applied sciences

MDPI

Article

A Compact Multi-Identity Fully Homomorphic Encryption Scheme Without Fresh Ciphertexts

Ziwei Wang, Ruwei Huang * and Xiyi Wei

School of Computer and Electronic Information, Guangxi University, Nanning 530004, China; 2213393048@st.gxu.edu.cn (Z.W.); sxwlyxh@163.com (X.W.)
* Correspondence: ruweih@gxu.edu.cn

Abstract: The lattice-based multi-identity fully homomorphic encryption scheme combines the quantum security of lattice cryptography with the advantage of identity-based encryption. However, existing schemes face challenges such as large key sizes, inefficient ciphertext expansion processes, and reliance on outdated trapdoor designs, limiting their compactness and practicality. In this study, we propose a novel Compact Multi-Identity Fully Homomorphic Encryption Scheme (WZ-MIBFHE) that eliminates the need for fresh ciphertexts during expansion. First, we construct a compact identity-based encryption scheme by combining the YJW23 trapdoor and ABB10 under the standard model, proving its IND-sID-CPA security. The scheme is then adapted to ensure correctness and security when integrated with the decomposition method for ciphertext expansion. This adaptation also utilizes approximation errors to reduce overall noise. Finally, we expand the modified IBE scheme's ciphertext using the decomposition method to construct the WZ-MIBFHE scheme. Compared to existing methods, WZ-MIBFHE reduces the lattice dimension to $n\log q + \log_b q$, improves public and private key sizes, and significantly lowers ciphertext expansion rates by removing the need for fresh ciphertexts. These improvements enhance both the compactness and efficiency of the scheme, making it a promising solution for multi-identity homomorphic encryption.

Keywords: fully homomorphic encryption; identity-based encryption; multi-identity; learning with errors; fresh ciphertext

Academic Editor: Douglas O'Shaughnessy

Received: 15 December 2024
Revised: 29 December 2024
Accepted: 30 December 2024
Published: 6 January 2025

Citation: Wang, Z.; Huang, R.; Wei, X. A Compact Multi-Identity Fully Homomorphic Encryption Scheme Without Fresh Ciphertexts. *Appl. Sci.* **2025**, *1*, 473. https://doi.org/10.3390/app15010473

1. Introduction

With the advancement of technology and the popularization of digitization, people are in a data-centric era, where the volume of data is growing rapidly and the circulation and interaction between data have become more frequent. Data owners, due to their own resource constraints, usually do not store or process the data directly, but entrust it to non-trusted third parties for storage or processing. We refer to this data processing model as the outsourced computing model. The rapid development of outsourced computing has brought convenience for people to solve more complex problems, but also introduced many new issues, privacy security being the first one. How to solve the contradiction between outsourced data storage and computation and privacy security is a new issue emerging from the outsourced computing model. Homomorphic encryption technology can perfectly solve the conflict between outsourced data storage and computation and privacy security in the outsourced computing model.

In 1978, Rivest et al. [1] first introduced the concept of homomorphic encryption, i.e., encryption methods that allow data to be encrypted in an encrypted state for spe-

cific computations. Based on different mathematical problems, cryptographers have constructed various homomorphic encryption schemes, such as the RSA scheme [2] based on the problem of integer factorization, the ElGamal scheme [3] based on the discrete logarithm problem, and the Paillier scheme [4] based on the composite residuosity assumption. However, with the rapid development of quantum computers, the limitations of these traditional number-theoretic homomorphic encryption schemes in resisting quantum algorithm attacks have been greatly amplified. Consequently, ideal lattice problems, which can withstand quantum attacks, have attracted the attention of researchers. In 2009, Gentry [5] constructed the first fully homomorphic encryption scheme based on ideal lattices. Since then, cryptographers have engaged in extensive and in-depth research on constructing homomorphic encryption schemes based on ideal lattices. Homomorphic encryption has different branches based on different foundational schemes. According to these foundational schemes, homomorphic encryption is divided into four generations: the first generation represented by GSW [6], the second generation represented by BGV [7], and the third generation represented by TFHE [8], Finally, there is the fourth generation of homomorphic encryption schemes, represented by CKKS [9].

Fully homomorphic encryption extends the functionality of traditional public key encryption systems, but like traditional public key encryption, it requires a complex certificate management system. In large-scale networks, managing a vast number of public keys and certificates becomes increasingly complex, affecting the system's efficiency. Identity-Based Encryption (IBE) schemes, on the other hand, can generate public keys and public parameters directly from a user's unique identity, eliminating the need for public key certificates for authentication. In an IBE system, a trusted Private Key Generator (PKG) creates the user's secret key and securely sends it to the user. The distribution mechanism is as follows: the user submits their identity information to the PKG, which generates the master key and the corresponding user private key based on the user's identity. These keys are then securely distributed to the user via encrypted transmission or similar methods. This approach avoids the overhead of public key certificates and allows for more efficient key management.

The integration of identity-based mechanisms with cryptographic schemes has been explored in various contexts to address application-specific challenges. For example, Ahmad and Hannusch [10] proposed a keyed hash function based on Latin squares and error-correcting codes, aiming to enhance user authentication in smart home environments. Their work demonstrates how lightweight cryptographic primitives can address identity-related security challenges in IoT applications. Similarly, our work leverages the advantages of IBE to reduce the public key overhead in homomorphic encryption systems. Identity-Based Fully Homomorphic Encryption (IBFHE) combines the strengths of both homomorphic encryption and identity-based encryption, enabling access control and homomorphic operations on identity-based ciphertexts while also facilitating efficient key management.

In 2013, Gentry et al. [6] introduced the method of approximate eigenvector and constructed a FHE scheme, known as the GSW scheme. The method of approximate eigenvector can transform any IBE scheme that meets specific conditions into an IBFHE scheme. Unfortunately, this IBFHE scheme only allows homomorphic operations on ciphertexts under the same identity, limiting its ability to address outsourced computation scenarios.In order to resolve this issue, Clear et al. [11] in 2015 extended the GSW scheme to support multiple identities by introducing a Mask System (MS). Through the MS, they expanded "fresh" ciphertext matrices encrypted under different identities into multi-identity ciphertext matrices. These extended ciphertext matrices could then undergo homomorphic operations, ultimately constructing the first selectively secure multi-identity fully

homomorphic encryption (MIBFHE) scheme in the oracle model. However, the ciphertext expansion process in this scheme was complex, and the noise growth occurred too rapidly.

In 2017, Canetti et al. [12] dynamically combined Multi-Key Fully Homomorphic Encryption (MKFHE) with IBE to construct a Multi-Identity Based Fully Homomorphic Encryption scheme. However, the ciphertext expansion in this scheme depended on the number of ciphertexts, making it less compact. That same year, Wang et al. [13] leveraged the MP12 trapdoor by Micciancio and Peikert [14] along with the MS to design a more efficient MIBFHE scheme. In 2019, Tu et al. [15] applied the MP12 trapdoor to improve the CHKP10 [16] identity-based scheme, upon which they constructed an MIBFHE scheme. However, since the size of the public key and the length of the ID in the CHKP10 scheme grow linearly in proportion, this greatly affects the storage space and computational efficiency of the MIBFHE system. In the same year, Shen et al. [17] optimized the ABB10 [18] scheme using the MP12 trapdoor, and based on this optimization, they built a highly efficient MIBFHE scheme. The optimized scheme significantly improved the size of the master secret key, identity public key, and ciphertext. In 2021, Shen et al. [19] utilized a compressible ciphertext extension technique to construct a compact MIBFHE scheme, which, to some extent, addressed the issue of low bandwidth efficiency in multi-identity settings. In 2022, Liu et al. [20] proposed a multi-hop MIBFHE scheme utilizing the ciphertext extension technique from PS16 [21], thereby expanding the functionality of MIBFHE schemes. That same year, Fan et al. [22] proposed an improved lattice-based MIBFHE scheme by combining the MP12 trapdoor with the Dual Regev algorithm to construct an enhanced IBE scheme. Based on this, they used MS to design a highly efficient MIBFHE scheme. Compared to similar schemes, their approach significantly reduced both lattice dimensions and ciphertext size. Although the aforementioned MIBFHE schemes have achieved varying degrees of optimization, the efficiency of MIBFHE still faces bottlenecks. The core issue lies in the fact that the trapdoors used in these schemes are outdated compared to the theoretical advancements in trapdoor research. These trapdoors rely on computationally expensive matrix inversion operations, and the preimage sampling algorithms require high-precision real-number orthogonal iteration during the sampling process. This results in large public parameter sizes and a lack of compactness in the schemes. While techniques for reducing public parameter sizes exist, they often lead to increased scheme complexity. Additionally, existing MIBFHE schemes typically use the MS for ciphertext extension, which requires first generating fresh ciphertexts and then converting them into extended ciphertexts. This leads to a cumbersome and inefficient overall process, and the noise expansion rate in previous ciphertext extension methods is excessively high.

Our Contributions: We present a Compact Multi-Identity Fully Homomorphic Encryption Scheme without Fresh Ciphertexts by integrating various optimizations to emphasize compactness. Specifically, our main contributions as follows:

1. We incorporated the YJW23 [23] trapdoor-based preimage sampling algorithm into the ABB10-IBE scheme, thereby proposing a compact foundational IBE scheme within the standard model. We also provide a proof that our scheme is IND-sID-CPA secure.
2. We made appropriate optimizations to the foundational IBE scheme by adjusting the relationship between the public key matrix and the identity vector to meet the security requirements for constructing a compact MIBFHE scheme using the decomposition method. And we modified the structure of the key so that the approximation error originally introduced can be subtracted from the noise generated during decryption, thereby reducing the overall noise in the scheme.
3. We introduce a new ciphertext extension method—the decomposition method—which directly extends our improved IBE scheme into an MIBFHE scheme, WZ-MIBFHE,

without the need to convert the IBE into an IBFHE and then apply ciphertext extension to the IBFHE scheme to construct the MIBFHE scheme. WZ-MIBFHE can directly generate extended ciphertexts for homomorphic evaluation without the need to pre-generate new ciphertexts. WZ-MIBFHE exhibits smaller noise growth, with the lattice dimension being only $n \log q + \log_b q$ and the ciphertext expansion rate is reduced to D.

2. Preliminaries

Notation. *Let $\mathbb{R}$ and $\mathbb{Z}$ represent the set of real numbers and integers, respectively. For a positive integer q, define the set $\mathbb{Z}_q$ as:*

$$\mathbb{Z}_q = \left\{ -\left\lfloor \frac{q}{2} \right\rfloor, -\left\lfloor \frac{q}{2} \right\rfloor + 1, \ldots, q - \left\lfloor \frac{q}{2} \right\rfloor - 1 \right\}.$$

When q is not divisible by 2, the floor function $\lfloor x \rfloor$ is used to ensure proper rounding during modular reductions. Modulo allowing negative values to be equivalent to positive values, we use the negative sign to denote half of the integer field. This symmetric representation provides a balanced interval for modular arithmetic, which is particularly beneficial in lattice-based cryptographic schemes. We use $\mathbf{a} \leftarrow D$ to represent drawing a sample $\mathbf{a}$ from the distribution D. For a finite set S, $U(S)$ denotes the uniform distribution over S, and $\mathbf{a} \leftarrow S$ indicates that the sample $\mathbf{a}$ is drawn according to the uniform distribution $U(S)$. The notation $[\mathbf{A} \mid \mathbf{B}]$ is used to indicate the concatenation of matrices $\mathbf{A}$ and $\mathbf{B}$. The Euclidean norm of a vector $\mathbf{A}$ is denoted as $\|\mathbf{A}\| = \sqrt{\sum_i A_i^2}$, and $\sigma_1(\mathbf{R})$ represents the largest singular value of matrix $\mathbf{R}$. For a vector $\mathbf{a} = (a_1, a_2, \ldots, a_n) \in \mathbb{Z}_q^n$, a_i denotes the i-th component of the vector. For a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, $\mathbf{A}[i, j]$ refers to the element in the i-th row and j-th column.

2.1. Definition

Below we provide some definitions that will be used in this paper.

Definition 1 (Negligible Function)**.** *Let n denote the input size of an algorithm. A function $negl(n)$ is called negligible if it is a function that approaches zero more rapidly than the inverse of any polynomial. Specifically, for any polynomial $poly(n)$, there exists an integer n such that for all $n \geqslant N$, the inequality $negl(n) \leq \frac{1}{poly(n)}$ always holds. If the probability of an event occurring is given by a negligible function negl(n), then the event is said to be negligible. Conversely, if the probability of an event occurring is $1 - negl(n)$, then the event is said to occur with overwhelming probability.*

Definition 2 (B-Bounded Distribution)**.** *A collection of distributions $\{\chi_n\}_{n \in N}$ over integers is called B-bounded if it satisfies the following equation.*

$$\Pr_{\mathbf{x} \leftarrow \succ_n} [\|\mathbf{e}\| > B] = negl(n)$$

Definition 3 (β-Noisy Ciphertext)**.** *A message msg encrypted under the secret key $\mathbf{sk} = \mathbf{t}$ results in a β-noisy ciphertext $\mathbf{C}$, satisfying $\mathbf{tC} = \bar{\mathbf{v}}\mathbf{tG}_n + \mathbf{e}$, where $||\mathbf{e}|| \leq \beta$.*

Definition 4 (Multi-Identity Based Fully Homomorphic Encryption Scheme)**.** *An MIBFHE scheme is comprised of six probabilistic polynomial-time (PPT) algorithms: Setup, Extract, Enc, Extend, Eval, and Dec, each defined as follows:*

Setup$(1^\lambda, 1^D, 1^L)$*: Input the security parameter λ, the maximum depth L of homomorphic operation circuits, and the maximum number of user identities D. Output the master public key (MPK) and master secret key (MSK).*

Extract(MPK, MSK, id): *Input the MPK, MSK, and identity vector id. Output the identity public key* $\mathbf{A}_{id}$ *and corresponding private key* $\mathbf{sk}_{id}$.

