applied sciences

MDPI

Article

Efficient Lattice-Based Cryptosystems with Key Dependent Message Security

Bo Yang, Ruwei Huang * and Jianan Zhao

School of Computer and Electronic Information, Guangxi University, Nanning 530004, China; yangbo@st.gxu.edu.cn (B.Y.); 1813392021@st.gxu.edu.cn (J.Z.)
* Correspondence: ruweih@gxu.edu.cn

Abstract: Key-dependent message (KDM) security is of great research significance, to better analyse and solve the potential security problems in complex application scenarios. Most of the current KDM security schemes are based on traditional hard mathematical problems, where the public key and ciphertext are not compact enough, and make the ciphertext size grow linearly with the degree of the challenge functions. To solve the above problems and the inefficient ciphertext operation, the authors propose a compact lattice-based cryptosystem with a variant of the RLWE problem, which applies an invertible technique to obtain the RLWE* problem. It remains hard after the modification from the RLWE problem. Compared with the ACPS scheme, our scheme further expands the set of challenge functions based on the affine function of the secret key, and the size of public key and ciphertext is $\widetilde{O}(n)$, which is independent of the challenge functions. In addition, this scheme enjoys a high level of efficiency, the cost of encryption and decryption is only ploylog(n) bit operations per message symbol, and we also prove that our scheme is KDM-CPA secure under the RLWE* assumption.

Keywords: key-dependent message; RLWE problem; invertible; challenge functions

Citation: Yang, B.; Huang, R.; Zhao, J. Efficient Lattice-Based Cryptosystems with Key Dependent Message Security. *Appl. Sci.* **2021**, *11*, 12161. https://doi.org/10.3390/app112412161

Received: 3 November 2021
Accepted: 12 December 2021
Published: 20 December 2021

1. Introduction

With the rise of cloud computing and cloud storage technology, some application scenarios also need to encrypt the secret key and its related information. In 1984, Goldwasser and Michali [1] first introduced the concept of key-dependent message security, which ensures the security of message $f(sk)$ directly calculated from the secret key sk. The KDM (Key-dependent message)-secure public key encryption scheme was originally applied to the hard disk encryption process, and the secret key and user's data were encrypted together. Later, it has also been widely used in formal proof [2,3], homomorphic encryption [4] and some advanced cryptographic protocols [5].

At Eurocrypt 2001, Camenisch and Lysyanskaya [5] presented a circular-secure encryption scheme of provable security under the random oracle model, and the KDM attack capability of the adversary is defined by the set of challenge functions that can be queried. In 2002, Black, Rogaway and Shrimp-ton [6] considered such a situation, that is, in the application process of hard disk encryption, an adversary was allowed to obtain a ciphertext, which was encrypted by the secret key $\{sk_1, \ldots, sk_\ell\}$ related function f of the user j under the public key pk_j. Compared with semantic security, the KDM security model has stronger security and a higher research value, which mainly depends on its efficiency and the set of challenge functions that can be queried. However, various KDM-secure public key encryption schemes are different in construction. Until 2008, Boneh et al. [7] proposed a public key encryption scheme based on the DDH (decisional Diffie–Hellman) assumption, and proved the KDM-CPA (Chosen Plaintext Attack) security of the scheme under the standard model. After that, Applebaum et al. [8] proposed the first lattice-based public key encryption scheme of KDM-CPA security, which was named the ACPS scheme. The security follows from the LWE (Learning with Error) assumption, because of its good linear structure, and has compact ciphertexts and a high level of computational efficiency.

Similarly, the ACPS scheme has post-quantum security and its challenge functions are affine functions.

At Crypto 2010, Brakerski and Goldwasser et al. [9] extended the technique in [7] and proposed further construction of KDM-secure schemes, so that the security of the scheme could be based on more mathematically hard problems, mainly the QR (Quadratic Residuosity) problem [10] and the DCR (Decisional Composite Residuosity) problem [11]. The KDM security of this scheme can be attributed to the indecipherable (IND) security. However, the encryption method in [9] is similar to the circular security assumption which encrypts the message in bit. Therefore, the KDM-secure scheme constructed according to the above method has the disadvantages of not being compact as well as inefficient encryption and decryption. At Eurocrypt 2010, under the standard model and standard assumption, Barakerski et al. [12] constructed a KDM-CPA secure scheme based on the DDH or LWE assumption. For arbitrary but fixed polynomials L and N, given the size of the secret key k, the adversary can attack at most $N(k)$ public keys and a circuit of size $L(k)$, namely, the set of challenge functions contains a Boolean circuit with polynomial size. Therefore, it is also known as a bounded KDM-secure scheme, which is inefficient and the ciphertext includes a garbled circuit of the same size as its set of challenge functions. In 2011, Brakerski, Goldwasser et al. [13] proposed a KDM-secure public key encryption scheme with respect to polynomial functions with a degree less than d, where d is a constant. The KDM-CPA security follows from the DDH or LWE assumption. Since the construction of the scheme still follows the construction of [7], the ciphertext is not compact enough and the ciphertext size is an exponential function related to d. In the same year, Malkin et al. [14] proposed a public key encryption scheme based on the DCR assumption with KDM-CPA security. The ciphertext size is a linear function related to d, which improves the efficiency of the above scheme.

With an increase of application scenarios, the KDM-secure encryption scheme also has a significant role in identity authentication. Under the LWE assumption, Peikert et al. [15] proposed the first identity-based encryption scheme with KDM security, where the challenger can answer encryption queries with respect to affine functions. In 2019, Chen et al. [16] focused on the KDM security of an identity-based encryption scheme, proposing a generic way to reach it from public key encryption, so that it remained KDM secure. Most of the discussed schemes directly encrypt the secret key, but in practice, the set of challenge functions may be composed of the secret key in more complex forms. At Asiacrypt 2020, Kitagawa et al. [17] proved an encryption scheme with circular security that can be transformed into a KDM-secure encryption scheme, in which circular security is the most basic form of KDM security, that is, it can securely encrypt a secret key in bit. Therefore, the question of how to face more complex encryption scenarios, as well as constructing compact ciphertext, is worth intensive study.

Motivation. Through the above comparison, we can observe three urgent problems in KDM-secure public key encryption schemes: (1) how to securely encrypt the complex functions of the secret key (not only itself); (2) how to construct the public-key encryption scheme with compact ciphertexts, and independent of the challenge functions, and (3) The existing compact cryptosystems are all based on lattice problems. A question is raised of how to modify the LWE problem to improve the efficiency of encryption and decryption.

