\mathbf{u}^2) = \mathrm{E}^2(e_\mathbf{u}) + \mathrm{Var}(e_\mathbf{u}) = \sigma^2$.

Using the mathematical analysis method, we first give the Taylor expansion of $\cos\alpha$

$$\cos\alpha = 1 - \frac{\alpha^2}{2!} + \frac{\alpha^4}{4!} - \frac{\alpha^6}{6!} + \cdots \frac{(-1)^n\alpha^{2n}}{2n!} + \frac{(-1)^{n+1}\cos\xi}{(2n+2)!}\alpha^{2n+2},\ \xi \in (0,\pi). \tag{5}$$

Let $\alpha = \frac{2\pi e_{\mathbf{u}}}{q}$, we have $\cos\frac{2\pi e_{\mathbf{u}}}{q} \in [-1,1]$. We find that starting from the third term, the positive term is greater than the negative term in two adjacent terms, (i.e., when $n \geq 1$ and n is even, $\frac{1}{2n!}(\frac{2\pi e_{\mathbf{u}}}{q})^{2n} - \frac{\cos\xi}{(2n+2)!}(\frac{2\pi e_{\mathbf{u}}}{q})^{2n+2} > 0$; when $n \geq 2$ and n is odd, $\frac{1}{(2n-2)!}(\frac{2\pi e_{\mathbf{u}}}{q})^{2n-2} - \frac{1}{2n!}(\frac{2\pi e_{u}}{q})^{2n} > 0$).

So, we have $\cos\frac{2\pi e_{\mathbf{u}}}{q} \geq 1 - \frac{1}{2}(\frac{2\pi e_{\mathbf{u}}}{q})^2$. Then

$$\mathrm{E}(\cos\frac{2\pi e_{\mathbf{u}}}{q}) \geq \mathrm{E}(1 - \frac{1}{2}(\frac{2\pi e_{\mathbf{u}}}{q})^2) = 1 - \frac{2\pi^2}{q^2}\mathrm{E}(e_{\mathbf{u}}^2) = 1 - \frac{2\pi^2}{q^2}\cdot\sigma^2 \tag{6}$$

For any $0 < \delta < 1$, by using Hoeffding bound, we can obtain

$$\begin{aligned}
&\Pr[\sum_{\mathbf{u}\in Z_q^n}(\cos\frac{2\pi e_{\mathbf{u}}}{q} - \mathrm{E}(1 - \frac{1}{2}(\frac{2\pi e_{\mathbf{u}}}{q})^2)) \leq -\delta q^n] \\
&= \Pr[\sum_{\mathbf{u}\in Z_q^n}(\cos\frac{2\pi e_{\mathbf{u}}}{q}) \leq (1 - \frac{2\pi^2}{q^2}\cdot\sigma^2) - \delta)q^n] \\
&\leq \Pr[\sum_{\mathbf{u}\in Z_q^n}(\cos\frac{2\pi e_{\mathbf{u}}}{q} - \mathrm{E}(\cos(\frac{2\pi e_{\mathbf{u}}}{q})) \leq -\delta q^n] \\
&< e^{-2\delta^2 q^{2n}/4},
\end{aligned} \tag{7}$$

Using (6) and (7), we have

$$\sum_{\mathbf{u}\in Z_q^n}\cos\frac{2\pi e_{\mathbf{u}}}{q} \geq \sum_{\mathbf{u}\in Z_q^n}\mathrm{E}(\cos(\frac{2\pi e_{\mathbf{u}}}{q}) - \delta q^n \geq (1 - \frac{2\pi^2}{q^2}\cdot\sigma^2 - \delta)q^n \tag{8}$$

Since $\cos\frac{2\pi e_{\mathbf{u}}}{q} \in [-1,1]$, for any $0 < \delta < 1$, using (4), the probability of outputting **sk** is

$$P \geq \frac{1}{q^{2n}}((1 - \frac{2\pi^2}{q^2}\cdot\sigma^2 - \delta)q^n)^2 = (1 - \frac{2\pi^2}{q^2}\sigma^2 - \delta)^2 \tag{9}$$

4. Quantum Misuse Attack

In this section, we first give a KR-CCA attack based on an improved quantum algorithm for solving quantum LWE. Then, we discuss the security of Frodo. In this attack, we consider an adversary with quantum access to a decryption oracle.

