Hindawi
Mathematical Problems in Engineering
Volume 2021, Article ID 6656764, 10 pages
https://doi.org/10.1155/2021/6656764

Research Article

Attribute-Based Fully Homomorphic Encryption Scheme from Lattices with Short Ciphertext

Yuan Liu,[1] **Yun Pan**,[2] **Lize Gu**,[1] **Yuan Zhang**,[1] **and Dezhi An**[3]

[1]*State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[2]*School of Computer Science, Communication University of China (CUC), 1 Dingfuzhuang East Street, Beijing 100024, China*
[3]*School of Cyber Security, Gansu University of Political Science and Law, Lanzhou 730070, China*

Correspondence should be addressed to Yun Pan; pany@cuc.edu.cn

Received 24 November 2020; Revised 4 January 2021; Accepted 15 January 2021; Published 2 February 2021

Academic Editor: Rongxing Lu

Attribute-based encryption (ABE) is a good choice for one-to-many communication and fine-grained access control of the encryption data in a cloud environment. Fully homomorphic encryption (FHE) allows cloud servers to make valid operations on encrypted data without decrypting. Attribute-based fully homomorphic encryption (ABFHE) from lattices not only combines the bilateral advantages/facilities of ABE and FHE but also can resist quantum attacks. However, in the most previous ABFHE schemes, the growth of ciphertext size usually depends on the total number of system's attributes which leads to high communication overhead and long running time of encryption and decryption. In this paper, based on the LWE problem on lattices, we propose an attribute-based fully homomorphic scheme with short ciphertext. More specifically, by classifying the system's attributes and using the special structure matrix in MP12, we remove the dependency of ciphertext size on system's attributes ℓ and the ciphertext size is no longer increased with the total number of system's attributes. In addition, by introducing the function $\mathbf{G}^{-1}$ in the homomorphic operations, we completely rerandomize the error term in the new ciphertext and have a very tight and simple error analysis using sub-Gaussianity. Besides, performance analysis shows that when $\ell = 2$ and $n = 284$ according to the parameter suggestion given by Micciancio and Dai et al., the size of ciphertext in our scheme is reduced by at least 73.3%, not to mention $\ell > 2$. The larger the ℓ, the more observable of our scheme. The short ciphertext in our construction can not only reduce the communication overhead but also reduce the running time of encryption and decryption. Finally, our scheme is proved to be secure in the standard model.

1. Introduction

Attribute-based encryption (ABE) [1], being proposed by Sahai and Waters in 2005, associates a user's identity with a set of attributes. Depending on the relevance of access policy, it can be divided into key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE) [2]. KP-ABE means that a user's secret key is generated relying on an access policy and the ciphertext is generated relying on an attributes set. On the contrary, in CP-ABE, a user's secret key is generated relying on an attribute set and the ciphertext is generated relying on an access policy. They all support one-to-many communication and fine-grained access control. In order to protect the users' data privacy and realize data security sharing in the cloud environment, ABE is a good choice.

In recent years, with the development of quantum computer, pairing-based ABE constructions face the potential threat of quantum computer. Lattice-based cryptography has been the focus of research in recent years because it is flexible in construction and resistant to quantum attack.

1.1. Related Works. In 2011, based on the learning with error (LWE) [3] problem, Zhang et al. [4] proposed a CP-ABE scheme which uses negative attributes and positive attributes denote the system's attributes and support AND operation among these attributes. In 2012, Zhang et al. [5] proposed another CP-ABE scheme with multivalued attributes and THRESHOLD access policy. And in the same year, Agrawal

et al. [6] proposed a fuzzy identity-based encryption scheme and extended it to a large universe ABE scheme. In 2013, Boyen [7] constructed a lattice-based KP-ABE scheme which uses the linear secret sharing scheme (LSSS) to express the access policy and Liu et al. [8] proposed a lattice-based ABE scheme which supports THRESHOLD access policy and attribute hierarchy. In the same year, Gorbunov et al. [9] also introduced a two-to-one recording technique to construct a lattice-based ABE scheme. In 2014, Wang [10] proposed two lattice-based CP-ABE schemes. These two schemes support AND operation among multivalued attributes. In addition, by using Boolean circuit to represent access policy, Zhao et al. [11] proposed a lattice-based KP-ABE scheme. In 2016, Brakerski and Vaikuntanathan [12] also proposed a circuit-ABE from LWE which support unbounded attributes and semiadaptive security. The lattice-based ABE schemes in [13–15] support multiple attribute authorities to manage all attributes in the system. A multiauthority ABE scheme can reduce the pressure of a single attribute authority and improve system efficiency. In 2019, based on Zhangjiang's construction [4], Gur et al. [16] made an implement of Zhangjiang's construction. And based on [9], Wang et al. [17] constructed a three-to-one recording technique and proposed another lattice-based CP-ABE scheme. In 2020, inspiring by [9], Dong et al. [18] proposed a lattice-based ABE scheme which is indirect revocable and satisfies efficient and secure user revocation in lattices. Brakerski and Vaikuntanathan [19] proposed another CP-ABE scheme which a circuit access policy, but in this scheme, they did not give a security reduction and leave the security as an open problem. Consider the following situation where a large amount of a user's messages $\mu_1, \mu_2, \ldots$ are encrypted and stored in the cloud server. To reduce the communication and computing overhead, he wants the encrypted data to be processed by the cloud server using the function f without privacy leakage, and the ciphertext which is processed by f can be decrypted to $f(\mu_1, \mu_2, \ldots)$. The above lattice-based ABE schemes [4–19] are not suitable for this scenario; that is, they do not support homomorphic operations on the ciphertext.

The first fully homomorphic encryption (FHE) scheme was proposed by Gentry [20] in 2009. In this scheme, he introduced a "bootstrapping" technique to control the increase of noise so as to ensure the correctness of decryption and then realized the homomorphic addition and homomorphic multiplication of ciphertext. However, the "bootstrapping" needs to encrypt the private key and set it as a public parameter. In 2013, based on LWE problem, Gentry, Sahai, and Waters [21] (GSW13) employed the approximate eigenvector method to construct fully homomorphic encryption (FHE) scheme, and then by making some relatively minor modifications on an LWE-based ABE scheme for circuits [9], they proposed the first fully homomorphic KP-ABE scheme. In the fully homomorphic KP-ABE scheme of GSW13, the system's attributes can be expressed by $\{1, 2, \ldots, \ell\}$ and the access policy is expressed by a Boolean circuit. In 2014, Boneh et al. [22] proposed a fully key homomorphic KP-ABE scheme which is used as the gadget matrix. However, in this scheme, it just only achieves a fully homomorphic of the users' private key but not the fully homomorphic of the ciphertext, and the size of ciphertext increases linearly with the total number of system attributes which leads to a high storage overhead. In 2016, based on the construction of Boneh et al. [22], Clear and McGoldrick [23] proposed a fully homomorphic KP-ABE scheme from lattices. However, in this scheme, it can evaluate unbounded depth circuits but with a bounded input; that is, the number of ciphertext is bounded. In the same year, Brakerski et al. [24] proposed another lattice-based fully homomorphic KP-ABE scheme by using the gadget matrix $\mathbf{G}$ and a function $\mathbf{G}^{-1}$ which are adopted from [22]. In 2017, based on the ring-LWE problem over ideal lattices, Tan and Samsudin [25] also proposed a lattice-based CP-ABE scheme based on homomorphic encryption. In the same year, Hiromasa and Kawai modified the scheme in [24] and proposed a dynamic homomorphic KP-ABE scheme [26]. However, in [24, 26], the size of ciphertext also increases linearly with the number of system attributes which leads to a high storage overhead. The above lattice-based fully homomorphic encryption schemes mostly are KP-ABE. The number of system's attributes has been fixed in the Setup phase, and in order to match an access circuit, it generates a ciphertext component for each attribute which leads to a high storage and communication cost. Additionally, each ciphertext component usually is a vector, and the computation of ℓ ciphertext vectors would directly lead to the increase of encryption and decryption time. Therefore, it is meaningful to construct an attribute-based fully homomorphic encryption scheme with short ciphertext.

1.2. Our Contribution. In this paper, we propose a lattice-based ABE scheme which supports homomorphic addition and homomorphic multiplication of ciphertext. This scheme is based on a basic CP-ABE, and by introducing $\mathbf{G}^{-1}$ function, it can support homomorphic operations. In our scheme, the ciphertext size is reduced by removing the ciphertext's dependence on the total number of system's attributes. The main contributions are as follows:

(1) In this scheme, we classify the system's attributes $U = \{1, 2, \ldots, \ell\}$ into k attribute categories. Each attribute category has some attribute values. In Setup phase, the system does not need to generate ℓ matrices as the public parameters for all attributes, just k matrices for the attribute categories. The size of public parameter is reduced due to that the number of attribute categories is much smaller than the total number of system's attributes.

(2) In addition, we introduce the special structure matrix with tag in [27]. By embedding the attribute values in the access structure into the tag, the size of ciphertext is remarkably reduced by at least 73.3%. Performance analysis shows that the size of ciphertext no longer increases linearly with the total number of system's attributes, and the size of ciphertext and running time are all reduced.

(3) In order to support the homomorphic operations, we introduce a function $\mathbf{G}^{-1}$ which is adopted from

[28]. By using $\mathbf{G}^{-1}$, we have a very tight and simple error analysis using sub-Gaussianity (see Corollary 2), and in the homomorphic multiplication, $\mathbf{G}^{-1}$ can completely rerandomize the error term in a ciphertext.