Our Results. In this paper, we analyse the KDM security of the public-key encryption scheme, and choose to use the RLWE (Ring-Learning with error) problem to build the compact cryptosystems. First, we apply the invertible technique [18] to obtain the RLWE* problem, then provide a new version by scaling the noise, and proving that it remains hard after the above modification. After that, we give a useful transformation to obtain the RLWE* assumption-Hermite normal form (HNF), namely, the secret chooses form error distribution. As it happens, through noise scaling, the secret key just fits into the message space R_t, so our scheme can securely encrypt the linear functions of its secret key. Therefore, we easily construct a compact public-key scheme, analyze its correctness, and prove its key-dependent message security under the RLWE* assumption.

In particular, through the proof of KDM-CPA security, we observe that the ciphertexts are pseudorandom with encrypting the secret key directly. If we do not expand the message space by scaling the noise, then it is possible to construct a symmetric-key scheme for KDM security by directly encrypting the secret key to its linear functions. Therefore, we further improve the RLWE* problem, propose its variant k-RLWE* problem, and demonstrate its hardness. For the message space R_2, given a small enough Hamming weight h and making $\begin{pmatrix} n \\ h \end{pmatrix}$ large enough, we can obtain a binary secret symmetric-key scheme with less ciphertext noise. Finally, we prove that our scheme is KDM-CPA secure under the special k-RLWE* assumption and the cost of encryption and decryption is only ploylog(n) bit operations per message symbol.

Organization. In Section 2, we describe some important lemmas and give the formal definition of KDM-secure cryptosystems. In Section 3, we first introduce the RLWE* problem and a HNF (Hermite normal form) transformation, then construct a compact public-key scheme with KDM-CPA security. In Section 4, similarly to the previous section, the variant k-RLWE* problem and symmetric-key scheme are presented. In Section 5, we provide a detailed performance comparison. Finally, the conclusion is given in Section 6.

2. Preliminaries

2.1. Basic Notation

In this paper, we use the following notation and lemmas. We will use a ring R. In our concrete instantiations, we prefer to use either $R = \mathbb{Z}$ (the integers) or the polynomial ring $R = \mathbb{Z}[x]/\left(x^d + 1\right)$, where d is a power of 2. For integer q, we use R_q to denote R/qR. Sometimes we will use abuse notation and use R_2 to denote the set of R-elements with binary coefficients, when $R = \mathbb{Z}$, R_2 may denote $\{0, 1\}$, and when R is a polynomial ring, R_2 may denote those polynomials that have $0/1$ coefficients. For $a \in R$, we use the notation $[a]_q$ to refer to $a \mod q$, with coefficients reduced into the range $(-q/2,\ q/2]$.

For the security parameter λ, denote a negligible function negl(λ). For some distribution χ, writing $e \leftarrow \chi$ means that e is distributed according to χ, the error distribution χ is the discrete gaussian distribution $D_{\mathbb{Z}^n,\sigma}$ for some $\sigma > 0$. The usual norm $\ell_1(s)$ over the reals equals $\sum_{i=1}^{n} |s_i|$. The $\ell_\infty(s)$ norm is defined as $\max\{|s_1|, |s_2|, \ldots, |s_n|\}$.

Lemma 1. (see [19]). *Let $n \in \mathbb{N}$. For any real number $\sigma = \omega\left(\sqrt{\log n}\right)$, we have*

$$\Pr_{x \leftarrow D_{\mathbb{Z}^n,\sigma}} [\|x\| > \sigma\sqrt{n}] \leq 2^{-n+1}. \tag{1}$$

Lemma 2. (see [20]). *Let $n \in \mathbb{N}$. For any real number $\sigma = \omega\left(\sqrt{\log n}\right)$,and any $c \in \mathbb{Z}^n$, the statistical distance between the distributions $D_{\mathbb{Z}^n,\sigma}$ and $D_{\mathbb{Z}^n,\sigma,c}$ is at most $\|c\|/\sigma$.*

Lemma 3. (see [21]). *Let $n \in \mathbb{N}$. $m = 2n$, and let $f(x) = \Phi_m(x) = x^n + 1$ and let $R = \mathbb{Z}[x]/(\Phi_m(x))$. For any $s, t \in R$, $\|s \cdot t (mod\ \Phi_m(x))\| \leq \sqrt{n} \cdot \|s\| \cdot \|t\|$ and $\|s \cdot t (mod\ \Phi_m(x))\|_\infty \leq n \cdot \|s\|_\infty \cdot \|t\|_\infty$.*

2.2. The RLWE Problem

This simple version of the RLWE problem comes from [22], and the LWE problem can choose the secret from the noise distribution by the transformation T.

Definition 1. (RLWE). *For security parameter λ, let $f(x) = x^d + 1$ where $d = d(\lambda)$ is a power of 2. Let $q = q(\lambda) \geq 2$ be an integer. Let $R = \mathbb{Z}[x]/(f(x))$ and let $R_q = R/qR$. Let $\chi = \chi(\lambda)$ be a distribution over R. The $RLWE_{d,q,\chi}$ problem is to distinguish the following two distributions: In the first distribution, one samples (a_i, b_i) uniformly from R_q^2. In the second distribution, one first draws $s \leftarrow R_q$ uniformly and then samples $(a_i, b_i) \in R_q^2$ by sampling $a_i \leftarrow \mathbb{R}_q$ uniformly,*

$e_i \leftarrow \chi$ and setting $b_i = a_i \cdot s + e_i$, let this distribution be $A_{s,\chi}$. The $RLWE_{d,q,\chi}$assumption is that the $RLWE_{d,q,\chi}$problem is infeasible.

Lemma 4. (see [8]). *Let $q = p^e$ be a prime power. There is a deterministic polynomial-time transformation T that, for arbitrary $s \in \mathbb{Z}_q^n$ and error distribution χ, maps $A_{s,\chi}$to $A_{\overline{x},\chi}$ where $\overline{x} \leftarrow \chi^n$, and maps $U\left(\mathbb{Z}_q^n \times \mathbb{Z}_q\right)$ to itself. The transformation also produces an invertible square matrix $\overline{\mathbf{A}} \in \mathbb{Z}_q^{n \times n}$ and $\overline{\mathbf{b}} \in \mathbb{Z}_q^n$ that, when mapping $A_{s,\chi}$ to $A_{\overline{x},\chi}$, satisfy $\overline{x} = -\overline{\mathbf{A}}^T s + \overline{\mathbf{b}}$.*

Theorem 1. (see [23]). *Let K be the mth cyclotomic number field having dimension $n = \varphi(m)$ and $R = \mathcal{O}_K$ be its ring of integers. Let $\alpha < \sqrt{\log n / n}$, and let $q = q(n) \geq 2$, $q = 1 \bmod m$ be a $poly(n)$ -bounded prime such that $\alpha q \geq \omega\left(\sqrt{\log n}\right)$. Then there is a polynomial-time quantum reduction from $\widetilde{O}\left(\sqrt{n}/\alpha\right)$ -approximate* SIVP (*or* SVP) *on ideal lattices in K to R-$\mathrm{DLWE}_{q,\Upsilon_\alpha}$. Alternatively, for any $\ell > 1$, we can replace the target problem by the problem of solving R-DLWE_{q,D_ξ} given only ℓ samples, where $\xi = \alpha(n\ell/\log(n\ell))^{1/4}$.*