We consider the meta-PKC construction in Section 2.2, let $S_{sk} = Z_q^{n_{sk}}, S_A = Z_q^{n_A}, S_B = Z_q^{n_B}, S_t = Z_q^{n_t}, S_U = Z_q^{n_U}, S_V = Z_q^{n_V}$. Define $W_U = V - U \times sk, pt' = decode(W_U), Z_U = V - encode(pt')$, where $U \in S_U, V \in S_V$. Hence, for any V

$$\begin{aligned}
Z_U &= V - encode(pt') \\
&= V - encode(decode(V - U \times sk)) \\
&= V - (V - U \times sk) + \delta_U) \\
&= U \times sk + \delta_U,
\end{aligned} \tag{10}$$

δ_U denotes the error introduced by encoding/decoding and δ_U follows the uniform distribution. Then, the decryption oracle can make the following mapping:

$$|U\ V\ Z\rangle \to |U\ V\ Z + Z_U\rangle$$

In Table 2, the decryption algorithm returns plaintext pt', so the Z_U can be obtained.

4.1. Key Recovery Algorithm

Define $S_{sk} = S_B = Z_q^{nm}, S_A = Z_q^{n^2}, S_t = S_U = Z_q^{mn}, S_V = Z_q^{m^2}$. The bilinear mappings are matrix multiplications; let

$$U = \begin{pmatrix} U_0 \\ U_1 \\ \cdots \\ U_{m-1} \end{pmatrix}_{m \times n}, sk = \begin{pmatrix} sk_0 & sk_1 & \cdots & sk_{m-1} \end{pmatrix}_{n \times m}$$

For $i \in [m], U_i \in Z_q^n$ is the ith row of U, and for $j \in [m], sk_j \in Z_q^n$ is the jth column of sk.

In the following, we give the quantum key recovery attack algorithm based on LWE encryption schemes in Algorithm 2. This algorithm can recover the key with constant success probability.

Algorithm 2: Quantum key recovery attack.

Input: $i, j \in [m]$ and V

Quantum oracle: $|U \ V \ Z\rangle \rightarrow |U \ V \ Z + Z_U\rangle$

1: Set the quantum state to $|0 \ V \ (1_{ij})_{i=j}\rangle \in Z_q^{mn} \times Z_q^{m^2} \times Z_q^{m^2}$.

2: Make a quantum Fourier transform on the first and third registers.

3: Make a quantum oracle query and obtain (by writing $Z' = Z + Z_U$).

$\frac{1}{\sqrt{q^{mn}}} \frac{1}{\sqrt{q^{m^2}}} \sum_{U,Z',} (\prod_{i=j} \omega^{Z'_{ij} - Z_{U_{ij}}}) |U \ V \ Z'\rangle$.

4: Discard the last two registers and apply the quantum Fourier transform.

5: Measure the first register and output α.

Theorem 1. *Let $U \in Z_q^{mn}$, $Z_{U_{ij}} = (U \times sk)_{ij} + \delta_{U_{ij}}$, let the expectation value of the error $\delta_{U_{ij}}$ be μ and the variance of the error $\delta_{U_{ij}}$ be σ^2. Then, the algorithm of Algorithm 2 can recover the full key sk with constant probability β.*

Proof. Prepare the state $|0 \ V \ (1_{ij})_{i=j}\rangle \in Z_q^{mn} \times Z_q^{m^2} \times Z_q^{m^2}$. By making a quantum Fourier transform on the first and third registers, we obtain

$$\frac{1}{\sqrt{q^{mn}}} \frac{1}{\sqrt{q^{m^2}}} \sum_{U,Z} (\prod_{i=j} \omega^{Z_{ij}}) |U \ V \ Z\rangle.$$

After querying a quantum oracle and letting $Z' = Z + Z_U$, we have

$$\frac{1}{\sqrt{q^{mn}}} \frac{1}{\sqrt{q^{m^2}}} \sum_{U,Z',} (\prod_{i=j} \omega^{Z'_{ij} - Z_{U_{ij}}}) |U \ V \ Z'\rangle.$$

If we discard the last two registers and apply quantum Fourier transform, we obtain

$$\frac{1}{q^{mn}} \sum_{U,\alpha} (\prod_{i=j} \omega^{-Z_{U_{ij}}}) \omega^{U \cdot \alpha} |\alpha\rangle.$$