Enc$(MPK, id, msg \in \{0,1\})$: *Input MPK, identity id, and message* $msg \in \{0,1\}$. *Output a fresh ciphertext* $\mathbf{C}_{id}$.

Extend$(MPK, (id_1, id_2, \cdots, id_D,), \mathbf{C}_{id})$: *Input MPK, the necessary identities* $(id_1, id_2, \cdots, id_D)$, *and the fresh ciphertext* $\mathbf{C}_{id}$. *Compute and output the extended ciphertext for the concatenated identities* $(id_1, id_2, \cdots, id_D)$

Eval$\left(MPK, \hat{\mathbf{C}}_{id_1}, \hat{\mathbf{C}}_{id_2} \cdots, \hat{\mathbf{C}}_{id_D}, f\right)$: *Input MPK, a Boolean circuit* f, *and the ciphertexts* $\left(\hat{\mathbf{C}}_{id_1}, \hat{\mathbf{C}}_{id_2} \cdots, \hat{\mathbf{C}}_{id_D}\right)$. *Output the result ciphertext* $\hat{\mathbf{C}}_{eval}$.

Dec$\left(MPK, \left(\mathbf{sk}_{id_1}, \mathbf{sk}_{id_2}, \cdots, \mathbf{sk}_{id_D}\right), \mathbf{C}_{id}\right)$: *Input MPK, the concatenated private keys of D identities, and the extended ciphertext or result ciphertext* $\mathbf{C}_{id}$. *Output the message* $msg \in \{0,1\}$.

Definition 5 (Indistinguishable from Random, Select-Identity, Chosen-Plaintext Attachment)**.** *(IND-sID-CPA) imposes additional restrictions on the adversary, requiring the adversary to declare the target identity it plans to attack before obtaining the public parameters. For an MIBFHE scheme, the security model between the challenger* $\mathcal{C}$ *and the PPT adversary* $\mathcal{A}$ *is defined as follows:*

Initialization Phase: *The adversary* $\mathcal{A}$ *first declares the target identity* id^* *it plans to attack. Then, given the maximum depth L of the computation circuit and the number of participating user identities D, the challenger* $\mathcal{C}$ *runs the initialization algorithm Setup to generate MPK and MSK, and sends the MPK to the adversary.*

Query Phase: *The adversary* $\mathcal{A}$ *initiates private key queries for* $id_i \neq id^* (i = 1, \cdots, D)$. *The challenger* $\mathcal{C}$ *runs the private key generation algorithm Extract to generate the corresponding private keys* $\mathbf{sk}_{id_1}, \cdots, \mathbf{sk}_{id_D}$ *and sends them to the adversary.*

Challenge Phase: *Adversary* $\mathcal{A}$ *submits a plaintext message msg as the challenge. Challenger* $\mathcal{C}$ *chooses a random bit r from* $\{0,1\}$ *and a random ciphertext c. If r equals* 0, *then* c^* *is defined as* $Encrpt(MSK, id^*, msg)$; *if r equals* 1, *then* c^* *equals c. Challenger* $\mathcal{C}$ *then dispatches* c^* *to adversary* $\mathcal{A}$ *as the challenge.*

Guess Phase: *The adversary* $\mathcal{A}$ *outputs* $r' \in \{0,1\}$ *as their guess. If* r' *equals r, then adversary* $\mathcal{A}$ *wins the game and is considered an IND-sID-CPA adversary. Let* $Adv(\mathcal{A}) = \left|Pr\left[r' = r\right] - \frac{1}{2}\right|$ *denote the advantage of adversary* $\mathcal{A}$ *in attacking the encryption scheme. If for all IND-sID-CPA adversaries the advantage is* $Adv(\mathcal{A}) = \left|Pr\left[r' = r\right] - \frac{1}{2}\right| = negl(n)$, *then the encryption scheme is IND-sID-CPA secure.*

2.2. Lattice

A lattice in the Euclidean space is a set of points arranged in a regular pattern, and the coordinates of these points can be represented by a set of integer-coefficient vectors in the space, referred to as the basis vectors of the lattice. The specific definition is as follows:

Definition 6 (Lattice)**.** *Let* $v_1, v_2, \ldots, v_n$ *be n linearly independent vectors in* $\mathbb{R}^m$, *let* $\boldsymbol{V} = \{v_1, v_2, \ldots, v_n\} \in \mathbb{R}^{m \times n}$. *The lattice* $\Lambda(\boldsymbol{V})$ *generated by the vectors in* $\boldsymbol{V}$ *is defined as follows:*

$$\Lambda(\boldsymbol{V}) = \{\textstyle\sum_i^n \mathbf{x}_i \mathbf{v}_i \in \mathbb{Z}\}$$

where $\{v_1, v_2, \ldots, v_n\}$ *are a set of basis vectors for the lattice* $\Lambda(\mathbf{V})$, *and a lattice can have multiple sets of bases. m represents the dimension of the lattice, and n is the rank of the lattice, with* $m \geqslant n$. *When* $m \geqslant n$, *the lattice* $\Lambda(\boldsymbol{V})$ *is referred to as a full-rank lattice.*

Definition 7 (q-ary Lattice)**.** *Given* $\boldsymbol{V} \in \mathbb{Z}_q^{m \times n}$, *a prime q, and* $m, n \in \mathbb{Z}$. *A q-ary lattice is defined as follows: For some* $\mathbf{x} \in \mathbb{Z}_q^n$

$$\Lambda_q(\boldsymbol{V}) = \left\{\mathbf{t} \in \mathbb{Z}_q^n : \mathbf{t} = \boldsymbol{V}^{\mathbf{t}} \cdot \mathbf{x} \ mod \ q\right\}$$

Definition 8 (Integral Lattice)**.**

$$\Lambda_q^{\perp}(\boldsymbol{V}) = \left\{ \mathbf{t} \in \mathbb{Z}_q^n : \mathbf{t} = \boldsymbol{V} \cdot \mathbf{t} = 0 \ mod \ q \right\}$$

If all the elements of the vectors in the lattice Λ are integers, then Λ is called an integral lattice. Let q be a prime number and $\boldsymbol{V} \in \mathbb{Z}_q^{m \times n}$. The q-ary integral lattice is defined as follows: For some $\mathbf{x} \in \mathbb{Z}_q^n$

$$\Lambda_q(\boldsymbol{V}) = \left\{ \mathbf{t} \in \mathbb{Z}_q^n : \mathbf{t} = \boldsymbol{V}^{\mathbf{t}} \cdot \mathbf{x} \ mod \ q \right\}$$

$$\Lambda_q^{\perp}(\boldsymbol{V}) = \left\{ \mathbf{t} \in \mathbb{Z}_q^n : \mathbf{t} = \boldsymbol{V} \cdot \mathbf{t} = 0 \ mod \ q \right\}$$

2.3. Discrete Gaussian Distribution

The Gaussian distribution is a commonly used probability distribution in the design of lattice cryptographic schemes. Next, we will introduce the relevant definitions and important lemmas involved in this paper.

Definition 9 (Gaussian Function)**.** *Given any real number $\sigma \in \mathbb{R} > 0$, with standard deviation σ and a center $\sigma \in \mathbb{R}^n$, the Gaussian function for all $\forall \mathbf{x} \in \mathbb{R}^n$ is defined as follows:*

$$\rho_{\sigma,c}(\mathbf{x}) = exp\left(\frac{-\pi \| \mathbf{x} - c \|^2}{\sigma^2} \right)$$

Definition 10 (Discrete Gaussian Distribution)**.** *Consider $\Lambda \in \mathbb{R}^{m \times n}$. Given a real number $\sigma \in \mathbb{R} > 0$, and a center $c \in \mathbb{R}^n$ with standard deviation σ, the discrete Gaussian distribution for any $\forall \mathbf{x} \in \Lambda$ is defined as follows:*

$$\mathcal{D}_{\Lambda,\sigma,c}(\mathbf{x}) = \frac{\rho_{\sigma,c}(\mathbf{x})}{\rho_{\sigma,c}(\Lambda)} = \frac{\rho_{\sigma,c}(\mathbf{x})}{\sum_{\mathbf{v} \in \Lambda} \rho_{\sigma,c}(\mathbf{v})}$$

For clarity, when $c = 0$, $\rho_{\sigma,0}$ and $\mathcal{D}_{\Lambda,\sigma,0}$ are simplified to ρ_σ and $\mathcal{D}_{\Lambda,\sigma}$, respectively. Similarly, when $\sigma = 1$, ρ_1 is denoted as ρ. The distribution $\mathcal{D}_{\Lambda,\sigma,c}$ is generally defined over the lattice $\Lambda = \Lambda_q^{\perp}(\mathbf{A})$ associated with a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, or over a shifted lattice $\Lambda = \mathbf{t} + \Lambda_q^{\perp}(\mathbf{A})$, where $\mathbf{t} \in \mathbb{Z}^m$.

Lemma 1 ([24])**.** *Consider $\mathbf{B}$ be a basis for the m-dimensional lattice Λ , and for some negligible function $\in m$, let $s \geqslant \eta_{\in}(\Lambda)$. Then,*

$$\Pr_{\mathbf{x} \leftarrow \mathcal{D}_{\Lambda,s}} \left[\|\mathbf{x}\| > s\sqrt{m} \right] \leq negl(m)$$

Lemma 2 ([25])**.** *Let n be a positive integer, and let $\mathbf{t}$ be a vector randomly selected from $\mathbb{Z}^m$. Let the error vector $\mathbf{y} \xleftarrow{\bar{\Psi}_\alpha^m} \mathbb{Z}_q^m$, where $0 < \alpha \leq \left(\omega\left(\sqrt{\log n}\right)\right)^{-1}$, and $\bar{\Psi}_\alpha$ represents the discrete Gaussian distribution over $\mathbb{Z}_q$ corresponding to a normal distribution with mean 0 and standard deviation $\frac{\alpha}{\sqrt{2\pi}}$ over $[0,1)$. If $\bar{\Psi}_\alpha^m$ represents an m-dimensional error vector randomly selected from the distribution $\bar{\Psi}_\alpha$, then $\left|\mathbf{t}^T \mathbf{y}\right|$ can be viewed as an integer in the range $[0, q-1]$ and satisfies*

$$\left|\mathbf{t}^T \mathbf{y}\right| \leq \|\mathbf{t}\| q \alpha \omega\left(\sqrt{\log m}\right) + \frac{\|\mathbf{t}\|\sqrt{m}}{2}$$

Lemma 3 ([26])**.** *Assume $m > (n+1)\log q + \omega \log n$, and q is a prime. Uniformly randomly select matrices $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ and $B \in \mathbb{Z}_q^{m \times n}$. Let $\mathbf{R}$ be an $m \times m$ matrix uniformly randomly selected*

from $\{0,1\}^{m\times m}$. *For all vectors* $w \in \mathbb{Z}_q^m$, *The distributions* $(\mathbf{A}, \mathbf{AR}, \mathbf{AR^T w})$ *and* $(\mathbf{A}, \mathbf{B}, \mathbf{R^T w})$ *are statistically indistinguishable.*

2.4. Learning with Errors

The LWE problem, a classic lattice problem defined by Regev, underpins the security of all the constructions presented in this paper. The LWE problems are divided into two primary categories: worst-case problems and average-case problems. In lattice cryptography schemes, the most frequently employed problems are LWE problem and the Small Integer Solution (SIS) assumption. The LWE problem is predominantly used for constructing public key encryption, attribute-based encryption schemes, and identity-based encryption. Conversely, the SIS assumption is mainly utilized in the creation of one-way hash functions, collision-resistant hash functions, digital signatures, and authentication schemes.

Definition 11 (LWE Distribution)**.** *For a uniformly random and fixed secret vector* $\mathbf{s} \in \mathbb{Z}_q^n$, *a vector* $\mathbf{a} \leftarrow \mathbb{Z}_q^n$ *is selected uniformly at random, and a random number e is drawn from a distribution* χ, *where* χ *is a discrete Gaussian error distribution over* $\mathbb{Z}_q$. *The LWE distribution is defined as the output of uniform samples of the form* $(\mathbf{a}, \mathbf{b} = \langle \mathbf{a}, \mathbf{s} \rangle + \mathbf{e} \ mod \ q) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, *denoted as* $\mathbf{A}_{\mathbf{s},\chi}$.

Definition 12 (Search LWE)**.** *Given m independent and uniformly random samples* $(\mathbf{a}_i, \mathbf{b}_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ *from the LWE distribution* $\mathbf{A}_{s,\chi}$, *the objective is to recover the unknown secret vector* $\mathbf{s}$.

Definition 13 (Decision LWE)**.** *Let* λ *be the security parameter,* $q = q(\lambda) \geq 2$ *be a prime, and* $\chi = \chi(\lambda)$ *be a discrete Gaussian error distribution over* $\mathbb{Z}_q$. *An instance of the* $LWE_{\lambda,q,\chi}$ *problem is to distinguish between the following two challenge oracles* $\mathcal{O}$: $\mathcal{O}_\$$: *Outputs uniformly random samples* $(\mathbf{a}_i, \mathbf{b}_i)$ *from* $\mathbb{Z}_q^n \times \mathbb{Z}_q$, *where* $\mathbf{a}_i \xleftarrow{\$} \mathbb{Z}_q^n$ *and* $\mathbf{b}_i \xleftarrow{\$} \mathbb{Z}_q$, "$\xleftarrow{\$}$" *denotes uniform random sampling.* $\mathcal{O}_s$: *Selects a uniformly random fixed secret vector* $\mathbf{s} \leftarrow \mathbb{Z}_q^n$, *then selects* $\mathbf{e}_i \leftarrow \chi$ *and samples* $\mathbf{a}_i \leftarrow \mathbb{Z}_q^n$ *uniformly, with* $\mathbf{b}_i = \langle \mathbf{a}_i, \mathbf{s} \rangle + \mathbf{e}_i$. *Outputs* $(\mathbf{a}_i, \mathbf{b}_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$.

