

Article

Identity-Based Online/Offline Encryption Scheme from LWE

Binger Zuo ¹, Jiguo Li ^{1,2,*}, Yichen Zhang ¹ and Jian Shen ³

¹ College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350117, China; qsx20221350@student.fjnu.edu.cn (B.Z.); zyc_718@163.com (Y.Z.)

² Fujian Provincial Key Laboratory of Network Security and Cryptology, Fuzhou 350117, China

³ School of Information Science and Engineering, Zhejiang Sci-Tech University, Hangzhou 310018, China; shenjian@zstu.edu.cn

* Correspondence: lijiguo@fjnu.edu.cn

Abstract: With quantum computers, the quantum resistance of cryptographic systems has gradually attracted attention. To overcome the shortcoming of existing identity-based encryption (IBE) schemes in resisting quantum attacks, we introduce an IBE scheme based on learning with errors (LWE). In addition, devices with limited computing power are becoming increasingly common in practice, making it increasingly important to improve the efficiency of online computation of encryption algorithms. The classic solution is to directly improve the efficiency of the Gaussian sampling algorithm, thereby increasing the overall efficiency of the scheme. However, our scheme combines the efficient Gaussian sampling algorithm, G-trapdoor, with online/offline method to further improve the online encryption efficiency of the encryption algorithm. Our scheme completes partial computation before knowing the message and receiver's identity, and once the message and receiver's identity are obtained, the online part encryption can be efficiently completed. We construct an identity-based online/offline encryption (IBOOE) scheme from LWE with G-trapdoor, improve the efficiency of online encryption while achieving quantum resistant security. We prove the scheme's security under the standard model for chosen-plaintext attack (CPA). By comparing with relevant schemes in terms of experiments and analysis, our scheme has improved efficiency by 65% to 80% compared to the classical LWE IBE scheme (increasing with LWE security parameters), and by 60% to 70% compared to the recent IBE scheme from LWE. This greatly improves the efficiency of online computing for low-power encryption devices while ensuring security.



Citation: Zuo, B.; Li, J.; Zhang, Y.; Shen, J. Identity-Based Online/Offline Encryption Scheme from LWE.

Information **2024**, *15*, 539. <https://doi.org/10.3390/info15090539>

Academic Editor: Wade Trappe

Received: 10 August 2024

Revised: 28 August 2024

Accepted: 1 September 2024

Published: 4 September 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: lattice; LWE; IBE; online/offline

1. Introduction

In IBE schemes, user submits an arbitrary string corresponding to the identity to key generation center (KGC). This user's private key which is authenticated is generated by the KGC and corresponds to the identity. Encrypting messages only requires knowing the identity of the recipient. This process does not require verifying the correctness of credentials in traditional public key architectures, especially for energy limited devices. With quantum computers' computing technology, traditional encryption algorithms face the danger of being attacked by quantum computers. However, traditional IBE schemes do not have quantum resistant security.

Lattice-based cryptography system has the characteristics of simple structure and complex mathematics, and is the most prospective type of anti-quantum cryptography technology. The lattice-based IBE schemes deserve further research due to the excellent performance in practical application scenarios and scalability advantages. Gentry, Peikert, and Vaikuntanathan [1] designed an approach for lattice-based signature algorithms and proved the method's security under the random oracle model; we abbreviate their scheme to GPV scheme. Cash et al. [2] proposed the LWE IBE scheme and proved this anti-quantum IBE scheme's security under the standard model. Furthermore, Agrawal et al. [3] brought

up an anti-quantum IBE scheme based on lattice under the standard model. In line with Agrawal et al.'s [3] work, their scheme has a simpler construct and shorter ciphertext compared to Cash et al.'s [2] scheme. Agrawal et al. treated identity as a chunk, and the lattice in their scheme consists of "left" and "right" lattices. The trapdoor for the left lattice is the true trapdoor for generating secret keys, while the trapdoor for the right lattice is only used in security proof. Our scheme learns their idea of trapdoor generation and further improves based on it.

However, the current IBE algorithm based on lattice structure still has shortcomings in computational efficiency. The biggest reason is that lattice-based encryption schemes are closely related to Gaussian sampling, and thus, many efficiency improvement schemes focus on improving the efficiency of Gaussian sampling. Since the current implementations of Gaussian sampling are still achieved through extensive simulations to infinitely approximate Gaussian distributions, which still affects the overall computational efficiency. In an effort to carry the efficiency of existing lattice-based IBE schemes to a new and higher level, we apply online/offline method to delegate most of the Gaussian sampling and the parts that do not require identity and message knowledge to powerful devices for offline computation.

1.1. Our Motivation and Contributions

Although existing IBE schemes can protect the confidentiality of data without checking certificates, they cannot resist attacks from quantum computers. To address this issue, an anti-quantum IBE scheme can be achieved by constructing on LWE, the classic hard problem on lattice. However, the current LWE based IBE schemes are less efficient. Thus, we propose an IBOOE scheme based on LWE; the offline phase completes Gaussian sampling before obtaining the message to be encrypted and identity. In this way, our scheme ensures the efficiency of the scheme while achieving anti-quantum security. Our contributions are shown below.

- (1) We first investigate the coexistence of anti-quantum security and efficiency in the IBE system, and design an IBOOE scheme from the LWE problem.
- (2) We then construct our concrete IBOOE scheme from LWE and prove the CPA secure under the standard model.
- (3) Finally, we aim to test the feasibility and effectiveness of our scheme through the contrast of the original scheme [3], our scheme, and the recent anti-quantum IBE scheme [4].

1.2. Paper Organization

The rest of this article is organized as follows. We introduce the relevant work of our paper in Section 2. In Section 3, we introduce some concepts and related definitions, and describe the security model and system architecture. In Section 4, we propose the construction of our efficient IBOOE based on LWE and analyze its correctness and security. In Section 5, we compare our scheme with classical and recent LWE based IBE schemes. In Section 6, we conclude this article.

2. Related Work

The GPV scheme [1] provided the underlying scheme for the lattice-based IBE cryptographic algorithms. Regev [5] presented a typical lattice difficulty problem, the LWE problem. In the research of anti-quantum cryptography schemes, especially for IBE schemes, considering quantum circuits' aspect, the proof of GPV scheme is conducted solely under the random oracle model, but without considering the security proof under the random oracle model from quantum technology. Zhandry [6] developed a new technology for random oracle model from the quantum technology, and then demonstrated that the GPV scheme is secure under the random oracle model from the quantum technology. Katsumata et al. [7] then provided more rigid proof for GPV scheme under the random oracle model from quantum technology. While Gao et al. [8] first constructed anti-quantum

IBE scheme from LWE and a quantum circuit, they proved their quantum IBE scheme's security under the random oracle model. Moreover, considering the enlargement of anti-quantum cryptography schemes in terms of functionality, Dutta et al. [9] first brought up the specific unidirectional construction of the proxy-re-encryption-based identity from LWE; they then proved under the standard model that the scheme is secure. In addition, for the sake of strengthening the security of proxy-re-encryption-based identity, on this basis, Wu et al. [10] added a function called re-encryption verifiability, which is a proxy re-encryption IBE scheme from basic lattice. Liu et al. [11] then extended the concept of server-aided revocable IBE to hierarchical IBE. In order to withstand side channel attack, Li et al. [12–15] presented some identity-based encryption schemes with leakage resilience. Furthermore, in terms of extending LWE itself, Abla et al. [16] brought up an IBE scheme based on ring LWE, with shorter main public key and stricter security analysis. Conversely, Fan et al. [17] brought up an adaptively secure scheme under the standard model, which is a fresh anti-quantum IBE scheme for middle product LWE. In addition, Lai et al. [18] promoted two-stage sampling approach of the GPV scheme, and proposed the new lattice two-stage sampling technology, which added noise not only to the ciphertext, but also to the key.

However, most of the current IBE schemes are inefficient, and they take up a lot of storage space. In terms of storage, the main issue is each user's ID has a parameter matrix, which yields a sharp increase in the scale of the system's public parameters. Zhang et al. [4] proposed a flexible trade-off mechanism using blocking technology to balance the scale of common parameters and the computational cost involved. They divide the identity into multiple parts and associate each part with a matrix, while slightly increasing the modulus of the lattice to maintain the same level of security. In the Gaussian sampling aspect, Weiden et al. [19] displayed that the running time consumed by Gaussian sampling accounts for half of the Lyubashevsky's lattice signature scheme [20]. For the sake of improving the efficiency of Gaussian sampling, Micciancio and Peikert [21] brought up a new approach for generating a trapdoor in the lattice, which is more efficient with smaller hidden constants; this trapdoor is called **G**-trapdoor. This method of generating trapdoors is more efficient because it does not involve any expensive Hermite normal form or matrix inversion computations. Next, Micciancio and Walter [22] developed a new Gaussian sampling algorithm and the algorithm is applicable to arbitrary and variable Gaussian distributions. By implementing more efficient Gaussian sampling, lattice-based cryptographic algorithms can be more widely applied. Furthermore, Sun et al. [23] also proposed a secure and efficient exponential Bernoulli sampling algorithm to achieve universal, efficient, and synchronized Gaussian sampling of integers.