1.3. Organization. The rest of this paper is organized as follows. In Section 2, we give the definition of related symbols, lattices, related algorithms, and decision learning with error (DLWE) problem. The definition of attribute-based fully homomorphic encryption scheme and security model are given in Section 3. In Section 4, we give our attribute-based fully homomorphic encryption scheme from lattices with short ciphertext, homomorphic operations, error analysis, correctness, and the security proof. In Section 5, we give a detailed comparison between our scheme and other related works. In Section 6, we summarize this paper.

2. Preliminaries

As shown in Table 1, we give the detailed description of the symbols.

2.1. Integer Lattice

Definition 1. Given n linearly independent vectors $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n \in \mathbb{R}^m$ and the lattice Λ generated by the following formula,

$$\Lambda = L(\mathbf{B}) = \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i : x_i \in \mathbb{Z}, (i = 1, \ldots, n) \right\}, \quad (1)$$

where $\mathbf{B} = [\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n]$ is a basis of Λ, m is the dimension, and n is the rank.

Definition 2. For prime $q, \mathbf{A} \in \mathbb{Z}_q^{n\times m}$, and $\mathbf{u} \in \mathbb{Z}_q^n$, define

$$\begin{aligned} \Lambda_q(\mathbf{A}) &= \left\{ \mathbf{y} \in \mathbb{Z}^m \text{ s.t. } \exists \mathbf{s} \in \mathbb{Z}_q^n \, \mathbf{A}^\top \mathbf{s} = \mathbf{y} \,(\mathrm{mod}\, q) \right\}, \\ \Lambda_q^{\perp}(\mathbf{A}) &= \left\{ \mathbf{y} \in \mathbb{Z}^m \text{ s.t. } \mathbf{A}\mathbf{y} = 0 \,(\mathrm{mod}\, q) \right\}, \\ \Lambda_q^{u}(\mathbf{A}) &= \left\{ \mathbf{y} \in \mathbb{Z}^m \text{ s.t. } \mathbf{A}\mathbf{y} = \mathbf{u} \,(\mathrm{mod}\, q) \right\}. \end{aligned} \quad (2)$$

2.2. Discrete Gaussians and Sub-Gaussian

Definition 3. For a vector $\mathbf{c} \in \mathbb{R}^m$ and a positive integer $s \in \mathbb{R}$, we define a Gaussian distribution with centre $\mathbf{c}$ and variance s as follows:

$$\mathscr{D}_{\Lambda,\sigma,\mathbf{c}} = \frac{\rho_{\sigma,\mathbf{c}}(\mathbf{x})}{\rho_{\sigma,\mathbf{c}}(\Lambda)} = \frac{\rho_{\sigma,\mathbf{c}}(\mathbf{x})}{\sum_{\mathbf{x}\in\Lambda} \rho_{\sigma,c}(\mathbf{x})}, \quad (3)$$

where $\sigma > 0$ is a parameter, and $\rho_{\sigma,c}(x) = \exp(-\pi(\|\mathbf{x}-\mathbf{c}\|^2/\sigma^2))$.

Definition 4 (see [28, 29]). Let $s > 0$ be a sub-Gaussian parameter. We call that X is a sub-Gaussian distribution, if for a random variable $x \sim X$ and all $t \in \mathbb{R}$, its generating function satisfies

Table 1: Notation.

Symbols	Definitions
$\mathbb{Z}_q$	An integer set of mod q residue class
Λ	A lattice
$\mathbf{A} \in \mathbb{Z}_q^{n\times m}$	An $n \times m$ matrix
$\mathbf{u} \in \mathbb{Z}_q^n$	An n-dimensional column vector
$\mathbf{u}^\top$	The transpose of vector $\mathbf{u}$
$\|\mathbf{A}\|$	ℓ_2-norm length of the longest column of $\mathbf{A}$
$\|\tilde{\mathbf{A}}\|$	The maximal Gram-Schmidt length of $\mathbf{A}$
$s_1(\mathbf{A})$	The maximal singular value of $\mathbf{A}$
$\mathrm{poly}(n)$	A polynomial function of n
$\mathrm{negl}(n)$	A negligible function of n
$\mathbf{A}_1 \in \mathbb{Z}_q^{n_1\times m}$, $\mathbf{A}_2 \in \mathbb{Z}_q^{n_2\times m}$	$[\mathbf{A}_1; \mathbf{A}_2] \in \mathbb{Z}_q^{(n_1+n_2)\times m}$
$\mathbf{B}_1 \in \mathbb{Z}_q^{n\times m_1}$, $\mathbf{B}_2 \in \mathbb{Z}_q^{n\times m_2}$	$[\mathbf{B}_1 \| \mathbf{B}_2] \in \mathbb{Z}_q^{n\times(m_1+m_2)}$

$$E[\exp(2\pi t x)] \le \exp\left(\pi s^2 t^2\right). \quad (4)$$

Lemma 1 (see [29]). *Let $\mathbf{X} \in \mathbb{R}^{n\times m}$ be an independent matrix that is sub-Gaussian with parameter s. Then, for a constant $c > 0$, it has*

$$\Pr\left[\|\mathbf{X}\|_2 > c \cdot s \cdot (\sqrt{n} + \sqrt{m})\right] \le \mathrm{negl}(n). \quad (5)$$

2.3. The Gadget Matrix

Lemma 2 (see [28]). *Let $\mathbf{g} = (1, 2, 2^2, \ldots, 2^{t-1})^\top$ where $t = \lceil \log q \rceil$. Define the gadget matrix $\mathbf{G} = \mathbf{g}^\top \otimes \mathbf{I}_N = diag(\mathbf{g}^\top, \mathbf{g}^\top, \ldots, \mathbf{g}^\top) \in \mathbb{Z}_q^{N\times Nt}$. There exists a function $\mathbf{G}^{-1}$: $\mathbb{Z}_q^{N\times M} \longrightarrow (0,1)^{Nt\times M}$, and for any matrix $\mathbf{A} \in \mathbb{Z}_q^{N\times M}$, it has $\mathbf{G}\cdot\mathbf{X} = \mathbf{A}$ where $\mathbf{X} = \mathbf{G}^{-1}(\mathbf{A})$ and $\mathbf{X}$ has sub-Gaussian parameter $O(1)$.*

2.4. Algorithms. Next, we give the related algorithms which are proposed in MP12 [27].

Let $q \ge 2, n \ge 1, \overline{n} = nt, t = \lceil \log q \rceil$, and $m = O(\log q)$, and there are two probabilistic polynomial-time (PPT) algorithms such that

(1) TrapGen $(\mathbf{A}', \mathbf{H})$, given a uniformly random matrix $\mathbf{A}' \in \mathbb{Z}_q^{n\times\overline{m}}$ and an invertible matrix $\mathbf{H} \in \mathbb{Z}_q^{n\times n}$, outputs a uniformly random matrix $\mathbf{A} = [\mathbf{A}' | \mathbf{H}\mathbf{G}_n - \mathbf{A}'\mathbf{T}_\mathbf{A}] \in \mathbb{Z}_q^{n\times m}$, and a trapdoor $\mathbf{T}_\mathbf{A} \in \mathbb{Z}_q^{\overline{m}\times\overline{n}}$ where the trapdoor size is $s_1(\mathbf{T}_\mathbf{A}) \le \sqrt{m} \cdot \omega(\sqrt{\log q})$

(2) SamplePre $(\mathbf{A}, \mathbf{T}_\mathbf{A}, \mathbf{u}, \sigma)$, given $\mathbf{A} = [\mathbf{A}' | \mathbf{H}\mathbf{G}_n - \mathbf{A}'\mathbf{T}_\mathbf{A}] \in \mathbb{Z}_q^{n\times m}$, a trapdoor $\mathbf{T}_\mathbf{A} \in \mathbb{Z}_q^{\overline{m}\times\overline{n}}$, $\mathbf{u} \in \mathbb{Z}_q^n$, and a Gaussian parameter $\sigma \ge s_1(\mathbf{T}_\mathbf{A})\|\widetilde{\mathbf{G}_n}\|$ where $s_1(\mathbf{T}_\mathbf{A})$ is the largest singular value of $\mathbf{T}_\mathbf{A}$ and $\|\widetilde{\mathbf{G}_n}\| = 2$ or $\sqrt{5}$, outputs a vector $\mathbf{e} \in \mathbb{Z}_q^{\overline{m}+\overline{n}}$ such that $\mathbf{A}\mathbf{e} = \mathbf{u}$

Note that $\mathbf{G}_n = \mathbf{g}^\top \otimes \mathbf{I}_n \in \mathbb{Z}_q^{n\times\overline{n}}$ is a gadget matrix and n denotes its dimension. $\mathbf{G}_n$ also has a deterministic function $\mathbf{G}_n^{-1}$ as mentioned in Lemma 2. However, an n-dimensional gadget matrix $\mathbf{G}_n$ is just only introduced in the TrapGen algorithm; thus, we denote it as $\mathbf{G}_n$.

Lemma 3 (see [27]). The vector e which is generated by the SamplePre algorithm is not statistically distinguishable from $\mathscr{D}_{\Lambda_q^{\mathbf{u}}(\mathbf{A}),\sigma\omega(\sqrt{\log n})}$ where

$$\Pr\left[\mathbf{e} \sim \mathscr{D}_{\Lambda_q^{\mathbf{u}}(\mathbf{A}),\sigma\omega(\sqrt{\log n})}: \|\mathbf{e}\| > \sigma\sqrt{m}\right] \leq \mathrm{negl}(n). \quad (6)$$

2.5. Hardness Assumption. In 2005, Regev proposed the learning with error (LWE) problem [3], i.e., given a positive integer n, a prime integer q, and a probability distribution χ over $\mathbb{Z}$, output $(\mathbf{a}, \mathbf{a}^\top\mathbf{s} + e)$ where $\mathbf{a}, \mathbf{s} \in \mathbb{Z}_q^n$ and e is an error term from χ.