The LWE problem is that it is difficult to distinguish between the two oracle outputs mentioned above.

2.5. Preimage Sampling Algorithm

Lemma 4 ([27])**.** *Let* $(\mathbf{A}, \mathbf{T})$ *be a matrix approximation trapdoor pair,* $\mathbf{B} = \begin{bmatrix} \mathbf{T} \\ -\mathbf{I}_N \end{bmatrix}$ *and* $(\mathbf{r}, \mathbf{\Sigma})$ *such that* $\sqrt{\mathbf{\Sigma}_p \oplus \mathbf{r}^2 \mathbf{I}_N} \geqslant \eta(\mathcal{L}(\mathbf{B}))$. *Use* $\mathbf{A}^{-1}$ *to denote* $\mathbf{ApproxPreSamp}(\mathbf{A}, \mathbf{T}, \cdot, \mathbf{r}, \mathbf{\Sigma})$. *The two distributions that follow are statistically indistinguishable:*

$$\left\{(\mathbf{A}, \mathbf{x}, \mathbf{u}, \mathbf{e}) : \mathbf{u} \xleftarrow{\$} \mathbb{Z}_Q^n, \mathbf{x} \leftarrow \mathbf{A}^{-1}(\mathbf{u}),\ \mathbf{e} = \mathbf{u} - \mathbf{A}\mathbf{x} \ mod \ Q\right\}$$

$$\left\{(\mathbf{A}, \mathbf{x}, \mathbf{u}, \mathbf{e}) : \mathbf{x} \leftarrow D_{\mathbb{Z}^m, \sqrt{\sum}}, \mathbf{e} \xleftarrow{\$} \mathbb{Z}_p^n,\ \mathbf{u} = \mathbf{A}\mathbf{x} + \mathbf{e} \ mod \ Q\right\}$$

The efficiency of basic Gaussian sampling is crucial to the overall performance of the Gaussian preimage sampling algorithm. The standard deviation σ is a significant measure of this algorithm's effectiveness. A smaller standard deviation σ indicates a higher quality of the Gaussian preimage sampling algorithm. Furthermore, the quality of the trapdoor matrix $\mathbf{R}$ also significantly influences the performance of the Gaussian preimage sampling algorithm.

3. Identity-Based Encryption Scheme

The efficiency of MIBFHE schemes is largely determined by the underlying IBE scheme. To construct a compact and streamlined MIBFHE scheme, the design of the underlying

IBE scheme is crucial. The two most mainstream IBE schemes are CHKP10 and ABB10. However, the size of the public key and the length of the identity ID in CHKP10 grow proportionally and linearly, which limits its storage space and computational efficiency. In this section, we incorporate the preimage sampling algorithm based on the YJW23 trapdoor into the ABB10 scheme, constructing a compact IBE scheme. The parameters of the improved scheme are more concise, and we have verified its correctness and security. Compared to similar IBE schemes, our compact IBE scheme achieves significant optimizations in its main parameters.

3.1. Our IBE Construction

The parameters of the scheme are defined as follows: Let λ be the security parameter, $Q = pq$ be the modulus where p and q are positive integers, and let $m_1 = n \log q$, $m = m_1 + n\omega$, $m' = m + 1$, and $\omega = \log_b q$. Let B_χ be the bounded error distribution, $\chi = \chi(\lambda)$. Construct a gadget matrix $\mathbf{F} = \mathbf{I}_n \otimes \mathbf{f}^T \in \mathbb{Z}^{n \times n\omega}$ where $\mathbf{f}^T = p \cdot \left[1, b^1, b^2, \ldots, b^{\omega-1}\right] \in \mathbb{Z}_Q^{1\times\omega}$, $\mathbf{I}_n$ is an $n \times n$ identity matrix, and b is a small integer. The identity encoding Full-Rank Differences (FRD) function $\mathbf{H} : \mathbb{Z}_Q^{n\times 1} \to \mathbb{Z}_Q^{n\times n}$ satisfies $\mathbf{H}_{id_1} - \mathbf{H}_{id_2} \neq 0$.

The IBE scheme constructed in this paper consists of four parts: the initialization algorithm **IBE.Setup**, the key generation algorithm **IBE.Extract**, the encryption algorithm **IBE.Enc**, and the decryption algorithm **IBE.Dec**:

(1) **IBE.Setup**(1^λ): Input the security parameter λ, choose $n = n(\lambda)$, error distribution $\chi = \chi(\lambda)$. Let $Q = pq$ and $m = m_1 + n\omega$. Uniformly and randomly select an n-dimensional vector $\mathbf{u} \xleftarrow{\$} \mathbb{Z}_Q^{n\times 1}$, a matrix $\overline{\mathbf{A}} \xleftarrow{\$} \mathbb{Z}_Q^{n\times m_1}$, and generate a uniformly random matrix $\mathbf{A} = \left[\overline{\mathbf{A}} \parallel -\overline{\mathbf{A}}\mathbf{R}\right] \in \mathbb{Z}_Q^{n\times m}$ with a trapdoor matrix $\mathbf{R} \in \mathbb{Z}_Q^{m_1\times n\omega}$. Outputs $MPK = (\mathbf{A}, \mathbf{u})$ as the master public key and $MSK = \mathbf{R}$ as the master secret key.

(2) **IBE.Extract**(MPK, MSK, id): Provide the MPK, MSK, and the user identity vector $id \in \mathbb{Z}_Q^{n\times 1}$ as input. Use the identity encoding FRD function $\mathbf{H} : \mathbb{Z}_Q^{n\times 1} \to \mathbb{Z}_Q^{n\times n}$ to generate an invertible matrix $\mathbf{H}_{id} \in \mathbb{Z}_Q^{n\times n}$ corresponding to each identity id. Let the user identity public key matrix be $\mathbf{A}_{id} = \mathbf{A} + [0 \parallel \mathbf{HG}] = \left[\mathbf{A} \parallel \mathbf{HF} - \overline{\mathbf{A}}\mathbf{R}\right] \in \mathbb{Z}_Q^{n\times m}$. Run the preimage sampling algorithm **ApproxPreSamp**$(\mathbf{A}_{id}, \mathbf{R}, \mathbf{u}, \sigma)$ to generate a sampling vector $\mathbf{t}_{id} \in \mathbb{Z}_Q^{m\times 1}$ that follows the discrete Gaussian distribution $\mathcal{D}_{\Lambda_q^u(\mathbf{A}_{id}),\sigma}$, satisfying $\mathbf{A}_{id}\mathbf{t}_{id} = \mathbf{u}_{id} - \mathbf{e}_{app} \ mod \ Q$, where $\mathbf{e}_{app}$ is the approximation error of the trapdoor. Let $\mathbf{A}'_{id} = [\mathbf{u} \parallel \mathbf{A}_{id}] \in \mathbb{Z}_Q^{n\times m'}$. Output the private key for each user identity $\mathbf{sk}_{id} = (1, -\mathbf{t}_{id}) \in \mathbb{Z}_Q^{m'\times 1}$, satisfying $\mathbf{A}'_{id}\mathbf{sk}_{id} = \mathbf{e}_{app} \ mod \ Q$.

(3) **IBE.Enc**(MPK, id, msg): Provide as input the MPK, user identity id, and a plaintext bit message $msg \in \{0, 1\}$. Define the vector $\bar{\mathbf{v}} = \left(msg \cdot \frac{Q}{2}, 0, \ldots, 0\right) \in \mathbb{Z}_q^{m'}$. Uniformly and randomly select a vector $\mathbf{y} \xleftarrow{\$} \{0,1\}^{n\times 1}$, and uniformly randomly select an error vector $\mathbf{e} \xleftarrow{\$} \chi_{\overline{\Psi}_\alpha}^{m'\times 1}$ from the LWE error distribution, with $\|\mathbf{e}\| < B_\chi$. Output the ciphertext $\mathbf{c}_{id} = \mathbf{A}_{id}'^T\mathbf{y} + \bar{\mathbf{v}} + \mathbf{e} \in \mathbb{Z}_Q^{m'\times 1}$.

(4) **IBE.Dec**$(MPK, \mathbf{sk}_{id}, \mathbf{c}_{id})$: Input MPK, user private key $\mathbf{sk}_{id}$, and ciphertext $\mathbf{c}_{id}$. Compute $\mathbf{s}_{id}^T \cdot \mathbf{c}_{id}$ and denote the result as $msg' = \mathbf{sk}_{id}^T \cdot \mathbf{c}_{id} \in \mathbb{Z}_Q$. When $\left|\left|msg' - \left\lfloor\frac{Q}{2}\right\rfloor\right|\right| < \left\lfloor\frac{Q}{4}\right\rfloor$, output $msg = 1$; otherwise, $||msg'|| < \left\lfloor\frac{Q}{4}\right\rfloor$, output $msg = 0$.

3.2. Correctness and Parameters

Theorem 1. *When* $m = n \cdot \omega(\log b + 1), Q = m^{\frac{3}{2}}\sqrt{n}\omega(\log n), \sigma = \sqrt{m}\omega(\log n), \alpha < \sigma \cdot \sqrt{m} \cdot \omega(\sqrt{\log n})^{-1}$. *According to Definition 1, we state the IBE we described in Section 3.1 achieves correct decryption with overwhelming probability.*

Proof of Theorem 1. From the decryption formula, we have

$$\begin{aligned}\mathbf{sk}_{id}^{T}\cdot\mathbf{c}_{id} &= \mathbf{sk}_{id}^{T}\left(\mathbf{A}_{id}^{'T}\mathbf{y}+\bar{\mathbf{v}}+\mathbf{e}\right)\\ &= \mathbf{sk}_{id}^{T}\mathbf{A}_{id}^{'T}\mathbf{y}+\left\langle\mathbf{sk}_{id}^{T},\bar{\mathbf{v}}\right\rangle+\left\langle\mathbf{sk}_{id}^{T},\mathbf{e}\right\rangle\\ &= \mathbf{e}_{app}\mathbf{y}+msg\left\lfloor\frac{Q}{2}\right\rfloor+\left\langle\mathbf{sk}_{id}^{T},\mathbf{e}\right\rangle\end{aligned}$$

Let $\mathbf{e}=(\mathbf{e_0}\parallel\mathbf{e_1})\in\mathbb{Z}_Q\times\mathbb{Z}_Q^{m\times 1}$,Then we have $\left|\left\langle\mathbf{sk}_{id}^{T},\mathbf{e}\right\rangle\right|=\left|\mathbf{e_0}-\langle\mathbf{t_{id}^{T}},\mathbf{e_1}\rangle\right|\leq|\mathbf{e_0}|+\left|\langle\mathbf{t}_{id}^{T},\mathbf{e_1}\rangle\right|$. From Lemma 1, we know that $\|\mathbf{t}_{id}\|\leq\sigma\sqrt{m}$, where $\sigma\geq s_1(\mathbf{R})\cdot\omega\left(\sqrt{\log n}\right)=\sqrt{m}\omega(\log n)$; From Lemma 2, we have

$$\left|\left\langle\mathbf{t}_{id}^{T},\mathbf{e}_1\right\rangle\right|\leq\|\mathbf{t}_{id}\|Q\alpha\omega\left(\sqrt{\log m}\right)+\frac{\|\mathbf{t}_{id}\|\sqrt{m}}{2}\leq\sigma\sqrt{m}Q\alpha\omega\left(\sqrt{\log m}\right)+\mathcal{O}(\sigma m)$$

$$\text{i.e., }\left|\left\langle\mathbf{sk}_{id}^{T},\mathbf{e}\right\rangle\right|=|\mathbf{e}_0|+\left|\left\langle\mathbf{t}_{id}^{T},\mathbf{e}_1\right\rangle\right|\leq\sigma\sqrt{m}Q\alpha\omega\left(\sqrt{\log m}\right)+\mathcal{O}(\sigma m).$$

To ensure the correctness of the IBE scheme's decryption, the relevant parameter values must satisfy the following conditions:

(1) To guarantee the decryption algorithm works correctly, it is necessary to ensure that the error term satisfies $\left|\left\langle\mathbf{sk}_{id}^{T},\mathbf{e}\right\rangle\right|<\frac{Q}{4}$. As stated in GPV08, this condition holds when $\alpha\leq\left(\sigma\sqrt{m+1}\cdot\omega(\sqrt{\log n})\right)^{-1}$ and $Q\geq 5\sigma(m+1)$, it is highly probable that $\left|\left\langle\mathbf{sk}_{id}^{T},\mathbf{e}\right\rangle\right|\leq\frac{Q}{5}<\frac{Q}{4}$, and $\left|\mathbf{e}_{app}\mathbf{y}\right|<\frac{Q}{20}$. When $\left|\left\langle\mathbf{sk}_{id}^{T},\mathbf{e}\right\rangle\right|<\frac{Q}{4}$, if $msg=1$, then $\left|\left|\left\langle\mathbf{sk}_{id}^{T},\mathbf{c}_{id}\right\rangle-\left|\frac{Q}{2}\right|\right|\right|<\frac{Q}{4}$; if $msg=0$, then $\left|\left\langle\mathbf{sk}_{id}^{T},\mathbf{c}_{id}\right\rangle\right|<\frac{Q}{4}$, Clearly, the decryption algorithm is capable of successfully decrypting with overwhelming probability.