Then, we perform a complete measurement in the computational basis. The probability of obtaining $Pr[\alpha]$ is given by

$$\begin{aligned} Pr[\alpha] &= \| \frac{1}{q^{mn}} \sum_{U} (\prod_{i=j} \omega^{-Z_{U_{ij}}}) \omega^{U \cdot \alpha} \|^2 \\ &= \| \frac{1}{q^{mn}} \sum_{U} (\prod_{i=j} \omega^{-U_i \cdot sk_j - \delta_{U_{ij}}}) (\prod_{i=j} \omega^{U_i \cdot sk_j}) \|^2 \\ &= \| \frac{1}{q^{mn}} \sum_{U_{ij}} (\prod_{i=j} \omega^{-\delta_{U_{ij}}}) \|^2 \\ &\geq (\frac{1}{q^{2mn}} (\sum_{U_{ij}} Re(\omega^{-\delta_{U_{ij}}}))^2)^m, \end{aligned} \tag{11}$$

where α is a matrix of m blocks, and the size of each block is n for α such that $U_i \cdot \alpha_j = 0$ (i.e., $\alpha_j = 0$) for $i \neq j$ and $\alpha_j = sk_j$ for $i = j$.

Using (9), we obtain

$$Pr[\alpha] \geq (1 - \frac{2\pi^2}{q^2}(\mu^2 + \sigma^2) - \delta)^{2m} \tag{12}$$

We can further reduce the number of oracle calls with the same success probability. The specific analysis is as follows.

We can see that the success probability of obtaining one column of sk is $p = (1 - \frac{2\pi^2}{q^2}(\mu^2 + \sigma^2) - \delta)^2$. Suppose we can fully recover sk with constant probability $Pr[\alpha] = \beta$ by k queries. Then, the probability of recovering the first column of sk at least once in k queries is $1 - (1 - p)^k$. So, we can fully recover secret sk with probability $(1 - (1 - p)^k)^m$. We expect

$$(1 - (1 - p)^k)^m \geq \beta, \tag{13}$$

and then we can obtain the value of k. We will analyze it in detail in the following Section 4.2, using Frodo as the example. □

4.2. Application to Post-Quantum Cryptosystem Frodo

We consider the IND-CPA secure public key encryption scheme FrodoPKE, which is based on the public-key encryption scheme presented by Lindner and Peikert in [24]. FrodoPKE is a family of conservative yet practical post-quantum public key encryptions with security based on the hardness of the LWE problem.

Before giving the public-key encryption scheme of Frodo, we first describe how bit strings are encoded as mod-q integer matrices. Let D denote the number of bits used for encoding. The encoding function $ec(\cdot)$ encodes an integer $0 \leq pt < 2^D$ as an element in Z_q by multiplying it by $\frac{q}{2^D}$:

$$ec(pt) := pt \cdot \frac{q}{2^D}. \tag{14}$$

By applying $ec(\cdot)$ to D-bit sub-strings sequentially and filling the matrix row by row entry-wise, the function Frodo.Encode encodes bit strings of length $l = D \cdot m \cdot \bar{n}$ as $m \cdot \bar{n}$ matrices with entries in Z_q in left column of Table 3. The corresponding decoding function Frodo.Decode is defined as shown in right column of Table 3. It decodes the $m \cdot \bar{n}$ matrix M into a bit string of length $l = D \cdot m \cdot \bar{n}$ and extracts B bits from each entry by applying the function $de(c)$:

$$de(c) := \lfloor c \cdot \frac{2^D}{q} \rfloor \bmod 2^D. \tag{15}$$

Table 3. Encode and Decode Functions of Frodo.

Frodo.Encode	**Frodo.Decode**
input: bit string $\mathbf{pt} \in \{0,1\}^l, l = D \cdot m \cdot \bar{n}$ output: matrix $\mathbf{M} \in Z_q^{m \times \bar{n}}$	input: matrix $\mathbf{M} \in Z_q^{m \times \bar{n}}$ output: bit string $\mathbf{pt} \in \{0,1\}^l, l = D \cdot m \cdot \bar{n}$
1: for $(i = 0; i < m; i \leftarrow i + 1)$ do 2: for $(j = 0; j < \bar{n}; j \leftarrow j + 1)$ do 3: $pt \leftarrow \sum_{l=0}^{D-1} \mathbf{pt}_{(i \cdot \bar{n}+j)D+l} \cdot 2^l$ 4: $\mathbf{M}_{i,j} \leftarrow ec(pt) = pt \cdot \frac{q}{2^D}$ 5: return $\mathbf{M} = (\mathbf{M}_{i,j})_{0 \le i < m, 0 \le j < \bar{n}}$	1: for $(i = 0; i < m; i \leftarrow i + 1)$ do 2: for $(j = 0; j < \bar{n}; j \leftarrow j + 1)$ do 3: $pt \leftarrow de(\mathbf{M}_{i,j}) = \lfloor \mathbf{M}_{i,j} \cdot \frac{2^D}{q} \rceil \bmod 2^D$ 4: $pt = \sum_{l=0}^{D-1} pt_l \cdot 2^l$ where $pt_l \in \{0,1\}$ 5: for $(l = 0; l < D; l \leftarrow l + 1)$ do 6: $\mathbf{pt}_{(i \cdot \bar{n}+j) \cdot D+l} \leftarrow pt_l$ 7: return pt