Significantly, in the sake of improving the expense of Gaussian sampling in lattice encryption algorithms, the online/offline method is also an effective way. In 2008, Guo et al. [24] first brought up the IBOOE scheme. The principal idea is to complete computing that consume a lot of resources in the offline part through powerful devices. These calculations do not require knowledge of messages and identities. Under this mindset, we propose an online/offline IBE scheme from LWE with **G**-trapdoor, complete Gaussian sampling during the offline phase. The offline part can be completed by powerful devices without the need to know identity and messages.

3. Preliminaries

We take values from the finite set Ω , and let A and B be random variables. Furthermore, the statistical distance between A and B , two ensembles of distributions indexed by s , is $\Delta(A; B) := \frac{1}{2} \sum_{s \in \Omega} |A(s) - B(s)|$. For an uniform and random variable U_{Ω} from Ω , if we have $\Delta(A; U_{\Omega}) \leq \delta$, then we have the random variable A is δ -uniform over Ω . More specifically, we let $A(\kappa)$ and $B(\kappa)$ be the two sets of random variables. Furthermore, set $d(\kappa) := \Delta(A(\kappa); B(\kappa))$, if $d(\kappa)$ is an ignorable function of κ , and in this way, we have that A and B are statistically approaching.

For vectors $S = \{s_1, \dots, s_k\} \in \mathbb{R}^{n \times k}$. L_2 norm is the shortest distance to go from one point to another, which is the sum of squared differences between points. $\|S\|$ indicates the S 's longest vector's L_2 length. $\|\tilde{S}\| := \{\tilde{s}_1, \dots, \tilde{s}_k\}$ indicates the Gram–Schmidt orthogonalization of the ordered vectors s_1, \dots, s_k as in above sequence.

We let $a_1, a_2, \dots, a_n \in \mathbb{R}^{n \times n}$ be n linearly independent vectors and $\mathbf{Y} = (a_1, a_2, \dots, a_n)$. Furthermore, the following additive discrete subgroup is called an n -dimensional lattice which is generated by \mathbf{Y} :

$$\Lambda = L(\mathbf{Y}) = \left\{ \sum_{i=1}^n x_i a_i : x_i \in \mathbb{Z} \right\}$$

For the three positive integers r, n , and q , where q is a prime number, we define $\mathbf{X} \in \mathbb{Z}_q^{r \times n}$ and $\partial \in \mathbb{Z}_q^r$, and consider two kinds of n -dimensional lattices defined by \mathbf{X} . The transposed rows of \mathbf{X} generates the first lattice and the first lattice is defined as:

$$\Lambda_q(\mathbf{X}) := \left\{ \mu \in \mathbb{Z}^n : \exists s \in \mathbb{Z}_q^r \text{ where } \mathbf{X}^\top s = \mu \pmod q \right\}.$$

Those integer vectors are ‘‘orthogonal’’ under the modulus q to the rows of \mathbf{X} . Furthermore, they constitute the second lattice. The second lattice is defined as:

$$\Lambda_q^\perp(\mathbf{X}) := \left\{ \mu \in \mathbb{Z}^n : \mathbf{X}\mu = 0 \pmod q \right\}.$$

Moreover, we let $\Lambda_q^\partial = \{ \mu \in \mathbb{Z}^n : \mathbf{X}\mu = \partial \pmod q \}$ for the arbitrary $\partial \in \mathbb{Z}^r$ be the coset.

For $c \in \mathbb{R}^n$ and $s > 0$, the Gaussian function is defined as $\rho_{s,c}(x) = \exp\left(-\pi\|(x - c)/s\|^2\right)$. Then, we let $\rho_{s,c}(\Gamma) = \sum_{x \in \Gamma} \rho_{s,c}(x)$ for any fixed countably subset $\Gamma \subseteq \mathbb{R}^n$. Next, the discrete Gaussian distribution for arbitrary $x \in \Gamma$ is defined as $D_{\Gamma,s,c}(x) = \rho_{s,c}(x) / \rho_{s,c}(\Gamma)$.

Definition 1. Let $\bar{\Psi}_\epsilon$ over \mathbb{Z}_q for an $\epsilon \in (0, 1)$ indicates the distribution of the random variable $\lfloor qA \rfloor \pmod q$ and a prime number q , $\lfloor qA \rfloor$ means $\lfloor qA + 1/2 \rfloor$, where A is a normal random variable, the mean of A is zero, and the standard deviation of A is $\epsilon / \sqrt{2\pi}$.

Definition 2. For a prime number q , a positive integer r , and the distribution $\bar{\Psi}_\epsilon$ in \mathbb{Z}_q , the $(\mathbb{Z}_q, r, \bar{\Psi}_\epsilon)$ -LWE problem is for the oracle access of samples, to differentiate between the distribution $(\partial_i, v_i) = (\partial_i, \partial_i^\top s + x_i) \in \mathbb{Z}_q^r \times \mathbb{Z}_q$ and the uniform distribution over $\mathbb{Z}_q^r \times \mathbb{Z}_q$, where $x_i \leftarrow \bar{\Psi}_\epsilon$, $\partial_i \leftarrow \mathbb{Z}_q^r$ and $s \leftarrow \mathbb{Z}_q^r$.

Theorem 1 ([5]). There is an efficient algorithm for approaching the SIVP and the GapSVP problems in the worst case, to within $\tilde{O}(r/\epsilon)$ factors in the L_2 norm, if for resolving the $(\mathbb{Z}_q, r, \bar{\Psi}_\epsilon)$ -LWE problem with $q > 2\sqrt{r}/\epsilon$ there exists an effective, probable quantum algorithm.

3.1. Framework and Security of IBOOE

Our IBOOE scheme is made up of the following five probabilistic polynomial-time (PPT) algorithms as below.

Setup: In the setup phase, it takes security parameter λ as the input, sets plaintext space and ciphertext space, then manufactures the global public parameters PP for following algorithms and the master secret key MK for the KGC.

Extract: In the process of extracting secret key, it takes public parameters PP, the master secret key MK and the id for generating the secret key SK_{id} , and SK_{id} corresponds to the identity id.

Enc^{off}: During the offline encrypting phase, it takes public parameters PP as input for generating the offline ciphertext $\bar{\zeta}$.

Enc^{on}: During the online encrypting phase, it takes public parameters PP, the message mes , the offline ciphertext $\bar{\zeta}$, and the id as inputs for generating online ciphertext ζ .

Dec: In the decrypting phase, it takes public parameters PP, the ciphertext ζ and the secret key SK_{id} of the receiver, whose identity is id as inputs for decrypting the message mes .

For the security proof of our construction, we reduce our lattice based IBE scheme to a classical difficult problem on lattices, the LWE problem.

The $(\mathbb{Z}_q, r, \overline{\Psi}_\epsilon)$ -LWE problem permits repetitive queries to the given challenge oracle \mathcal{O} . Furthermore, we say that if the following:

$$LWE - adv[\mathcal{A}] := \left| Pr[\mathcal{A}^{\mathcal{O}_\theta} = 1] - Pr[\mathcal{A}^{\mathcal{O}_\$} = 1] \right|$$

is non-ignorable for the random s from \mathbb{Z}_q^r , then the algorithm \mathcal{A} resolves the $(\mathbb{Z}_q, r, \overline{\Psi}_\epsilon)$ -LWE problem. \mathcal{O}_θ returns the real LWE sample and $\mathcal{O}_\$$ is for the random case. The $Pr[\mathcal{A}^{\mathcal{O}_\theta} = 1]$ means the probability of \mathcal{A} guessing correctly when \mathcal{A} accesses \mathcal{O}_θ . The same applies to $Pr[\mathcal{A}^{\mathcal{O}_\$} = 1]$.

Security Game. In order to ensure strong privacy in our IBOOE scheme, we describe a game that caches a character called “indistinguishable from random”. This implies that the challenge ciphertext from the ciphertext space appears to be a random element, making it difficult to decipher. For the security parameter λ , we define the scheme’s message space as \mathcal{M}_λ and the scheme’s ciphertext space as ζ_λ . How the game works is described below.

Init: In the initial phase, the adversary \mathcal{A} first outputs its target identity id^* .

Setup: In the setup phase, the challenger then runs the algorithm **Setup** and gives the adversary \mathcal{A} public parameters PP. Furthermore, the challenger keeps the master key MK to itself.

Phase 1: In the first phase, the adversary \mathcal{A} sends private key queries q_1, \dots, q_n and the query q_i is for id_i . We request that id_i cannot equal to id^* . For private key d_i corresponds to the identity id_i , and the challenger runs algorithm **Extract** to respond. Then, the challenger sends d_i to \mathcal{A} . The above queries are all adaptive.

Challenge: After adversary \mathcal{A} ’s judgement of that the first phase is completed, a plaintext $M \in \mathcal{M}_\lambda$ will be output. Furthermore, this is the plaintext that \mathcal{A} intends to be challenged. Then, for the following simulation, the challenger chooses the random bit $a \in \{0, 1\}$ corresponding to different situation, and the challenger also chooses a random ciphertext $\zeta \in \zeta_\lambda$.