(2) The hardness assumption of the LWE problem requires that $\alpha Q>2\sqrt{n}$. From the above, we know that when α and Q are chosen to their extreme values, we can achieve, We can ensure $\alpha\cdot Q=\frac{5\sqrt{m+1}}{\omega\left(\sqrt{\log n}\right)}>\frac{5\sqrt{2n\log q}}{\omega\left(\sqrt{\log n}\right)}>2\sqrt{n}$, meeting the security condition of the LWE problem $\alpha Q>2\sqrt{n}$.

Based on the above analysis, we set the scheme parameters (m,Q,σ,α) as follows:

$$\begin{aligned}m &= n\log q+n\log_b q=n\cdot\omega(\log b+1)\\ Q &= m^{\frac{3}{2}}\sqrt{n}\omega(\log n)\\ \sigma &= \sqrt{m}\omega(\log n)\\ \alpha &< \sigma\cdot\sqrt{m}\cdot\omega(\sqrt{\log n})^{-1}\end{aligned}$$

□

3.3. Security Analysis

Theorem 2. *The enhanced IBE scheme proposed in this paper is proven to be IND-sID-CPA secure under the assumption that the $LWE_{\lambda,Q,\chi}$ problem is hard.*

Proof of Theorem 2. The security proof for the enhanced IBE scheme involves a sequence of IND-sID-CPA games conducted between the adversary $\mathcal{A}$ and the challenger $\mathcal{C}$ within the standard model. In this paper, we use the term "game" to describe the interaction process between the attacker and the encryption system, rather than referring to an actual game. The proof process is summarized as follows:

Game 0: The initial standard IND-sID-CPA game between the adversary $\mathcal{A}$ and the challenger $\mathcal{C}$ for the IBE scheme.

Game 1: The adversary $\mathcal{A}$ declares the target identity id^* to be attacked. Compared to Game 0, the challenger $\mathcal{C}$ in Game 1 changes the generation method of the matrix $\mathbf{A}$, uniformly randomly generating the matrix

$$\mathbf{A} = \left[\bar{\mathbf{A}} \parallel -\mathbf{H}_{id^*}\mathbf{F} - \bar{\mathbf{A}}\mathbf{R}\right]$$

instead of

$$\mathbf{A} = \left[\bar{\mathbf{A}} \parallel \mathbf{H}_{id}\mathbf{F} - \bar{\mathbf{A}}\mathbf{R}\right]$$

in Game 0. According to Lemma 3, for the adversary $\mathcal{A}$, the matrix $\mathbf{A}$ generated in Game 0 is statistically indistinguishable from the matrix $\mathbf{A}$ generated in Game 1. Therefore, the ability of adversary $\mathcal{A}$ to distinguish between Game 1 and Game 0 is extremely limited, with an advantage so small it can be considered negligible.

Game 2: In Game 2, compared to Game 1, the challenger $\mathcal{C}$ changes the response method for private key queries for $id \neq id^*$. Game 2 uses the public matrix $\mathbf{F}$ and the trapdoor matrix $\mathbf{R}$ of the lattice $\Lambda_Q^{\perp}(\mathbf{F})$, retaining the form of

$$\mathbf{A} = \left[\bar{\mathbf{A}} \parallel -\mathbf{H}_{id^*}\mathbf{F} - \bar{\mathbf{A}}\mathbf{R}\right]$$

from Game 1, then

$$\mathbf{A}_{id} = \left[\bar{\mathbf{A}} \parallel (\mathbf{H}_{id} - \mathbf{H}_{id^*})\mathbf{F} - \bar{\mathbf{A}}\mathbf{R}\right].$$

Based on the definition of the identity encoding FRD function, $(\mathbf{H}_{id} - \mathbf{H}_{id^*})$ is guaranteed to be non-singular. To respond to the adversary's private key query, the challenger utilizes preimage sampling on the trapdoor matrix $\mathbf{R}$ by executing the preimage sampling algorithm

$$\mathbf{ApproxPreSamp}(\mathbf{A}_{id}, \mathbf{R}, \mathbf{u}, \sigma) \rightarrow \mathbf{t}_{id},$$

and the private key $\mathbf{sk}_{id} = (1, -\mathbf{t}_{id})$ is provided to the adversary $\mathcal{A}$. If $id = id^*$, then $(\mathbf{H}_{id} - \mathbf{H}_{id^*})$ becomes a singular matrix, causing the game to terminate. According to Lemma 4, the distribution $\mathbf{sk}_{id}$ in Game 2 is statistically indistinguishable from $\mathbf{sk}_{id}$ in Game 1 as $\mathcal{D}_{\Lambda_Q^u(\mathbf{A}_{id}),\sigma\omega(\sqrt{\log n})}$. Therefore, the advantage of the adversary $\mathcal{A}$ in distinguishing Game 2 from Game 1 is negligible.

Game 3: Compared to Game 2,the challenger $\mathcal{C}$ always selects random independent elements from the ciphertext space $\mathbb{Z}_Q^{m'}$ as the challenge ciphertext. Thus, the challenge ciphertext appears as an indistinguishable random ciphertext within the ciphertext space, making the adversary's advantage negligible.

For the PPT adversary $\mathcal{A}$, we still need to use the hardness of the $LWE_{\lambda,Q,\chi}$ assumption to prove that the adversary cannot computationally distinguish Game 2 from Game 3. Suppose the adversary $\mathcal{A}$ has a non-negligible advantage in distinguishing Game 2 from Game 3. Simulator $\mathcal{S}$ for the $LWE_{\lambda,Q,\chi}$ assumption can use the adversary $\mathcal{A}$ to distinguish whether the oracle $\mathcal{O}$ is a truly random oracle $\mathcal{O}_\$$ or a pseudo-random oracle$\mathcal{O}_\$$. The steps for the simulator $\mathcal{S}$ are as follows:

Instance: The challenger $\mathcal{C}$ samples $m_1 + 1$ samples $(\mathbf{u}_i, \mathbf{v}_i) \in \mathbb{Z}_Q^{n\times 1} \times \mathbb{Z}_Q$ from the oracle $\mathcal{O}$, where $i = 0, 1, \ldots, m_1$.

Target: The adversary $\mathcal{A}$ declares the target identity id^* to be attacked to the challenger $\mathcal{C}$.

Setup: The challenger $\mathcal{C}$ sets up the MPK based on the target identity id^* declared by the adversary $\mathcal{A}$.

(1) The challenger C constructs the matrix $\bar{\mathbf{A}} = (\mathbf{u}_1 \parallel \mathbf{u}_2 \parallel \cdots \parallel \mathbf{u}_{m_1}) \in \mathbb{Z}_Q^{n \times m_1}$ using the sampled samples.

(2) Let $\mathbf{u}_0$ be the public random vector $\mathbf{u} = \mathbf{u}_0 \in \mathbb{Z}_Q^{n \times 1}$.

(3) Choose $\mathbf{R}$ from the distribution $\mathcal{D}^{m_1 \times n\omega}$ and form the matrix $\mathbf{A}_1 = -\mathbf{H}_{id^*}\mathbf{F} - \bar{\mathbf{A}}\mathbf{R}$.

(4) Output the public parameters $\left\{\mathbf{u}, \bar{\mathbf{A}}, \mathbf{A}_1\right\}$ to the adversary $\mathcal{A}$.

Queries 1: As in Game 2,the challenger $\mathcal{C}$ provide the adversary $\mathcal{A}$ with each private key query for $id \neq id^*$.

Challenge: The adversary $\mathcal{A}$ provides the challenge identity id^* associated with the challenge plaintext $msg^* \in \{0,1\}$. The challenger $\mathcal{C}$ then generates the challenge ciphertext for the target identity id^* using the following process:

(1) Let $\mathbf{v}^* = (v_1, \ldots, v_{m_1})^T \in \mathbb{Z}_Q^{m_1 \times 1}$;

(2) Hide the plaintext bit message msg^* with $c_0^* = v_0 + msg^* \left\lfloor \frac{Q}{2} \right\rfloor$;

(3) Let $\mathbf{c}_1^* = \begin{bmatrix} \mathbf{v}^* \\ -\mathbf{R}^T\mathbf{v}^* + \mathbf{e} \end{bmatrix} \in \mathbb{Z}_Q^m$, where $\mathbf{e} \xleftarrow{\Psi_\alpha} \mathbb{Z}_Q^{n\omega}$;

(4) Select a random bit $r \xleftarrow{\$} \{0,1\}$. If $r = 0$, the challenger sends $\mathbf{c}^* = (\mathbf{c}_0^*, \mathbf{c}_1^*)$ to the adversary $\mathcal{A}$; if $r = 1$, a vector $\mathbf{c}_{id} \in \mathbb{Z}_Q^{m'}$ is uniformly sampled and sent to $\mathcal{A}$. When $\mathcal{O} = \mathcal{O}_s$, the distribution of $\mathbf{c}^*$ is indistinguishable from the challenge ciphertext in Game 2. By the definition of $LWE_{\lambda,Q,\chi}$, $\mathbf{v}_0 = \mathbf{u}_0^T\mathbf{sk} + \mathbf{e_0}$ and $\mathbf{v}^* = \bar{\mathbf{A}}^T\mathbf{sk} + \mathbf{e_1}$. Furthermore, $\mathbf{A}_{id^*} = \left[\bar{\mathbf{A}} \parallel (\mathbf{H}_{id^*} - \mathbf{H}_{id^*})\mathbf{F} - \bar{\mathbf{A}}\mathbf{R}\right] = \left[\bar{\mathbf{A}} \parallel -\bar{\mathbf{A}}\mathbf{R}\right]$, we get

$$\mathbf{c}_1^* = \begin{bmatrix} \mathbf{v}^* \\ -\mathbf{R}^T\mathbf{v}^* + \mathbf{e} \end{bmatrix} = \mathbf{A}_{id^*}^T\mathbf{sk} + \begin{bmatrix} \mathbf{e_1} \\ -\mathbf{R}^T\mathbf{e_1} + \mathbf{e} \end{bmatrix}$$

which is exactly the challenge ciphertext $\mathbf{c}_1$ in Game 2, The part $\mathbf{c}_0^* = \mathbf{v}_0 + msg^* \left\lfloor \frac{Q}{2} \right\rfloor = \mathbf{u}_0^T\mathbf{sk} + \mathbf{e_0} + msg^* \left\lfloor \frac{Q}{2} \right\rfloor$ is the challenge ciphertext $\mathbf{c}_0$, Thus, $\mathbf{c}^*$ is a valid ciphertext for the plaintext bit msg^* associated with the identity id^*. When $\mathcal{O} = \mathcal{O}_\$$, $\mathbf{v}_0 \in \mathbb{Z}_Q$ and $\mathbf{v}^* \in \mathbb{Z}_Q^{m_1 \times 1}$ are uniformly sampled at random. According to Lemma 3, the matrix $-\mathbf{R}^T\mathbf{v}^*$ adheres to a discrete random distribution, the expression $-\mathbf{R}^T\mathbf{v}^* + \mathbf{e}$ similarly conforms to a discrete random distribution. Consequently, the distribution of the challenge ciphertext c^* in Game 2 is indistinguishable from its distribution in Game 3.

Queries 2: The adversary $\mathcal{A}$ may proceed to make private key queries in the same manner described in Queries 1.

Guess: The adversary $\mathcal{A}$ attempts to determine whether the ciphertext is a random vector in the ciphertext space $\mathbb{Z}_Q^{m'}$ or the actual ciphertext of the plaintext bit message msg^*. The challenger $\mathcal{C}$ determines whether the sampled samples from the oracle $\mathcal{O}$ are $LWE_{\lambda,Q,\chi}$ samples from $\mathcal{O}_s$ or random samples from $\mathcal{O}_s$ based on the guess.

In summary, when $\mathcal{O} = \mathcal{O}_s$, the adversary $\mathcal{A}$ experiences the scenario as in Game 2; when $\mathcal{O} = \mathcal{O}_s$, the scenario is perceived as in Game 3. Given that the simulator $\mathcal{S}$'s capability to resolve the $LWE_{n,Q,\chi}$ assumption is equivalent to the adversary $\mathcal{A}$'s ability to differentiate between Game 2 and Game 3, and considering that no PPT simulator $\mathcal{S}$ can effectively solve the $LWE_{n,Q,\chi}$ assumption, it follows that the IBE scheme discussed in this paper is secure under the IND-sID-CPA model. This completes the proof. □

3.4. Efficiency Analysis of Our IBE Scheme

We compared the parameters of the proposed IBE scheme with the most classic ABB10 scheme and another scheme with better parameters, focusing on critical parameters

such as the lattice dimension, the size of the master private key, the identity public key, and the ciphertext, the comparison results are presented in Table 1, where our scheme demonstrates improvements in all these key parameters. Additionally, we provide a set of instantiated parameters $(Q = 393216,\ p = 1536,\ q = 2^8, b = 16,\ n = 1024)$ to more intuitively compare the efficiency of the scheme. the comparison results are presented in Table 2.

Table 1. Primary Comparison of Parameters in Similar Schemes.

Scheme	Dimension	Master Private Key Size	Identity Public Key Size	Ciphertext Size
ABB10 [18]	$6n\log q$	$36n^2\log^2 q$	$18n^2\log q + n$	$2m + 1$
Fan [22]	$2n\log q$	$n^2\log^2 q$	$2n^2\log q + n$	$m + 1$
Ours	$n\log q + n\log_b q$	$n\log q \times n\ \log_b q$	$n^2\log q + n^2\log_b q + n$	$m + 1$

Table 2. Comparison of Instantiated Parameters.