Definition 5. Decision learning with error (DLWE) problem [3]: for a security parameter λ, let $n = n(\lambda)$, $q = q(\lambda)$, and a distribution $\chi = \chi(\lambda)$ over $\mathbb{Z}$. The DLWE problem is to distinguish between the following two distributions:

$$\begin{aligned}&(\mathbf{A}, \mathbf{A}^\top\mathbf{s} + \mathbf{e}),\\ &(\mathbf{A}, \mathbf{b}),\end{aligned} \quad (7)$$

where $\mathbf{A} = (\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m) \in \mathbb{Z}_q^{n\times m}$, $\mathbf{s} \in \mathbb{Z}_q^n, \mathbf{b} \in \mathbb{Z}_q^m$, and $\mathbf{e} = (e_1, e_2, \ldots, e_m)^\top$ is a noise from distribution χ^m.

Definition 6. B-bounded distribution [21]: for $n \in N$, a distribution ensemble χ_n, supported over the integers, is called B-bounded if

$$\Pr_{e\leftarrow\chi_n}[|e| > B] = \mathrm{negl}(n). \quad (8)$$

Corollary 1 (see [3, 27]). *For any $B = B(n)$ and $q = q(n)$, there is a B-bounded distribution $\chi = \chi(n)$ such that $DLWE_{n,q,\chi}$ is at least as hard as the quantum hardness $GapSVP_\gamma$ and $SIVP_\gamma$ for $\gamma = \widetilde{O}(nq/B)$.*

3. Definitions of the Scheme and Security Model

3.1. Definition of the System Algorithm. Before we give the definition, we firstly give the definition of fully homomorphic encryption.

Definition 7. Fully homomorphic encryption [21]: a fully homomorphic encryption consists of four algorithms (KeyGen, Encrypt, Decrypt, and Eval):

(1) KeyGen (1^n): on input the security parameter 1^n. This algorithm outputs the public key pk and secret key sk.

(2) Encrypt (pk, μ): on input public key pk, and a message μ. The algorithm outputs a ciphertext c.

(3) Decrypt $(\mathrm{sk}, c) \longrightarrow \mu$: on input secret key sk and ciphertext c, and it outputs the message μ.

(4) Eval $(\mathrm{pk}, c_1, c_2, \ldots, c_k, f)$: on input public key pk, ciphertext list $c_1, c_2, \ldots, c_k$, a function $f \in \mathscr{F}$, and output a new ciphertext c_f where Decrypt $(\mathrm{sk}, c_f) = f(\mu_1, \mu_2, \ldots, \mu_k)$.

An attribute-based fully homomorphic encryption scheme consists of the following five algorithms:

(1) Setup $(1^n) \longrightarrow (\mathrm{PP}, \mathrm{MK})$: on input the security parameter 1^n. This algorithm outputs the public parameters PP and master secret key MK.

(2) Extract $(\mathrm{PP}, \mathrm{MK}, L) \longrightarrow \mathrm{SK}_L$: on input public parameters PP, master key MK, and a user's attribute list $L = \{l_i\}_{l_i\in S_i}$. It outputs the user's privacy key SK_L.

(3) Encrypt $(\mathrm{PP}, W, \mu) \longrightarrow \mathbf{C}$: on input public parameters PP, access policy W, and a message $\mu \in \{0, 1\}$. The algorithm outputs a ciphertext C.

(4) Decrypt $(\mathrm{PP}, \mathbf{C}, \mathrm{SK}_L) \longrightarrow \mu$: on input public parameters PP, private key SK_L, and ciphertext C, if L does not satisfy W, outputs $\perp$; otherwise it outputs the message μ.

(5) Eval $(\mathrm{PP}, \mathbf{C}_1, \mathbf{C}_2, \ldots, \mathbf{C}_k, f)$: on input public parameters PP, k ciphertexts $\mathbf{C}_1, \mathbf{C}_2, \ldots, \mathbf{C}_k$, under the same access policy, a function $f \in \mathscr{F}$, and output a new ciphertext $\mathbf{C}_f$ where Decrypt $(\mathrm{PP}, \mathbf{C}_f, \mathrm{SK}_L) = f(\mu_1, \mu_2, \ldots, \mu_k)$.

Correctness: for a user's attributes list L, all messages $\mu_1, \mu_2, \ldots, \mu_k$, $\mathbf{C}_j \leftarrow$ Encrypt (PP, W, μ_j), and $\mathbf{C}_f \leftarrow$ Eval $(\mathrm{PP}, \mathbf{C}_1, \ldots, \mathbf{C}_k, f)$, we have $\Pr[\mathrm{Decrypt}(PP, SK_L, \mathbf{C}_f) = f(\mu_1, \mu_2, \ldots, \mu_k)] = 1 - \mathrm{negl}(n)$, if L and W match each other.

3.2. Security Model. Here, we give the definition of the security model, and the security is adopted from [4, 5], in which the adversary specifies the challenge access structure before the Setup phase. Consider a game between a challenger $\mathscr{B}$ and an adversary $\mathscr{A}$ which is described as follows:

Init: the adversary $\mathscr{A}$ chooses the challenge access structure W^* and sends it to the simulator $\mathscr{B}$.

Setup: the challenger runs the Setup algorithm and sends the public parameters PP to the adversary.

Queries: in this step, $\mathscr{A}$ can adaptively make key queries for a sequence of attribute list L. However, he cannot query an attribute list which satisfies W^*. $\mathscr{B}$ answers the queries.

Challenge: the adversary $\mathscr{A}$ sends a message $\mu^* \in \mathbb{Z}_q$ to $\mathscr{B}$. The simulator $\mathscr{B}$ randomly chooses $b \in \{0, 1\}$. If $b = 1$, $\mathscr{B}$ sends $\mathbf{C}^* = \mathrm{Encrypt}(\mathrm{PP}, W^*, \mu^*)$ to $\mathscr{A}$. If $b = 0$, it sends a random ciphertext to $\mathscr{A}$.

Continuation: Queries phase is repeated.

Guess: $\mathscr{A}$ outputs his guess $b' \in \{0, 1\}$.

The advantage of the adversary $\mathscr{A}$ is $\mathrm{Adv}(\mathscr{A}) = |\Pr[b' = b] - (1/2)|$.

Definition 8. Our attribute-based fully homomorphic scheme from lattices with short ciphertext is secure if the advantage of any PPT adversary $\mathscr{A}$ is a negligible function.

4. Attribute-Based Fully Homomorphic Encryption Scheme from Lattices with Short Ciphertext

In the existing homomorphic ABE schemes from lattices, the size of ciphertext is usually related to the total number of system's attributes which lead to a high communication cost. In this section, we propose an attribute-based fully homomorphic encryption scheme from lattices with short ciphertext. In our construction, we firstly assume that all the system attributes $U = \{1, 2, \ldots, \ell\}$ can be classified into k attribute categories, and each attribute category has n_i attribute values, i.e., $U = \{S_1, S_2, \ldots, S_k\}$ where $S_i = (\mathbf{v}_{i,1}, \mathbf{v}_{i,2}, \ldots, \mathbf{v}_{i,n_i})_{1 \le i \le k}$. A user's attribute list is $L = \{l_i\}_{l_i \in S_i}$, and the access structure is an "AND" gates between attributes such that $W = (S_1 = \mathbf{v}_{1,t1}) \wedge (S_2 = \mathbf{v}_{2,t2}) \wedge \cdots \wedge (S_k = \mathbf{v}_{1,tk})$. Thanks to the special matrix structure of $\mathbf{A}$, we can embed a user's attribute list in it such that $\mathbf{A}_L = [\mathbf{A}'|\mathbf{H}_L\mathbf{G}_\mathbf{n} - \mathbf{A}'\mathbf{T}_\mathbf{A}] \in \mathbb{Z}_q^{n \times m}$. Here, we need an encoding with full-rank difference (FRD) function.

Definition 9 (see [30]). Let q be a prime and n be a positive integer, we say a function H: $\mathbb{Z}_q^n \longrightarrow \mathbb{Z}_q^{n \times n}$ is an encoding with full-rank difference (FRD) function if

(i) for any $\mathbf{x} \neq \mathbf{y}$, the matrix $H(\mathbf{x}) - H(\mathbf{y})$ is full rank, and

(ii) H is computable in polynomial time (in $n \log q$).

4.1. Our Construction. The attribute-based fully homomorphic encryption scheme from lattices with short ciphertext consists of the following five algorithms.

Let $\overline{n} = nt, t = \lceil \log q \rceil$, $\overline{m} = m - \overline{n}$, and $M = (m + 1)\lceil \log q \rceil$:

(1) Setup $(1^n) \longrightarrow (\mathrm{PP}, \mathrm{MK})$: on input the security parameter 1^n, do as follows:

(i) Perform algorithm TrapGen $(\mathbf{A}', \mathbf{H})$ $\mathbf{H}$ to generate a pair matrix $(\mathbf{A}, \mathbf{T}_\mathbf{A})$ where $\mathbf{A} = [\mathbf{A}'|\mathbf{G}_n - \mathbf{A}'\mathbf{T}_\mathbf{A}] \in \mathbb{Z}_q^{n \times m}$ is a uniformly random matrix and $\mathbf{T}_\mathbf{A} \in \mathbb{Z}^{\overline{m} \times \overline{n}}$ is a trapdoor for $\mathbf{A}$ with associated tag matrix $\mathbf{H} = \mathbf{I}$ where $\mathbf{I}$ is an identity matrix.