2.3. Key-Dependent Message Security

We now define key-dependent message security by a game played between the challenger and the adversary $\mathcal{A}$, and KDM security guarantees the direct encryption of the secret key sk and its correlation function $f(sk)$. The KDM attack capability of the adversary $\mathcal{A}$ is mainly determined by the collection of secret key functions $\mathcal{F}$ that it can query, expressed as $\mathcal{F} \subset \left\{ f | f : \mathcal{K}^\ell \to \mathcal{M} \right\}$, where $\mathcal{K}$ and $\mathcal{M}$ are the secret key space and message space of the encryption scheme. Given public keys $\{pk_1, \ldots, pk_\ell\}$ and encryption of the key-dependent message $f(sk_1, \ldots, sk_\ell)$, the adversary $\mathcal{A}$ cannot effectively distinguish it from the ciphertext that is encrypted by the message $\{0, 1\}$, and so we can call the scheme KDM-CPA secure with respect to $\mathcal{F}$. $\mathcal{F}$ is a family of sets of functions parameterized by the security parameter λ and the number of users ℓ. The game proceeds as follows:

1. The challenger chooses a bit $\mu \leftarrow \{0, 1\}$. Run the scheme's key generation algorithm ℓ times. It gives $\{pk_1, \ldots, pk_\ell\}$ to the adversary $\mathcal{A}$.

2. Adversary $\mathcal{A}$ makes encryption queries of the form (i, f), where $1 < i < \ell$ and $f \in \mathcal{F}$. To process a query, the challenger computes $m \leftarrow f(sk_1, \ldots, sk_\ell)$, then computes the challenge ciphertexts and returns to the adversary $\mathcal{A}$.

$$c = \begin{cases} Enc(pk_i, m), & \mu = 0, \\ Enc\left(pk_i, 0^{|m|}\right), & otherwise. \end{cases} \tag{2}$$

3. Adversary $\mathcal{A}$ attempts to guess μ and outputs $\mu' \in \{0, 1\}$.

The scheme is KDM-CPA secure if for every probabilistic polynomial-time adversary $\mathcal{A}$, the distinguishing advantage $Adv(\mathcal{A}) = |\Pr[\mu = \mu'] - 1/2| \leq \mathrm{negl}(n)$. This shows that the scheme can securely encrypt any functions $\mathcal{F}$ of its own secret key, taking the place of a message.

The KDM-CPA security definition of the symmetric-key scheme is similar. In the first stage, the challenger generates the secret key without giving anything to the adversary $\mathcal{A}$. In the second stage, it uses the secret key for encryption (and uses it as the input of $f(sk)$). Everything else is just the same.

3. Compact Public-Key Cryptosystem with KDM Security

In this section, we will describe the construction of a public-key scheme based on the variant of the RLWE problem. At first, we introduce the RLWE* problem by applying the invertible technique, and then give the new version by scaling the noise. After that, to ensure that the secret chooses form error distribution, a useful transformation is given to obtain the RLWE* assumption-Hermite normal form. Finally, we construct a compact public-key scheme, analyze its correctness, and prove its key-dependent message security.

3.1. The Invertible Version of RLWE Problem

According to [18], authors presented a variant of RLWE problem, defined as the RLWE* problem. It is similar to the RLWE problem except that a chooses from R_q^*, in which R_q^* is the ser of invertible elements of R_q. Therefore, we call RLWE* the invertible variant.

RLWE* problem. For $s \in R_q$ and error distribution χ, we define $A_{s,\chi}^*$ as the distribution obtained by sampling the pair $(a,\ as+e) \in R_q^* \times R_q$, where R_q^* denote the set of invertible elements of R_q. The Decision RLWE* problem is to distinguish between $A_{s,\chi}^*$ and $U\left(R_q^* \times R_q\right)$. Please note that for R_q^*, [23] claim that for any $q \geq 2$, the fraction of invertible elements in R_q is at least $1/\mathrm{poly}(n, \log q)$. Moreover, ref. [18] further shows that as long as $q = \Omega(n)$, an element choosing from $U(R_q)$ is invertible with overwhelming probability. Hence, the RLWE problem remains hard even when applying the invertible technique.

Scaling the noise. This technique was first formally proposed in [24] and generated the RLWE* samples as $(a,\ a \cdot s + t \cdot e)$; security is not affected when $t \in \mathbb{Z}_q^*$ and q are relatively prime, and other parameters are as above.

Definition 2. (Decision RLWE*). *The average-case decision version of the* RLWE* *problem, denoted* $\mathrm{RLWE}_{q,\chi}^*$, *is to distinguish the following two distributions with non-negligible advantage: In the first distribution, one samples* (a_i, b_i) *uniformly from* R_q^2. *In the second distribution, one first draws* $s \leftarrow R_q$ *uniformly and then samples* $(a, b = a \cdot s + t \cdot e) \in R_q^2$ *by sampling* $a \leftarrow R_q^*$ *uniformly, where* R_q^* *denote the set of invertible elements of* R_q, $e \leftarrow \chi$ *and* $t \in \mathbb{Z}_q^*$.

3.2. A Generic Transformation

In this section, we make a useful transformation to sampling $s \leftarrow \chi$. There is no loss of security, and it is ensured that the secret can be placed in the message space. The transformation lemma follows.

Lemma 5. *For modulus* q, *arbitrary* $s \in R_q$ *and the error distribution* χ, *there is a deterministic polynomial-time transformation* T, *which maps* $A_{s,\chi}^*$ *to* $A_{\phi,\chi}^*$ *where* $\phi \leftarrow \chi$, *and maps*$U\left(R_q^* \times R_q\right)$ *to itself.*

Proof. The transformation T to access the distribution D over $R_q^* \times R_q$, possibly $A_{s,\chi}^*$ or $U\left(R_q^* \times R_q\right)$. Then, we prove it in two steps.

The first step. Transformation T generates the sample $\left(\overline{a}, \overline{b}\right) \in R_q^* \times R_q$ by drawing from the distribution D. When $D = A_{s,\chi}^*$, we have $\overline{b} = \overline{a} \cdot s + t \cdot \overline{x}$, where $\overline{x} \leftarrow \chi$.

The second step. To transform samples from D into samples from a different distribution, the sample $(a, b) \in R_q^* \times R_q$ from D will be transformed into $(a', b') \in R_q^* \times R_q$, where $a' = -\overline{a}^{-1} \cdot a$, $b' = b + a' \cdot \overline{b}$.