Scheme	Dimension	Master Private Key Size	Identity Public Key Size	Ciphertext Size
ABB10 [18]	$48n$	$2304\ n^2$	$432n^2 + n$	$2m + 1$
Fan [22]	$16n$	$256n^2$	$48n^2 + n$	$m + 1$
Ours	$9.75n$	$14n^2$	$9.75n^2 + n$	$m + 1$

4. Modifed Identity-Based Encryption Scheme

In Section 3, we constructed a compact IBE scheme, but this scheme cannot be directly combined with the decomposition method to construct an MIBFHE scheme. The decomposition method requires the identity to be represented as a vector in the security proof, whereas in Section 3, our IBE scheme uses the FRD function to map the identity into a matrix form and incorporate it into the identity public key.

Therefore, before combining the foundational IBE scheme with the decomposition method, it is necessary to appropriately transform the foundational IBE scheme to ensure the security and correctness of the constructed MIBFHE scheme. Additionally, based on our observations, modifying the identity private key can cleverly utilize the trapdoor error to reduce the overall noise of the scheme.

4.1. Modifed IBE Construction

The parameters of the scheme are defined as follows: difine security parameter as λ, $n = n(\lambda)$, and Let $Q = p \cdot q$ represent the modulus, where p and q are both positive integers. $m_1 = n\log q$, $m = m_1 + n\omega$, $m' = m + 1$, and $\omega = \log_b q$. Let B_χ be the bounded error distribution $\chi = \chi(\lambda)$. Construct an gadget matrix $\mathbf{F} = \mathbf{I}_n \otimes \mathbf{f}^T \in \mathbb{Z}^{n\times n\omega}$, where $\mathbf{f}^T = p \cdot \left[1, b^1, b^2, \ldots, b^{\omega-1}\right] \in \mathbb{Z}_Q^{1\times\omega}$, $\mathbf{I}_n$ is an $n \times n$ identity matrix, and b is a small integer.

The IBE scheme constructed in this chapter consists of four parts: **IBE.Setup**, **IBE.Extract**, **IBE.Enc**, **IBE.Dec**.

(1) **IBE.Setup**(1^λ): Input the security parameter λ, choose $n = n(\lambda)$, and the error distribution $\chi = \chi(\lambda)$. Generate the basic parameters $Q = pq$, $m = m_1 + n\omega$. Uniformly select an invertible matrix $\mathbf{H} \xleftarrow{\$} \mathbb{Z}_Q^{n\times n}$, a uniformly random matrix $\overline{\mathbf{A}} \xleftarrow{\$} \mathbb{Z}_Q^{n\times m_1}$ and a collision-resistant hash function H: $\mathbb{Z}_Q^* \to \mathbb{Z}_Q^n$. Sample the trapdoor matrix $\mathbf{R} \leftarrow D_{R^{m_1\times n\omega},\sigma}$, generate a uniformly random matrix $\mathbf{A} = \left[\overline{\mathbf{A}} \parallel -\overline{\mathbf{A}}\mathbf{R}\right] \in \mathbb{Z}_Q^{n\times m}$, and provide the master public key $MPK = (\mathbf{A}, \mathbf{H})$ along with the master private key $MSK = \mathbf{R}$. For different identities, the matrix $\mathbf{A}$ remains unchanged.

(2) **IBE.Extract**(MPK, MSK, id): Provide the master public key MPK, the master private key MSK, and the user identity vector $id \in \mathbb{Z}_Q^*$ as input. Use the hash function $H : \mathbb{Z}_Q^* \to \mathbb{Z}_Q^n$ to map each user identity id into an identity vector $\mathbf{u}_{id} \in \mathbb{Z}_Q^n$. Let the user identity public key matrix be $\mathbf{A}_{id} = \mathbf{A} + [0 \parallel \mathbf{HG}] = \left[\mathbf{A} \parallel \mathbf{HF} - \overline{\mathbf{A}}\mathbf{R}\right] \in \mathbb{Z}_Q^{n \times m}$. For each different identity, the matrix $\mathbf{A}_{id}$ remains the same. Run **ApproxPreSample**$(\mathbf{A}_{id}, \mathbf{R}, \mathbf{u}_{id}, \sigma)$ to generate a sampling vector $\mathbf{t}_{id} \in \mathbb{Z}_Q^m$ that follows the discrete Gaussian distribution $\mathcal{D}_{\Lambda_Q^{\mathbf{u}}(\mathbf{A}_{id}),\sigma}$, satisfying $\mathbf{A}_{id}\mathbf{t}_{id} = \mathbf{u}_{id} - \mathbf{e}_{app} \ mod \ Q$. Let $\mathbf{A}'_{id} = [\mathbf{u}_{id} \parallel \mathbf{A}_{id}] \in \mathbb{Z}_Q^{n \times m'}$ and output the private key corresponding to each user id as $\mathbf{sk}_{id} = (-1, \mathbf{t}_{id}) \in \mathbb{Z}_Q^{m'}$, satisfying $\mathbf{A}'_{id}\mathbf{sk}_{id} = -\mathbf{e}_{app} \ mod \ Q$.

(3) **IBE.Enc**(MPK, id, msg): Input MPK, the user identity id and a message $msg \in \{0,1\}$ to be encrypted. Let the vector $\bar{\mathbf{v}} = \left(msg\frac{Q}{2}, 0, \ldots, 0\right) \in \mathbb{Z}_Q^{m' \times 1}$. Uniformly select a vector $\mathbf{y} \xleftarrow{\$} \{0,1\}^{n \times 1}$, and uniformly select an error vector $\mathbf{e} \xleftarrow{\$} \chi_{\Psi_\alpha}^{m' \times 1}$, such that $\|\mathbf{e}\| < B_\chi$. Output the ciphertext vector

$$\mathbf{c}_{id} = \mathbf{A}_{id}^{'T}\mathbf{y} + \bar{\mathbf{v}} + \mathbf{e} \in \mathbb{Z}_Q^{m' \times 1}.$$

(4) **IBE.Dec**$(MPK, \mathbf{sk}_{id}, \mathbf{c}_{id})$: Input MPK, the private key $\mathbf{sk}_{id}$ under identity id, and the ciphertext $\mathbf{c}_{id}$ under identity id. Set $msg' = sk_{id}^T \cdot c_{id} \in \mathbb{Z}_Q$, Calculate

$$\begin{aligned}\mathbf{sk}_{id}^T \cdot \mathbf{c}_{id} &= \mathbf{sk}_{id}^T\left(\mathbf{A}_{id}^{'T}\mathbf{y} + \bar{\mathbf{v}} + \mathbf{e}\right) \\ &= \mathbf{sk}_{id}^T\mathbf{A}_{id}^{'T}\mathbf{y} + \left\langle \mathbf{sk}_{id}^T, \bar{\mathbf{v}} \right\rangle + \left\langle \mathbf{sk}_{id}^T, \mathbf{e} \right\rangle \\ &= -\mathbf{e}_{app}\mathbf{y} + msg\left\lfloor \frac{Q}{2} \right\rfloor + \left\langle \mathbf{sk}_{id}^T, \mathbf{e} \right\rangle\end{aligned}$$

If $\left|\left|msg' - \left|\frac{Q}{2}\right|\right|\right| < \left|\frac{Q}{4}\right|$, let $msg = 1$; if $\left|\left|msg'\right|\right| < \left|\frac{Q}{4}\right|$, let $msg = 0$. Output $msg = 1$.

4.2. Parameters, Security Analysis, And Effciency Analysis

In the aforementioned improved IBE scheme, we introduce a collision-resistant hash function $H : Z_q^* \to Z_q^n$ and reconstruct the public key $\mathbf{A}_{id}^{'}$, thereby modifying the relationship between the identity public key and the identity vector. Since our extended method eliminates the need for the eigenvector approach to transform the IBE scheme into the IBFHE scheme, the identity private key vector no longer requires its first component to be 1. Instead, we redefine the identity key as $(-1, \mathbf{sk}_{id})$. This change allows the approximation error from the approximate trapdoor in our improved IBE scheme to partially cancel out the decryption noise, effectively reducing the scheme's overall noise. The noise size of the modified IBE scheme is given as follows:

$$||\beta_{IBE}|| = \left|\left|\left\langle \mathbf{sk}_{id}^T, \mathbf{e} \right\rangle - \mathbf{e}_{app}\mathbf{y}\right|\right| \leq ||\mathbf{sk}_{id}\mathbf{e}|| - ||\mathbf{e}_{app}\mathbf{y}||.$$

Clearly, the noise in the modified IBE scheme is smaller than that in the basic IBE scheme, enabling the modified scheme to perform correct decryption. The reduced noise allows the MIBFHE scheme in Section 5 to support more homomorphic operations. Other parameter choices remain the same as those in the IBE scheme presented in Section 3.

5. Multi-Identity Full Homomorphic Encryption Scheme

In Section 4, we proposed a modified IBE scheme suited solely for single-identity scenarios, where ciphertexts encrypted under different identities are unable to directly engage in homomorphic operations with one another. To overcome this limitation, in this section,

we build upon the improved IBE scheme from Section 4 and apply the decomposition method [28] for ciphertext extension, resulting in an MIBFHE scheme that does not require fresh ciphertexts.We refer to this scheme as WZ-MIBFHE.

5.1. The Decomposition Method

Previous MIBFHE schemes required the IBFHE encryption algorithm to generate fresh ciphertexts for homomorphic operations. These fresh ciphertexts were then extended using the Mask System technique to produce extended ciphertexts that support multi-identity operations.In contrast, the decomposition method can directly extend the ciphertexts of the IBE scheme into extended ciphertexts that support multi-identity homomorphic operations, eliminating the need for the intermediate step of generating fresh ciphertexts.

Before introducing the decomposition method, we will briefly outline the ciphertext extension approach using the Mask System. Assume there are $(D = 2)$ participants, and any number of participants D can be analogously processed using this method. Suppose in the IBFHE scheme, under participant identities id_1 and id_2 the fresh ciphertexts $\mathbf{C}_1$ and $\mathbf{C}_2$ are obtained by encrypting plaintext bit messages msg_1 and msg_2 , respectively. Here, identities id_1 and id_2 correspond to private keys $\mathbf{sk}_1$ and $\mathbf{sk}_2$, which satisfy $\mathbf{sk}_1^T\mathbf{C}_1 = msg_1\mathbf{sk}_1^T\mathbf{M} + \mathbf{e}_1$ and $\mathbf{sk}_2^T\mathbf{C}_2 = msg_2\mathbf{sk}_2^T\mathbf{M} + \mathbf{e}_2$ and $\mathbf{M}$ represents the preimage matrix, satisfying $\mathbf{M}\mathbf{M}^{-1}(\mathbf{A}) = \mathbf{A}$. By expanding the ciphertexts $\mathbf{C}_1, \mathbf{C}_2 \in \mathbb{Z}_Q^{m^{'} \times N}$ according to the number of participants D, they become extended ciphertexts $\hat{\mathbf{C}}_1, \hat{\mathbf{C}}_2 \in \mathbb{Z}_Q^{2m^{'} \times 2N}$, satisfying

$$\left[\mathbf{sk}_1^T, \mathbf{sk}_2^T\right]\hat{\mathbf{C}}_1 = msg_1\left[\mathbf{sk}_1^T, \mathbf{sk}_2^T\right]\begin{bmatrix}\mathbf{M} & 0\\ 0 & \mathbf{M}\end{bmatrix} + \text{error},$$

$$\left[\mathbf{sk}_1^T, \mathbf{sk}_2^T\right]\hat{\mathbf{C}}_2 = msg_2\left[\mathbf{sk}_1^T, \mathbf{sk}_2^T\right]\begin{bmatrix}\mathbf{M} & 0\\ 0 & \mathbf{M}\end{bmatrix} + \text{error}.$$

The general method for converting a IBFHE scheme into a MIBFHE scheme involves expanding the ciphertext matrix, originally encrypted under a single identity, into a general matrix with dimensions $Dm^{'} \times DN$, where $N = m^{'} \log q$. In this way, the extended ciphertexts $\hat{\mathbf{C}}_1$ and $\hat{\mathbf{C}}_2$ corresponding to id_1 and id_2, respectively, both have dimensions $2m^{'} \times 2N$. Homomorphic operations can be performed by inputting $\hat{\mathbf{C}}_1$ and $\hat{\mathbf{C}}_2$ into a binary logic circuit f. Previous MIBFHE schemes required the IBFHE encryption algorithm to generate fresh ciphertexts $\mathbf{C}$ for homomorphic operations. These fresh ciphertexts were then extended using the Mask System technique to produce extended ciphertexts $\hat{\mathbf{C}}$ that support multi-identity operations.

Next, we describe using the decomposition method to extend ciphertexts. First, we restructure the form of the extended ciphertext and decompose the new ciphertext into two parts. The new ciphertext can be defined as: $\mathbf{C} = \mathbf{A}\mathbf{R} + msg\mathbf{F}_n$. The first part is a combination of the public key matrix $\mathbf{A}$ and the trapdoor $\mathbf{R}$, and the second part is a combination of the plaintext msg and the public matrix $\mathbf{F}$. With this ciphertext form, the second part of the new ciphertext can be directly extended during decryption. The method of ciphertext extension is no longer to extend the entire ciphertext $\mathbf{C} \to \hat{\mathbf{C}}$, but to extend the first and second parts of the ciphertext separately. Adding these two parts together naturally gives us the extended ciphertext we desire. Moreover, the MIBFHE scheme constructed using the decomposition method can directly generate extended ciphertexts that are executable for homomorphic operations without the need to generate new ciphertexts, making the scheme more concise and reducing the operations that users need to perform.