(ii) Select k uniformly random matrices $\mathbf{B}_i \in \mathbb{Z}_q^{n \times n}$ as the public parameters for each attribute categories.

(iii) Select a uniformly random vector $\mathbf{u} \in \mathbb{Z}_q^n$.

(iv) Output the public parameters $\mathrm{PP} = \{\mathbf{A}, (\mathbf{B}_i)_{1 \le i \le k}, \mathbf{u}\}$ and the master key $\mathrm{MK} = (\mathbf{T}_\mathbf{A})$.

(2) Extract $(\mathrm{PP}, \mathrm{MK}, L) \longrightarrow \mathrm{SK}_L$: on input public parameters PP, master key MK, and a user's attribute list $L = \{l_i\}_{l_i \in S_i}$, do as follows:

(i) For each attribute value in L, compute the tag $\mathbf{H}_L' = \sum_{\forall \mathbf{v}_{i,j} \in L} \mathbf{B}_i H(v_{i,j})$.

(ii) Compute $\mathbf{A}_L = \mathbf{A} + [0|\mathbf{B}_L\mathbf{G}_n] = [\mathbf{A}'|\mathbf{H}_L\mathbf{G}_n - \mathbf{A}'\mathbf{T}_\mathbf{A}]$ where $\mathbf{H}_L = \mathbf{H}_L' - \mathbf{I}$.

(iii) Sample $\mathbf{r}_L \in \mathbb{Z}_q^m$ as $\mathbf{r}_L$. $\mathbf{r}_L \leftarrow \mathrm{SamplePre}(\mathbf{A}, \mathbf{H}_L, \mathbf{G}_n, \mathbf{T}_\mathbf{A}, \mathbf{u}, \sigma)$.

(iv) Output the user's secret key $\mathrm{SK}_L = \{\mathbf{r}_L\}$.

(3) Encrypt $(\mathrm{PP}, W, \mu) \longrightarrow \mathbf{C}$: on input public parameters PP, access policy W, and message $\mu \in \{0, 1\}$, do as follows:

(i) For each attribute value in the access policy W, compute $\mathbf{H}_W' = \sum_{\forall \mathbf{v}_{i,j} \in W} \mathbf{B}_i H(\mathbf{v}_{i,j})$. And then construct $\mathbf{A}_W = \mathbf{A} + [0|\mathbf{B}_W\mathbf{G}_n] = [\mathbf{A}'|\mathbf{H}_W\mathbf{G}_n - \mathbf{A}'\mathbf{T}_\mathbf{A}]$ where $\mathbf{H}_W = \mathbf{H}_W' - \mathbf{I}$.

(ii) Choose a uniformly random matrix $\mathbf{S} \in \mathbb{Z}_q^{n \times M}$.

(iii) Choose noise term $\mathbf{e}_0 \leftarrow \chi^M$ and noise matrix $\mathbf{E} = (\mathbf{e}_1, \ldots, \mathbf{e}_M) \leftarrow \chi^{m \times M}$.

(iv) For a message μ, compute

$$\mathbf{C} = \begin{bmatrix} \mathbf{u}^\top \\ \mathbf{A}_W^\top \end{bmatrix} \mathbf{S} + \begin{bmatrix} \mathbf{e}_0^\top \\ \mathbf{E} \end{bmatrix} + \mu\mathbf{G} \in \mathbb{Z}_q^{(1+m) \times M} \pmod q, \tag{9}$$

where $\mathbf{G} = \mathbf{g}^\top \otimes \mathbf{I}_{1+m}$ is a gadget matrix as defined in Lemma 2.

(v) Output the ciphertext $\mathbf{C}$.

(4) Decrypt $(\mathrm{PP}, \mathbf{C}, \mathrm{SK}_L) \longrightarrow \mu$: on input public parameters PP, private key SK_L, and ciphertext C, if L does not satisfy W, output $\perp$; otherwise do as follows:

(i) Given a private key $\mathrm{SK}_L = \{\mathbf{r}_L\}$ associate to a user's attribute list, let $\mathbf{v} = (1; -\mathbf{r}_L) \in \mathbb{Z}_q^{1+m}$.

(ii) Consider the first t columns of $\mathbf{G}$. Let $\mathbf{g}_i$ be the i'th column of $\mathbf{G}$. Then, we have $\mathbf{g}_{t-1} = (2^{t-2}, 0, \ldots, 0)^\top$ where $2^{t-2} \in [q/4, q/2)$. Let $g_{t-1,1} = 2^{t-2}$ denote the first element of $\mathbf{g}_{t-1}$.

(iii) Let $\mathbf{C}_i$ denote the i'th column of $\mathbf{C}$, and $e_{0,i}$ is the i'th element of $\mathbf{e}_0$. Compute

$$x_i = \mathbf{v}^\top \mathbf{C}_i = \mu \mathbf{v}^\top \mathbf{g}_i + \mathbf{v}^\top \begin{bmatrix} e_{0,i} \\ \mathbf{e}_i \end{bmatrix}. \tag{10}$$

(iv) Output $\mu = \lfloor x_{t-1}/g_{t-1,1} \rceil$.

(5) Eval $(\mathrm{PP}, \mathbf{C}_1, \mathbf{C}_2, \ldots, \mathbf{C}_k, f)$: on input public parameters PP, k ciphertexts $\mathbf{C}_1, \mathbf{C}_2, \ldots, \mathbf{C}_k$, under the same access policy, a function $f \in \mathcal{F}$, and output a new ciphertext $\mathbf{C}_f$ where Decrypt $(\mathrm{PP}, \mathbf{C}_f, \mathrm{SK}_L) = f(\mu_1, \mu_2, \ldots, \mu_k)$.

Homomorphic addition: $\mathbf{C}_f^+ = \mathbf{C}_1 + \mathbf{C}_2$.

Homomorphic multiplication: $\mathbf{C}_f^\times = \mathbf{C}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2)$.

Note that homomorphic multiplication of k ciphertexts is defined as

$$\mathbf{C}_f = \mathbf{C}_1 \cdot \mathbf{G}^{-1}\left(\mathbf{C}_2 \cdot \mathbf{G}^{-1}\left(\ldots \mathbf{C}_{k-1} \cdot \mathbf{G}^{-1}(\mathbf{C}_k)\right)\right). \tag{11}$$

4.2. Homomorphic Operations and Correctness. As mentioned above, the ciphertext $\mathbf{C} = \begin{bmatrix} \mathbf{u}^\top \\ \mathbf{A}_W^\top \end{bmatrix} \mathbf{S} + \begin{bmatrix} \mathbf{e}_0^\top \\ \mathbf{E} \end{bmatrix} + \mu\mathbf{G} \in \mathbb{Z}_q^{(1+m) \times M}$. Let $\overline{\mathbf{A}} = [\mathbf{u}^\top; \mathbf{A}_W^\top]$ and $\overline{\mathbf{E}} = [\mathbf{e}_0^\top; \mathbf{E}]$. Then,

$\mathbf{C} = \overline{\mathbf{A}}\mathbf{S} + \overline{\mathbf{E}} + \mu\mathbf{G}$. For a decryption key $\mathbf{v}$, we have $v^\top \mathbf{C} = \mu\mathbf{v}^\top\mathbf{G} + \mathbf{v}^\top\overline{\mathbf{E}}$ since $\mathbf{v}^\top\overline{\mathbf{A}} = (1|(-\mathbf{r}_L)^\top)\begin{bmatrix}\mathbf{u}^\top \\ \mathbf{A}_W^\top\end{bmatrix} = 0$.

Homomorphic operations: let $\mathbf{C}_1$ and $\mathbf{C}_2$ be two ciphertexts which are, respectively, encrypted under μ_1 and μ_2. Then, $\mathbf{v}^\top\mathbf{C}_1 = \mu_1\mathbf{v}^\top\mathbf{G} + \mathbf{v}^\top\overline{\mathbf{E}}_1$ and $\mathbf{v}^\top\mathbf{C}_2 = \mu_2\mathbf{v}^\top\mathbf{G} + \mathbf{v}^\top\overline{\mathbf{E}}_2$:

$$\begin{aligned}\mathbf{v}^\top(\mathbf{C}_1 + \mathbf{C}_2) &= \mathbf{v}^\top\mathbf{C}_1 + \mathbf{v}^\top\mathbf{C}_2 = \mu_1\mathbf{v}^\top\mathbf{G} + \mathbf{v}^\top\overline{\mathbf{E}}_1 + \mu_2\mathbf{v}^\top\mathbf{G} \\ &\quad + \mathbf{v}^\top\overline{\mathbf{E}}_2 = (\mu_1+\mu_2)^\top\mathbf{G} + \underbrace{\mathbf{v}^\top(\overline{\mathbf{E}}_1 + \overline{\mathbf{E}}_2)}_{\text{error term}},\end{aligned} \tag{12}$$

$$\begin{aligned}\mathbf{v}^\top\left(\mathbf{C}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2)\right) &= \mathbf{v}^\top C_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2) \\ &= (\mu_1\mathbf{v}^\top\mathbf{G} + \mathbf{v}^\top\overline{\mathbf{E}}_1)\cdot\mathbf{G}^{-1}(\mathbf{C}_2) \\ &= \mu_1\mathbf{v}^\top\mathbf{C}_2 + \mathbf{v}^\top\overline{\mathbf{E}}_1\cdot\mathbf{G}^{-1}(\mathbf{C}_2) \\ &= \mu_1(\mu_2\mathbf{v}^\top\mathbf{G} + \mathbf{v}^\top\overline{\mathbf{E}}_2) + \mathbf{v}^\top\overline{\mathbf{E}}_1\cdot\mathbf{G}^{-1}(\mathbf{C}_2) \\ &= \mu_1\mu_2\mathbf{v}^\top\mathbf{G} + \underbrace{\mathbf{v}^\top\left(\mu_1\overline{\mathbf{E}}_2 + \overline{\mathbf{E}}_1\cdot\mathbf{G}^{-1}(\mathbf{C}_2)\right)}_{\text{error term}}.\end{aligned} \tag{13}$$

Referring to equations (12) and (13), our scheme satisfies homomorphic addition and homomorphic multiplication. Note that referring to (13), the growth of the error term depends on old error terms $\overline{\mathbf{E}}_1$, $\overline{\mathbf{E}}_2$, μ_1, and $\mathbf{G}^{-1}$. The dependence on $\overline{\mathbf{E}}_1$ and $\overline{\mathbf{E}}_2$ seems unavoidable. $\mathbf{G}^{-1}$ is a matrix in $\{0,1\}^{M\times M}$. However, the growth depended on μ_1 presents a concern. Thus, according to the suggestion in [21], we restrict the message space to small message.