Especially $a' \in R_q^*$ is uniform due to $\overline{a} \leftarrow R_q^*$ being invertible modulo q and a chooses from $U\left(R_q^*\right)$. If $D = U\left(R_q^* \times R_q\right)$, then (a', b') is also subject to $U\left(R_q^* \times R_q\right)$. If $D = bA_{s,\chi}^*$, then $b = a \cdot s + t \cdot e$, so we have

$$b' = b + a' \cdot \overline{b} = a \cdot s + t \cdot e + a' \cdot (\overline{a} \cdot s + t \cdot \overline{x}) = a' \cdot (t \cdot \overline{x}) + t \cdot e, \tag{3}$$

where $\phi = t \cdot \overline{x}$, therefore, (a', b') is subject to $bA_{\phi,\chi}^*$, as desired. □

Definition 3. (The RLWE* assumption-Hermite normal form). *As in the previous definition, for all security parameters* $\lambda \in \mathbb{N}$, *the* RLWE* *assumption suggests that, for any* $\ell = \mathrm{poly}(\lambda)$, *we have*

$$\{(a_i, a_i \cdot s + t \cdot e_i)\}_{i \in [\ell]} \approx \{(a_i, u_i)\}_{i \in [\ell]}, \tag{4}$$

in which s *is sampled from the noise distribution* χ, *and other parameters remain unchanged.*

3.3. Basic RLWE-Based Encryption Scheme*

For security parameter λ, let $q = 1 \bmod 2n$ and $t \in \mathbb{Z}_q^*$ relatively prime, in which $\{1, \ldots, q-1\} \supseteq \mathbb{Z}_q^*$. Let $\chi = D_{\mathbb{Z}^n,\sigma}$ be an error distribution with $\sigma \geq \omega\left(\sqrt{\log n}\right)$ and $\sigma \ll t$; we sampled s from error distribution χ, so all $s \in R_t$ with overwhelming probability when the secret chooses from error distribution. Let $R = \mathbb{Z}[x]/(f(x))$, $R_q = \mathbb{Z}_q[x]/(f(x))$ where $f(x) = x^n + 1$ and $n = n(\lambda)$ is a power of 2.

- **RPKE**1.**KeyGen**$\left(1^\lambda\right)$: Sample $s \leftarrow \chi$. Output $sk = s$. Sample $a \leftarrow R_q^*$ uniformly, $e \leftarrow \chi$ and set $b = a \cdot s + t \cdot e$, where $t \in \mathbb{Z}_q^*$ and R_q^* denote the set of invertible elements of R_q. Output the public key $pk = (a, b) \in R_q^* \times R_q$.
- **RPKE**1.**Enc**(pk, m): Notice that $m \in R_t$, due to the lemma by the noise scaling. Sample $r, e_1, e_2 \leftarrow \chi$. Compute $c_1 = a \cdot r + t \cdot e_1$, $c_2 = b \cdot r + t \cdot e_2 + m$, output the ciphertext $c = (c_1, c_2) \in R_q \times R_q$.
- **RPKE**1.**Dec**(sk, c): Input the corresponding secret key and ciphertext, then output $m = (c_2 - c_1 \cdot s) \bmod q \bmod t$.

The correctness of the scheme is obvious, compute $(c_2 - c_1 \cdot s) = m + te_2 - te_1 s + ter$, according to the Lemma 3, we have

$$\begin{aligned} \|te_2 - te_1 s + ter\|_\infty &= t \cdot \|e_2\|_\infty + t \cdot \|e_1 s\|_\infty + t \cdot \|er\|_\infty \\ &= t \cdot \sigma\sqrt{n} + 2t \cdot n\left(\sigma\sqrt{n}\right)^2 < q/2 \end{aligned} \tag{5}$$

if $q > t \cdot \mathrm{poly}(n) \cdot \sigma^2$, where $t = \sigma\sqrt{n}$, the ciphertext can be decrypted correctly.

The KDM-CPA security follows from the RLWE* assumption by noting the pseudorandom distribution $A_{s,\chi}^*$. Observe that $f(sk) = k \cdot s + t \cdot w \in R_t$, where k, s, w all choose from error distribution. The ciphertext is indistinguishable from uniform even if m is replaced with any linear function of the scheme's own secret key.

Theorem 2. *Let $k \leftarrow D_{\mathbb{Z}^n,\sigma}$ and $w \leftarrow D_{\mathbb{Z}^n,\sigma'}$, where $\sigma' \geq 2^{\omega(\log n)} \cdot \sigma^2$, $\sigma = \omega\left(\sqrt{\log n}\right)$. Under the* RLWE* *assumption, the above cryptosystem RPKE1 about $f(sk) = k \cdot s + t \cdot w$ satisfies KDM-CPA security.*

Proof. For any probabilistic polynomial-time adversary $\mathcal{A}$, we use a three-step hybrid game to prove that the ciphertext with key-dependent message $f(sk)$ in the RPKE1 scheme is computationally indistinguishable from one that carries no information on the message. Therefore, the distinguishing advantage of the adversary $\mathcal{A}$ is negligible.

Game $\boldsymbol{H}_0$: Let $pk = (a, b) \leftarrow$ **RPK**1.**KeyGen**$\left(1^\lambda\right)$, the remaining parameters are as above, and Hybrid game $\boldsymbol{H}_0$ is mainly used to generate the challenge ciphertexts.

$$c = \begin{cases} (c_1 = a \cdot r + t \cdot e_1,\ c_2 = b \cdot r + t \cdot e_2 + k \cdot s + t \cdot w), & \mu = 0 \\ (c_1 = a \cdot r + t \cdot e_1,\ c_2 = b \cdot r + t \cdot e_2 + 0\ ), & \mu = 1 \end{cases} \tag{6}$$

Game $\boldsymbol{H}_1$: Similar to the hybrid game $\boldsymbol{H}_0$, hybrid game $\boldsymbol{H}_1$ generates the challenge ciphertexts related to $f(sk)$ in different ways.

$$c = \begin{cases} \left(c_1^* = a',\ c_2^* = a' \cdot s + t \cdot w\right), & \mu = 0 \\ (c_1 = a \cdot r + t \cdot e_1,\ c_2 = b \cdot r + t \cdot e_2), & \mu = 1 \end{cases} \tag{7}$$

where $a' = a \cdot r + k$, $k \leftarrow \chi$ and $w \leftarrow D_{\mathbb{Z}^n,\sigma'}$. Observe that $c_1 = a \cdot r + t \cdot e_1$, r and e_1 choose from the error distribution χ, just like the ciphertext $c_1^* = a \cdot r + k$ without scaling the noise, hence c_1^* is indistinguishable from c'. In addition, observe $c_2 = b \cdot r + t \cdot e_2 + k \cdot s + t \cdot w$, compute

$$c_2 = (a \cdot s + t \cdot e) \cdot r + t \cdot e_2 + k \cdot s + t \cdot w = (a \cdot r + k) \cdot s + t \cdot (w + e_2 + er) \tag{8}$$

define $a' = a \cdot r + k$, then $c_2 = a' \cdot s + t \cdot (w + e_2 + er)$. By Lemma 1 and Lemma 2, we have

$$\|e_2 + er\| \leq \|e_2\| + \sqrt{n} \cdot \|e\| \cdot \|r\| \leq \sigma\sqrt{n} + \sqrt{n} \cdot \left(\sigma\sqrt{n}\right)^2 = n^{0.5} \cdot \sigma + n^{1.5} \cdot \sigma^2 \quad (9)$$