We will better explain the decomposition method through the following example. Consider the case of two users, where user $i = \{1, 2\}$. The ciphertext $\mathbf{C}_i = \mathbf{A}_i\mathbf{R}_i + msg_i\mathbf{G}_n \in$

$\mathbb{Z}_q^{n\times m}$ is the fresh ciphertext. Let $\hat{\mathbf{sk}}_{1,2} = (\mathbf{sk}_1, \mathbf{sk}_2)$ be the concatenation of the two keys. Using the decomposition method, the extended ciphertext is constructed in the following two steps:

(1) Construct $\mathbf{X}_i$, such that $\mathbf{X}_i$ satisfies $\hat{\mathbf{sk}}_{1,2} \cdot \mathbf{X}_i = \hat{\mathbf{e}}_{1,2} \in \mathbb{Z}_Q^{2m}$;

(2) Construct $\mathbf{Y}_i$, such that $\mathbf{Y}_i = msg_i\mathbf{F}_{2n}$ and satisfies $\hat{\mathbf{sk}}_{1,2} \cdot \mathbf{Y}_i = msg_i\hat{\mathbf{sk}}_{1,2}\mathbf{F}_{2n} \in \mathbb{Z}_Q^{2m}$.

Compared to traditional ciphertext extension methods, the new ciphertext produced by the decomposition method is no longer just a part of the extended ciphertext. The newly generated ciphertext can directly perform homomorphic operations. The overall scheme does not require generating new ciphertexts, allowing users to execute fewer operations, making the scheme more concise.

5.2. Our MIBFHE Construction

The WZ-MIBFHE scheme is composed of five components: **MIBFHE**.**Setup**, **MIBFHE**.**Extract**, **MIBFHE**.**Enc**, **MIBFHE**.**Eval**, and **MIBFHE**.**Dec**.

The basic parameters of the scheme are defined as follows: Let λ be the security parameter, $Q = pq$ be the modulus, $m = O(n\log q)$, $\mathbf{A} \in \mathbb{Z}_Q^{n\times m}$ be a uniformly random matrix, and $\mathbf{R} \in \mathbb{Z}^{m_1\times n\omega}$ be its trapdoor, where $m_1 = n\log q$ and $m = m_1 + n\omega$. Construct a gadget matrix $\mathbf{F} = \mathbf{I}_n \otimes \mathbf{f}^T \in \mathbb{Z}^{n\times n\omega}$ where $\mathbf{f}^T = p \cdot \left[1, b^1, b^2, \ldots, b^{\omega-1}\right] \in \mathbb{Z}_Q^{1\times\omega}$, $\mathbf{I}_n$ is an $n \times n$ identity matrix, and $\omega = \log_b q$. Let $m' = m + 1$.

(1) **MIBFHE**.**Setup**$\left(1^\lambda, 1^L, 1^D\right)$: Takes as input the security parameter λ, the maximum circuit depth L for homomorphic operations, and the maximum number of users D allowed in the scheme. Execute **IBE**.**Setup** and output $MPK = (\mathbf{A}, \mathbf{H})$ and $MSK = \mathbf{R}$.

(2) **MIBFHE**.**Extract**$(MPK, MSK, [id_i])$: Input MPK, MSK, and $[id_i]_{i\in[D]} \in \mathbb{Z}_Q^{n\times 1}$. Run **IBE**.**Extract** to sequentially generate the private keys $\mathbf{sk}_{id_1}, \ldots, \mathbf{sk}_{id_D}$ corresponding to the identities $id_1, \ldots, id_D$, and the corresponding identity public key matrices $\mathbf{A}'_{id_1}, \ldots, \mathbf{A}'_{id_D}$. Output the private keys set $\left\{\mathbf{sk}_{id_i}\right\}_{i\in[D]}$ and the identity public key matrices set $\left\{\mathbf{A}'_{id_i}\right\}_{i\in[D]}$.

(3) **MIBFHE**.**Enc**$(MPK, \{id_i\}, msg)$: Input MPK, the user identity vectors $\{id_i\}_{i\in[D]}$, and the plaintext $msg \in \{0,1\}$. Let $\hat{\mathbf{sk}}_{id} = \left(\mathbf{sk}_{id_1}, \ldots, \mathbf{sk}_{id_D}\right) \in \mathbb{Z}_Q^{Dm'}$ be the concatenation of the private keys corresponding to the D identities. Select a series of matrices to compute the extended ciphertext $\hat{\mathbf{C}}_{id_i} = \mathbf{X}_{id_i} + \mathbf{Y}_{id_i} \in \mathbb{Z}_q^{D(m\times 1)\times D(m\times 1)\omega}$. First, compute $\mathbf{X}_{id_i}$:

$$\mathbf{X}_{id_i} = \begin{bmatrix} \mathbf{A}_{id_i}\overset{\sim}{\mathbf{M}}_i^1 & & \cdots & & 0 \\ \vdots & \ddots & & & \\ \mathbf{A}_{id_i}\overset{\sim}{\mathbf{M}}_i^1 & \cdots & \mathbf{A}_{id_i}\overset{\sim}{\mathbf{M}}_i^i & \cdots & \mathbf{A}_{id_i}\overset{\sim}{\mathbf{M}}_i^D \\ \vdots & & & \ddots & \\ 0 & & 0 & & \mathbf{A}_{id_i}\overset{\sim}{\mathbf{M}}_i^D \end{bmatrix} \tag{1}$$

where $\left(\overset{\sim}{\mathbf{M}}_i^1, \overset{\sim}{\mathbf{M}}_i^2, \cdots, \overset{\sim}{\mathbf{M}}_i^D\right) \in \{0,1\}^{n\times m'\omega}$ are random matrices. Compute:

$$\begin{aligned} \mathbf{sk}_{id_i}\mathbf{A}'_{id_j} + \mathbf{sk}_{id_j}\mathbf{A}'_{id_i} &= \left(-1, \mathbf{t}_{id_i}^T\right)\begin{pmatrix}\mathbf{u}_{id_j}^T \\ \mathbf{A}^T\end{pmatrix} + \left(-1, \mathbf{t}_{id_j}^T\right)\begin{pmatrix}\mathbf{u}_{id_i}^T \\ \mathbf{A}^T\end{pmatrix} \\ &= \mathbf{u}_{id_j}^T - \mathbf{t}_{id_i}^T\mathbf{A}^T + \mathbf{u}_{id_i}^T - \mathbf{t}_{id_j}^T\mathbf{A}^T \\ &= -\mathbf{e}_{app_i} - \mathbf{e}_{app_j}; \end{aligned}$$

And accordingly to Formula (1):

$$\hat{\mathbf{sk}}_{id}\mathbf{X}_{id_i} = \left(\mathbf{sk}_{id_1}, \mathbf{sk}_{id_2}, \cdots, \mathbf{sk}_{id_D}\right)\mathbf{X}_{id_i} = -\hat{\mathbf{e}}_{app_i}^{Dm'\omega}.$$

To construct $\mathbf{Y}_{id_i}$, we define

$$\begin{aligned}\mathbf{Y}_{id_i} &= msg_i\mathbf{F}_{Dm'} + \mathbf{E}_{id_i} \\ &= msg_i\left(\mathbf{I}_{Dm'} \otimes \mathbf{f}\right) + \mathbf{E}_{id_i} \\ &= msg_i\begin{pmatrix} \mathbf{G}_{m'} & \cdots & 0^{m'\times m'\omega} \\ \vdots & \ddots & \vdots \\ 0^{m'\times m'\omega} & \cdots & \mathbf{G}_{m'} \end{pmatrix}_{D\times D} + \mathbf{E}_{id_i}\end{aligned} \tag{2}$$

where the error matrix $\mathbf{E}_{id_i} \leftarrow \chi^{Dm'\times Dm'\omega}$. Then,

$$\hat{\mathbf{sk}}_{id}\mathbf{Y}_{id_i} = msg_i\hat{\mathbf{sk}}_{id}\mathbf{F}_{Dm'} + \hat{\mathbf{sk}}_{id}\mathbf{E}_{id_i}$$

Now that we have completed the generation and extension of the ciphertext, accordingly to Formulas (1) and (2), $\hat{\mathbf{C}}_{id_i}$ can be described as:

$$\begin{aligned}\hat{\mathbf{C}}_{id_i} &= \mathbf{X}_{id_i} + \mathbf{Y}_{id_i} \\ &= \begin{bmatrix} \mathbf{A}_{id_i}\overset{\sim 1}{\mathbf{M}}_i & & \cdots & & 0 \\ \vdots & \ddots & & & \\ \mathbf{A}_{id_i}\overset{\sim 1}{\mathbf{M}}_i & \cdots & \mathbf{A}_{id_i}\overset{\sim i}{\mathbf{M}}_i & \cdots & \mathbf{A}_{id_i}\overset{\sim D}{\mathbf{M}}_i \\ \vdots & & & \ddots & \\ 0 & & 0 & & \mathbf{A}_{id_i}\overset{\sim D}{\mathbf{M}}_i \end{bmatrix} + msg_i\mathbf{G}_{Dm'} + \mathbf{E}_{id_i}\end{aligned}$$

Then,

$$\hat{\mathbf{sk}}_{id}\hat{\mathbf{C}}_{id_i} = \hat{\mathbf{sk}}_{id}\mathbf{X}_{id_i} + \hat{\mathbf{sk}}_{id}\mathbf{Y}_{id_i} = -\hat{\mathbf{e}}_{app_i} + msg_i\hat{\mathbf{sk}}_{id}\mathbf{G}_{Dm'} + \hat{\mathbf{sk}}_{id}\mathbf{E}_{id_i}.$$

(4) **MIBFHE.Eval**$\left(MPK, \left(\hat{\mathbf{C}}_{id_1}, \cdots, \hat{\mathbf{C}}_{id_D}\right), f\right)$: Input MPK, a Boolean circuit f, and the number of identities D involved in the computation supported by the scheme. Output the ciphertext $\hat{\mathbf{C}}_{eval}$ after homomorphic evaluation. The above ciphertexts are of the GSW type, and the homomorphic operations are similar to those in the GSW scheme. The definitions for homomorphic addition, multiplication, and NAND operations are as follows:

$$\begin{aligned}\text{GSW.Add}\left(\hat{\mathbf{C}}_{id_1}, \hat{\mathbf{C}}_{id_2}\right) &= \hat{\mathbf{C}}_{id_1} + \hat{\mathbf{C}}_{id_2} \\ &= \left(\mathbf{X}_{id_1} + \mathbf{X}_{id_2}\right) + \left(\mathbf{Y}_{id_1} + \mathbf{Y}_{id_2}\right) \\ &= \left(\mathbf{X}_{id_1} + \mathbf{X}_{id_2}\right) + \left(msg_1 + msg_2\right)\mathbf{G}_{Dm'} \in \mathbb{Z}_q^{Dn\times Dn\omega}\end{aligned}$$

$$\begin{aligned}\text{GSW.Multi}\left(\hat{\mathbf{C}}_{id_1}, \hat{\mathbf{C}}_{id_2}\right) &= \hat{\mathbf{C}}_{id_1} \cdot \mathbf{G}_{Dm'}^{-1}\left(\hat{\mathbf{C}}_{id_2}\right) \\ &= \left(\mathbf{X}_{id_1} + msg_1\mathbf{G}_{Dm'}\right) + \mathbf{E}_{id_1} \cdot \mathbf{G}_{Dm'}^{-1}\left(\hat{\mathbf{C}}_{id_2}\right) \\ &= \left(\mathbf{X}_{id_1} + \mathbf{E}_{id_1}\right) \cdot \mathbf{G}_{Dm'}^{-1}\left(\hat{\mathbf{C}}_{id_2}\right) + msg_1\left(\mathbf{X}_{id_2} + msg_2\mathbf{G}_{Dm'} + \mathbf{E}_{id_2}\right) \\ &= msg_1msg_2\mathbf{G}_{Dm'} + \left(\mathbf{X}_{id_1} + \mathbf{E}_{id_1}\right) \cdot \mathbf{G}_{Dm'}^{-1}\left(\hat{\mathbf{C}}_{id_2}\right) + msg_1\left(\mathbf{X}_{id_2} + \mathbf{E}_{id_2}\right)\end{aligned}$$

$$\begin{aligned}\text{GSW.NAND}\left(\hat{\mathbf{C}}_{id_1}, \hat{\mathbf{C}}_{id_2}\right) &= \mathbf{G}_{Dm'} - \hat{\mathbf{C}}_{id_1} \cdot \mathbf{G}_{Dm'}^{-1}\left(\hat{\mathbf{C}}_{id_2}\right) \\ &= \left(1 - msg_1msg_2\right)\mathbf{G}_{Dm'} - \left(\mathbf{X}_{id_1}\mathbf{G}_{Dm'}^{-1}\left(\hat{\mathbf{C}}_{id_2}\right) + msg_1\mathbf{X}_{id_2}\right)\end{aligned}$$

In our scheme, the homomorphic operations are as follows:
Homomorphic Addition $\hat{\mathbf{t}}\hat{\mathbf{C}}^{+}$:

$$\begin{aligned}\hat{\mathbf{t}}\hat{\mathbf{C}}^{+} &= \hat{\mathbf{t}}(\hat{\mathbf{C}}_{id_1} + \hat{\mathbf{C}}_{id_2}) \\ &= \hat{\mathbf{t}}(\mathbf{X}_{id_1} + \mathbf{X}_{id_2}) + (msg_1 + msg_2)\hat{\mathbf{t}}\mathbf{G}_{Dm'} \\ &= (msg_1 + msg_2)\hat{\mathbf{t}}\mathbf{G}_{Dm'} - (\hat{\mathbf{e}}_{app_1} + \hat{\mathbf{e}}_{app_2})\end{aligned}$$