Corollary 2. *Referring to equations (12) and (13), it is obvious that* $\mathbf{C}_1 + \mathbf{C}_2$ *has error* $\overline{\mathbf{E}}_1 + \overline{\mathbf{E}}_2$ *and* $\mathbf{C}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2)$ *has error* $\mu_1\overline{\mathbf{E}}_2 + \overline{\mathbf{E}}_1\cdot\mathbf{X}$ *where* $\mathbf{X} = \mathbf{G}^{-1}(\mathbf{C}_2)$ *satisfies* $\mathbf{G}\mathbf{X} = \mathbf{C}_2$. *Thus, after a single homomorphic addition, the error is amplified by a factor of 2, and after a single homomorphic multiplication, the error is amplified by a factor of* $O(1)\cdot\sqrt{M} + 1$. *According to Lemmas 1 and 2,* $\|\mathbf{X}\| \le c\cdot O(1)\cdot(2\sqrt{M}) \approx O(1)\cdot\sqrt{M}$. *Since* $\mu \in \{0,1\}$, *thus the latter error is amplified by a factor of* $O(1)\cdot\sqrt{M} + 1$. *Let* k *denote the maximum number of homomorphic operations. Refer to equations (14) and (15), and the error* $\overline{\mathbf{E}}_f \le [(k-1)\cdot O(1)\cdot\sqrt{M} + 1]\overline{\mathbf{E}} \approx (O(1)\cdot\sqrt{M} + 1)\overline{\mathbf{E}}$.

Note that the increase of the error term mainly depends on the homomorphic multiplication. To ensure the correctness of decryption, next we will give an analysis of the homomorphic multiplication of k ciphertexts:

$$\begin{aligned}&\mathbf{v}^\top\mathbf{C}_1\cdot\mathbf{G}^{-1}\left(\mathbf{C}_2\cdot G^{-1}\left(\ldots\mathbf{C}_{k-1}\cdot\mathbf{G}^{-1}(\mathbf{C}_k)\right)\right) \\ &\quad = \mu_1\mu_2\ldots\mu_k\mathbf{v}^\top\mathbf{G} + \underbrace{\mathbf{v}^\top\overline{\mathbf{E}}_f}_{\text{error term}},\end{aligned} \tag{14}$$

where

$$\begin{aligned}\overline{\mathbf{E}}_f &= \mu_1\ldots\mu_{k-1}\overline{\mathbf{E}}_k + \mu_1\ldots\mu_{k-2}\overline{\mathbf{E}}_{k-1}G^{-1} \\ &\quad (\mathbf{C}_k) + \cdots + \mu_1\overline{\mathbf{E}}_2\mathbf{G}^{-1}\left(\mathbf{C}_3\cdot\mathbf{G}^{-1}\left(\ldots\mathbf{C}_{k-1}\cdot\mathbf{G}^{-1}(\mathbf{C}_k)\right)\right) \\ &\quad + \overline{\mathbf{E}}_1\cdot\mathbf{G}^{-1}\left(\mathbf{C}_2\cdot\mathbf{G}^{-1}\left(\ldots\mathbf{C}_{k-1}\cdot\mathbf{G}^{-1}(\mathbf{C}_k)\right)\right).\end{aligned} \tag{15}$$

Let $\overline{\mathbf{E}}_{f,i}$ be the i'th column of $\overline{\mathbf{E}}_f$ and $\overline{\mathbf{E}}_i = \begin{bmatrix}e_{0,i}\\ \mathbf{e}_i\end{bmatrix}$ be the i'th column of $\overline{\mathbf{E}}$. To decrypt the ciphertext $\mathbf{C}_f$, refer to Corollary 2 and equation (14), and we have

$$\mathbf{v}^\top\mathbf{C}_{f,i} = \mu_1\mu_2\ldots\mu_k\mathbf{v}^\top\mathbf{g}_i + \underbrace{\mathbf{v}^\top\overline{\mathbf{E}}_{f,i}}_{\text{error term}}. \tag{16}$$

Let $\mu_f = \mu_1\mu_2\ldots\mu_k$, and according to the decryption algorithm, we have

$$\mu_f = \left\lfloor\frac{\mathbf{v}^\top\mathbf{C}_{f,t-1}}{g_{t-1,1}}\right\rceil = \left\lfloor\frac{\mu_f g_{t-1,1} + \mathbf{v}^\top\overline{\mathbf{E}}_{f,t-1}}{g_{t-1,1}}\right\rceil = \left\lfloor\mu_f + \frac{\mathbf{v}^\top\overline{\mathbf{E}}_{f,t-1}}{g_{t-1,1}}\right\rceil. \tag{17}$$

Since $g_{t-1,1} = 2^{t-2} \in [q/4, q/2)$ and $\lfloor\cdot\rceil$ is a rounding function, thus to ensure the correctness of decryption, $\mathbf{v}^\top\overline{\mathbf{E}}_{f,t-1}/g_{t-1,1} < 1/2$; that is, the error term $\mathbf{v}^\top\overline{\mathbf{E}}_{f,t-1}$ should be less than $q/8$. The error term is

$$\begin{aligned}&\left|\mathbf{v}^\top\overline{\mathbf{E}}_{f,t-1}\right| \\ &\le \left|\mathbf{v}^\top(O(1)\cdot\sqrt{M} + 1)\overline{\mathbf{E}}_{t-1}\right| \\ &= (O(1)\cdot\sqrt{M} + 1)\left(e_{0,t-1} - \mathbf{r}_L\mathbf{e}_{t-1}\right)\Big| \\ &\le (O(1)\cdot\sqrt{M} + 1)\left(\|e_{0,t-1}\| + \|\mathbf{r}_L\mathbf{e}_{t-1}\|\right) \\ &\le (O(1)\cdot\sqrt{M} + 1)(B + \sigma\sqrt{m}\cdot\sqrt{m}B) \\ &= B(O(1)\cdot\sqrt{M} + 1)(1 + \sigma m).\end{aligned} \tag{18}$$

To ensure the correctness of decryption, the error term should be less than $q/8$ with overwhelming probability (w.h.p.), i.e., $B(O(1)\cdot\sqrt{M} + 1)(1 + \sigma m) < q/8$. Then, we have $q < 8B(O(1)\cdot\sqrt{M} + 1)(1 + \sigma m)$ where $\sigma \ge s_1(\mathbf{T}_\mathbf{A})\|\widetilde{\mathbf{G}_n}\| \ge \sqrt{m}\cdot\omega(\sqrt{\log q})\|\widetilde{\mathbf{G}_n}\|$.

4.3. Security Analysis. Before we start the security proof, we give a simple lemma based on $\mathrm{DLWE}_{n,q,\chi}$ problem.

Lemma 4. *Let* $\mathbf{S} = (\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_M) \in \mathbb{Z}_q^{n\times M}$. χ *is a distribution over* $\mathbb{Z}$. *Define a distribution whose samples are* $(\mathbf{A}, \mathbf{A}^\top\mathbf{s}_1 + \mathbf{e}_1, \ldots, \mathbf{A}^\top\mathbf{s}_M + \mathbf{e}_M)$ *where* $\mathbf{A} = (\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m) \in \mathbb{Z}_q^{n\times m}$, *and* $\mathbf{e}_j = (e_{1,j}, e_{2,j}, \ldots, e_{m,j})^\top$ *is a noise from distribution* χ^m. *If* $DLWE_{n,q,\chi}$ *holds, then the two distributions* $(\mathbf{A}, \mathbf{A}^\top\mathbf{S} + \mathbf{E})$ *and* $(\mathbf{A}, \mathbb{Z}_q^{m\times M})$ *are statistically indistinguishable.*