- (1) For $a = 0$, challenger uses algorithm **Encrypt** for setting challenge ciphertext as $\zeta^* := \mathbf{Encrypt}(PP, id^*, M)$.
- (2) For $a = 1$, the challenger directly uses the challenge ciphertext chosen before and sets $\zeta^* := \zeta$.

The challenger then sends ζ^* as the ciphertext for challenge to adversary \mathcal{A} .

Phase 2: Then, in the second phase, the adversary \mathcal{A} adaptively sends the supplemental queries from $n + 1$ to r , and the query q_i corresponds to the id_i ’s private key extraction query, where id_i cannot be equivalent to id^* . Just like in phase 1, the challenger sends q_i to adversary \mathcal{A} .

Guess: Lastly, adversary \mathcal{A} sends the guess $a' \in \{0, 1\}$ as its output for result that the challenger chose before. \mathcal{A} wins the game when $a = a'$. For the positive of adversary for attacking an IBE scheme, we define it as:

$$Adv_{\mathcal{A}}(\lambda) = |Pr[a = a'] - 1/2|.$$

The possibility of the adversary winning depends on the random bits which are used by the challenger and the adversary \mathcal{A} .

Definition 3. If for every $INDr$ -sID-CPA PPT adversary we have $Adv_{\mathcal{A}}(\lambda)$, which is an ignorable function, then we are able to say that an IBE scheme is selective-identity, indistinguishable from random.

Lastly, we define the corresponding adaptive identity of our aforesaid concept, that is, in the attack game process, the init phase is removed so that the adversary can reveal the id^* that it wants to attack, namely its target identity, until the challenge phase. In the first phase, we permit the adversary to send random private key queries and then the adversary selects the random target identity id^* . Furthermore, the only limitation is that in the phase 1, the adversary will not send the private key query for id^* . Our security concept obtained in this way is defined in Definition 3, which is defined as IND_r-ID-CPA.

3.2. Sampling Algorithms

For $r, q \in \mathbb{Z}$, q is an odd number, $k = \lceil \log_2 q \rceil$, namely the result of rounding up $\log_2 q$. We denote the $g^\top \in \mathbb{Z}_q^{1 \times k}$ as $[1 \ 2 \ 4 \ \dots \ 2^{k-1}]$. Let $\mathbf{G} = \mathbf{I}_r \otimes g^\top \in \mathbb{Z}_q^{r \times rk}$ be a public matrix and \otimes means tensor product. The \mathbf{G} -trapdoor for the lattice $\Lambda^\perp(\mathbf{X})$ was proposed in the scheme [21].

Definition 4 ([21]). *Given a matrix $\mathbf{X} \in \mathbb{Z}_q^{r \times n}$, $\mathbf{G} \in \mathbb{Z}_q^{r \times \omega}$ with $n \geq \omega \geq r$, q is an odd number. If there pertains some invertible matrix $\mathbf{S} \in \mathbb{Z}_q^{r \times r}$, and we have $\mathbf{X} \begin{bmatrix} T_{\mathbf{X}} \\ \mathbf{I} \end{bmatrix} = \mathbf{S}\mathbf{G}$, then $T_{\mathbf{X}} \in \mathbb{Z}_q^{(n-\omega) \times \omega}$ is named a \mathbf{G} -trapdoor for \mathbf{X} . We say that the greatest singular value of $T_{\mathbf{X}}$ is denoted as $s_1(T_{\mathbf{X}})$, and the quality of this trapdoor $T_{\mathbf{X}}$ is judged by $s_1(T_{\mathbf{X}})$.*

Theorem 2 ([21]). *Let $q \geq 2, r \geq 1$ and $\mathbf{S} \in \mathbb{Z}_q^{r \times r}$ is invertible matrix. For $k = \lceil \log_2 q \rceil$ and $n > r \log q$, there is a randomized algorithm **GenTrap**($1^r, 1^n, q, \mathbf{S}$), and the algorithm's output is a parity-check matrix $\mathbf{X} \in \mathbb{Z}_q^{r \times n}$ with \mathbf{G} -trapdoor $T_{\mathbf{X}}$. The distribution of \mathbf{X} approximately follows uniform distribution.*

Moreover, for any $\partial \in \mathbb{Z}_q^r$ and sufficiently large $q > \sqrt{r \log q}$, randomized algorithm **SampleD**($T_{\mathbf{X}}, \mathbf{X}, \mathbf{S}, \partial, \rho$), which outputs sampling results from distribution $D_{\Lambda_q^\partial(\mathbf{X}), \rho}$ within $\text{negl}(r)$ statistical distance.

Lemma 1 ([3]). *Suppose that $n > (r + 1) \log_2 q + \omega(\log r)$, where $q > 2$ and q is a prime number. Let $n \times k$ matrix \mathbf{R} be an uniform matrix from $\{1, -1\}^{n \times k} \bmod q$. Let \mathbf{X} and \mathbf{Y} be two uniform matrices from $\mathbb{Z}_q^{r \times n}$ and $\mathbb{Z}_q^{r \times k}$ separately. Then, for all of the vectors w from \mathbb{Z}_q^n , the distribution $(\mathbf{X}, \mathbf{X}\mathbf{R}, \mathbf{R}^\top w)$ and the distribution $(\mathbf{X}, \mathbf{Y}, \mathbf{R}^\top w)$ is statistically approaching.*

We look back at some sampling algorithms from [3,21]. Let \mathbf{X}, \mathbf{Y} be matrices in $\mathbb{Z}_q^{r \times n}$, the matrix $\mathbf{M}_1 \in \mathbb{Z}_q^{r \times n_1}$, and $\mathbf{R} \in \{-1, 1\}^{n \times n}$. Set $F_1 := (\mathbf{X} \mid \mathbf{M}_1)$, $F_2 := (\mathbf{X} \mid \mathbf{X}\mathbf{R} + \mathbf{Y})$.

- **SampleL**($\mathbf{X}, \mathbf{M}_1, T_{\mathbf{X}}, \partial, \rho$) $\rightarrow \mu$: For matrix $\mathbf{X} \in \mathbb{Z}_q^{r \times n}$ and its \mathbf{G} -trapdoor $T_{\mathbf{X}}$, matrix $\mathbf{M}_1 \in \mathbb{Z}_q^{r \times n_1}$, vector $\partial \in \mathbb{Z}_q^r$ and parameter $\rho \geq \left\| \widetilde{T_{\mathbf{X}}} \right\| \cdot \omega(\sqrt{\log(n + n_1)})$, the algorithm outputs a vector μ distributed statistically approaching to $D_{\Lambda_q^\partial(F_1), \rho}$.
- **SampleR**($\mathbf{X}, \mathbf{Y}, \mathbf{R}, T_{\mathbf{Y}}, \partial, \rho$) $\rightarrow \mu$: For matrix $\mathbf{Y} \in \mathbb{Z}_q^{r \times n}$ and its \mathbf{G} -trapdoor $T_{\mathbf{Y}}$, matrix $\mathbf{X} \in \mathbb{Z}_q^{r \times n}$, uniformly random matrix \mathbf{R} from $\{-1, 1\}^{n \times n}$, vector $\partial \in \mathbb{Z}_q^r$, and parameter $\rho \geq \left\| \widetilde{T_{\mathbf{Y}}} \right\| \cdot \sqrt{n} \cdot \omega(\sqrt{\log n})$, the algorithm outputs a vector μ distributed statistically close to $D_{\Lambda_q^\partial(F_2), \rho}$.

3.3. Encoding Identities as Matrices

The encoding function $\mathbf{N}: \mathbb{Z}_q^r \rightarrow \mathbb{Z}_q^{r \times r}$ is used to map identities in \mathbb{Z}_q^r to matrices in $\mathbb{Z}_q^{r \times r}$. \mathbf{N} is an explicit full-rank differences (FRD) construction, which means for all different id_1 and id_2 from \mathbb{Z}_q^r , the matrix $[\mathbf{N}(id_1) - \mathbf{N}(id_2)] \in \mathbb{Z}_q^{r \times r}$ is full-rank. Furthermore, the method is to build an additive subgroup \mathbb{G} from $\mathbb{Z}_q^{r \times r}$ of size q^r . All of the non-zero matrices from \mathbb{G} are full-rank. In this way, for all different $\mathbf{X}, \mathbf{Y} \in \mathbb{G}$, the difference between them is also in \mathbb{G} , as a consequence, $\mathbf{X} - \mathbf{Y}$ is full-rank.

Although we are primarily interested in the finite field \mathbb{Z}_q , we represent the structure of a random field \mathbb{P} . In cases where polynomial $f \in \mathbb{P}[x]$ of degree less than r , we define the r -vector of coefficients of f as $\text{ces}(f) \in \mathbb{P}^r$ and express it as a row vector. However, in cases where f is of degree less than $r - 1$, we add zeroes to the right of the coefficients vector, so it becomes r -vector. The case in point is, for $r = 8$ we have $\text{ces}(x^5 + 7x^2 + 1) = (1, 0, 7, 0, 0, 1, 0, 0) \in \mathbb{P}^8$. We let p of degree r be some irreducible polynomial from $\mathbb{P}[x]$. Think back that the polynomial f from $\mathbb{P}[x] \bmod p$ has degree less than r , consequently, the $\text{ces}(f \bmod p)$ is a vector from \mathbb{P}^r .