Homomorphic Multiplication $\hat{\mathbf{t}}\hat{\mathbf{C}}^{\times}$:

$$\begin{aligned}\hat{\mathbf{t}}\hat{\mathbf{C}}^{\times} &= \hat{\mathbf{t}}\hat{\mathbf{C}}_{id_1} \cdot \mathbf{G}^{-1}_{Dm'}(\hat{\mathbf{C}}_{id_2}) \\ &= \hat{\mathbf{t}}\left(\mathbf{X}_{id_1}\mathbf{G}^{-1}_{Dm'}(\hat{\mathbf{C}}_{id_2}) + msg_1\mathbf{X}_{id_2}\right) + msg_1 msg_2\hat{\mathbf{t}}\mathbf{G}_{Dm'} \\ &= msg_1 msg_2\hat{\mathbf{t}}\mathbf{G}_{Dm'} - \left(\hat{\mathbf{e}}_{app_1}\mathbf{G}^{-1}_{Dm'}(\hat{\mathbf{C}}_{id_2}) + msg_1\hat{\mathbf{e}}_{app_2}\right)\end{aligned}$$

Homomorphic NAND $\hat{\mathbf{t}}\hat{\mathbf{C}}^{NAND}$:

$$\begin{aligned}\hat{\mathbf{t}}\hat{\mathbf{C}}^{NAND} &= (1 - msg_1 msg_2)\hat{\mathbf{t}}\mathbf{G}_{Dm'} - \hat{\mathbf{t}}\left(\mathbf{X}_{id_1}\mathbf{G}^{-1}_{Dm'}(\hat{\mathbf{C}}_{id_2}) + msg_1\mathbf{X}_{id_2}\right) \\ &= (1 - msg_1 msg_2)\hat{\mathbf{t}}\mathbf{G}_{Dm'} - \left(\hat{\mathbf{e}}_{app_1}\mathbf{G}^{-1}_{Dm'}(\hat{\mathbf{C}}_{id_2}) + msg_1\hat{\mathbf{e}}_{app_2}\right)\end{aligned}$$

(5) **MIBFHE.Dec**$\left(MPK, \hat{\mathbf{sk}}_{id}, \hat{\mathbf{C}}_{id_i}\right)$: Input MPK, the concatenation of D keys $\hat{\mathbf{sk}}_{id}$, and the extended ciphertext $\hat{\mathbf{C}}_{id_i}$. Set the vector $\widetilde{\mathbf{v}} = \left(msg \cdot \left\lceil \frac{Q}{2} \right\rfloor, 0, \cdots, 0\right)^T \in \mathbb{Z}_Q^{Dm'}$, and compute:

$$\begin{aligned}msg' &= \hat{\mathbf{sk}}_{id}\hat{\mathbf{C}}_{id_i}\mathbf{G}^{-1}_{Dm'}\left(\widetilde{\mathbf{v}}\right) \\ &= \left(\hat{\mathbf{e}}_{app} + msg_i\hat{\mathbf{sk}}_{id}\mathbf{G}_{Dm'} + \hat{\mathbf{sk}}_{id}\mathbf{E}_{id_i}\right) \cdot \mathbf{G}^{-1}_{Dm'}\left(\widetilde{\mathbf{v}}\right) \\ &= msg\left\langle \hat{\mathbf{sk}}_{id}, \widetilde{\mathbf{v}} \right\rangle + \hat{\mathbf{sk}}_{id}\mathbf{E}_{id_i}\mathbf{G}^{-1}_{Dm'}\left(\widetilde{\mathbf{v}}\right) \\ &= msg \cdot \left\lceil \frac{Q}{2} \right\rfloor + \left(\hat{\mathbf{sk}}_{id}\mathbf{E}_{id_i} - \hat{\mathbf{e}}_{app}\right)\mathbf{G}^{-1}_{Dm'}\left(\widetilde{\mathbf{v}}\right)\end{aligned}$$

If $\left\| msg' - \left\lceil \frac{Q}{2} \right\rfloor \right\| \leq \frac{Q}{4}$, output $msg' = 1$. If $\left\| msg' \right\| \leq \frac{Q}{4}$, output $msg' = 0$.

5.3. Correctness and Parameters

During the encryption phase, the ciphertext is extended to $\hat{\mathbf{C}}_{id_i}$, and the noise term $\widetilde{\beta}_{enc} = \hat{\mathbf{sk}}_{id}\mathbf{E}_{id_i} - \hat{\mathbf{e}}_{app}$ is calculated, where $\left\|\mathbf{E}_{id_i}\right\| \leq B_\chi$. We compute:

$$\left\|\widetilde{\beta}_{enc}\right\| = \left\|\hat{\mathbf{sk}}_{id}\mathbf{E}_{id_i} - \hat{\mathbf{e}}_{app}\right\| \leq \left\|\hat{\mathbf{sk}}_{id}\mathbf{E}_{id_i}\right\| - \left\|\hat{\mathbf{e}}_{app}\right\| = DB_\chi\left(m'\right) - p,$$

so the noise level of the ciphertext $\hat{\mathbf{C}}_{id_i}$ is $DB_\chi\left(m'\right) - p$. We refer to $\hat{\mathbf{C}}_{id_i}$ as a ciphertext with noise level $DB_\chi\left(m'\right) - p$.

During the homomorphic computation phase, the noise generated by homomorphic multiplication is the largest, so we mainly analyze the noise of homomorphic multiplication. The computation process of homomorphic multiplication is as follows:

$$\begin{aligned}\mathrm{GSW.Multi}\left(\hat{\mathbf{C}}_{id_1}, \hat{\mathbf{C}}_{id_2}\right) &= \hat{\mathbf{C}}_{id_1} \cdot \mathbf{G}_{Dm'}^{-1}\left(\hat{\mathbf{C}}_{id_2}\right) \\ &= \left(\mathbf{X}_{id_1} + msg_1\mathbf{G}_{Dm'} + \mathbf{E}_{id_1}\right) \cdot \mathbf{G}_{Dm'}^{-1}\left(\hat{\mathbf{C}}_{id_2}\right) \\ &= \left(\mathbf{X}_{id_1} + \mathbf{E}_{id_1}\right) \cdot \mathbf{G}_{Dm'}^{-1}\left(\hat{\mathbf{C}}_{id_2}\right) \quad + msg_1\left(\mathbf{X}_{id_2} + msg_2\mathbf{G}_{Dm'} + \mathbf{E}_{id_2}\right) \\ &= msg_1 msg_2\mathbf{G}_{Dm'} \quad + \left(\mathbf{X}_{id_1} + \mathbf{E}_{id_1}\right) \cdot \mathbf{G}_{Dm'}^{-1}\left(\hat{\mathbf{C}}_{id_2}\right) \quad + msg_1\left(\mathbf{X}_{id_2} + \mathbf{E}_{id_2}\right).\end{aligned}$$

Thus, we have:

$$\begin{aligned}\hat{\mathbf{sk}}_{id}\hat{\mathbf{C}}_{id}^{\times} &= \hat{\mathbf{sk}}_{id}\hat{\mathbf{C}}_{id_1}^{\times} \cdot \mathbf{G}_{Dm'}^{-1}\left(\hat{\mathbf{C}}_{id_2}\right) \\ &= msg_1 msg_2\hat{\mathbf{sk}}_{id}\mathbf{G}_{Dm'} \quad + \left(\hat{\mathbf{e}}_{app_1} + \hat{\mathbf{sk}}_{id}\mathbf{E}_{id_1}\mathbf{G}_{Dm'}^{-1}\right)\left(\hat{\mathbf{C}}_{id_2}\right) \\ &\quad + msg_1\left(-\hat{\mathbf{e}}_{app_2} + \hat{\mathbf{sk}}_{id}\mathbf{E}_{id_2}\right).\end{aligned}$$

Then, the homomorphic computation error is

$$\widetilde{\beta}_{eval} = \left(-\hat{\mathbf{e}}_{app_1} + \hat{\mathbf{sk}}_{id}\mathbf{E}_{id_1}\mathbf{G}_{Km'}^{-1}\right)\left(\hat{\mathbf{C}}_{id_2}\right) + msg_1\left(-\hat{\mathbf{e}}_{app_2} + \hat{\mathbf{sk}}_{id}\mathbf{E}_{id_2}\right)$$

Based on the analysis of circuit noise growth, with error control under correct decryption conditions, we can infer the upper bounds on the circuit computation depth L and the number of users D involved in the computation.

$$\left\|\widetilde{\beta}_{eval}\right\| = \left\|\left(-\hat{\mathbf{e}}_{app_1} + \hat{\mathbf{sk}}_{id}\mathbf{E}_{id_1}\mathbf{G}_{Dm'}^{-1}\right)\left(\hat{\mathbf{C}}_{id_2}\right) + msg_1\left(-\hat{\mathbf{e}}_{app_2} + \hat{\mathbf{sk}}_{id}\mathbf{E}_{id_2}\right)\right\| \leq D^2\left(B_\chi \cdot \omega \cdot m' - p\right)$$

The final error is:

$$\left\|\widetilde{\beta}_{eval}\right\| \leq D^{2^L}\left(B_\chi \cdot \omega \cdot m' - p\right) \tag{3}$$

When the noise is less than $\frac{Q}{4}$, the decryption algorithm can correctly decrypt. Therefore, by selecting $Q \geq D^{2^L}(B_\chi \cdot \omega \cdot m' - p)$, the WZ-MIBFHE scheme can correctly decrypt.

5.4. Security Analysis

Theorem 3. *Under the assumption that the $LWE_{\lambda,Q,\chi}$ assumption is hard, the WZ-MIBFHE scheme is IND-sID-CPA secure.*

Proof of Theorem 3. The security of the WZ-MIBFHE scheme is established through an IND-sID-CPA game played between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$. The proof proceeds as follows:

Suppose the adversary $\mathcal{A}$ targets the identity id^*, and let $Adv[i]$ represent the adversary's advantage in game i.

Game 0: The standard IND-sID-CPA game in the WZ-MIBFHE scheme is conducted between the adversary $\mathcal{A}$ and the challenger $\mathcal{C}$.

Game 1: The adversary $\mathcal{A}$ declares the target identity id^*. Compared to Game 0, the challenger $\mathcal{C}$ changes the way the MPK matrix $\mathbf{A}$ is generated in Game 1. A uniformly random matrix $\mathbf{A}''$ is generated, and $MPK = (\mathbf{A}'', \mathbf{H})$. According to Lemma 3, for the adversary $\mathcal{A}$, the matrix $\mathbf{A}$ in Game 0 is statistically indistinguishable from the matrix $\mathbf{A}''$ in Game 1. Therefore, the advantage of the adversary $\mathcal{A}$ in distinguishing Game 1 from Game 0 is negligible.

Game 2: Compared to Game 1, the challenger $\mathcal{C}$ changes the way public and private keys are generated in Game 2. In Game 2, a public matrix $\mathbf{F}$ and a trapdoor matrix $\mathbf{R}$ of

the lattice $\Lambda_Q^{\perp}(\mathbf{F})$ are generated. The adversary $\mathcal{A}$ sends a set of identities $\{id_\alpha\}_{\alpha\in \mathrm{poly}(\lambda)}$ to the challenger $\mathcal{C}$ for hash queries. The challenger $\mathcal{C}$ chooses a uniformly random vector $\mathbf{u}''_{id_\alpha}$ and sets $\mathbf{A}''_{id_\alpha} = \left[\mathbf{u}''_{id_\alpha} \middle|\middle| \mathbf{A}''\right]$. If the identity $id^* \in \{id_\alpha\}_{\alpha\in \mathrm{poly}(\lambda)}$, the game terminates. Otherwise, the challenger $\mathcal{C}$ runs $\mathbf{ApproxPreSamp}(\mathbf{A}''_{id_\alpha}, \mathbf{R}, \mathbf{u}''_{id_\alpha}, \sigma)$ to generate $\mathbf{t}''_{id_\alpha}$, which satisfies $\mathbf{A}''_{id_\alpha} \cdot \mathbf{t}''_{id_\alpha} = \mathbf{u}''_{id_\alpha} - \mathbf{e}_{app}\ mod\ Q$. Set $\mathbf{sk}''_{id_\alpha} = (-1, \mathbf{t}''_{id_\alpha})$ and return it to the adversary $\mathcal{A}$. The challenger $\mathcal{C}$ ensures that $(id_\alpha, \mathbf{u}''_{id_\alpha}, \mathbf{t}''_{id_\alpha}) \in$ store is stored. Therefore, for the same identity id, the adversary $\mathcal{A}$ receives the same result for each query. Thus, the public and private keys in Game 2 and Game 1 are statistically indistinguishable. Consequently, the adversary $\mathcal{A}$ is unable to differentiate between Game 2 and Game 1 within polynomial time with any significant advantage, i.e.,

$$|\mathrm{Adv}[2] - \mathrm{Adv}[1]| = \mathrm{negl}(\lambda)$$

Game 3: The adversary $\mathcal{A}$ chooses a pair of messages (msg_0, msg_1) for the challenger $\mathcal{C}$. The challenger $\mathcal{C}$ generates extended ciphertexts in Game 3 differently than in Game 2. The challenger $\mathcal{C}$ chooses a uniformly random matrix $\hat{\mathbf{P}} \in \mathbb{Z}_Q^{Dm'\times Dm'\omega}$ and $\hat{\mathbf{E}} \in \mathbb{Z}_Q^{Dm'\times Dm'\omega}$, generating the ciphertext $\hat{\mathbf{C}}_{id^*} = \hat{\mathbf{P}} + msg_r\mathbf{G}_{Dm'} + \hat{\mathbf{E}}$ for the message msg_r, where $r \in \{0,1\}$, and sends the extended ciphertext $\hat{\mathbf{C}}_{id^*}$ to the adversary $\mathcal{A}$.