Proof of Lemma 4. It is sufficient to make a proof of Lemma 4 in the case of $M = 2$. Suppose there is a PPT algorithm $\mathscr{F}_1$ who can distinguishes two distributions $(\mathbf{A}, \mathbf{A}^\top\mathbf{s}_1 + \mathbf{e}_1, \mathbf{A}^\top\mathbf{s}_2 + \mathbf{e}_2)$ and $(\mathbf{A}, \mathbb{Z}_q^m, \mathbb{Z}_q^m)$ with a nonnegligible advantage ε. Then, we use $\mathscr{F}_1$ to construct a PPT algorithm $\mathscr{F}_2$ to solve the $\mathrm{DLWE}_{n,q,\chi}$ problem. Let $(\mathbf{A}, \mathbf{b}_1)$ be $\mathscr{A}_2$'s sample which is sampled from either $(\mathbf{A}, \mathbf{A}^\top\mathbf{s}_1 + \mathbf{e}_1)$ or $(\mathbf{A}, \mathbb{Z}_q^m)$. Then, $\mathscr{A}_2$ randomly chooses $r \in \{0,1\}$. When $r1 =$, $\mathscr{F}_2$ chooses $\mathbf{s}_2 \in \mathbb{Z}_q^n$ and error term $\mathbf{e}_2 \leftarrow \chi^m$, computes $\mathbf{A}^\top\mathbf{s}_2 + \mathbf{e}_2$ and joints it to the original sample such that $(\mathbf{A}, \mathbf{A}^\top\mathbf{s}_1 + \mathbf{e}_1, \mathbf{A}^\top\mathbf{s}_2 + \mathbf{e}_2)$. When $r = 0$, $\mathscr{F}_2$ chooses a uniformly random vector $\mathbf{b}_2 \in \mathbb{Z}_q^m$ and sets the sample as $(\mathbf{A}, \mathbf{b}_1, \mathbf{b}_2)$. Finally, $\mathscr{A}_2$ outputs the new sample as $\mathscr{F}_1$'s input. If $\mathscr{F}_1$ decides that the sample is from $(\mathbf{A}, \mathbb{Z}_q^m, \mathbb{Z}_q^m)$, $\mathscr{F}_2$ will decide that the sample

is from $(\mathbf{A}, \mathbb{Z}_q^m)$. If $\mathcal{F}_1$ decides that the sample is from $(\mathbf{A}, \mathbf{A}^\top \mathbf{s}_1 + \mathbf{e}_1, \mathbf{A}^\top \mathbf{s}_2 + \mathbf{e}_2)$, $\mathcal{F}_2$ will decide that the sample is from $(\mathbf{A}, \mathbf{A}^\top \mathbf{s}_1 + \mathbf{e}_1)$. Since $\mathcal{F}_1$ has 1/2 probability of getting a sample, thus $\mathcal{F}_2$ can solve the $\mathrm{DLWE}_{n,q,\chi}$ problem with advantage $\varepsilon/2$. □

Theorem 1. *If the $\mathrm{DLWE}_{n,q,\chi}$ assumption holds, based on Lemma 4, our attribute-based fully homomorphic encryption scheme from lattices is secure against selective chosen plaintext attack.*

Proof of Theorem 1. we proof the security by using a sequence of games. As defined in Section 3.2, we use W_i to denote the event that the adversary correctly guesses $b' = b$ in Game_i, and then the advantage of an adversary $\mathcal{A}$ is $|\Pr[W_i] - (1/2)| = |\Pr[b' = b] - (1/2)|$.

Game_0: this is the real game as defined in Section 3.2 between an adversary $\mathcal{A}$ and the challenger $\mathcal{B}$. So, we have

$$\mathrm{Adv}(\mathcal{A}) = \mathrm{Adv}_{W_0}(\mathcal{A}). \tag{19}$$

Game_1: in Game_0, the challenger $\mathcal{B}$ generates the public parameters $\mathrm{PP} = \{\mathbf{A}, (\mathbf{B}_i)_{1 \le i \le k}, \mathbf{u}\}$ and the master key $\mathrm{MK} = (\mathbf{T}_\mathbf{A})$ where $\mathbf{A} = [\mathbf{A}'|\mathbf{G}_n - \mathbf{A}'\mathbf{T}_\mathbf{A}]$. In this game, let W^* be the challenge access structure, and we change the way A is generated. $\mathcal{B}$ firstly selects k uniformly random matrix $\mathbf{B}_i \in \mathbb{Z}_q^{n \times n}$ as the public parameters for each attribute categories and then computes $\mathbf{H}_{W^*} = \sum_{\forall \mathbf{v}_{i,j} \in W^*} \mathbf{B}_i H(\mathbf{v}_{i,j}) - \mathbf{I}$. Finally $\mathcal{B}$ constructs $\mathbf{A} = [\mathbf{A}'| - \mathbf{H}_{W^*}\mathbf{G}_n - \mathbf{A}'\mathbf{T}_\mathbf{A}]$. The matrix $\mathbf{A}$ in Game_0 and Game_1 is statistically indistinguishable.

The adversary makes key query for attribute list L, and L does not satisfy W^*. $\mathcal{B}$ answers the key query. He computes $\mathbf{A}_L = \mathbf{A} + [0|\mathbf{H}_L\mathbf{G}_n] = [\mathbf{A}'|(\mathbf{H}_L - \mathbf{H}_{W^*})\mathbf{G}_n - \mathbf{A}'\mathbf{T}_\mathbf{A}]$ and samples $\mathbf{r}_L \in \mathbb{Z}_q^m$ for $\mathcal{A}$ as $\mathbf{r}_L \leftarrow \mathrm{SamplePre}(\mathbf{A}, \mathbf{H}_L, \mathbf{G}_n, \mathbf{T}_\mathbf{A}, \mathbf{u}, \sigma)$. Then, $\mathcal{B}$ sends $\mathbf{r}_L$ to $\mathcal{A}$. Note that if $L = W^*$, it has $\mathbf{H}_L - \mathbf{H}_{W^*} = 0$, and $\mathbf{A}_L = [\mathbf{A}'| - \mathbf{A}'\mathbf{T}_\mathbf{A}]$. $\mathcal{B}$ can no longer answer the key query. Since $\mathcal{B}$ answers, the key queries are statistically indistinguishable in Game_0 and Game_1. The advantage of adversary in Game_0 is at most negligibly different from it in Game_1, i.e.,

$$\left|\mathrm{Adv}_{W_1}(\mathcal{A}) - \mathrm{Adv}_{W_0}(\mathcal{A})\right| = \mathrm{negl}(n). \tag{20}$$

Game_2: in this scheme, we change the way that $\mathbf{C}^*$ is generated. Different to Game_1, $\mathbf{C}^*$ is chosen uniformly from $\mathbb{Z}_q^{(1+m)\times M}$. Since the challenge ciphertext $\mathbf{C}^*$ is always a random matrix in this scheme, the adversary's advantage is 0; that is,

$$\mathrm{Adv}_{W_2}(\mathcal{A}) = 0. \tag{21}$$

Reduction from LWE: suppose $\mathcal{A}$ has a nonnegligible advantage in distinguishing Game_1 and Game_2. Based on Lemma 4, we use $\mathcal{A}$ to construct an LWE algorithm denoted $\mathcal{B}$.

$\mathcal{B}$ receives $(\overline{m} + 1) \times M$ samples such that

$$\begin{aligned}
&\left\{\left(\mathbf{a}_0, b_{0,1}\right), \left(\mathbf{a}_1, b_{1,1}\right), \ldots, \left(\mathbf{a}_{\overline{m}}, b_{\overline{m},1}\right)\right\} \in \left(\mathbb{Z}_q^n \times \mathbb{Z}_q\right),\\
&\left\{\left(\mathbf{a}_0, b_{0,2}\right), \left(\mathbf{a}_1, b_{1,2}\right), \ldots, \left(\mathbf{a}_{\overline{m}}, b_{\overline{m},2}\right)\right\} \in \left(\mathbb{Z}_q^n \times \mathbb{Z}_q\right),\\
&\cdots\cdots\\
&\left\{\left(\mathbf{a}_0, b_{0,M}\right), \left(\mathbf{a}_1, b_{1,M}\right), \ldots, \left(\mathbf{a}_{\overline{m}}, b_{\overline{m},M}\right)\right\} \in \left(\mathbb{Z}_q^n \times \mathbb{Z}_q\right),
\end{aligned} \tag{22}$$

which is sampled from either $(\mathbf{A}, \mathbf{A}^\top \mathbf{S} + \mathbf{E})$ or $(\mathbf{A}, \mathbb{Z}_q^{m \times M})$.

Init: the adversary $\mathcal{A}$ chooses the challenge access structure W^*, and send it to the simulator $\mathcal{B}$.

Setup: the challenger $\mathcal{B}$ constructs PP as follows:

(1) Let $\mathbf{A}' = (\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{\overline{m}}) \in \mathbb{Z}_q^{n \times \overline{m}}$ and $\mathbf{u} = \mathbf{a}_0$. Construct the other public parameters, namely, $\mathbf{B}_i$ and $\mathbf{A}$, as Game_1.
(2) Send $\mathrm{PP} = \{\mathbf{A}, (\mathbf{B}_i)_{1 \le i \le k}, \mathbf{u}\}$ to $\mathcal{A}$.

Queries: in this step, $\mathcal{A}$ can make key queries for a sequence of attribute list L. However, he cannot query an attribute list which satisfies W^*. $\mathcal{B}$ answers the queries as Game_1.