Yet, for an input $h = (h_0, \dots, h_{r-1}) \in \mathbb{P}^r$, the polynomial $f_h(x) = \sum_{i=0}^{r-1} h_i x^i \in \mathbb{P}[x]$. We define $\mathbf{N}(h)$ as:

$$\mathbf{N}(h) := \begin{pmatrix} \text{ces}(f_h) \\ \text{ces}(x \cdot f_h \bmod p) \\ \text{ces}(x^2 \cdot f_h \bmod p) \\ \vdots \\ \text{ces}(x^{r-1} \cdot f_h \bmod p) \end{pmatrix} \in \mathbb{P}^{r \times r}.$$

Because for all of the prime numbers q and the integer $r > 1$, there are irreducible polynomials of degree r from $\mathbb{Z}_q[x]$, and the structure can cater for any pair of q and r .

Theorem 3 ([25]). *Let \mathbb{P} be a field and the p is a polynomial from $\mathbb{P}[x]$. The function \mathbf{N} is an encoding with FRD, if the p is irreducible from $\mathbb{P}[x]$.*

Let $r = 4$, and $p(x) = x^4 + x - 1$. The function $\mathbf{N}(h)$, where $h = (h_0, h_1, h_2, h_3)$, works as below.

$$\mathbf{N}(h) = \mathbf{N}(h_0, h_1, h_2, h_3) := \begin{pmatrix} h_0 & h_1 & h_2 & h_3 \\ h_3 & h_0 - h_3 & h_1 & h_2 \\ h_2 & h_3 - h_2 & h_0 - h_3 & h_1 \\ h_1 & h_2 - h_1 & h_3 - h_2 & h_0 - h_3 \end{pmatrix}.$$

Theorem 3 proves that for all prime numbers q , the function \mathbf{N} is FRD, where $x^4 + x - 1$ is irreducible from $\mathbb{Z}_q[x]$.

4. New Lattice-Identity-Based Online/Offline Encryption

The construction of our lattice based IBOOE scheme is on the basis of the following idea. In the offline phase, we generate offline ciphertext with high computational complexity and no need to know identity and messages. During the online phase, we generate online ciphertext by using identity, messages, and offline ciphertext.

4.1. Construction

As shown in Figure 1, in our IBOOE scheme, KGC generates public parameters and master secret key. With the master secret key, KGC generates the private key for the Data User. For performing the offline encryption operation, the Offline Server completes Gaussian sampling and sends offline ciphertext to the Data Owner. Using the offline ciphertext, the Data Owner completes online encryption with the Data User's id and the message mes . The Data User decrypts ciphertext for the final message mes . The concrete algorithms are as below.

Setup: KGC takes r to be the security parameter, sets $n = 2r^{1+\delta}$, $q = n^{2.5} \cdot \omega(\sqrt{\log r})$, $\rho = n \cdot \omega(\sqrt{\log r})$, $\epsilon = [n^2 \cdot \omega(\sqrt{\log r})]^{-1}$. Then, it rounds up n to next larger integer and rounds up q to next larger prime number. Among above formulas, δ is for $r^\delta = O(\log r)$. By using algorithm **GenTrap**, it selects a uniform and random $r \times n$ -matrix $\mathbf{X}_0 \in \mathbb{Z}_q^{r \times n}$ with the **G**-trapdoor $T_{\mathbf{X}_0}$ as defined in Definition 4. It then selects two uniform and random

$r \times n$ matrices \mathbf{X}_1, \mathbf{Y} in $\mathbb{Z}_q^{r \times n}$. It selects a uniform and random r -vector ∂ in \mathbb{Z}_q^r . Lastly, KGC outputs public parameters PP and the master key MK:

$$PP = (\mathbf{X}_0, \mathbf{X}_1, \mathbf{Y}, \partial); MK = T_{\mathbf{X}_0}.$$

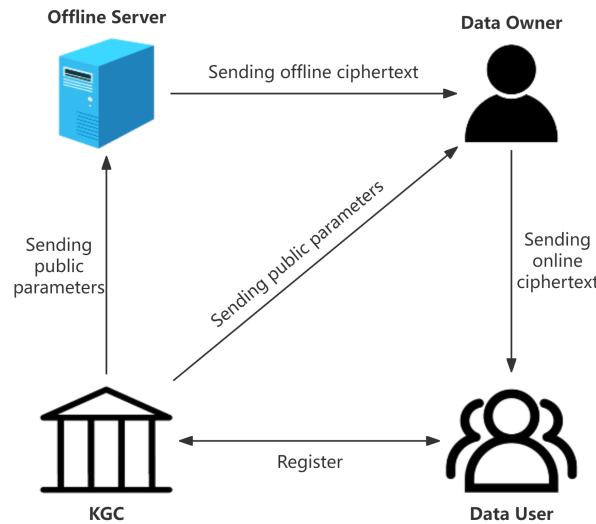


Figure 1. Our IBOOE scheme’s architecture.

Extract: KGC takes public parameters PP, the master key MK, and an identity $id \in \mathbb{Z}_q^r$ as inputs, then KGC samples $\mu \in \mathbb{Z}^{2n}$ as:

$$\mu \leftarrow \text{SampleL}(\mathbf{X}_0, \mathbf{X}_1 + \mathbf{N}(id)\mathbf{Y}, T_{\mathbf{X}_0}, \partial, \rho).$$

In the above formula, \mathbf{N} is the FRD map as described in Section 3.3 and μ is distributed as $D_{\Lambda_q^\partial(F_{id}), \rho}$. Let $F_{id} := (\mathbf{X}_0 \mid \mathbf{X}_1 + \mathbf{N}(id)\mathbf{Y})$, which means $F_{id} \cdot \mu = \partial$. For the chosen id , KGC outputs the following secret key:

$$SK_{id} := \mu.$$

Enc^{off}: The Offline Server takes public parameters PP as input and completes Gaussian sampling, which does not need the identity and the message that needs to be encrypted in following online algorithm. It also chooses the uniform and random vector $s \xleftarrow{R} \mathbb{Z}_q^r$ and the uniform and random matrix \mathbf{R} from $\{-1, 1\}^{n \times n}$. It also chooses $x \xleftarrow{\Psi} \mathbb{Z}_q$ and $y \xleftarrow{\Psi^n} \mathbb{Z}_q^n$ for noise vectors, which both follow the distribution of Definition 1, and set $z \leftarrow \mathbf{R}^T y \in \mathbb{Z}_q^n$. Offline Server computes $\bar{\zeta}_0 = \partial^T s + x \in \mathbb{Z}_q$ and $\bar{\zeta}_1 = \begin{bmatrix} y \\ z \end{bmatrix}$ and stores the offline ciphertext for the online phase:

$$\bar{\zeta} := (\bar{\zeta}_0, \bar{\zeta}_1, s)$$

Enc^{on}: The Data Owner takes PP, identity id , and a message $mes \in \{0, 1\}$ as inputs. Then, it sets F_{id} as $(\mathbf{X}_0 \mid \mathbf{X}_1 + \mathbf{N}(id)\mathbf{Y})$. It also sets $\zeta_0 = \bar{\zeta}_0 + mes \lfloor \frac{q}{2} \rfloor \in \mathbb{Z}_q$ and $\zeta_1 = F_{id}^T s + \begin{bmatrix} y \\ z \end{bmatrix} \in \mathbb{Z}_q^{2n}$. The Data Owner outputs the online ciphertext:

$$\zeta := (\zeta_0, \zeta_1).$$

Dec: The Data User takes public parameters PP, the private key SK_{id} , and the online ciphertext ζ as inputs, it then computes $\omega \leftarrow \zeta_0 - SK_{id}^T \zeta_1$ in \mathbb{Z}_q . It compares ω and $\lfloor \frac{q}{2} \rfloor$, the downward rounding of $\frac{q}{2}$, treat them as integers from \mathbb{Z} . If the two integers are approaching, namely, if $|\omega - \lfloor \frac{q}{2} \rfloor| < \lfloor \frac{q}{4} \rfloor$ from \mathbb{Z} , output 1, otherwise output 0.

In the above encryption, the matrix \mathbf{R} has significant importance in security proof. The matrix is a tool for a specific distribution required by the simulation, which is used to sample noise vectors (y, z) .

4.2. Parameters and Correctness

We define our scheme’s correctness below.

Correctness. If $(\text{PP}, \text{MK}) \leftarrow \text{Setup}(\lambda)$, the **Extract** algorithm runs as $\text{SK}_{\text{id}} \leftarrow \text{Extract}(\text{PP}, \text{MK}, \text{id})$ and ciphertexts generated as $\tilde{\zeta} \leftarrow \text{Enc}^{\text{off}}(\text{PP})$, $\zeta \leftarrow \text{Enc}^{\text{on}}(\text{PP}, \text{id}, \text{mes}, \tilde{\zeta})$, then **Dec** $(\text{PP}, \text{SK}_{\text{id}}, \zeta)$ outputs “mes” with an overwhelming probability.