Let $\Delta = n^{0.5} \cdot \sigma + n^{1.5} \cdot \sigma^2$, $\sigma' \geq 2^{\omega(\log n)} \cdot \sigma^2$, compute $\frac{\Delta}{\sigma'} \leq \frac{n^{0.5} \cdot \sigma + n^{1.5} \cdot \sigma^2}{2^{\omega(\log n)} \cdot \sigma^2} = 2^{-\omega(\log n)}$. By Lemma 3, $D_{\mathbb{Z}^n,\sigma'}$ is statistically indistinguishable from $D_{\mathbb{Z}^n,\sigma',\Delta}$, it holds that $c_2 \approx a' \cdot s + t \cdot w$, and therefore, the challenge ciphertext $c_2^* = a' \cdot s + t \cdot w$ is indistinguishable from c_2. To sum up, the distinguishing advantage between the $\boldsymbol{H}_1$ and $\boldsymbol{H}_0$ is negligible, namely

$$|adv(\mathcal{A}, \boldsymbol{H}_0) - adv(\mathcal{A}, \boldsymbol{H}_1)| \leq \text{negl}(n). \quad (10)$$

Game $\boldsymbol{H}_2$: Hybrid game $\boldsymbol{H}_2$ generates the challenge ciphertext from $U\left(R_q \times R_q\right)$ when $\mu = 0$. Everything else is exactly the same.

$$c = \begin{cases} \left(c_1^* = u_1,\ c_2^* = u_2\right), & \mu = 0 \\ \left(c_1 = a \cdot r + t \cdot e_1,\ c_2 = b \cdot r + t \cdot e_2\right), & \mu = 1 \end{cases} \quad (11)$$

where u_i $(i = 1, 2)$ chooses from $U\left(R_q\right)$. Observe the hybrid game $\boldsymbol{H}_1$, $a' = a \cdot r + k$ is indistinguishable from uniform, $\left(c_1^* = a',\ c_2^* = a' \cdot s + t \cdot w\right) \in R_q \times R_q$ just happens to be an instance of the RLWE problem. Therefore, $\left(c_1^*,\ c_2^*\right)$ is pseudorandom, and then

$$|adv(\mathcal{A}, \boldsymbol{H}_1) - adv(\mathcal{A}, \boldsymbol{H}_2)| \leq \text{negl}(n). \quad (12)$$

Since the challenge ciphertext $(u_1,\ u_2) \in U\left(R_q \times R_q\right)$, thus we have

$$adv(\mathcal{A}, \boldsymbol{H}_2) = \text{negl}(n). \quad (13)$$

Finally, we conclude that

$$\begin{array}{c} adv(\mathcal{A}, \boldsymbol{H}_0) = (adv(\mathcal{A}, \boldsymbol{H}_0) - adv(\mathcal{A}, \boldsymbol{H}_1)) + adv(\mathcal{A}, \boldsymbol{H}_1) \\ \leq |adv(\mathcal{A}, \boldsymbol{H}_0) - adv(\mathcal{A}, \boldsymbol{H}_1)| + adv(\mathcal{A}, \boldsymbol{H}_1) \\ \leq |adv(\mathcal{A}, \boldsymbol{H}_0) - adv(\mathcal{A}, \boldsymbol{H}_1)| + |adv(\mathcal{A}, \boldsymbol{H}_1) - adv(\mathcal{A}, \boldsymbol{H}_2)| \\ + adv(\mathcal{A}, \boldsymbol{H}_2) = \text{negl}(n). \end{array} \quad (14)$$

This proves the KDM-CPA security of the RPKE1 scheme. □

4. Efficient Symmetric-Key Encryption Scheme

The above public-key scheme expands the message space due to the noise scaling, resulting in low efficiency. In this section, we will introduce a KDM secure symmetric-key scheme without scaling the noise. For the symmetric-key scheme, we can generate the following ciphertext $(c_1 = a,\ c_2 = b + m)$ by the RLWE* problem, where $b = a \cdot s + e$. If secret key s replaces message m, consider the ciphertext $(c_1 = a,\ c_2 = b + s)$, we will have that $c = (a,\ (a + 1) \cdot s + e)$. If we define $a' = a + 1$, then $(a',\ a' \cdot s + e)$ is an instance of the RLWE problem, so the challenge ciphertext $(c_1 = a',\ c_2 = a' \cdot s + e)$ is pseudorandom, and it is easy to prove the KDM security. By way of the above, we can easily extend to any linear function about s, just like $f(sk) = k \cdot s + w$, where $k \in R_q$ and $w \leftarrow \chi$. Then, we will obtain a challenge ciphertext $(a, (a + k) + w + e)$, therefore, for the sake of convenience, we might wish to define the following problem.

4.1. The Variant of RLWE* Problem

Definition 4. (k-RLWE*). *As in the previous Definition 2, the k-RLWE* problem is to distinguish the following two distributions with non-negligible advantage: In the first distribution, one samples (a, b) uniformly from $R_q \times R_q$. In the second distribution, one samples $(a, b) \in R_q^* \times R_q$ by sampling $a, k \leftarrow R_q^*$ uniformly, where $s \in R_q$, $e \leftarrow \chi$ and setting $b = (a + k) \cdot s + e$, let this distribution be $bA_{s,\chi}^*$.*

Observe that the k-RLWE* problem, when $k = 0$, is a complete RLWE* problem. If $k \neq 0 \in R_q$,we give a probability polynomial-time reduction to prove that the k-RLWE* problem remains hard, even when $A^*_{s,\chi}$ is respectively replaced by $bA^*_{s,\chi}$.

Lemma 6. *For any $n \geq 1$, $q \geq 2$, and error distribution χ, there is a probability polynomial-time reduction from* RLWE* *to the* k-RLWE* *that reduces the advantage by at most* 2^{-n}.

Proof. Given a sample $(a_0, b_0) \in R^*_q \times R_q$ and a sample $(k, b_1) \in R^*_q \times R_q$ from the given RLWE* oracle, the reduction outputs a new instance $(a' = a_0, b' = b_0 + b_1) \in R^*_q \times R_q$.

If samples (a_0, b_0) and (k, b_1) are chosen from $U\left(R^*_q \times R_q\right)$, then b_0 and b_1 are uniform in R_q, and b_1 is pseudorandom by RLWE problem, the reduction outputs a uniform sample $(a' = a_0, b' = b + b_1) \in R^*_q \times R_q$, up to statistical distance 2^{-n}.

