Hindawi
Security and Communication Networks
Volume 2021, Article ID 2847731, 11 pages
https://doi.org/10.1155/2021/2847731

Research Article

Efficient Identity-Based Broadcast Encryption Scheme on Lattices for the Internet of Things

Kai He,[1] **Xueqiao Liu**,[2] **Jia-Nan Liu**,[3] **and Wei Liu**[3]

[1]*School of Cyberspace Security, Dongguan University of Technology, DongGuan 523808, China*
[2]*Institute of Cybersecurity and Cryptology, School of Computing and Information Technology, University of Wollongong, Wollongong 2522, Australia*
[3]*The College of Cyber Security, Jinan University, Guangzhou 510632, China*

Correspondence should be addressed to Jia-Nan Liu; j.n.liu@foxmail.com

Received 11 June 2021; Accepted 22 November 2021; Published 13 December 2021

Academic Editor: David Megias

In an identity-based broadcast encryption (IBBE) scheme, the ciphertext is usually appended with a set of user identities to specify intended recipients. However, as IBBE is adopted in extensive industries, the demand of anonymity for specific scenarios such as military applications is urgent and ought no more to be ignored. On the contrary, how to optimize computation and communication is an unavoidable challenge in the IBBE scheme construction, especially in the large-scaled resource-limited wireless networks such as the Internet of Things (IoT), where the cost of computation and communication should be mitigated as much as possible since other functions including connectivity and privacy should be given the top priority. Thus, we present an IBBE scheme from the lattice, in which we employ the Chinese remainder theorem and lattice basis delegation in fixed dimensions to obtain several desirable characteristics, such as constant-size public parameter, private key, and ciphertext. In addition, our encryption and decryption algorithms are more efficient than broadcast encryption (BE) schemes based on number-theoretic problems. To be noticed, our scheme can simultaneously achieve confidentiality and outsider anonymity against the chosen-plaintext attack under the hardness of the learning with error (LWE) problem.

1. Introduction

IoT is a network of interconnected things/devices, in which sensors, software, network connections, and necessary electronic devices are integrated to collect and exchange information and respond to real-time data requests. IoT allows data accumulation from and exchange between the physical world and computer systems through existing network infrastructures. With these connected tiny and smart devices, one's life can be of higher quality, safer, smarter, more convenient, comfortable, and timely informed than ever before. Security is one of the main concerns mentioned by cybersecurity experts. They believe that even end device connectivity and information sharing can be exploited to have a negative impact on a person safety and well-being. Besides hacking IoT devices to compromise online data and privacy, it can also become the entry point of invading the entire network [1, 2].

Remote terminal unit (RTU) [1] is an electronic device, which is installed in a remote site (generally, few people supervise the distant site). It is used to monitor and control sensors and equipment remotely and widely adopted in the supervisory control and data acquisition (SCADA) system. RTU usually converts the measured state or signal into a data format that can be sent on the communication medium by using the Modbus protocol. It can also receive commands sent by the central monitor computer to execute functional control of the equipment. As the Modbus protocol does not apply data encryption mechanism, the data flow between the monitor center and RTU is in plaintext. As a consequence, the data transmitted in the open network may be eavesdropped or tampered with. What is worse, the data tampering may cause disorder in the automated production process or even serious accidents of equipment damage. To keep the confidentiality of data transmission, cryptographic

modules can be embedded in data collection equipment such as RTU/DTU and effectively help prevent data theft and command tampering [2]. Once the concern of confidentiality is got rid of, such devices can be safely applied to industrial control industries such as oil and gas exploitation, environmental monitoring, power transmission and transformation, oil and gas pipeline networks, and hydrological monitoring.

Fiat and Naor [3] first introduced broadcast encryption, which allows a sender to send an encrypted message to a large number of receivers via public channels, and only authorized users can obtain the message, as shown in Figure 1. Compared with the public key encryption for a single recipient, BE significantly saves computing and communication costs. Therefore, BE has been promoted to numerous applications, such as key distributing [4], encrypted file sharing [5], satellite TV subscription [6], digital right management [7], and social network service [8]. Take pay service as an example. As shown in Figure 2, nonpaying user U_2 cannot enjoy the service or just is able to enjoy limited service, while paying users $(U_1, U_3, \ldots, U_n)$ can enjoy entire and high-quality service. There are a large number of related works that can be classified into the conventional BE [6, 9–13] since they are based on number-theoretic problems, such as big integer factoring and discrete logarithm problem, and rarely meet the requirements of industrial applications.