Proof. When our scheme is operated as specified, during decryption, we have:

$$\omega = \zeta_0 - \text{SK}_{\text{id}}^\top \tilde{\zeta}_1 = \text{mes} \left\lfloor \frac{q}{2} \right\rfloor + x - \text{SK}_{\text{id}}^\top \begin{bmatrix} y \\ z \end{bmatrix}.$$

For recovering *mes* correctly, we can compute the error term as $x - \text{SK}_{\text{id}}^\top \begin{bmatrix} y \\ z \end{bmatrix}$, and it needs to be less than $q/5$. Since $x \in \overline{\Psi}_\epsilon$ and $y \in \overline{\Psi}_\epsilon^n$, we have $|x| < q\epsilon\omega(\sqrt{\log n}) + 1/2$ and $|y| < q\epsilon\omega(\sqrt{\log n}) + \sqrt{n}/2$. For $\|\text{SK}_{\text{id}}\|$ is sampled by **SampleL**, we have $\|\text{SK}_{\text{id}}\| \leq q\sqrt{2n}$. Let $\text{SK}_{\text{id}} = (\mu_1, \mu_2)$, with the error term as follows:

$$x - \text{SK}_{\text{id}}^\top \begin{bmatrix} y \\ z \end{bmatrix} = x - \mu_1^\top y - \mu_2^\top z = x - (\mu_1 - \mathbf{R}\mu_2)^\top y.$$

For a random matrix \mathbf{R} chosen from $\{-1, 1\}^{n \times n}$, we have $\|\mathbf{R}\| \leq O(\sqrt{n})$. Since $\|\mu_1 - \mathbf{R}\mu_2\| \leq \|\mu_1\| + \|\mathbf{R}\mu_2\| \leq O(qn)$ ([3]), the error term $\left| x - \text{SK}_{\text{id}}^\top \begin{bmatrix} y \\ z \end{bmatrix} \right|$ is then limited by:

$$|x| + \left| (\mu_1 - \mathbf{R}\mu_2)^\top y \right| \leq q\epsilon\omega(\sqrt{\log n}) + O(qn^{3/2}).$$

In order for the system to function properly, we must make sure that the error term described as above in **Dec** is lower than $q/5$. **GenTrap** needs $n > r \log q$ and $q > \sqrt{r \log q}$ to operate correctly. **SampleR** and **SampleL** need q to be large enough, $q > n\omega(\sqrt{\log n})$. Furthermore, our security proof needs $q > 2\sqrt{r}/\epsilon$.

For the sake of meeting the requirements of accuracy and safety, we set the parameters as follows, using r as security parameter:

$$n = 2r^{1+\delta}, \quad q = n^{2.5} \cdot \omega(\sqrt{\log r})$$

$$q = n \cdot \omega(\sqrt{\log r}), \quad \epsilon = \left[n^2 \cdot \omega(\sqrt{\log r}) \right]^{-1}$$

which round up n to the next greater integer, and round up q to the next greater prime number. Furthermore, δ is for $r^\delta > \lceil \log q \rceil = O(\log r)$. \square

4.3. Security Proof

We demonstrate that our IBOOE scheme is indistinguishable from randomness under the selective identity attack in Definition 3. Being indistinguishable from randomness implies that, in the ciphertext space, the challenge ciphertext cannot be distinguished from randomly selected elements in the ciphertext space.

Theorem 4. *If the $(\mathbb{Z}_q, r, \overline{\Psi}_\epsilon)$ -LWE assumption holds true, the IBOOE scheme is secure for INDr-sID-CPA.*

Proof. Our security proof follows a series of games, where the first one of these games is identical as INDr-sID-CPA game, which is described in Definition 3. Furthermore, the

adversary \mathcal{A} has no positive in the final game. Because when the adversary gets the ciphertext in the last game, it is always a randomly selected element from ciphertext space. We demonstrate that the upside of the PPT adversary winning the rudimentary INDr-sID-CPA game is ignorable by demonstrating that the adversary cannot distinguish the series of games presented below. The proof of indistinguishability between the Game 2 and the Game 3 is reduced to the LWE difficulty problem. \square

Game 0: The Game 0 is between the adversary \mathcal{A} for our scheme and the INDr-sID-CPA challenger, it is just as described in Definition 3, namely the original game.

Game 1:

Init: In the initial phase, the adversary \mathcal{A} first outputs its target identity id^* .

Setup: In the setup phase, the challenger then runs algorithm **Setup** and chooses \mathbf{R}^* to construct \mathbf{X}_1 as:

$$\mathbf{X}_0\mathbf{R}^* - \mathbf{N}(\text{id}^*)\mathbf{Y} \tag{1}$$

The challenger provides the system public parameters PP to the adversary \mathcal{A} and keeps the master key MK secrete from \mathcal{A} .

Phase 1: In the first phase, the adversary \mathcal{A} sends the private key queries q_1, \dots, q_n to the challenger and the query q_i is for id_i . We request that id_i cannot equal to id^* . For private key d_i which corresponds to the identity id_i , the challenger runs algorithm **Extract** to respond. The challenger sends d_i to \mathcal{A} . The above queries are all adaptive.

Challenge: After the adversary’s judgment of the first phase is completed, a plaintext $M \in \mathcal{M}_\lambda$ will be output. Furthermore, this is the plaintext that \mathcal{A} intends to be challenged. Then, for the following simulation, the challenger selects a random bit $a \in \{0, 1\}$ corresponding to a different situation, and it also picks a random ciphertext $\zeta \in \zeta_\lambda$.

- (1) For $a = 0$, the challenger uses algorithm **Encrypt** for setting the challenge ciphertext as $\zeta^* := \text{Encrypt}(\text{PP}, \text{id}^*, M)$.
- (2) For $a = 1$, the challenger directly uses the ciphertext chosen before and sets $\zeta^* := \zeta$.

The challenger then sends ζ^* as the ciphertext for challenge to adversary \mathcal{A} .

Phase 2: Then, in the second phase, the adversary \mathcal{A} adaptively sends supplemental queries from $n + 1$ to r , and the query q_i corresponds to the id'_i s private key extraction query, where id_i cannot be equivalent to id^* . Just like in phase 1, the challenger sends q_i to adversary \mathcal{A} .

Guess: Lastly, the adversary \mathcal{A} sends the guess $a' \in \{0, 1\}$ as its output for result that the challenger chose before. \mathcal{A} wins the game when $a = a'$. For the positive of adversary for attacking an IBE scheme, we define it as:

$$\text{Adv}_{\mathcal{A}}(\lambda) = |\text{Pr}[a = a'] - 1/2|.$$

Game 2:

Init: In the initial phase, the adversary \mathcal{A} first outputs its target identity id^* .

Setup: In the setup phase, the challenger then runs algorithm **Setup**, generates \mathbf{X}_0 as a random matrix and generates \mathbf{Y} using **GenTrap** with G-trapdoor $T_{\mathbf{Y}}$, and constructs $\mathbf{X}_1 \leftarrow \mathbf{X}_0\mathbf{R}^* - \mathbf{N}(\text{id}^*)\mathbf{Y}$. The challenger provides the system public parameters PP to the adversary \mathcal{A} and keeps the master key MK secrete from \mathcal{A} .

Phase 1: In the first phase, the adversary \mathcal{A} sends the private key queries q_1, \dots, q_n to the challenger and the query q_i is for id_i . We request that id_i cannot equal to id^* . For the private key d_i , which corresponds to the identity id_i , the challenger runs **Extract** to respond. During **Extract**, the challenger uses **SampleR**($\mathbf{X}_0, (\mathbf{N}(\text{id}) - \mathbf{N}(\text{id}^*))\mathbf{Y}, \mathbf{R}^*, \partial, \varrho$) to get $\mu \in D_{\Lambda_q^{\partial}(E_{\text{id}}), \varrho}$ where:

$$E_{\text{id}} := (\mathbf{X}_0 \mid \mathbf{X}_0\mathbf{R}^* + (\mathbf{N}(\text{id}) - \mathbf{N}(\text{id}^*))\mathbf{Y}) \tag{2}$$

The challenger then sends d_i to \mathcal{A} . The above queries are all adaptive.

Challenge: After the adversary’s judgement of the first phase is completed, a plaintext $M \in \mathcal{M}_\lambda$ will be output. Furthermore, this is the plaintext that \mathcal{A} wants to be challenged. Then, for the following simulation, the challenger selects a random bit $a \in \{0, 1\}$ corresponding to different situation, and it also picks a random ciphertext $\zeta \in \zeta_\lambda$.

- (1) For $a = 0$, the challenger uses algorithm **Encrypt** for setting challenge ciphertext as $\zeta^* := \text{Encrypt}(\text{PP}, \text{id}^*, M)$.
- (2) For $a = 1$, the challenger directly uses the ciphertext chosen before and sets $\zeta^* := \zeta$.

The challenger then sends ζ^* to adversary \mathcal{A} .

Phase 2: Then, in the second phase, the adversary \mathcal{A} adaptively sends the supplemental queries from $n + 1$ to r , and the query q_i corresponds to the id'_i s private key extraction query, where id'_i cannot be equivalent to id^* . Just like in phase 1, challenger sends q_i to adversary \mathcal{A} .

Guess: Lastly, the adversary \mathcal{A} sends the guess $a' \in \{0, 1\}$ as its output for result that the challenger chose before. \mathcal{A} wins the game when $a = a'$. For the positive of adversary for attacking the IBE scheme, we define it as $\text{Adv}_{\mathcal{A}}(\lambda) = |\text{Pr}[a = a'] - 1/2|$.