Let $m, n, \bar{n}$ be integer parameters and $q \geq 2$ be an integer power of 2. In Table 4, we depict the public-key encryption scheme of Frodo. The symbol $\xleftarrow{\chi}$ denotes a sample is chosen according to χ. FrodoPKE works with $S_{sk} = S_B = Z_q^{n\bar{n}}, S_A = Z_q^{n^2}, S_t = S_U = Z_q^{mn}$, and $S_V = Z_q^{m\bar{n}}$ with L_∞ norm, $\delta_U \in [-\rho_+, \rho_+]$, where $\rho_+ = \frac{q}{8}$, $M = encode(\mathbf{pt}') \in Z_q^{m \times \bar{n}}$.

Table 4. The CPA version of Frodo.

Alice		**Bob**
1. Frodo.CPAPKE.Gen() 1.1 Generate matrix $A \in Z_q^{n \times n}$ 1.2 Sample $S, E \xleftarrow{\chi} Z_q^{n \times \bar{n}}$ 1.3 $B = A \cdot S + E$ 1.4 Output (B, S)	$\xrightarrow{B}$	2. $\mathbf{pt} \in \{0,1\}^{lm\bar{n}}$ 3. Frodo.CPAPKE.Enc(B, m) 3.1 Generate matrix $A \in Z_q^{n \times n}$ 3.2 $S', E' \xleftarrow{\chi} Z_q^{m \times n}$, $E'' \xleftarrow{\chi} Z_q^{m \times \bar{n}}$ 3.3 $U = S'A + E'$ 3.4 $V = S'B + E'' + encode(\mathbf{pt})$ 3.5 Output (U, V)
4. Frodo.CPAPKE.Dec(U, V, S) 4.1 $M = V - US$ 4.2 $\mathbf{pt}' = decode(M)$ 4.3 Output pt'	$\xleftarrow{U,V}$	

In FrodoPKE, χ is a discrete Gaussian distribution, and the error δ_U introduced by encoding/decoding is chosen according to uniform distribution with range $[-\rho_+, \rho_+]$. In Table 5, we give the other parameters of Frodo.

Table 5. Parameter sets for Frodo.

	n	q	D	$m \times \bar{n}$	sk **Ranges**	ρ_+
Frodo640	640	2^{15}	2	8×8	$[-12, 12]$	2^{12}
Frodo976	976	2^{16}	3	8×8	$[-10, 10]$	2^{12}
Frodo1344	1344	2^{16}	4	8×8	$[-6, 6]$	2^{11}

For Frodo640, $q = 2^{15}$, δ_U is chosen according to uniform distribution with range $[-\rho_+, \rho_+]$; this is $[-2^{12}, 2^{12}]$. The variance of δ_U is 5593770.67; then

$$Pr[sk_0] \geq (1 - \frac{2\pi^2}{q^2}(\mu^2 + \sigma^2) - \delta)^2 = 0.81$$

Using Equation (11), $(1 - (1 - 0.81)^k)^8 = 0.81^8$, we can obtain $k = 1$. So, we can fully recover the secret sk with probability more than $0.81^8 = 0.18$ with only 1 query.

For Frodo976, $q = 2^{16}$, δ_U is chosen according to uniform distribution with range $[-\rho_+, \rho_+]$, this is $[-2^{12}, 2^{12}]$. The variance of δ_U is 5,593,770.67; then

$$Pr[sk_0] \geq (1 - \frac{2\pi^2}{q^2}(\mu^2 + \sigma^2) - \delta)^2 = 0.95$$

Using Equation (11), $(1 - (1 - 0.95)^k)^8 = 0.95^8$, we can obtain $k = 1$. So, we can fully recover the secret sk with probability more than $0.95^8 = 0.66$ with only 1 query.