Challenge: the adversary $\mathcal{A}$ sends a message $\mu^* \in \{0, 1\}$ to $\mathcal{B}$. The simulator $\mathcal{B}$ generates the challenge ciphertext as follows:

(1) Let $\mathbf{b}_0 = (b_{0,1}, b_{0,2}, \ldots, b_{0,M})$ and

$$\mathbf{B} = \left(b_{i,j}\right) = \begin{bmatrix} b_{1,1}, b_{1,2}, \ldots, b_{1,M} \\ b_{2,1}, b_{2,2}, \ldots, b_{2,M} \\ \cdots \\ b_{\overline{m},1}, b_{\overline{m},2}, \ldots, b_{\overline{m},M} \end{bmatrix} \in \mathbb{Z}_q^{\overline{m} \times M}. \tag{23}$$

(2) Compute $\mathbf{T}_\mathbf{A}^\top \mathbf{B}$ and let $\mathbf{B}^* = \begin{bmatrix} \mathbf{B} \\ -\mathbf{T}_\mathbf{A}^\top \mathbf{B} + \widehat{\mathbf{E}} \end{bmatrix}$ where $\widehat{\mathbf{E}} \longleftarrow \chi^{\overline{n} \times M}$.
(3) Compute the challenge ciphertext

$$\mathbf{C}^* = \begin{bmatrix} \mathbf{b}_0 \\ \mathbf{C}^* \end{bmatrix} + \mu^* \mathbf{G}. \tag{24}$$

If the samples are drawn from $(\mathbf{A}, \mathbf{A}^\top \mathbf{S} + \mathbf{E})$, we have

$$\mathbf{b}_0 = \mathbf{a}_0^\top \cdot (\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_M) + \left(e_{0,1}, e_{0,2}, \ldots, e_{0,M}\right) = \mathbf{a}_0^\top \mathbf{S} + \mathbf{e}_0. \tag{25}$$

The same to $\mathbf{b}_0$, we have

$$\mathbf{B} = \left(b_{i,j}\right) = \begin{bmatrix} \mathbf{a}_1^\top \mathbf{S} + \mathbf{e}_1 \\ \mathbf{a}_2^\top \mathbf{S} + \mathbf{e}_2 \\ \cdots \\ \mathbf{a}_{\overline{m}}^\top \mathbf{S} + \mathbf{e}_{\overline{m}} \end{bmatrix} = (\mathbf{A})'^\top \mathbf{S} + \mathbf{E}', \tag{26}$$

where $\mathbf{E}' = (\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_{\overline{m}})^\top$. Thus, referring to equation (26), we have

Table 2: The comparing of related lattice-based schemes.

Scheme	PP size	MK size	SK_L size	Ciphertext size	Security	Fully homomorphic
[4]	$(2\ell m + m + 1)n \log q$	m^2	$\ell m \log q$	$(2\ell - \lvert A_c \rvert)m \log q + \log q$	SM sCPA	No
[17]	$(2\ell m + 9)n \log q$	$(2\ell + 9)m^2$	$3m^2 \log q$	$(\ell m + \lvert g_w \rvert + 1)\log q$	SM sCPA	No
[19]	$2\ell mn \log q$	m^2	$m \log q$	$(\ell + 1)mnt \log q$	No security reduction	No
[21]	$(2\ell m + 1)n \log q$	$2\ell m^2$	$2m^2 \log q$	$[(\ell m + 1)t]^2 \log q$	SM sCPA	Yes
[24]	$(\ell nt + nt + m + 1)n \log q$	m^2	$(m + nt)\log q$	$(\ell nt + nt + m + 1)(nt + m + 1)t \log q$	SM sCPA	Yes
Ours	$(kn + m + 1)n \log q$	$\overline{m} \times \overline{n}$	$m \log q$	$(m + 1)^2 t \log q$	SM sCPA	Yes

$t = \lceil \log q \rceil$, $\overline{n} = nt$, $\overline{m} = m - \overline{n}$, ℓ: the maximum number of system's attributes. k: the maximum number of system attribute categories. $\ell = \sum_{i=1}^{k} S_k$, $\lvert A_c \rvert$: the number of ciphertext's attribute in [4]. $\lvert g_w \rvert$: the number of gates in access policy in [17]. SM: standard model. sCPA: selective chosen plaintext attack.

$$\mathbf{B}^* = \begin{bmatrix} \mathbf{B} \\ -\mathbf{T}_{\mathbf{A}}^{\top}\mathbf{B} + \mathbf{E} \end{bmatrix} = \begin{bmatrix} (\mathbf{A})'^{\top}\mathbf{S} + \mathbf{E}' \\ \left(-\mathbf{A}'\mathbf{T}_{\mathbf{A}}\right)^{\top}\mathbf{S} - \mathbf{T}_{\mathbf{A}}^{\top}\mathbf{E}' + \widehat{\mathbf{E}} \end{bmatrix} = \mathbf{A}_{W^*}^{\top}\mathbf{S} + \begin{bmatrix} \mathbf{E}' \\ -\mathbf{T}_{\mathbf{A}}^{\top}\mathbf{E}' + \widehat{\mathbf{E}} \end{bmatrix}, \tag{27}$$

where $\mathbf{A}_{W^*}$ is the same as it in Game_1. Referring to equations (25) and (27), the challenge ciphertext $\mathbf{C}^*$ in equation (24) is valid as it is in Game_1.

If the samples are drawn from a uniformly random distribution, $\mathbf{b}_0$ and $\mathbf{B}$ are uniformly random. Therefore, the challenge ciphertext $\mathbf{C}^*$ is uniformly random as it is in Game_2.

Continuation: Queries phase is repeated.

Guess: $\mathscr{A}$ guesses if it is interacting with a Game_1 or Game_2 challenger. $\mathscr{B}$ outputs $\mathscr{A}$'s guess as the answer to the $\text{DLWE}_{n,q,\chi}$ challenge it is trying to solve. Thus, the advantage of $\mathscr{B}$ in solving $\text{DLWE}_{n,q,\chi}$ problem is equal to the adversary's advantage in distinguish Game_1 or Game_2. So, we have $\lvert \text{Adv}_{W_2}(\mathscr{A}) - \text{Adv}_{W_1}(\mathscr{A}) \rvert \leq \text{DLWE} - \text{Adv}(\mathscr{B})$. □

5. Performance Analysis

In this section, we make a comparison between our scheme and related lattice-based ABE schemes.

As shown in Table 2, the public parameters in [4] consist of $(2\ell + 1)$ $n \times m$ matrices and an n-dimensional vector, the public parameters in [17] consist of $(2\ell + 9)$ $n \times m$ matrices, the public parameters in [19] consist of 2ℓ $n \times m$ matrices, the public parameters in [21] consist of 2ℓ $n \times m$ matrices and an n-dimensional vector, the public parameters in [24] consist of $\ell + 1$ $n \times nt$ matrices, an $n \times m$ matrix, and an n-dimensional vector, and the public parameters in our construction consist of k $n \times n$ matrices, an $n \times m$ matrix, and an n-dimensional vector. Observe that the total number of system's attributes ℓ contributes the most to the growth of PP size in [4, 17, 19, 21, 24] while the total number of system's attribute categories k contributes the most to the growth of PP size in our scheme. Due to the fact that $\ell = \sum_{i=1}^{k} S_k$ (see Section 4), the PP size in our scheme is much smaller than it in [4, 21, 24]. The MK size in [17, 21] is also related to ℓ, so it is larger than [4, 19, 24] and ours. The user's private keys in [4] are related to the number of system's attributes ℓ; therefore, the SK_L size is the largest among all the related schemes. Taken together, the SK_L size in both our scheme and [24] is smaller than others. The ciphertext sizes in [4, 17, 19] are relatively small, but they cannot support fully homomorphic. The ciphertext size in our scheme is the smallest among the all schemes which support fully homomorphism because the ciphertext is a $(1 + m) \times (1 + m)t$ matrix which is not related to the number of system's attributes. However, the ciphertext is a $(\ell m + 1)t \times (\ell m + 1)t$ matrix in [21], and in [24], the ciphertext consists of ℓ $nt \times (nt + m + 1)t$ matrices and a $(nt + m + 1) \times (nt + m + 1)t$ matrix. It is obvious that the ciphertext sizes in [21, 24] depend on the total number of system's attributes ℓ. In our scheme, we remove this dependency on ℓ by making a classification of system's attributes. Besides, although [19] is a lattice-based ABE scheme which is constructed under the LWE problem, it does not give a security reduction and leave the security reduction as an open problem. Under the DLWE assumption, the lattice-based ABE schemes [4, 17, 21, 24] and our scheme are secure against selective chosen ciphertext attack (sCPA) in the standard model. Since [4, 17, 19] cannot support homomorphic operations on ciphertext, so we only make a comparison of the ciphertext size between our scheme and [21, 24] which support homomorphic operations on ciphertext. In our scheme, we classify ℓ system's attributes into k attribute categories. Each attribute can be denoted by two parts: attribute category and attribute value. Each attribute category has some different attribute values. In the user's attribute set and access policy, at most one attribute value can be set under each attribute category. It is obvious that the size is dependency on the number of attribute categories k. As shown in Figure 1, according to the suggestion in [16, 27, 31], we set the parameters $n = 284$, $q = 2^{24}$, and $\ell = 1, 2, 4, 8, 32, 128$, respectively. The comparison shows that the ciphertext sizes of [21, 24] growth based on the total number of system's attributes ℓ while it is fixed in our scheme no matter what the total number of system's attributes ℓ is, and when $\ell = 2$, the size of ciphertext in our scheme is reduced by at least 73.3%, not to mention $\ell > 2$.

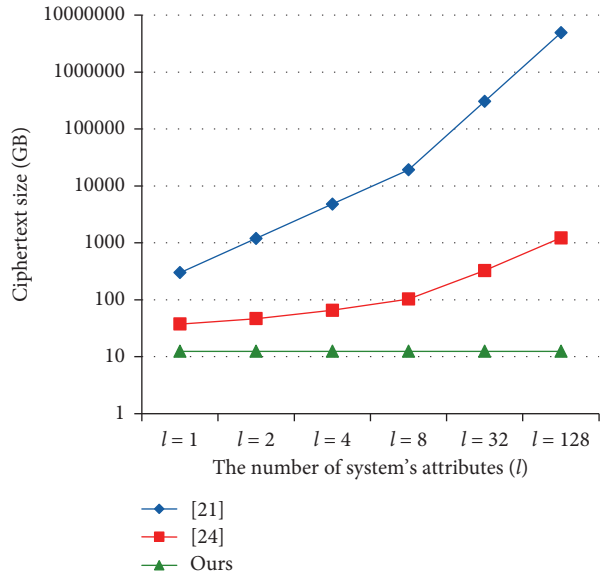

Figure 1: The storage overhead of ciphertext comparing between our scheme and related ABFHE.