With the advent of quantum cryptography, the security of conventional BE schemes is heavily threatened. In FOCS′94, Shor [14] proposed a quantum algorithm to solve the problem of discrete logarithm and factorization in polynomial time. Thereafter, it becomes one of the most urgent topics to design BE schemes against quantum attacks.

Lattice cryptography can resist quantum-computing attacks [15] and has multiple advantages over the conventional cryptography. Firstly, lattice is a vector space composed of n linearly independent vectors $b_1, \ldots, b_n$ in $\mathbb{R}^m$, which only request lightweight operations such as modular addition and matrix multiplication. Thus, it is suitable for devices with limited computational ability such as smart cards. Secondly, lattice cryptography enjoys pretty strong security guaranteed by the worst-case hardness assumptions [16, 17], such as shortest vector problem (SVP) [18] and closest vector problem (CVP) [18]. Thirdly, lattice cryptography can be adopted to comparable extensive industries as its conventional cryptography was, given almost all conventional public key encryption (PKE) schemes based on big integer factoring or discrete logarithm problems can also be realized in lattice cryptography.

A desirable BE scheme on lattices should keep not only confidentiality but also anonymity as anonymity is an extremely favourable characteristic for diverse BE systems [19]. To distinguish authorized receivers from the unauthorized, BE ciphertext usually includes the intended recipients' identities. This means users' identity information is revealed. Specifically, such identity exposure is expected to be avoided when users' identities are sensitive. For instance, in the military field, the set of broadcast receiver identities undoubtedly implies specific military objectives or personnel. Meanwhile, to support a large number of receivers in a BE system, the public key of every receiver can be conveniently chosen as a meaningful string, which is their unique identification, such as a passport number or an e-mail address. This is exactly the motivation of proposing an IBBE system that is capable to support exponential user scale.

1.1. Our Results. Each BE system involves multiple recipients. Thus, it is intricate to construct a BE scheme in a lattice context. Our main contributions include the construction of an anonymous IBBE from the lattice and the security reduction to the LWE problem. Our design is inspired by the lattice-based BE scheme of Wang et al. [20], which depends on the Chinese remainder theorem to achieve the dynamic anonymity. In this work, we rely on the Chinese remainder theorem to construct an IBBE scheme, and the core idea is as follows.

The Chinese remainder theorem offers one-dimensional linear congruence equation $x \equiv a_i \,(\mathrm{mod} q_i)$ that has and only has one solution $x = Q_1 Q_1' a_1 + \cdots + Q_k Q_k' a_k \,(\mathrm{mod} Q)$. In order to construct a BE scheme on lattices, we combine the Chinese remainder theorem with the LWE hardness assumption.

(i) Firstly, we extend the Chinese remainder theorem to a matrix form, such as x and a_i are extended to matrices X and A_i with dimension $n \times m$, respectively. Thus, the system of linear congruence equations has the similar solution; that is, $X = Q_1 Q_1' A_1 + \cdots + Q_k Q_k' A_k \,(\mathrm{mod} Q)$, where X is close to uniform distribution [20] if A_i is a random matrix over Z_q^n.

(ii) Then, choose a random vector s, which is to blind X. Blind results are used to encapsulate symmetric keys K, e.g., $C_2 = (\sum_{i=1}^{k} Q_i Q_i' A_i)(\sum_{i=1}^{k} Q_i Q_i' s) + 2e + K) \,(\mathrm{mod} Q)$, where A_i and q_i are receiver i's public keys and e is an error vector. Since the key encapsulation is constructed by the Chinese remainder theorem, its distribution is indistinguishable from the uniform distribution [20].

(iii) Thirdly, when authorized receiver i decrypts the ciphertext, he does not need to know the other users' identities. He firstly computes C_2 mod q_i, where qi is his public key. and then C_2 is transformed to a LWE instance vector related to his public key A_i, i.e., $C_2 \,(\mathrm{mod} q_i) = (A_i^{\top} s + 2e + K) \,(\mathrm{mod} q_i)$. Now, authorized receiver i uses his private key to decrypt $(A_i^{\top} s + 2e + K) \,(\mathrm{mod} q_i)$ to obtain the symmetric key K and then gets the broadcast message.