For Frodo1344, $q = 2^{16}$, δ_U is chosen according to uniform distribution with range $[-\rho_+, \rho_+]$; this is $[-2^{11}, 2^{11}]$. The variance of δ_U is 1,398,784; then

$$Pr[sk_0] \geq (1 - \frac{2\pi^2}{q^2}(\mu^2 + \sigma^2) - \delta)^2 = 0.99$$

Using Equation (11), $(1 - (1 - 0.99)^k)^8 = 0.99^8$, we can obtain $k = 1$. So, we can fully recover the secret sk with probability more than $0.99^8 = 0.92$ with only 1 query.

5. Conclusions and Discussion

In this paper, we developed a quantum algorithm to recover the key against LWE-based NIST candidates PKEs. Based on the improved quantum algorithm for solving LWE, we considered the success probability for solving the quantum LWE problem when the noise follows a discrete Gaussian distribution. Then, we proposed a new quantum key-recovery attack algorithm and gave a specific analysis for FrodoPKE. Compared with the existing algorithm [22], our algorithm can reduce the number of oracle calls with the same success probability.

In reality, the key is usually misused in a very short time, which leads to the number of queries being taken as the prime optimization goal with respect to misuse attack. During this short time, if an adversary can only make one oracle query, the misuse attack that requires four queries does not work for an adversary. However, our algorithm only needs one query to recover the key with probability 1. Therefore, the fewer oracle queries required, the greater the advantage for an adversary.

Author Contributions: Formal analysis, Y.W. and H.J.; supervision, H.J. and Z.M.; writing—original draft preparation, Y.W.; writing—review and editing, Y.W. and H.J.; funding acquisition, Z.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Key R&D Program of China (2021YFB3100100), the National Natural Science Foundation of China (62002385, 61972413), and the China Postdoctoral Science Foundation (2021M703321).

Data Availability Statement: The data presented in this study are available within the article.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following acronyms are used in this manuscript:

PKE	Public-key encryption
KEM	Key encapsulation mechanisms
NIST	National Institute of Standards and Technology
PQC	Post-quantum cryptography
LWE	Learning with error
PKC	Public key cryptosystem
KR-PCA	Key recovery under plaintext checking attacks
KR-CPA	Key recovery under chosen plaintext attacks
KR-CC	Key recovery under chosen ciphertext attacks
IND-CPA	INDistinguishability against chosen plaintext attacks
IND-CCA	INDistinguishability against chosen ciphertext attacks