If sample (a_0, b_0) is chosen from $U\left(R^*_q \times R_q\right)$ and the distribution of (k, b_1) is $A^*_{s,\chi}$, then b_0 is uniform in R_q, and $b_1 = k \cdot s + e_1$ is pseudorandom, the reduction outputs a uniform sample $(a' = a_0, b' = b + b_1) \in R^*_q \times R_q$, up to statistical distance 2^{-n}. In addition, a sample (a_0, b_0) from $A^*_{s,\chi}$ and a sample (k, b_1) from $U\left(R^*_q \times R_q\right)$ are the same as above.

On the other hand, if given samples (a_0, b_0) and (k, b_1) from the distribution $A^*_{s,\chi}$, the equation $b' = b_0 + b_1 = a_0 \cdot s + e_0 + k \cdot s + e_1 = (a_0 + k) \cdot s + (e_0 + e_1)$. Let $e' = e_0 + e_1$, we notice that $(a', b') \in R^*_q \times R_q$ is exactly a k-RLWE* instance, the reduction outputs a sample $(a' = a_0, b' = (a + k) \cdot s + e') \in R^*_q \times R_q$ from $bA^*_{s,\chi}$, up to statistical distance 2^{-n}.

To sum up, if the RLWE* problem is infeasible, then the k-RLWE* problem is also infeasible—namely, $bA^*_{s,\chi}$ is indistinguishable from uniform, as desired. □

After that, we also give the Hermite normal form of the k-RLWE* problem, this modification makes the secret short and useful in the following symmetric-key scheme.

Lemma 7. *For modulus q, arbitrary $s \in R_q$ and the error distribution χ, there is a deterministic polynomial-time transformation T, which maps $bA^*_{s,\chi}$ to $bA^*_{\phi,\chi}$ where $\phi \leftarrow \chi$, and maps $U\left(R^*_q \times R_q\right)$ to itself.*

The proof will be showed in Appendix A.

Definition 5. (The k-RLWE* assumption-Hermite normal form). *As in the previous definition 4, for any $\ell = \mathrm{poly}(\lambda)$, the k-RLWE* assumptionholds that,*

$$\{(a_i, (a_i + 1) \cdot s + e_i)\}_{i \in [\ell]} \approx \{(a_i, u_i)\}_{i \in [\ell]}, \tag{15}$$

where sampling $s \leftarrow \chi$, other parameters remain unchanged.

4.2. Symmetric-Key Scheme with KDM Security

As in the previous section, given the security parameter λ, let $q = q(\lambda) \geq 2$, and an error distribution $\chi = \chi(\lambda)$. Let $R = \mathbb{Z}[x]/(f(x))$, $R_q = \mathbb{Z}_q[x]/(f(x))$ where $f(x) = x^n + 1$ and $n = n(\lambda)$ is a power of 2. We demonstrate a symmetric-key scheme based on the k-RLWE* problem. In order to reduce the norm of ciphertext noise, [25] uses a binary secret $s \in R_2$, which shows that the scheme is secure under this optimization, as long as the Hamming weight h is small enough and $\binom{n}{h}$ is large enough. In the final results, they construct a somewhat homomorphic encryption scheme by setting $t = 2$, $h = 63$ and $f(x) = x^n + 1$, where $m \in R_t$. Therefore, as a symmetric-key scheme, the security is not affected when the results for the RLWE setting continue to the k-RLWE* setting.

- **RSKE2.KeyGen**$\left(1^\lambda\right)$: Sample $s \leftarrow R_2$. Output $sk = s$ as the secret key.

- **RSKE2.Enc**(sk, m): To encrypt a message $m \in R_2$, sample uniformly, $e \leftarrow \chi$ and set $b = (a+1) \cdot s + 2e$. Output the ciphertext $c = (c_1 = a+1, c_2 = b+m) \in R_q \times R_q$.
- **RSKE2.Dec**(sk, c): Compute $c_2 - c_1 \cdot s$, then output $m = (c_2 - c_1 \cdot s) \bmod q \bmod 2$.

According to the encryption algorithm, $c_2 - c_1 \cdot s = m + 2e$, compared with the previous public-key encryption scheme, the ciphertext noise is small, that is $\|2e_\infty\| < q/2$, namely $q > 4\sigma\sqrt{n}$, then the ciphertext can be decrypted correctly.

The KDM-CPA security is similar to that of Section 3.3, except that there is no public key. Although the message space is reduced to R_2, there still exists a linear function $f(sk) = k \cdot s + 2w \in R_2$ to realize KDM security.

Theorem 3. *Sample $k \leftarrow R_q$ uniformly and $w \leftarrow D_{\mathbb{Z}^n,\sigma}$, where $\sigma \geq \omega(\sqrt{\log n})$. There exists a linear function $f(sk) = k \cdot s + 2w \in R_2$ that makes the RSKE2 scheme satisfy KDM-CPA security, assuming that k-RLWE* is hard.*

Proof. The proof of Theorem 2 is similar to RPK1. Therefore, this section gives a brief narrative. First, by $f(sk)$ replacing m, we generate the challenge ciphertext $c = (c_1 = a+1, c_2 = (a+1) \cdot s + 2e + k \cdot s + 2w)$, where $k \xleftarrow{U} R_q$ and $w \leftarrow D_{\mathbb{Z}^n,\sigma}$. Observe that $c_2 = (a+1+k) \cdot s + 2(e+w)$, defining $a' = a+1$ and $e' = w+e$, then we have the challenge ciphertext $c = (a', (a'+k) \cdot s + 2e',)$, which is exactly an instance of the k-RLWE* problem. It means that the challenge ciphertext c is pseudorandom, namely the adversary $\mathcal{A}$ cannot distinguish it from the ciphertext that is encrypted by the message 0. Therefore, the above RSK2 scheme is KDM-CPA under the k-RLWE* problem. □

5. Performance

In this section, we give a detailed performance comparison between our RPKE1 scheme, RSKE2 scheme and the ACPS scheme [8]. For the same security parameter λ, through the analysis of the ACPS scheme, it is easy to see the difference between the lattice problems on which these schemes are based. Firstly, our scheme has replaced LWE through RLWE, which improves its application efficiency. Secondly, about the noise distribution, in order to obtain the appropriate key-dependent ciphertexts, the ACPS scheme introduces the noise flooding technique (namely, $e \leftarrow \Psi_{\sigma'}$), which leads to the growth of the modulo q and the decline of efficiency. Due to the problem of quantum reduction of the LWE problem, the standard deviation of the additional noise distribution is $\sigma' \approx n^{-1} \cdot \sigma^{-4}$, where $\sigma = \omega(\sqrt{\log n})$, and $m = O(n \log n) \leq n \log n \approx n \cdot \sigma^2$, $p = \widetilde{O}(\sqrt{mn}) \approx n \cdot \sigma^3$, $q = p^2 \approx n^2 \cdot \sigma^6 = \text{ploy}(n) \cdot \sigma^6$. As shown in Table 1, we have the same standard deviation $\sigma = \omega(\sqrt{\log n})$, but no extra noise distribution $\Psi_{\sigma'}$ in the ciphertext generation. The $w \leftarrow D_{\mathbb{Z}^n,\sigma'}$ in the hybrid game is irrelevant, because this does not affect the efficiency of the scheme at all. In addition, we also greatly reduce the message space R_t and the modulo size $q = t \cdot \text{ploy}(n) \cdot \sigma^2$, where $t = \sigma\sqrt{n}$. Note the last line, adding the symmetry scheme; ACPS also gave a symmetric-key cryptosystem similar to it. Although different in types, as a variant of RPKE1 it also highlights its advantages.