(iv) To obtain an IBBE scheme, we need to connect users' public keys A_i and q_i to identity ID_i. Firstly, we use an encoding function $H_1 \colon \mathbb{Z}_q^n \longrightarrow \mathbb{Z}_q^{n \times n}$ to map identities $ID_i \in \mathbb{Z}_q^n$ to matrices $A_i \in \mathbb{Z}_p^{n \times h}$, i.e., $A_i = H_1(ID_i)$ [21], and a division intractable hash function $H_2 \colon \{0,1\}^* \longrightarrow \mathbb{Z}_q^n$ to map identities $ID_i \in \mathbb{Z}_q^n$ to integer $q_i \in \mathbb{Z}_p^n$. Note that integer q_i is a prime with an overwhelming probability [22] so

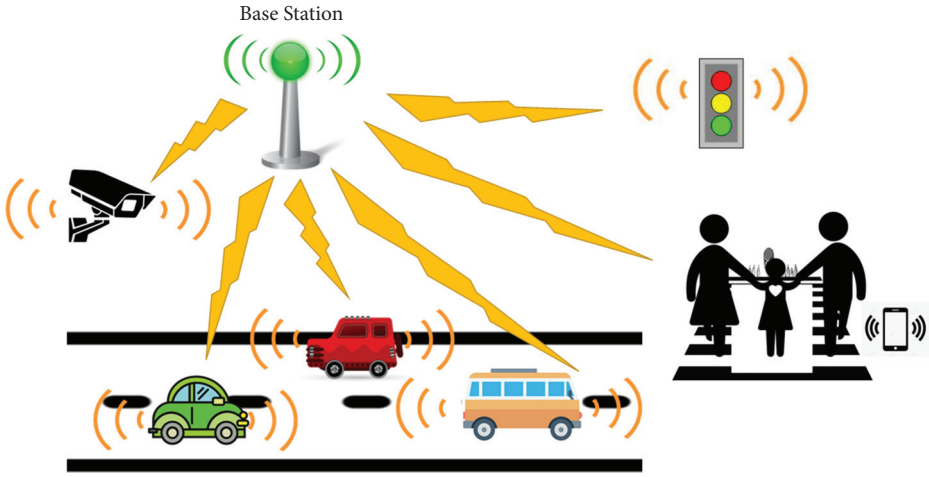

Figure 1: Broadcast in the Internet of Vehicles network.

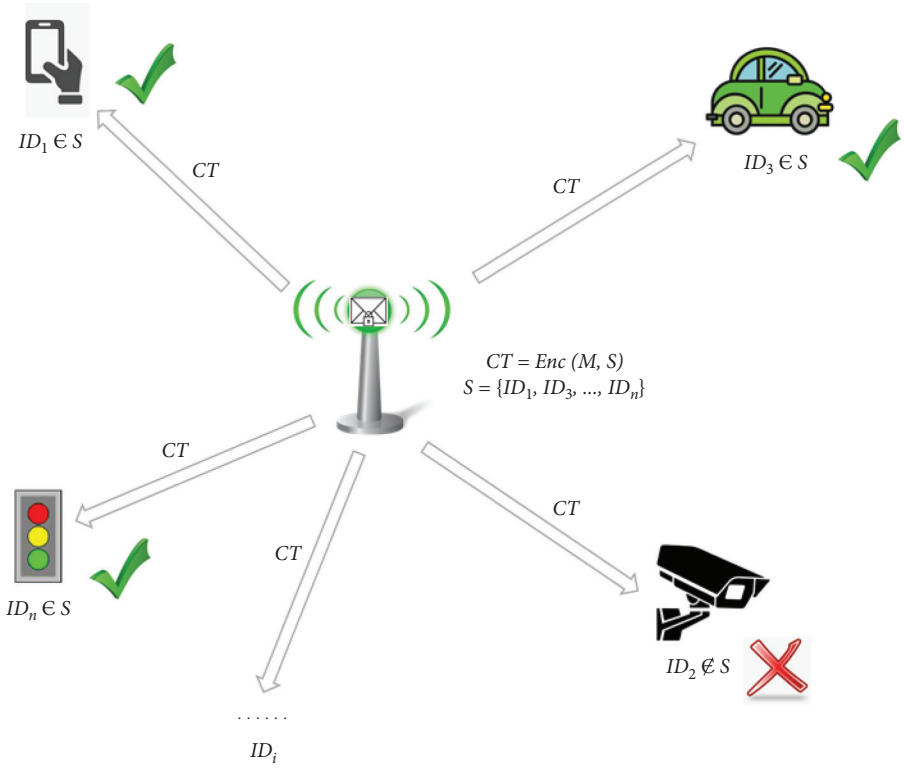

Figure 2: IBBE for pay service.

that user i's public key q_i and user j's public key q_j are ensured mutually prime.