Table 3: The comparison on time complexity of related ABFHE.

Scheme	Encryption	Decryption
[21]	$O(\ell^2 m^2 t^2 + \ell nm)$	$O(\ell m)$
[24]	$O(\ell mn^2 t^2 + \ell n^3 t^3 + m^2 nt + mn^2 t^2)$	$O(m^2 t + mnt^2 + n^2 t^3)$
Ours	$O(m^2 nt)$	$O(m)$

$t = \lceil \log q \rceil$, ℓ: the maximum number of system attributes

The comparison of time complexity is shown in Table 3. The encryption time in our scheme is smaller than [21, 24] since the encryption time in [21, 24] is related to the total number of system's attribute ℓ. According to the suggestion given in [27, 31], let $\ell = n/4$ and $m \approx 2n \log q$. The encryption time in [21, 24] is approximately equal to $O(n^4 t^3)$ while it is approximately equal to $O(n^3 t^2)$ in our construction. As for the decryption time, our scheme and [21] both use one column of ciphertext for decryption, but in [24], a $(nt + m + 1) \times (nt + m + 1)t$ ciphertext matrix is used for decryption. Therefore, the decryption time in [24] is the longest. In addition, the growth of decryption time in [21] is based on the total number of system's attributes ℓ, so the decryption time is also longer than our scheme.

6. Conclusion

In this paper, based on the LWE problem, we propose an attribute-based fully homomorphic encryption scheme with short ciphertext which is suitable for the cloud computing environment. A short ciphertext can not only reduce the communication overhead but also reduce the running time of encryption, decryption, and homomorphic operations. In our scheme, by classifying the system's attributes and using the special structure matrix, the size of ciphertext is no longer increased with the total number of system's attributes. Moreover, by using the function $\mathbf{G}^{-1}$, we have a very tight and simple error analysis by using sub-Gaussianity, and in the homomorphic multiplication, $\mathbf{G}^{-1}$ can completely rerandomize the error term in a ciphertext. Unfortunately, in order to improve the efficiency of space and time, we just set an "AND" access policy. Next, we will continue to study the attribute-based fully homomorphic encryption scheme from lattices that support more flexible access policy.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Key Reaearch and Development Program of China (2017YFB0803001), the Shandong Provincial Key Research and Development Program of China (2018CXGC0701), the National Natural Science Foundation of China (NSFC) (no. 61972050), the BUPT Excellent Ph.D. Students Foundation (no. CX2019119), the Beijing Natural Science Foundation (no. L191012), the Team Project of Collaborative Innovation in Universities of Gansu Province (no. 2017-16), and the Major Project of Gansu University of Political Science and Law (no. 2016XZD12).

References

[1] A. Sahai and B. Waters, "Fuzzy identity-based encrypton," in *Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'05)*, pp. 457–473, Aarhus, Denmark, 2005.

[2] V. Goyal, Q. Pandey O, A. Sahai et al., "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS'06)*, pp. 89–98, Alexandria, VI, USA, 2006.

[3] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in *Proceedings of the 37th Annual Acm Symposium on Theory of Computing (STOC'05)*, pp. 84–93, Baltimore, UK, May 2005.

[4] J. Zhang and Z. F. Zhang, "A Ciphertext policy attribute-based encryption scheme without pairing," in *Proceedings of the 7th International Conference on Information Security and Cryptology (Inscrypt'11)*, pp. 324–340, Beijing, China, 2011.

[5] J. Zhang, Z. F. Zhang, and A. J. Ge, "Ciphertext policy attribute-based encryption from lattices," in *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security (ASIACCS'12)*, pp. 16-17, Seoul, Korea, May 2012.

[6] S. Agrawal, X. Boyen, V. Vaikuntanathan et al., "Functional encryption for threshold functions (or Fuzzy IBE) from lattices," in *Proceedings of the 15th International Conference on Practice and Theory in Public Key Cryptography (PKC'12)*, pp. 280–197, Darmstadt, Germany, May 2012.

[7] X. Boyen, "Attribute-based functional encryption on lattices," in *Proceedings of the 10th Theory of Cryptography Conference on Theory of Cryptography (TCC'13)*, pp. 122–142, Tokyo, Japan, March 2013.

[8] X. Liu, J. Ma, J. Xiong, Q. Li, T. Zhang, and H. Zhu, "Threshold attribute-based encryption with attribute hierarchy for lattices in the standard model," *IET Information Security*, vol. 8, no. 4, pp. 217–223, 2014.

[9] S. Gorbunov, V. Vaikuntanathan, and H. Wee, "Attribute-based encryption for circuits," in *Proceedings of the 44th Annual ACM Symposium on Theory of Computing (STOC'13)*, pp. 545–554, Palo Alto, California, USA, June 2013.

[10] Y. T. Wang, "Lattice ciphertext policy attribute-based encryption in the standard model," *International Journal of Network Security*, vol. 16, no. 6, pp. 444–451, 2014.

[11] J. Zhao, H. Y. Gao, and J. Q. Zhang, "Attribute-based encryption for circuits on lattices," *Tsinghua Science and Technology*, vol. 19, no. 5, pp. 463–469, 2014.

[12] Z. Brakerski and V. Vaikuntanathan, "Circuit-ABE from LWE: unbounded attributes and semi-adaptive security," in *Proceedings of the 36th International Cryptology Conference (CRYPTO'16)*, pp. 363–384, Santa Barbara, CA, USA, August 2016.

[13] G. Y. Zhang, J. Qin, and S. Qazi, "Multi-authority attribute-based encryption scheme from lattices," *Journal of Universal Computer Science*, vol. 21, no. 3, pp. 483–501, 2015.

[14] L. H. Liu, S. P. Wang, and Q. Yan, "A multi-authority key-policy ABE scheme from lattices in mobile Ad Hoc Network," *Ad Hoc Sensor Wireless Networks*, vol. 37, pp. 117–143, 2017.

[15] Y. Liu, L. C. Wang, L. X. Li et al., "Secure and efficient multi-authority attribute-based encryption scheme from lattices," *IEEE Access*, vol. 7, pp. 3665–3674, 2018.

[16] K. Gur, Y. Polyakov, K. Rohloff et al., "Practical applications of improved Gaussian sampling for trapdoor lattices," *IEEE Transactions of Computers*, vol. 68, no. 4, pp. 570–584, 2019.

[17] G. Wang, Z. Liu Z, and D. Gu, "Ciphertext policy attribute-based encryption for circuits from LWE assumption," in *Proceedings of the 21st International Conference on Information and Communications Security (ICICS'19)*, pp. 278–396, Beijing, China, December 2019.

[18] X. Dong, Y. Zhang, B. Wang et al., "Server-aided revocable attribute-based encryption from lattices," *Security and Communication Networks*, vol. 2020, no. 13, 2020.

[19] Z. Brakerski and V. Vaikuntanathan, "Lattice-inspired broadcast encryption and succinct ciphertext-policy ABE," *IACR Cryptology*, vol. 191, 2020.

[20] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proceedings of the 41st Annual ACM Symposium on Symposium on Theory of Computing (STOC'09)*, p. 169, Bethesda, MD, USA, June 2009.

[21] C. Gentry, A. Sahai, and B. Waters, "Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-based," in *Proceedings of the 33rd Annual International Conference on Cryptology (CRYPTO'13)*, pp. 75–92, Santa Barbara, California, USA, August 2013.

[22] D. Boneh, C. Gentry, S. Gorbunov et al., "Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuit," in *Proceedings of 33nd Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'14)*, pp. 533–556, Copenhagen, Denmark, May 2014.

[23] M. Clear and C. McGoldrick, "Attribute-based fully homomorphic encryption with a bounded number of inputs," in *Proceedings of the 8th International Conference on Cryptology in Africa (AFRICACRYPT'16)*, pp. 307–324, Morocco, April 2016.

[24] Z. Brakerski, D. Cash D, R. Tsabary et al., "Targeted homomorphic attribute-based encryption," in *Proceedings of Theory of Cryptography (TCC'16)*, pp. 330–360, Beijing, China, 2016.

[25] S. Tan and A. Samsudin, "Ciphertext policy-attribute based homomorphic encryption (CP-ABHER-LWE) scheme: a fine-grained access control on outsourced cloud data computation," *Journal of Information Science and Engineering*, vol. 33, pp. 675–694, 2017.

[26] R. Hiromasa and Y. Kawai, "Dynamic multi target homomorphic attribute-based encryption," in *Proceedings of IMA International Conference on Cryptography and Coding (IMACC'17)*, pp. 25–43, Oxford, UK, December 2017.

[27] D. Micciancio and C. Peikert, "Trapdoors for lattices: simpler, tighter, faster, smaller," in *Proceedings of 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'12)*, vol. 7237, pp. 700–718, Heidelberg, Germany, 2012.

[28] J. Alperin-Sheriff and C. Peikert, "Faster bootstrapping with polynomial error," in *Proceedings of the 34th Annual Cryptology Conference (CRYPTO'14)*, pp. 297–314, Santa Barbara, CA, USA, August 2014.

[29] R. Vershynin, *Compressed Sensing, Theory and Applications*, Cambridge University Press, Yonina Eldar, Gitta Kutyniok, UK, 2012.

[30] S. Agrawal, D. Boneh, and X. Boyen, "Efficient lattice (H)IBE in the standard model," in *Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'10)*, vol. 6110, pp. 553–572, Heidelberg, Germany, May 2010.

[31] W. Dai, Y. Doroz, Y. Polyakov et al., "Implementation and evaluation of a lattice-based key-policy ABE scheme," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 5, pp. 1169–1184, 2018.