Table 1. Parameter setting of ACPS and our schemes.

Schemes	σ	σ'	Message Space	Modulo q	Challenge $\mathcal{F}$
ACPS	$\omega(\sqrt{\log n})$	$n^{-1} \cdot \sigma^{-4}$	$\mathbb{Z}_p$, $p = n \cdot \sigma^3$	$\text{ploy}(n) \cdot \sigma^6$	affine functions
RPKE1	$\omega(\sqrt{\log n})$	/	$R_t, t = \sqrt{n} \cdot \sigma$	$\text{ploy}(n) \cdot \sigma^3$	linear functions
RSKE2	$\omega(\sqrt{\log n})$	/	$R_2, t = 2$	$\sqrt{n} \cdot \sigma$	linear functions

Finally, we estimate the concrete parameters for our scheme. Compared with ACPS, we have greatly improved its efficiency; the cost of encryption and decryption is only

polylog(n) bit operations per message symbol. By these parameters including modulus q, degree n and error distribution $\chi = D_{\mathbb{Z}^n,\sigma}$, we can obtain concrete secret key size, public key and ciphertext size. For example, the public key size of the ACPS scheme is $m \cdot n \cdot \log q \approx n^2 \cdot \log^2 n = \widetilde{O}(n^2)$, the ciphertext size is $n \cdot \log q = \widetilde{O}(n)$ and the secret key for ACPS and RPKE1 are $\sigma \cdot \sqrt{n}$ (both $s \leftarrow \chi$). Performance comparison of ACPS and our scheme are listed in Table 2. All sizes are in bits.

Table 2. Performance comparison of ACPS and our schemes.

Schemes	pk	sk	Ciphertext	Enc/Dec	KDM Security
ACPS	$\widetilde{O}(n^2)$	$\sigma \cdot \sqrt{n}$	$\widetilde{O}(n)$	$n \cdot$ polylog(n)	Yes
RPKE1	$\widetilde{O}(n)$	$\sigma \cdot \sqrt{n}$	$\widetilde{O}(n)$	polylog(n)	Yes
RSKE2	/	1	$\widetilde{O}(n)$	polylog(n)	Yes

There are many encryption schemes for KDM security, not only ACPS, but also many schemes based on traditional mathematical problems. However, in terms of computational efficiency, the lattice-based cryptosystems are still safer and more efficient. Additionally, the ciphertext operations mainly consist of encryption and decryption, but other schemes do not have compact ciphertexts. Hence, from the usability perspective, our schemes are superior to previous schemes.

6. Conclusions

In this paper, we introduce lattice-based cryptosystems with strong security properties to solve the problem that the ACPS scheme is inefficient when sampling from discrete gaussian distribution with sufficiently large standard deviation and generating extra "malformed" distributions. The public-key and symmetric-key cryptosystems provide security for key-dependent messages. Compared with the previous scheme, our scheme is compact and has a stable set of challenge functions. Both the size of public key and ciphertext are $\widetilde{O}(n)$, and the cost of encryption and decryption is only ploylog(n) bit operations per message symbol. Therefore, our scheme satisfies KDM-CPA security under the RLWE* assumption, and carries the advantages of having simple operation, parallelization and improved asymptotic efficiency.

However, there are still some problems to be explored and improved in this scheme, such as using an additional noise distribution in the hybrid game, and future work is still required to construct a fully homomorphic encryption scheme with circular security.

Author Contributions: Conceptualization: B.Y. and R.H.; methodology, B.Y.; validation, B.Y.; R.H. and J.Z.; formal analysis, J.Z.; writing—original draft preparation, B.Y.; writing—review and editing, B.Y.; funding acquisition, R.H. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Natural Science Foundation Project of China under Grant No. 62062009 and the Guangxi Innovation-driven Development Project under Grant Nos. AA17204058-17 and AA18118047-7.

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

Appendix A. Proof of Lemma 7

Proof. The transformation T to access the distribution D over $R_q^* \times R_q$, possibly $bA_{s,\chi}^*$ or $U\left(R_q^* \times R_q\right)$. Then, we prove it in two steps.

The first step. Transformation T generates the sample $\left(\overline{a}, \overline{b}\right) \in R_q^* \times R_q$ by drawing from the distribution D. When $D = bA_{s,\chi}^*$, we have $\overline{b} = (\overline{a} + k) \cdot s + \overline{x}$, where $\overline{x} \leftarrow \chi$.

The second step. To transform samples from D into samples from a different distribution. The sample $(a, b) \in R_q^* \times R_q$ from D will be transformed into $(a', b') \in R_q^* \times R_q$, where $a' = -\overline{a}^{-1} \cdot a$, $b' = b - \varphi + a' \cdot \overline{b}$, and $\varphi = (a' + k) \cdot s + e_1$, $e_1 \leftarrow \chi$.

Particularly $a' \in R_q^*$ is uniform due to $\overline{a} \leftarrow R_q^*$ is invertible modulo q and a chooses from $U\left(R_q^*\right)$. If $D = U\left(R_q^* \times R_q\right)$, then (a', b') is also subject to $U\left(R_q^* \times R_q\right)$. If $D = bA_{s,\chi}^*$, then $b = (a+k) \cdot s + e$, so we have

$$\begin{aligned} b' &= b - \varphi + a' \cdot \overline{b} = \left(a - a'\right) \cdot s + (e - e_1) + a' \cdot (\overline{a} + k) \cdot s + a' \cdot \overline{x} \\ &= \left(a - a'\right) \cdot s + (e - e_1) + \left(-a + a'\right) \cdot s + a' \cdot \overline{x} \\ &= (k-1) \cdot a' \cdot s + a' \cdot \overline{x} + (e - e_1) \end{aligned}$$

Notice that we cannot obtain a reasonable distribution $bA_{\phi,\chi}^*$, set $k = 1$; in fact, the k-RLWE* problem remains hard. Then we have

$$b' = a' \cdot \overline{x} + (e - e_1) = \left(a' + 1\right) \cdot \overline{x} + (e - e_1 - \overline{x}) = \left(a' + 1\right) \cdot \phi + e',$$

where $\phi = \overline{x}$ and $e' = e - e_1 - \overline{x}$, therefore, (a', b') is subject to $bA_{\phi,\chi}^*$, as desired. □