(v) Lattice basis delegation mechanisms were proposed by Cash et al. [23] and Agrawal et al. [21]. Given a matrix $A \in \mathcal{Z}_q^{n \times m}$ and a lattice basis T_A of $\Lambda_q^{\perp}(A)$, a matrix B from A and a random basis T_B for $\Lambda_q^{\perp}(B)$ can be generated. However, in [21, 23], the dimension of matrix B is larger than the dimension of the given matrix A. So, the ciphertext and private key sizes of their HIBE schemes increase as the hierarchy deepens. Thus, in terms of private key generation of our scheme, we employ lattice basis delegation with constant dimension technology [21] to generate the user private key, where $B = AR^{-1} \in \mathcal{Z}_q^{n \times m}$ and B has the same dimension as A. Thence, the private key size of our scheme is constant, and the size of the ciphertext has nothing to do with the number of recipients.

1.2. Related Work. Identity-based encryption (IBE) [24] is a special kind of BE. There is one receiver set specifying intended receivers, and in an IBE scheme, the user public

key can be any string as long as the string can be a uniquely identified user, such as a passport number and e-mail address. In 2008, Craig et al. [25] proposed the technology of lattice-based one-way trapdoor function and constructed an IBE scheme whose security is based on the LWE problem [26] in the random oracle model. In their scheme, trapdoor sampling algorithm [27] is used for generating the master public key and master secret key. Then, the preimage sampler [25] takes the master secret key as the input to generate the user's secret key. Finally, both the master public key and the user's identity are used to generate two separate pseudorandom LWE instances as the ciphertexts.

Hierarchical identity-based encryption (HIBE) [28, 29] is also a special kind of BE. Users in the broadcast set have a hierarchical structure, and the lower-level users' keys are generated by the higher-level users. In 2010, Cash et al. [23, 30] proposed a new concept of cryptography, called bonsai tree, and constructed an HIBE scheme based on the LWE problem by utilizing the lattice basis delegation technique, which allows one to use a short basis of a certain integer lattice L to generate a short random basis for a new lattice L_0 derived from L. However, in their HIBE scheme, the dimension of the child lattice L_0 is greater than that of the parent lattice L for the reason that, as the hierarchical structure increases, the private key and ciphertext also become longer. Shweta Agrawal and Boyen [31] proposed a lattice basis delegation technique which does not increase the dimension of the lattices involved and presented two HIBE schemes with shorter ciphertext and private keys with and without the random oracle based on the LWE problem, respectively.

Attribute-based encryption (ABE) [32] and BE are both one kind of one-to-many encryption. In the ABE system, the private key and the ciphertext are related to the attributes; when the attributes owned by the user match the ciphertext attributes, the user can obtain the ciphertext. Boyen [33] proposed an efficient ABE scheme and proved its security in the selective sense from LWE hardness assumption in the standard model. Nevertheless, BE needs to specify which users are authorized receivers.

Fiat and Naor first introduced BE [3]. In 2005, Boneh et al. [11] proposed the first fully collusion-resistant BE scheme with static security, and both the size of ciphertexts and private keys are constant, but the size of the public key is proportional to the number of receivers. In 2009, Craig and Waters [13] proposed a BE scheme with adaptive security in the random oracle model. In 2007, Delerablée [34] proposed the first IBBE scheme, which obtains adaptive chosen-ciphertext attack (CCA) in the random oracle model, as well as has constant-size ciphertexts and private keys. In 2009, Craig and Waters [13] presented the first IBBE scheme, which is against adaptively chosen-plaintext secure in the standard model. In 2014, Boneh et al. [35] proposed the first IBBE scheme, which obtains selectively CCA-secure from multilinear maps and has constant-size ciphertexts. In 2015, Jongkil Kim et al. [36] proposed an IBBE scheme, which is adaptively CCA-secure in the standard model, but uses dual encryption technique. In 2016, Dan and Zhandry [37] proposed a BE scheme, which obtains adaptive security by using indistinguishability obfuscation technique and has short ciphertexts, secret keys, and public keys.

Anonymity is a good security property; however, the aforementioned scheme cannot be obtained because the recipients' identities are broadcasted as ciphertext. Thus, the identities' information is exposed. In 2006, Adam et al. [12] presented two fully anonymous BE constructions; both of them obtain CCA security. The first one is a generic construction, and the decryption cost has a linear relationship with the number of receivers. The second is a specific construction, requiring a certain number of decryption operations, and the security proof relies on a random oracle model. In 2012, Libert et al. [19] proposed some fully anonymous BE schemes, which are fully anonymous and have adaptive CCA security in the standard model; at the same time, the formal security definition of the anonymous BE scheme is given. In 2012, two anonymous BE schemes with outsider anonymous were proposed by Fazio and Milinda Perera [38], and the two BE schemes have sublinear-size ciphertexts. In 2016, two anonymous BE schemes were proposed by He et al. [39]; the first one is the general scheme [39], and the second one is the specific scheme [39]. Both of these schemes are proven to be adaptive CCA-secure. However, all the aforementioned traditional BE/IBBE schemes cannot resist quantum attacks.