Game 3:

Init: In the initial phase, the adversary \mathcal{A} first outputs its target identity id^* .

Setup: The challenger then runs algorithm **Setup**, generates \mathbf{X}_0 as a random matrix and generates the matrix \mathbf{Y} using **GenTrap** with **G**-trapdoor $T_{\mathbf{Y}}$, and constructs $\mathbf{X}_1 \leftarrow \mathbf{X}_0 \mathbf{R}^* - \mathbf{N}(\text{id}^*) \mathbf{Y}$. The challenger provides the system public parameters PP to the adversary \mathcal{A} and keeps the master key MK secret from \mathcal{A} .

Phase 1: In the first phase, the adversary \mathcal{A} sends the private key queries q_1, \dots, q_n to the challenger and the query q_i is for id_i . We request that id_i cannot equal to id^* . The private key d_i corresponds to the identity id_i , and the challenger runs **Extract** to respond. During **Extract**, the challenger uses **SampleR** to get $\mu \in D_{\Lambda_{q_i}^*(F_{\text{id}}), q}$ where F_{id} is as in Formula (2). The challenger sends d_i to \mathcal{A} . The above queries are all adaptive.

Challenge: After the adversary’s judgement of the first phase is completed, a plaintext $M \in \mathcal{M}_\lambda$ will be output. Furthermore, this is the plaintext that \mathcal{A} wants to be challenged. Then, for the following simulation, the challenger selects a random bit $a \in \{0, 1\}$ corresponding to different situation, and it also picks a random ciphertext $\zeta \in \zeta_\lambda$, but always sets the challenge ciphertext as $\zeta^* := \zeta$.

The challenger then sends ζ^* to adversary \mathcal{A} .

Phase 2: In the second phase, the adversary \mathcal{A} adaptively sends the supplemental queries from $n + 1$ to r , and the query q_i corresponds to the id'_i s private key extraction query, where id'_i cannot be equivalent to id^* . Just like in phase 1, the challenger responds q_i to adversary \mathcal{A} .

Guess: Lastly, the adversary \mathcal{A} sends the guess $a' \in \{0, 1\}$ as its output for the result that challenger chose before. \mathcal{A} wins the game when $a = a'$. For the positive of adversary for attacking an IBE scheme, we define it as $\text{Adv}_{\mathcal{A}}(\lambda) = |\text{Pr}[a = a'] - 1/2|$.

Theorem 5. *Game 0 and Game 1 are statistically indistinguishable.*

Proof. The challenger uses random matrices $\mathbf{X}_0, \mathbf{X}_1, \mathbf{Y}$ to generate public parameters PP and the trapdoor $T_{\mathbf{X}_0}$ in Game 0. The challenger generates challenge ciphertext ζ^* during the challenge phase. We use \mathbf{R}^* from $\{-1, 1\}^{n \times n}$ to represent a random matrix, which is used to generate ζ^* .

The challenger chooses \mathbf{R}^* and constructs \mathbf{X}_1 as in Formula (1) in Game 1. Furthermore, identity id^* is the identity which will be attacked by \mathcal{A} . This means we change a little in how the challenger generates the matrix \mathbf{X}_1 in public parameters.

Lemma 1 shows that Game 0 is statistically indistinguishable from Game 1. We use matrix \mathbf{R}^* for constructing \mathbf{X}_1 and challenge ciphertext in Game 1. We are able to know that the distribution $(\mathbf{X}_0, \mathbf{X}_0 \mathbf{R}^*, z)$ is statistically approaching to $(\mathbf{X}_0, \mathbf{X}'_1, z)$ by Lemma 1. The \mathbf{X}'_1

is a uniform matrix from $\mathbb{Z}_q^{r \times n}$. In this way, matrix $\mathbf{X}_0 \mathbf{R}^*$ is statistically approaching to the uniform one in \mathcal{A} 's view. Therefore, the \mathbf{X}_1 as defined in Formula (1) is also approaching to the uniform one. As a result, \mathbf{X}_1 are indistinguishable in the Game 0 and the Game 1. \square

Theorem 6. *Game 1 and Game 2 are statistically indistinguishable.*

Proof. We construct matrix \mathbf{X}_0 as a random matrix in Game 2, and for \mathbf{Y} , we generate it by running algorithm GenTrap with \mathbf{G} -trapdoor $T_{\mathbf{Y}}$. Construct \mathbf{X}_1 as in Game 1. For private key queries, the challenger uses matrix \mathbf{R} to respond. Furthermore, for $\text{id} \neq \text{id}^*$, for the sake of answering the private key queries, the challenger uses the short vector μ from $\Lambda_q^\partial(F_{\text{id}})$ and sets F_{id} as in Formula (2). According to the structure, the difference between $\mathbf{N}(\text{id})$ and $\mathbf{N}(\text{id}^*)$ is non-singular, namely $[\mathbf{N}(\text{id}) - \mathbf{N}(\text{id}^*)]$. Now, for private key query, challenger runs algorithm SampleR to respond. As in Game 1, algorithm SampleR outputs the vector μ from \mathbb{Z}^{2n} , which is sampled from distribution statistically approaching to $D_{\Lambda_q^\partial(F_{\text{id}}), q}$.

In other aspects, Game 2 is as same as Game 1. Because the response to the private key queries is statistically very approaching to the response in the Game 1, \mathcal{A} 's positive over the Game 1 and Game 2 has an almost ignorable difference. \square

Theorem 7. *Game 2 and Game 3 are statistically indistinguishable.*

Proof. Game 3 is just like Game 2, although it differs in that the challenge ciphertext (ζ_0^*, ζ_1^*) is always picked as an independent and random element from $\mathbb{Z}_q \times \mathbb{Z}_q^{2n}$. Since the challenge ciphertext in the ciphertext space is always a novel random element and adversary \mathcal{A} has no positive in Game 3, then for a PPT adversary, the second and third games are computationally indistinguishable, and we do this by reducing it to the LWE problem.

Assuming \mathcal{A} has significant superiority in differentiating between the Game 2 and the Game 3. Then, we apply the adversary \mathcal{A} for an LWE algorithm \mathcal{L} .

As described in Definition 2, an LWE problem instance is to differentiate between truly random sample and noisy pseudo-random for some secret s in \mathbb{Z}_q^r . In our security game, we set \mathcal{O}_s as the truly random sample and the \mathcal{O}_θ as the LWE sample. \mathcal{L} makes a distinction between the two with the adversary \mathcal{A} , and operates as below:

Instance. Simulator \mathcal{L} approaches from \mathcal{O} and for each $i = 0, \dots, n$, simulator \mathcal{L} achieves a fresh pair $(\partial_i, v_i) \in \mathbb{Z}_q^r \times \mathbb{Z}_q$.

Targeting. The adversary declares to \mathcal{L} that the object it wants to attack is id^* .

Setup. Simulator \mathcal{L} generates the system's public parameters PP as below:

- (a) From n of the given LWE samples, it makes the random matrix $\mathbf{X}_0 \in \mathbb{Z}_q^{r \times n}$ and for all $i = 1, \dots, n$ the i -th column of \mathbf{X}_0 is the r -vector ∂_i .
- (b) Specify the zeroth LWE sample as a publicly available random r -vector $\partial_0 \in \mathbb{Z}_q^r$. The zeroth LWE sample has not been used yet.
- (c) Use id^* and \mathbf{R}^* to create the remaining of public parameters as in Game 2.
- (d) Lastly, it sends public parameters $\text{PP} = (\mathbf{X}_0, \mathbf{X}_1, \mathbf{Y}, \partial_0)$ to the adversary.

Queries. For each of the private key extraction query, simulator \mathcal{L} answers just as in Game 2.

Challenge. With the target id^* , when adversary prompts the message bit $\text{mes}^* \in \{0, 1\}$ and the challenge ciphertext, \mathcal{L} responds as below:

- (a) Set v_0, \dots, v_n as the entries from the LWE instance and set $v^* = \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}$ from \mathbb{Z}_q^n .
- (b) Letting $\zeta_0^* = v_0 + \text{mes}^* \lfloor \frac{q}{2} \rfloor \in \mathbb{Z}_q$ for masking message bit.
- (c) Set $\zeta_1^* = \begin{bmatrix} v^* \\ (\mathbf{R}^*)v^* \end{bmatrix} \in \mathbb{Z}_q^{2n}$.
- (d) Send $\zeta^* = (\zeta_0^*, \zeta_1^*)$ to the adversary.