References

1. Goldwasser, S.; Micali, S. Probabilistic encryption. *J. Comput. Syst. Sci.* **1984**, *28*, 270–299. [CrossRef]
2. Adão, P.; Bana, G.; Herzog, J.; Scedrov, A. Soundness of Formal Encryption in the Presence of Key-Cycles. In *European Symposium on Research in Computer Security, Milan, Italy, 12–14 September 2005*; Springer: Berlin/Heidelberg, Germany, 2005.
3. Laud, P.; Corin, R. Sound Computational Interpretation of Formal Encryption with Composed Keys. In *Proceedings of the International Conference on Information Security and Cryptology, Seoul, Korea, 27–28 November 2003*; Springer: Berlin/Heidelberg, Germany, 2003.
4. Gentry, C. Fully homomorphic encryption using ideal lattices. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC'09), Bethesda, MD, USA, 31 May–2 June 2009*; ACM: New York, NY, USA, 2009; pp. 169–178.
5. Camenisch, J.; Lysyanskaya, A. An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. In *Proceedings of the International Conference on the Theory & Application of Cryptographic Techniques: Advances in Cryptology, Innsbruck, Austria, 6–10 May 2001*; Springer: Berlin/Heidelberg, Germany, 2001.
6. Black, J.; Rogaway, P.; Shrimpton, T. Encryption-Scheme Security in the Presence of Key-Dependent Messages. In *International Workshop on Selected Areas in Cryptography*; Springer: Berlin/Heidelberg, Germany, 2002; pp. 62–75.
7. Dan, B.; Alevi, S.; Hamburg, M.; Ostrovsky, R. Circular-Secure Encryption from Decision Diffie-Hellman. In Proceedings of the Advances in Cryptology—CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, 17–21 August 2008.
8. Applebaum, B.; Cash, D.; Peikert, C.; Sahai, A. Fast Cryptographic Primitives and Circular-Secure Encryption Based on Hard Learning Problems. In Proceedings of the Advances in Cryptology-Crypto, International Cryptology Conference, Santa Barbara, CA, USA, 16–20 August 2009.
9. Brakerski, Z.; Goldwasser, S. Circular and leakage resilient public-key encryption under subgroup indistinguishability (or: Quadratic residuosity strikes back). In *Proceedings of the Advances in Cryptology-crypto, Cryptology Conference, Santa Barbara, CA, USA, 15–19 August 2010*; Springer: Berlin/Heidelberg, Germany, 2010.
10. Shafi, G.; Micali, S. Probabilistic Encryption and How to Play Mental Poker Keeping Secret All Partial Information. In Proceedings of the 14th Annual ACM Symposium on Theory of Computing, San Francisco, CA, USA, 5–7 May 1982.
11. Damg, I.B.; Jurik, M. A Generalisation, A Simplification and Some Applications of Paillier's Probabilistic Public-Key System. In *Proceedings of the PKC 2001, Cheju Island, Korea, 13–15 February 2001*; Springer: Berlin/Heidelberg, Germany, 2001; pp. 119–136.
12. Barak, B.; Haitner, I.; Hofheinz, D.; Ishai, Y. Bounded Key-Dependent Message Security. In *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, France, 30 May–3 June 2010*; Springer: Berlin/Heidelberg, Germany, 2010.
13. Brakerski, Z.; Goldwasser, S.; Kalai, Y.T. Black-Box Circular-Secure Encryption Beyond Affine Functions. In *Proceedings of the TCC 2011, Providence, RI, USA, 28–30 March 2011*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 201–218.
14. Malkin, T.; Teranishi, I.; Yung, M. Efficient Circuit-Size Independent Public Key Encryption with KDM Security. In *Proceedings of the EUROCRYPT 2011, Tallinn, Estonia, 15–19 May 2011*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 507–526.
15. Alperin-Sheriff, J.; Peikert, C. Circular and KDM security for identity-based encryption. In *Proceedings of the International Workshop on Public Key Cryptography, Darmstadt, Germany, 21–23 May 2012*; Springer: Berlin/Heidelberg, Germany, 2012.
16. Chen, Y.; Zhang, J.; Deng, Y.; Chang, J. KDM Security for Identity-Based Encryption: Constructions and Separations. *Inf. Sci.* **2019**, *486*, 450–473. [CrossRef]
17. Kitagawa, F.; Matsuda, T. Circular Security Is Complete for KDM Security. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security ASIACRYPT 2020: Advances in Cryptology–ASIACRYPT, Daejeon, South Korea, 7–11 December 2020; pp. 253–285.

18. Stehle, D.; Steinfeld, R. Making NTRU as Secure Worst-case Problems over Ideal Lattice. In *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, 15–19 May 2011*; Springer: Berlin/Heidelberg, Germany, 2011; Volume 6630, pp. 27–47.
19. Micciancio, D.; Regev, O. Worst-case to average-case reductions based on gaussian measures. *SIAM J. Comput.* **2007**, *37*, 267–302. [CrossRef]
20. Goldwasser, S.; Kalai, Y.T.; Peikert, C.; Vaikuntanathan, V. *Robustness of the Learning with Errors Assumption*; Yao, A.C.-C., Ed.; Tsinghua University Press: Beijing, China, 2010; pp. 230–240.
21. Lyubashevsky, V.; Micciancio, D. *Generalized Compact Knapsacks Are Collision Resistant*; Bugliesi, M., Preneel, B., Sassone, V., Wegener, I., Eds.; Springer: Heidelberg, Germany, 2006; Volume 4052, pp. 144–155.
22. Brakerski, Z.; Gentry, C.; Vaikuntanathan, V. (Leveled)fully homomorphic encryption without bootstrapping. In Proceedings of the 3rd Conference on Innovations in Theoretical Computer Science, ITCS 2012, Association for Computing Machinery, New York, NY, USA, 8–10 January 2012; pp. 309–325.
23. Lyubashevsky, V.; Peikert, C.; Regev, O. A Toolkit for Ring-LWE Cryptography. In *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, 26–30 May 2013*; Springer: Berlin/Heidelberg, Germany, 2013.
24. Brakerski, Z.; Vaikuntanathan, V. Fully homomorphic encryption from ring-LWE and security for key dependent messages. In *Proceedings of the Advances in Cryptology—CRYPTO2011, Santa Barbara, CA, USA, 14–18 August 201*; Springer: Berlin, Germany, 2011; Volume 6841, pp. 505–524.
25. Fan, J.; Vercauteren, F. Somewhat practical fully homomorphic encryption. *IACR Cryptol. Eprint Arch.* **2012**, *2012*, 144.