In 2010, Wang and Bi [40] proposed a secure lattice-based IBBE scheme using the basis delegation technique [23], and their scheme can be easily extended to a hierarchical IBBE. However, their lattice basis delegation technique increases the dimension of users' identity matrix. In 2013, Georgescu [41] used a tag-based hint system which is secure based on ring-LWE hardness and an IND-CCA-secure public key encryption scheme from LWE to construct a CCA-secure lattice-based anonymous BE scheme. In 2015, Wang et al. [20] used the Chinese remainder theorem to construct a dynamical and outsider-anonymous BE scheme over the lattice, which is proven semantic secure in the standard model under the hardness of the LWE problem. In 2020, Brakerski and Vaikuntanathan [42] proposed a lattice-based BE scheme where the size of the key and ciphertext has a logarithmic correlation with the number of users. However, their BE construction is based on a heuristic that allows to "invert" the key succinctness of the BGG + KP-ABE scheme [43] and does not have a security reduction for this heuristic; its security is an open problem. In 2020, Agrawal and Yamada [44] improved Boneh et al.'s [35] BE scheme which used multilinear maps by using LWE and bilinear mapping, and the parameters of the improved solution were also very small. Thus, in this paper, we construct an anonymous IBBE scheme on the lattice. We make a detailed function comparison between our scheme and other schemes in Table 1.

Table 1: Comparisons with related works.

Scheme	Identity-based	Anonymity
[41]	×	√
[20]	×	√
[40]	√	×
[42]	×	×
Ours	√	√

2. Preliminaries

Let us briefly introduce some of the symbols and definitions used throughout the paper.

2.1. Collision Intractability [22]. $\mathscr{H} = \{H_k\}_{k\in\mathscr{N}}$ is a family of hash functions. If it is difficult to find two inputs that hash to the same output, $\mathscr{H}$ is collision intractable. Formally, for every probability polynomial-time (PPT) adversary $\mathscr{A}$, there is a negligible function negl() such that

$$Pr^{\mathscr{A}}_{H\in H_k}\left[\mathscr{A}(H) = (x, x'), \text{s.t. } x \neq x' \text{ and } H(x) = H(x')\right] = \text{negl}(k)a. \tag{1}$$

2.2. Division Intractability [22]. $\mathscr{H}$ is a hashing family; if it is division intractable, it is hard to find distinct inputs $x_1, \ldots, x_n, y$ such that $h(y)$ divides $\prod_{i=1}^{n} h(x_i)$. Formally, for every PPT adversary $\mathscr{A}$, there is a negligible function negl() such that

$$Pr^{\mathscr{A}}_{h\in H_k}\left[\begin{array}{c}\mathscr{A}(h) = \left(\{x_i\}_{i\in[n]}, y\right),\\ \text{s.t. } y \neq \{x_i\}_{i\in[n]} \text{ and } h(y) \text{ divides } \prod_{i=1}^{n} h(x_i)\end{array}\right] = \text{negl}(k). \tag{2}$$

It is not difficult to see that a hash family $\mathscr{H}$ that is division intractable must also be collision intractable, but the reverse is not true. Such a function is easy to obtain by setting $H_0(X) = H(X)|1$ (or only the lowest bit of $H(X)$) to be one.

2.3. Lattice and Lattice Problems

2.3.1. Lattice [45]. Lattice Λ is generated by a set of n linearly independent vectors $B = \{b_1, b_2, \ldots, b_n\}$ such that

$$\Lambda = \{Bc | Bc = c_1 b_1 + c_2 b_2 + \cdots + c_n b_n \in \mathbb{Z}\}. \tag{3}$$

2.3.2. q-ary Lattices [45]. (q, m, n) are some integers, $A \in \mathbb{Z}_q^{n\times m}$ is a parity check matrix, and q-ary lattices are defined as

$$\Lambda_q^{\perp}(A) = \left\{e \in \mathbb{Z}_q^m, Ae = 0 (\text{mod} q)\right\}. \tag{4}$$

In fact, all vectors in lattice $\Lambda_q^{\perp}(A)$ are orthogonal modulo q to the matrix A row vector.