If the LWE oracle is pseudo-random, namely $\mathcal{O} = \mathcal{O}_\theta$, ζ^* will be distributed as in Game 2. Firstly, inspect that the $F_{id^*} = (\mathbf{X}_0 \mid \mathbf{X}_0 \mathbf{R}^*)$. Secondly, by the definition of \mathcal{O}_θ we are able to know that for some random noise vector $y \in \mathbb{Z}_q^n$, which is distributed as $\overline{\Psi}_\epsilon^n$, $v^* = \mathbf{X}_0^\top s + y$. Thus, ζ_1^* defined as above in the step (c) satisfies:

$$\zeta_1^* = \begin{bmatrix} \mathbf{X}_0^\top s + y \\ (\mathbf{R}^*)^\top \mathbf{X}_0^\top s + (\mathbf{R}^*)^\top y \end{bmatrix} = (F_{id^*})^\top s + \begin{bmatrix} y \\ (\mathbf{R}^*)^\top y \end{bmatrix}$$

and the ζ_1 part in Game 2 is the quantity on the right, namely the efficacious challenge ciphertext. We also notice that $v_0 = \partial_0^\top s + x$, and the x 's distribution is as the $\overline{\Psi}_\epsilon$. In this way, ζ_0^* in step (b) satisfies $\zeta_0^* = \partial_0^\top s + x + mes^* \lfloor \frac{q}{2} \rfloor$, just like the ζ_0 part of the challenge ciphertext described in the Game 2.

In the case that $\mathcal{O} = \mathcal{O}_\$,$ we have v_0 is uniform from \mathbb{Z}_q and v^* is uniform from \mathbb{Z}_q^n . According to the standard left-over-hash-lemma, which describes the hash function defined by the matrix $(\mathbf{X}_0^\top \mid v^*)$. It makes sure that the two quantities $\mathbf{X}_0 \mathbf{R}^*$ and $(\mathbf{R}^*)^\top v^*$ are uniformly independent. Thus, ζ_1^* , which is defined as in step (c) is uniformly independent in \mathbb{Z}_q^{2n} . As a result, the challenge ciphertext in $\mathbb{Z}_q \times \mathbb{Z}_q^{2n}$ is always uniform just as in Game 3. □

Guess. After allowing supplemental queries, \mathcal{A} speculates that this is a challenger of Game 2 or Game 3. The simulator \mathcal{L} finally outputs the guess of \mathcal{A} as a solution to the LWE problem for which it is attempting to resolve.

We have mentioned before that in the case of $\mathcal{O} = \mathcal{O}_\theta$, the adversary \mathcal{A} 's opinion is just like in the Game 2. Furthermore, in the case of $\mathcal{O} = \mathcal{O}_\$,$ the adversary \mathcal{A} 's opinion is just like in the Game 3. Consequently, the positive of smulator \mathcal{L} in resolving LWE is equal to the positive of \mathcal{A} in differentiating between the Game 2 and the Game 3. At this point, we have fully introduce the algorithm \mathcal{L} and provide corresponding proof.

5. Comparison and Analysis

We compare our scheme with existing schemes [3,4] in terms of storage and computing. In Table 1, the performance of the schemes are analyzed from the aspects of PP size, SK size, online ciphertext size, offline ciphertext size, and security. We compare the computation efficiency of schemes in Table 2, from online computation, offline computation, and dimension. In addition, we also demonstrate through experimental simulations that our scheme is more efficient than existing schemes [3,4].

Table 1. Comparison of storage space.

| | Scheme [3] | Scheme [4] | Our Scheme |
|-------------------------|-------------------|--------------------|-----------------------|
| PP Size | $2nr \log q$ | $2nr \log q$ | $2nr \log q$ |
| SK Size | $2n \log q$ | $2nr \log q$ | $2n \log q$ |
| Online Ciphertext Size | $(2n + 1) \log q$ | $(2n + 1)r \log q$ | $(2n + 1) \log q$ |
| Offline Ciphertext Size | - | - | $(2n + r + 1) \log q$ |
| Security | CPA | CPA | CPA |

Table 2. Comparison of computation efficiency.

| | Online Computation | Offline Computation | Dimension |
|------------|--------------------|---------------------|-------------|
| Scheme [3] | $r^2 + 4nr$ | - | $6r \log q$ |
| Scheme [4] | $r^2 + 3nr$ | - | $2r \log q$ |
| Our scheme | $2nr$ | $r^2 + 2nr$ | $2r \log q$ |

5.1. Theoretical Comparison

The schemes in Tables 1 and 2 are secure against CPA under the standard model, where n is the dimension of the lattice, r is the security parameter, and q is the modulus. Furthermore, the limiting relationship between them is $n > r \log q$. Table 1 shows the storage cost and security among Agrawal et al.'s anti-quantum IBE scheme [3], our online/offline anti-quantum IBE scheme, and Zhang et al.'s anti-quantum IBE scheme [4]. Our scheme uses the more efficient trapdoor generation method **G**-trapdoor to generate trapdoors in scheme. Moreover, the scheme [4] is a lattice based IBE scheme proposed by Zhang et al. in 2020, which is an efficient IBE scheme with short parameters over lattice. With the same security level, our scheme has a smaller SK size than scheme [4], and also has a smaller online ciphertext size. This is friendly to low-power encryption devices.

We also compare the efficiency of different schemes in Table 2 in terms of the computational cost of online ciphertext, the computational cost of offline ciphertext, and the dimension of lattice. It is easy to see through a comparison that our scheme has the highest efficiency in online ciphertext calculation compared to the scheme [3,4]. In addition, our scheme not only supports expansion into adaptive security scheme, but also into multi-bit encryption and HIBE, and has been proven to be secure in the standard model.

5.2. Experimental Simulation

Furthermore, we compare the clock cycles for implementing the online part of Agrawal et al.'s anti-quantum IBE scheme, Zhang et al.'s anti-quantum IBE scheme and our online/offline anti-quantum IBE scheme from LWE. In our scheme, the Gaussian sampling parts which do not request id and *mes* are placed on the Offline Server for operation. Our implementation is carried out on an Intel i7-12700 2.7GHz CPU, which is manufactured by Intel, Shanghai, China, with double precision floating point numbers for non integers in C++. We use the "time.h" to measure clock cycles. The one-dimensional sampler [26] is a modified rejection sampler. We set q and r for different LWE security [27]. In our settings, $q = 2^{12}, r = 2^9$ for 108.7-bit LWE security; $q = 2^{24}, r = 2^{11}$ for 279.7-bit LWE security; $q = 2^{34}, r = 2^{13}$ for 454.7-bit LWE security; and $q = 2^{60}, r = 2^{14}$ for 531.7-bit LWE security.

The scheme in [3] is a classic IBE scheme based on LWE, while the scheme in [4] is a recently published efficient LWE IBE scheme. The scheme in [4] balances efficiency and public parameter size through clever ideas in identity processing, and our scheme focuses on improving the efficiency of online computing while ensuring security. As shown in Figure 2, for the efficiency of the online part, our online/offline scheme has improved by 65% to 80% compared to the initial anti-quantum IBE scheme [3] from LWE, and by 60% to 70% compared to the scheme [4]. The improvement in efficiency increases with the increase of LWE security parameters. Because our scheme not only uses the efficient trapdoor generation method of **G**-trapdoor in generating trapdoors, but also performs offline calculation in advance to enable the online part to only complete necessary operations with lower cost. This is very practical in scenarios where encryption devices have low power consumption, because through online/offline technology, high calculation overhead can be completed in advance, and this part of the calculation does not require message and receiver's identity. In this way, the efficiency of encryption devices can be maximized during the online phase.

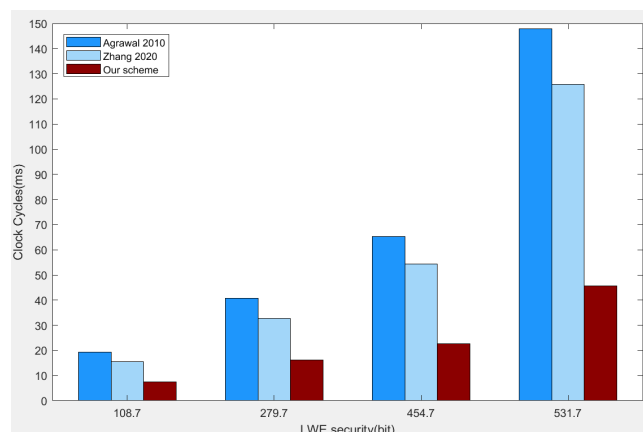


Figure 2. The comparison of online part between our online/offline scheme and other schemes [3,4] for different LWE security. In the above figure, the LWE security corresponds to different security parameter r : 108.7-bit LWE security corresponds to $r = 2^9$; 279.7-bit LWE security corresponds to $r = 2^{11}$; 454.7-bit LWE security corresponds to $r = 2^{13}$; and 531.7-bit LWE security corresponds to $r = 2^{14}$.

6. Conclusions

With the rapid development of quantum computing technology, how to design efficient IBE schemes that resist quantum attacks is currently a hot research topic. In this paper, our innovative suggestion is to design an IBOOE scheme by utilizing the difficult problem of lattice-based cryptography, which can efficiently perform online encryption even if the device's computing power is limited. Furthermore, the offline phase can be achieved without the need of the message to be encrypted and the recipient's identity. In addition, we use G-trapdoor for generating "strong trapdoors" in lattice. Compared to most existing schemes, our scheme is simpler and more efficient, greatly reducing online computing costs. We prove under the standard model that the scheme is CPA secure. Through the performance and security analysis, our scheme improve the performance of the classic LWE IBE scheme [3] by 65% to 80% (increased by LWE security parameters), and by 60% to 70% in comparison with the scheme [4]. This greatly increases the efficiency of online computing for low-power encryption devices while guaranteeing security.