References

1. Wei, S.J.; Wang, T.; Dong, R.; Long, G.L. Quantum computing. *Sci. Sin.* **2017**, *10*, 1277–1299.
2. Shor, P. Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, Santa Fe, NM, USA, 20–22 November 1994; pp. 124–134.
3. Diffie, W.; Hellman, M.E. New directions in cryptography. *IEEE Trans. Inf. Theory* **1976**, *22*, 644–654. [CrossRef]
4. Rivest, R.L.; Shamir, A.; Adleman, L.M. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
5. Nist: National Institute for Standards and Technology. Post Quantum Crypto Project. 2017. Available online: https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions (accessed on 3 January 2017).
6. Micciancio, D.; Oded, R. Lattice-based cryptography. In *Post-Quantum Cryptography*; Springer: Berlin, Heidelberg, 2009.
7. Eiichiro, F.; Tatsuaki, O. Secure integration of asymmetric and symmetric encryption schemes. In *Advances in Cryptology—CRYPTO*; Springer: Berlin/Heidelberg, Germany, 1999; pp. 537–554.
8. Aurelien, G.; Simon, M.; Guenael, R. Attack on lac key exchange in misuse situation. In *Cryptology and Network Security*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 549–569.
9. Ding, J.T.; Fluhrer, S.; Rv, S. Complete attack on rlwe key exchange with reused keys, without signal leakage. In *Information Security and Privacy*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 467–486.
10. Qin, Y.; Cheng, C.; Ding, J. An efficient key mismatch attack on the nist second round candidate kyber. *IACR Cryptol. ePrint Arch.* **2019**, *2019*, 1343. https://eprint.iacr.org/2019/1343 (accessed on 22 November 2019).
11. Satoshi, O.; Yuntao, W.; Tsuyoshi, T. Improving key mismatch attack on newhope with fewer queries. In *Information Security and Privacy*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 505–524.
12. Qin, Y.; Cheng, C.; Ding, J.T. A complete and optimized key mismatch attack on nist candidate newhope. In *Computer Security–ESORICS*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 504–520.
13. Zhang, X.; Cheng, C.; Qin, Y.; Ding, R. Small leaks sink a great ship: An evaluation of key reuse resilience of pqc third round finalist ntru-hrss. *Inf. Commun. Secur.* **2021**, *2021*, 283–300.
14. Daniel, B. Chosen ciphertext attacks against protocols based on the rsa encryption standard pkcs #1. In *Advances in Cryptology–CRYPTO*; Springer: Berlin/Heidelberg, Germany, 1998; pp. 1–12.
15. Menezes, A.; Ustaoglu, B. On reusing ephemeral keys in diffie-hellman key agreement protocols. *Int. Appl. Cryptogr.* **2010**, *2*, 154–158. [CrossRef]
16. Fluhrer, S. Cryptanalysis of ring-lwe based key exchange with key share reuse. *Cryptol. ePrint Arch.* **2016**, 2016, 85. Available online: https://eprint.iacr.org/2016/085 (accessed on 31 January 2016).
17. Ding, J.; Alsayigh, S.; Saraswathy, R.V.; Fluhrer, S.; Lin, X. Leakage of signal function with reused keys in rlwe key exchange. In Proceedings of the ICC 2017—2017 IEEE International Conference on Communications, Paris, France, 21–25 May 2017.
18. Bauer, A.; Gilbert, H.; Renault, G.; Rossi, M. Assessment of the key-reuse resilience of newhope. In Proceedings of the Cryptographers Track at the Rsa Conference, San Francisco, CA, USA, 4–8 March 2019; pp. 272–292.
19. Alkim, E.; Ducas, L.; Pppelmann, T.; Schwabe, P. Post-quantum key exchange—A new hope. *IACR Cryptol. ePrint Arch.* **2015**, *1092*, 327–343. Available online: https://eprint.iacr.org/2015/1092 (accessed on 10 November 2015).
20. Qin, Y.; Cheng, C.; Zhang, X.H.; Pan, Y.B.; Hu, L.; Ding, J.T. A systematic approach andanalysis ofkey mismatch attacks onlattice-based nist candidate kems. In *Advances in Cryptology–ASIACRYPT*; Springer: Berlin/Heidelberg, Germany, 2021; Volume 13093, pp. 92–121.
21. Gorjan, A.; Stacey, J.; Maris, O.; Alexander, P. On quantum chosen-ciphertext attacks and learning with errors. *Cryptography* **2020**, 4, 10.
22. Băetu, C.; Durak, F.B.; Huguenin-Dumittan, L.; Talayhan, A.; Vaudenay, S. Misuse attacks on post-quantum cryptosystems. In Proceedings of the 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), Darmstadt, Germany, 19–23 May 2019; Volume 11477, pp. 747–776.
23. Bundesamt für Sicherheit in der Informationstechnik. BSI TR-021021: Cryptographic Mechanisms: Recommendations and Key Lengths, Version 2022-1. 2022. Available online: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf (accessed on 1 January 2022).
24. Lindner, R.; Peikert, C. Better key sizes (and attacks) for lwe-based encryption. In *Topics in Cryptology*; Springer: Berlin/Heidelberg, Germany, 2011; Volume 6558, pp. 319–339.
25. Oded, R. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM* **2009**, 56, 1–40.
26. Grilo, A.B.; Kerenidis, I.; Zijlstra, T. Learning with errors problem is easy with quantum samples. *Phys. Rev. A* **2019**, *99*, 032314. [CrossRef]
27. Michael, J.K.; Yishay, M.; Dana, R.; Ronitt, R.; Schapire, R.E.; Linda, S. On the learnability of discrete distributions. In Proceedings of the Twenty-Sixth Annual ACM Symposium on Theory of Computing, Montreal, QC, Canada, 23–25 May 1994; pp. 273–282.
28. Wang, Y.R.; Jiang, H.D.; Ma, Z.; Wang, H.; Duan, Q.H. An improved quantum algorithm for the quantum learning with errors problem. *Quantum Inf. Process.* **2022**, *21*, 1–14. [CrossRef]