2.3.3. Gaussian over Lattices [45]. Gaussian function ρ_s: $\mathbb{R}^m \longrightarrow (0, 1]$ is defined as

$$\rho_s(x) = \exp\left(-\pi \frac{\|x\|^2}{s^2}\right), \tag{5}$$

for any $s > 0$ and dimension $m \geq 1$. The discrete Gaussian distribution $D_{\Lambda_y^{\perp}(A),s}$ over the coset $L = t + \Lambda_y^{\perp}(A)$, $t \in \mathbb{Z}^m$, whose probability is proportional to $\rho_s(x)x \in \Lambda_y^{\perp}(A)$, and probability is zero elsewhere.

2.3.4. LWE Problem [26, 45]. Let $A \leftarrow_R \mathbb{Z}_q^{m\times n}$, $s \leftarrow_R \mathbb{Z}_q^n$, the error distribution χ be over $\mathbb{A}_{(s,\chi)}$, and e be distributed according to χ. Given $(A, As + e(\text{mod}q))$, the decision variant LWE problem is to distinguish $(A, As + e(\text{mod}q))$ from uniform distribution.

2.3.5. Gaussian Error Distributions Φ_α^m 26. The standard error distribution Φ_α^m is the Gaussian distribution on $\mathbb{Z}_q^m$, and the deviation is $q\alpha > \sqrt{n}$. According to the distribution Φ_α^m, the error vector can be effectively sampled, as shown in the following:

(i) Sample $\eta_1, \eta_2, \ldots, \eta_m$ comes from the Gaussian distribution D_α on $\mathscr{R}$

(ii) Let $e_i = (q\eta_i)(\text{mod}q)$ where (x) is used to represent the integer closest to x

(iii) Let $e = (e_1, \ldots, e_m)$ be the error vector in the LWE problem instance

2.3.6. Trapdoor Sampling Algorithm [21]. Let $q \geq 3$ be odd and $m := \lceil 6n \log q \rceil$. There exists a PPT algorithm (TrapGen) (q, n), and it outputs a matrix A and a full rank set $T \in \mathbb{Z}^{m\times m}$, where A's distribution is statistically close to a uniform distribution, T is a lattice basis of $\Lambda^{\perp}(A)$, which satisfies $\|\widetilde{T}\| \leq \mathcal{O}(\sqrt{(n \log q)})$, and $\|T\| \leq \mathcal{O}(n \log q)$ with almost negligible probability.

The trapdoor T can be utilized to solve the LWE problem; that is, given $y = A^t s + e(\text{mod}q)$ where e is any "short enough" vector, it can be used to recover s as follows [25]:

(i) Calculate $T^t y = T^t(A^t s + e) = (AT)^t s + T^t e = T^t e$ (mod$q$) and $e = (T^t)^{-1} T^t e(\text{mod}q)$. Now, since both T and e contain small entries, each entry of the vector $T^t e$ is less than q, so $T^t e(\text{mod}q) = T^t e$.

(ii) LWE secret s can be recovered via A, e, y.

2.3.7. Algorithm Basis Delegation [21]. The basic delegation algorithm *BasisDel* (A, R, T_A, σ) will not increase the dimension of the basic matrix [21]. On inputting a rank n matrix A in $\mathbb{Z}_q^{n\times m}$, a $\mathbb{Z}_q$-invertible matrix R in $\mathbb{Z}^{m\times m}$ sampled from $\mathscr{D}_{m\times m}$, a basis T_A of $\Lambda_q^{\perp}$, and the parameter $\sigma \in \mathbb{R}_{>0}$, output a basis T_B of $\Lambda_q^{\perp}(B)$, where $B = AR^{-1}$ in $\mathbb{Z}_q^{n\times m}$.

2.3.8. Algorithm Sample R (1^n)21. Our security proof uses algorithm sample R. The sample matrix in $\mathbb{Z}^{m\times m}$ comes from

a distribution that is statistically close to $\mathscr{D}_{m\times m}$ [21]. On the canonical basis T of the lattice $\mathbb{Z}^m$, run $r_i \leftarrow_R$ Sample Gaussian $(\mathbb{Z}^m, T, \sigma, 0)$ for $i = 1, \ldots, m$. If R is $\mathbb{Z}_q-$ invertible, then output R; otherwise, run the sample Gaussian algorithm repeatedly.

Algorithm sample R with basis is used in our security proof, which gives a random rank n matrix A in $\mathbb{Z}_{n\times m}^q$ and generates a "low-norm" matrix R from $\mathbb{D}_{m\times m}$ and the short base of $\Lambda_q^{\perp}(AR^{-1})$ as follows.