Our online/offline scheme based on IBE from LWE materializes high performance while resisting quantum interference. Although our scheme can be easily expanded into an adaptive security scheme [3], and can also convert to the Hierarchical IBE scheme [2], it lacks practical features in daily life, such as flexible user changes. In the future, we will further design attribute-based encryption schemes [28–31] from LWE, which has fine-grained access control function.

Author Contributions: Conceptualization, B.Z., J.L. and Y.Z.; Methodology, B.Z. and J.L.; Software, B.Z. and J.L.; Validation, B.Z. and J.L.; Formal analysis, B.Z. and J.L.; Investigation, B.Z. and J.L.; Resources, B.Z., J.L. and Y.Z.; Data curation, B.Z., J.L., J.S. and Y.Z.; Writing—original draft, B.Z. and J.L.; Writing—review & editing, B.Z., J.L., J.S. and Y.Z.; Visualization, B.Z. and J.L.; Supervision, J.L. and Y.Z.; Project administration, J.L., J.S. and Y.Z. All authors have read and agreed to the published version of the manuscript.

Funding: Jiguo Li was supported by the National Natural Science Foundation of China (62072104, U21A20465); Jian Shen was supported by the National Natural Science Foundation of China (U21A20465).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in the study are included in the article, further inquiries can be directed to the corresponding author.

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

References

1. Gentry, C.; Peikert, C.; Vaikuntanathan, V. Trapdoors for Hard Lattices and New Cryptographic Constructions. In Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing, Victoria, BC, Canada, 17–20 May 2008.
2. Cash, D.; Hofheinz, D.; Kiltz, E.; Peikert, C. Bonsai Trees, or How to Delegate a Lattice Basis. *J. Cryptol.* **2012**, *25*, 601–639. [[CrossRef](#)]
3. Agrawal, S.; Boneh, D.; Boyen, X. Efficient Lattice (H)IBE in the Standard Model. In *Advances in Cryptology—EUROCRYPT 2010, Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, France, 30 May–3 June 2010*; Springer: Berlin/Heidelberg, Germany, 2010; Volume 6110, pp. 553–572.
4. Zhang, Y.; Liu, Y.; Guo, Y.; Zheng, S.; Wang, L. Adaptively Secure Efficient (H)IBE over Ideal Lattice with Short Parameters. *Entropy* **2020**, *22*, 1247. [[CrossRef](#)] [[PubMed](#)]
5. Regev, O. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. *J. ACM (JACM)* **2009**, *56*, 1–40. [[CrossRef](#)]
6. Zhandry, M. Secure Identity-based Encryption in the Quantum Random Oracle Model. *Int. J. Quantum Inf.* **2015**, *13*, 1550014. [[CrossRef](#)]
7. Katsumata, S.; Yamada, S.; Yamakawa, T. Tighter Security Proofs for GPV-IBE in the Quantum Random Oracle Model. *J. Cryptol.* **2021**, *34*, 5. [[CrossRef](#)]
8. Gao, W.; Yang, L.; Zhang, D.; Liu, X. Quantum Identity-based Encryption from the Learning with Errors Problem. *Cryptography* **2022**, *6*, 9. [[CrossRef](#)]
9. Dutta, P.; Susilo, W.; Duong, D.H.; Baek, J.; Roy, P.S. Lattice-based Unidirectional IBPRE Secure in Standard Model. *arXiv* **2020**, arXiv:2005.06741.
10. Wu, L.; Yang, X.; Zhang, M.; Wang, X. IB-VPRE: Adaptively Secure Identity-based Proxy Re-encryption Scheme from LWE with Re-encryption Verifiability. *J. Ambient. Intell. Humaniz. Comput.* **2022**, *13*, 469–482.
11. Liu, Y.; Sun, Y. Generic Construction of Server-aided Revocable Hierarchical Identity-based Encryption. *Int. Conf. Inf. Secur. Cryptol.* **2020**, 12612, 73–82.
12. Li, J.; Teng, M.; Zhang, Y.; Yu, Q. A Leakage-Resilient CCA-Secure Identity-Based Encryption Scheme. *Comput. J.* **2016**, *59*, 1066–1075. [[CrossRef](#)]
13. Li, J.; Guo, Y.; Yu, Q.; Lu, Y.; Zhang, Y. Provably Secure Identity-based Encryption Resilient to Post-challenge Continuous Auxiliary Input Leakage. *Secur. Commun. Netw.* **2016**, *9*, 1016–1024.
14. Li, J.; Yu, Q.; Zhang, Y. Identity-based Broadcast Encryption with Continuous Leakage Resilience. *Inf. Sci.* **2018**, *429*, 177–193. [[CrossRef](#)]
15. Yu, Q.; Li, J.; Ji, S. Hierarchical Identity-Based Online/Offline Encryption Scheme with Leakage Resilience. *Secur. Commun. Netw.* **2022**, 2022, 6849761.
16. Abla, P.; Liu, F.H.; Wang, H.; Wang, Z. Ring-based Identity Based Encryption—Asymptotically Shorter MPK and Tighter Security. In *Theory of Cryptography: 19th International Conference, TCC, Raleigh, NC, USA, 8–11 November 2021*; Springer: Cham, Switzerland, 2021; Volume 13044, pp. 157–187.
17. Fan, J.; Lu, X.; Au, M.H. Adaptively Secure Identity-Based Encryption from Middle-Product Learning with Errors. In Proceedings of the Australasian Conference on Information Security and Privacy, Brisbane, QLD, Australia, 5–7 July 2023; Volume 13915, pp. 320–340.
18. Lai, Q.; Liu, F.H.; Wang, Z. New Lattice Two-Stage Sampling Technique and Its Applications to Functional Encryption – Stronger Security and Smaller Ciphertexts. In *Advances in Cryptology—EUROCRYPT 2021, Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, 17–21 October 2021*; Springer: Cham, Switzerland, 2021; Volume 12696, pp. 498–527.
19. Weiden, P.; Hülsing, A.; Cabarcas, D.; Buchmann, J. Instantiating Treeless Signature Schemes. *Cryptol. ePrint Arch.* **2013**, *2013*, 65.
20. Lyubashevsky, V. Lattice Signatures without Trapdoors. In *Advances in Cryptology—EUROCRYPT 2012, Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, 15–19 April 2012*; Springer: Berlin/Heidelberg, Germany, 2012; Volume 7237, pp. 738–755.
21. Micciancio, D.; Peikert, C. Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller. In *Advances in Cryptology—EUROCRYPT 2012, Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, 15–19 April 2012*; Springer: Berlin/Heidelberg, Germany, 2012; Volume 7237, pp. 700–718.
22. Micciancio, D.; Walter, M. Gaussian Sampling over the Integers: Efficient, Generic, Constant-Time. In *Advances in Cryptology—CRYPTO 2017, Proceedings of the 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, 20–24 August 2017*; Springer: Cham, Switzerland, 2017; Volume 10402, pp. 455–485.
23. Sun, S.; Zhou, Y.; Ji, Y.; Zhang, R.; Tao, Y. Generic, Efficient and Isochronous Gaussian Sampling over the Integers. *Cybersecurity* **2022**, *5*, 10.
24. Guo, F.; Mu, Y.; Chen, Z. Identity-based Online/Offline Encryption. *Financ. Cryptogr. Data Secur.* **2008**, *5143*, 247–261.
25. Cramer, R.; Damgård, I. On the Amortized Complexity of Zero-Knowledge Protocols. In *Advances in Cryptology, Proceedings of the Annual International Cryptology Conference 2009, Santa Barbara, CA, USA, 16–20 August 2009*; Springer: Berlin/Heidelberg, Germany, 2009; Volume 5677, p. 177.
26. Karney, C.F.F. Sampling Exactly from the Normal Distribution. *Acm Trans. Math. Softw. (TOMS)* **2016**, *42*, 1–14. [[CrossRef](#)]

27. Chen, Y.; Genise, N.; Mukherjee, P. Approximate Trapdoors for Lattices and Smaller Hash-and-sign Signatures. In *Advances in Cryptology—ASIACRYPT 2019, Proceedings of the 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, 8–12 December 2019*; Springer: Cham, Switzerland, 2019; Volume 11923, pp. 3–32.
28. Chen, S.; Li, J.; Zhang, Y.; Han, J. Efficient Revocable Attribute-based Encryption with Verifiable Data Integrity. *IEEE Internet Things J.* **2024**, *11*, 10441–10451.
29. Chen, N.; Li, J.; Zhang, Y.; Guo, Y. Efficient CP-ABE Scheme with Shared Decryption in Cloud Storage. *IEEE Trans. Comput.* **2022**, *71*, 175–184.
30. Li, J.; Zhang, Y.; Ning, J.; Huang, X.; Poh, G.S.; Wang, D. Attribute Based Encryption with Privacy Protection and Accountability for CloudIoT. *IEEE Trans. Cloud Comput.* **2022**, *10*, 762–773. [[CrossRef](#)]
31. Zhang, R.; Li, J.; Lu, Y.; Han, J.; Zhang, Y. Key Escrow-free Attribute Based Encryption with User Revocation. *Inf. Sci.* **2022**, *600*, 59–72.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.