Lemma 5 ([25]). *Assuming the parameters satisfy the $LWE_{\lambda,Q,\chi}$ hypothesis. For the above generated $m = O(n\omega)$ and $(\mathbf{A}, \mathbf{AM})$, the joint distribution $(\mathbf{A}, \mathbf{AM})$ is computationally indistinguishable from a uniform distribution over $Z_Q^{n\times m} \times Z_Q^{n\times m}$.*

Analyzing the structure of $\mathbf{X}_i$, we observe that the diagonal elements $\left(\mathbf{A_i}\mathbf{M_i}^1, \mathbf{A_i}\mathbf{M_i}^2, \ldots, \mathbf{A_i}\mathbf{M_i}^D\right)$ and the elements $\left(\mathbf{A}_1\mathbf{M_i}^1, \mathbf{A}_2\mathbf{M_i}^2, \ldots, \mathbf{A}_D\mathbf{M_i}^D\right)$ are both suitable for Lemma 5. Given that the remaining elements of $\mathbf{X}_i$ are zero, we can conclude that $\mathbf{X}_i$ and $\mathbf{P}$ are computationally indistinguishable. Thus,

$$|Adv[3] - Adv[2]| = negl(\lambda)$$

Based on the above analysis, in WZ-MIBFHE scheme, the advantage of the adversary $\mathcal{A}$ is negligible within polynomial time, and the security is based on the $LWE_{\lambda,Q,\chi}$ hypothesis. The proof is complete. □

5.5. Efficiency Analysis of Ours MIBFHE SCHEME

We compare the existing MIBFHE schemes with the WZ-MIBFHE scheme, focusing on two main aspects: scheme attributes and scheme parameters. The results are shown in Tables 3 and 4.

According to Equation (3), the overall error of the scheme after L homomorphic operations for D identities is

$$\left\|\widetilde{\beta}_{eval}\right\| \leq D^{2^L}\left(B_\chi \cdot \omega \cdot m' - p\right)$$

Since the number of user participation D is known, according to this formula we need to choose the parameters rigorously to ensure the decryption correctness of the scheme. Based on Tables 3 and 4, The IBE architecture of WZ-MIBFHE and the IBE architecture from [22] are both based on ABB10; therefore, our public and private key structures are similar, and their sizes appear to be the same. However, WZ-MIBFHE has a lower dimension, resulting in smaller public and private key sizes as well as ciphertext sizes, significantly enhancing the compactness of the scheme. WZ-MIBFHE employs the decomposition method for

ciphertext expansion, allowing users to generate expandable ciphertexts directly from the encryption algorithm without needing to generate fresh ciphertexts in advance. This approach reduces the overall operations required, making the scheme more concise. Additionally, with the increase in the number of users participating in WZ-MIBFHE compared to similar schemes, our noise expansion rate is significantly lower, indicating that we can perform more homomorphic evaluations. Compared to [20], WZ-MIBFHE has better performance and parameters, but does not implement the multi-hop property.

Table 3. Comparison of Trapdoor, IBE Architecture, Ciphertext Extension Method, Fresh Ciphertext Requirement, and Multi-hop Support in Similar Schemes.

Scheme	Trapdoor	IBE Architecture	Ciphertext Extension Method	Must Fresh Ciphertext	Multi-Hop Support
[11]	GPV08	Dual Regev	Mask system	Yes	No
[20]	MP12	Dual Regev	Mask system	Yes	Yes
[22]	MP12	ABB10	Mask system	Yes	No
WZ-MIBFHE	YJW23	Our modified IBE	The decomposition method	No	No

Table 4. Comparison of Dimension, Secret Key Size, Ciphertext Size, and Noise Expansion Rate in Similar Schemes.

Scheme	Dimension	Secret Key Size	Expanded Ciphertext Size	Noise Expansion Rate
[11]	$6n\log q$	Dm'^2	$D^2m'^2\omega^2$	$1+n\omega$
[20]	$2n\log q$	Dm'^2	$D^2m'^2\omega^2$	$1+7n\omega$
[22]	$2n\log q$	Dm'	$D^2m'^2\omega$	$(1+2n)+3n(1+2n\omega)^3$
WZ-MIBFHE	$n\log q+\log_b q$	Dm'	$D^2m'^2\omega$	D

6. Conclusions

In this study, we optimized the ABB10 scheme using the pre-image sampling algorithm based on YJW23, resulting in a foundational IBE scheme that satisfies IND-sID-CPA security. We modified the relationship and generation method of the identity vector and identity public key in our IBE scheme to meet the requirements of the decomposition method. Utilizing the decomposition method and the modified IBE scheme, we proposed a compact MIBFHE scheme. Comparisons with other MIBFHE schemes show that our proposal optimizes parameters such as lattice dimension, public and private key sizes, and noise growth rates, making it more concise and efficient. Overall, WZ-MIBFHE offers a practical solution in the field of multi-identity fully homomorphic encryption, demonstrating good security and scalability. In the future, we aim to extend the functionality of WZ-MIBFHE to include multi-hop attributes. Additionally, we are keenly aware of the practical application prospects of MIBFHE in areas like privacy-preserving cloud computing [29–32]. We also plan to extend WZ-MIBFHE scheme to rings, leveraging the unique properties of rings to further enhance the efficiency of the MIBFHE scheme. To the best of our knowledge, no existing scheme has addressed the IBFHE and MIBFHE problems from the perspective of ring-based LWE.

Author Contributions: Conceptualization, Z.W. and R.H.; methodology, X.W.; software, Z.W.; validation, R.H., Z.W. and X.W.; formal analysis, Z.W.; investigation, Z.W.; resources, X.W.; data curation, Z.W.; writing—original draft preparation, Z.W.; writing—review and editing, Z.W.; visualization, Z.W.; supervision, Z.W.; project administration, X.W.; 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 Key Research and Development Program Project No. AB24010340.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article.

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

References

1. Rivest, R.L.; Adleman, L.; Dertouzos, M.L. On data banks and privacy homomorphisms. *Found. Secur. Comput.* **1978**, *4*, 169–180.
2. Rivest, R.L.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
3. ElGamal, T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inf. Theory* **1985**, *31*, 469–472. [CrossRef]
4. Paillier, P. Public-key cryptosystems based on composite degree residuosity classes. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Prague, Czech Republic, 2–6 May 1999; Springer: Berlin/Heidelberg, Germany, 1999; pp. 223–238.
5. Gentry, C. Fully homomorphic encryption using ideal lattices. In Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing, Bethesda, MD, USA, 31 May–2 June 2009; pp. 169–178.
6. Gentry, C.; Sahai, A.; Waters, B. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In Proceedings of the Advances in Cryptology–CRYPTO 2013: 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 2013; Proceedings, Part I; Springer: Berlin/Heidelberg, Germany, 2013; pp. 75–92.
7. Brakerski, Z.; Gentry, C.; Vaikuntanathan, V. (Leveled) fully homomorphic encryption without bootstrapping. *ACM Trans. Comput. Theory TOCT* **2014**, *6*, 1–36. [CrossRef]
8. Chillotti, I.; Gama, N.; Georgieva, M.; Izabachène, M. TFHE: Fast fully homomorphic encryption over the torus. *J. Cryptol.* **2020**, *33*, 34–91. [CrossRef]
9. Cheon, J.H.; Kim, A.; Kim, M.; Song, Y. Homomorphic encryption for arithmetic of approximate numbers. In Proceedings of the Advances in Cryptology—ASIACRYPT 2017: 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, 3–7 December 2017; Proceedings, Part I 23; Springer: Berlin/Heidelberg, Germany, 2017; pp. 409–437.
10. Ahmad, H.; Hannusch, C. A New Keyed Hash Function Based on Latin Squares and Error-Correcting Codes to Authenticate Users in Smart Home Environments. In Proceedings of the Codes, Cryptology and Information Security: 4th International Conference, C2SI 2023, Rabat, Morocco, 29–31 May 2023 ; pp. 129–135.
11. Clear, M.; McGoldrick, C. Multi-identity and multi-key leveled FHE from learning with errors. In Proceedings of the Advances in Cryptology–CRYPTO 2015: 35th Annual Cryptology Conference, Santa Barbara, CA, USA, 16–20 August 2015; Proceedings, Part II 35; Springer: Berlin/Heidelberg, Germany, 2015; pp. 630–656.
12. Canetti, R.; Raghuraman, S.; Richelson, S.; Vaikuntanathan, V. Chosen-ciphertext secure fully homomorphic encryption. In Proceedings of the IACR International Workshop on Public Key Cryptography, Amsterdam, The Netherlands, 28–31 March 2017; Springer: Berlin/Heidelberg, Germany, 2017; pp. 213–240.
13. Wang, W.L.; Hu, B.; Zao, X.F. An efficient multi-identity homomorphic encryption scheme. *J. Shandong Univ. Natural Sci.* **2017**, *52*, 85–94.
14. Micciancio, D.; Peikert, C. Trapdoors for lattices: Simpler, tighter, faster, smaller. In 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; pp. 700–718.
15. Tu, G.; Yang, X.; Zhou, T. Efficient identity-based multi-identity fully homomorphic encryption scheme. *J. Comput. Appl.* **2019**, *39*, 750.
16. Cash, D.; Hofheinz, D.; Kiltz, E.; Peikert, C. Bonsai trees, or how to delegate a lattice basis. *J. Cryptol.* **2012**, *25*, 601–639. [CrossRef]
17. Shen, T.; Wang, F.; Chen, K.; Wang, K.; Li, B. Efficient leveled (multi) identity-based fully homomorphic encryption schemes. *IEEE Access* **2019**, *7*, 79299–79310. [CrossRef]
18. Agrawal, S.; Boneh, D.; Boyen, X. Efficient lattice (H) IBE in the standard model. In Proceedings of the Advances in Cryptology–EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, France, 30 May–3 June 2010; Proceedings 29; Springer: Berlin/Heidelberg, Germany, 2010; pp. 553–572.

19. Shen, T.; Wang, F.; Chen, K.; Shen, Z.; Zhang, R. Compressible Multikey and Multi-Identity Fully Homomorphic Encryption. *Secur. Commun. Netw.* **2021**, *2021*, 6619476. [CrossRef]
20. Liu, W.; Wang, F.; Jin, X.; Chen, K.; Shen, Z. Leveled Multi-Hop Multi-Identity Fully Homomorphic Encryption. *Secur. Commun. Netw.* **2022**, *2022*, 1023439. [CrossRef]
21. Peikert, C.; Shiehian, S. Multi-key FHE from LWE, revisited. In Proceedings of the Theory of Cryptography Conference, Tel Aviv, Israel, 10–13 January 2016; Springer: Berlin/Heidelberg, Germany, 2016; pp. 217–238.
22. Fan, H.; Huang, R.; Luo, F. Efficient multi-identity full homomorphic encryption scheme on lattice. *Appl. Sci.* **2023**, *13*, 6343. [CrossRef]
23. Yu, Y.; Jia, H.; Wang, X. Compact lattice gadget and its applications to hash-and-sign signatures. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 2023; Springer: Berlin/Heidelberg, Germany, 2023; pp. 390–420.
24. Micciancio, D.; Regev, O. Worst-case to average-case reductions based on Gaussian measures. In Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science, Rome, Italy, 17–19 October 2004; pp. 372–381. [CrossRef]
25. 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; pp. 197–206.
26. Dodis, Y.; Reyzin, L.; Smith, A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In Proceedings of the Advances in Cryptology-EUROCRYPT 2004: International Conference on The Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, 2–6 May 2004; Proceedings 23; Springer: Berlin/Heidelberg, Germany, 2004; pp. 523–540.
27. Jia, H.; Hu, Y.; Tang, C.; Wang, L. Towards compact identity-based encryption on ideal lattices. In Proceedings of the Cryptographers' Track at the RSA Conference, San Francisco, CA, USA, 6–9 May 2024 Springer: Berlin/Heidelberg, Germany, 2024; pp. 354–378.
28. Tu, G.; Liu, W.; Zhou, T.; Yang, X.; Zhang, F. Concise and Efficient Multi-Identity Fully Homomorphic Encryption Scheme. *IEEE Access* **2024**, *12*, 49640–49652. [CrossRef]
29. Zhou, L.; Wang, Z.; Cui, H.; Zhang, X.; Wang, X.; Yu, Y. HEAD: An FHE-based Privacy-preserving Cloud Computing Protocol with Compact Storage and Efficient Computation. *Cryptol. Eprint Arch. Pap.* **2022**, 2022/238, *preprint*.
30. Marcolla, C.; Sucasas, V.; Manzano, M.; Bassoli, R.; Fitzek, F.H.P.; Aaraj, N. Survey on Fully Homomorphic Encryption, Theory, and Applications. *Proc. IEEE* **2022**, *110*, 1572–1609. [CrossRef]
31. Abdulsalam, Y.S.; Hedabou, M. Security and privacy in cloud computing: Technical review. *Future Internet* **2021**, *14*, 11. [CrossRef]
32. Rezaeibagha, F.; Mu, Y.; Huang, K.; Chen, L.; Zhang, L. Toward Secure Data Computation and Outsource for Multi-User Cloud-Based IoT. *IEEE Trans. Cloud Comput.* **2023**, *11*, 217–228. [CrossRef]