2.3.9. Algorithm Sample R with Basis (A) *21.* $a_1, \ldots, a_m \in \mathbb{Z}_q^n$ are the m columns of the matrix $A \in \mathbb{Z}_q^{n\times m}$.

(i) Run TrapGen(q, n) to generate a matrix $B \in \mathbb{Z}_q^{n\times m}$ with random rank n, as well as lattice $\lambda_q^{\perp}(B)$ base T_B, where

$$\left\|\widetilde{T_B}\right\| \le \widetilde{L}_{TG} = \frac{\sigma_R}{w(\sqrt{\log m})}. \tag{6}$$

(ii) For $i = 1, \ldots, m$, do

(1) Sample r_i by running SamplePre$(B, T_B, a_i, \ldots)$, and we have $Br_i = a_i \bmod q$, $Br_i = a_i \bmod q$, where r_i is sampled from a distribution statistically close to $D_{\Lambda_q^{a_i}(B),\rho_R}$

(2) Repeat Step (1) until r_i is linearly independent of $r_1, \ldots, r_{i-1}$

(iii) Let $R \in \mathbb{Z}^{m\times n}$ be the matrix with columns $r_1, \ldots, r_m$. Then, R has rank m. Output R and T_B.

2.3.10. Chinese Remainder Theorem [46]. If q_i and q_j are integers, gcd $(q_i, q_j) = 1$, and $\{a_i\}_{1\le i\le k}$ are arbitrary integers, a system of linear congruence

$$\begin{cases} x \equiv a_1 \pmod{q_1}, \\ \vdots, \\ x \equiv a_k \pmod{q_k}, \end{cases} \tag{7}$$

equations has only one solution:

$$x = Q_1 Q_1' a_1 + \cdots + Q_k Q_k' a_k \pmod{Q}, \tag{8}$$

where $Q = q_1 q_2 \ldots q_k$, $Q_i = Q/q_i$, and $Q_i Q_i' = 1 \pmod{q_i}$ for $1 \le i \le k$.

We can also extend the Chinese remainder theorem to a matrix form, such as x and a_i are extended to matrices X and A_i with dimension $n \times m$, respectively; the system of linear congruence has the same solution; that is,

$$X = Q_1 Q_1' A_1 + \cdots + Q_k Q_k' A_k \pmod{Q}, \tag{9}$$

where X is close to uniform distribution [20].

3. Identity-Based Broadcast Encryption

(i) Init: adversary $\mathscr{A}$ outputs two receiver subsets S_0 and S_1 that he wants to attack; it is required that $|S_0| = |S_1|$ in order to avoid trivial attacks

(ii) Setup: challenger $\mathscr{C}$ first runs Setup to generate the public parameters params and a master secret key msk, then gives params to adversary $\mathscr{A}$, and keeps msk to itself

(iii) Phase 1: adversary $\mathscr{A}$ adaptively issues the private key for identity $I\ D \notin S_0 \cup S_1$ query, and challenger $\mathscr{C}$ runs $sk_{I\ D} \leftarrow$ Extract $(msk, I\ D)$ and returns $sk_{I\ D}$ to adversary $\mathscr{A}$

(iv) Challenge: adversary $\mathscr{A}$ selects two equal-length messages $M_0, M_1 \in \mathscr{M}$ and sends to challenger $\mathscr{C}$, and challenger $\mathscr{C}$ flips a random coin $\beta \in \{0, 1\}$ and returns the challenge ciphertext $CT^* \leftarrow$ Encrypt $(\text{params}, S_\beta, M_\beta)$ to adversary $\mathscr{A}$

(v) Phase 2: adversary $\mathscr{A}$ continues to adaptively issue queries as in Phase 1

(vi) Guess: adversary $\mathscr{A}$ outputs a guess $\beta' \in \{0, 1\}$

Definition 1. An IBBE scheme consists of four algorithms (Setup, Extract, Enc, Dec) [19, 34] as follows:

(i) Setup (1^λ): intake a security parameter λ, and output the public parameters params and a master secret key msk

(ii) Extract (msk, ID): intake a master secret key msk and an identity ID, and output a private key $sk_{I\ D}$ for identity ID

(iii) Enc (params, S, M): intake the public parameters params, a receiver set S, and a message $M \in \mathscr{M}$, and output a ciphertext CT

(iv) Dec $(sk_{I\ D}, CT)$: intake a private key $sk_{I\ D}$ and a ciphertext CT, and output either a message M or an error symbol $\perp$

The correctness property requires that, for all $I\ D \in S$, if $(\text{params}, msk) \leftarrow$ Setup (1^λ), $sk_{I\ D} \leftarrow$Extract $(msk, I\ D)$, and $CT \leftarrow Enc(\text{params}, S, M)$, then Dec $(sk_{I\ D}, CT) = M$ with overwhelming probability.

In the above definition, the set S is not required to intake the decryption algorithm which keeps the anonymity of an IBBE system.

We now present the security requirements for an IBBE scheme to be outsider anonymous against the chosen-plaintext attack (CPA). In an outsider-anonymous IBBE scheme, when the adversary receives a ciphertext of which he is not a legal recipient, he will be unable to learn anything about the identities of the legal recipients, but for those ciphertexts for which the adversary is in the authorized set of recipients, he might also learn the identities of some other legal recipients. First, we define the CPA of an outsider-anonymous IBBE scheme as a game, which we term oAIBBE-IND-CPA, played between a probabilistic polynomial-time (PPT) adversary $\mathscr{A}$ and a challenger $\mathscr{C}$. Meanwhile, we present a selective indistinguishable chosen-plaintext security game (sIND-CPA), where selective security is a weaker notion which forces the adversary $\mathscr{A}$ to announce ahead of time the identities it will target.

Definition 2. The oAIBBE-sIND-CCA game defined for an oAIBBE scheme $\Pi = (\text{Setup, Extract, Enc, Dec})$, a PPT adversary $\mathscr{A}$, and a challenger $\mathscr{C}$ is as follows:

Definition 3. Define adversary $\mathscr{A}$'s advantage in the above oAIBBE-sIND-CPA game as $A\,dv_{\mathscr{A},IBBE}^{\text{oAIBBE-sIND-CPA}} = |\Pr[\beta' = \beta] - 1/2|$. We say that an IBBE scheme is oAIBBE-sIND-CPA secure if for any PPT adversary $\mathscr{A}$, the advantage $A\,dv_{\mathscr{A},IBBE}^{\text{oAIBBE-sIND-CPA}}$ is negligible in the above oAIBBE-sIND-CPA game.

4. Construction

Our lattice-based IBBE scheme is designed by translating the lattice-based BE scheme of Wang et al. [20] into an identity-based environment. The private key generation depends on the lattice basis delegation without increasing the dimension [21].

(i) Setup (n): intake a secure parameter n, set $q \geq 3$ to be odd and $m := \lceil 6n \log q \rceil$, and let $H_1: \{0,1\}^* \longrightarrow \{0,1\}^n$ be a division intractability hash function and $H_2: \{0,1\}^* \longrightarrow \mathbb{Z}_q^{m \times m}$ be a hash function. Invoke trapdoor sampling algorithm $TrapGen\ (q,n)$ to generate a uniformly random matrix $A_0 \in \mathbb{Z}_q^{n \times m}$ with a basis $T_0 \in \mathbb{Z}^{m \times m}$ satisfying $A_0 T_0 = 0 (\text{mod} q)$ such that $\|T_0\| \leq \mathcal{O}(n \log q)$. Output public parameters

$$mpk = (n, m, q, A_0, H_1, H_2). \tag{10}$$

and a master key $msk = T_0$.

(ii) Extract (mpk, msk, ID): intake public parameters mpk, a master key msk, and an identity $ID \in \{0,1\}^*$, and compute $R_{ID} = H_2(ID) \in \mathbb{Z}_q^{m \times m}$ and $A_{ID} = A_0 R_{ID}^{-1} \in \mathbb{Z}_q^{n \times m}$. Evaluate

$$SK_{ID} \leftarrow \text{Basis Del}(A_0, R_{ID}, T_0, \sigma) \tag{11}$$

to obtain a short random basis $SK_{I\,D}$ for $\Lambda_q^{\perp}(A_{ID})$. Output identity $I\ D$'s private key SK_{ID}.

(iii) Encrypt (mpk, S, M): intake public parameters mpk, a broadcast set $S = \{ID_1, \ldots, ID_d\}$, and message $M \in \{0,1\}^m$, and compute $q_{ID_i} = H_1(ID_i)$ for $ID_i \in S$. Moreover, to ensure the correctness of decryption, we need $q_{ID_i} > q$. According to the Chinese remainder theorem, it needs to compute $Q = q_{ID_1} \ldots q_{ID_d}$ and $Q_{ID_i} = Q/q_{ID_i}$, where $Q_{ID_i} Q_{ID_i}' \equiv 1 (\text{mod} q_{ID_i})$. Calculate

$$A_{ID_i} = A_0 H_2(ID_i)^{-1} \in \mathbb{Z}_q^{n \times m}, \tag{12}$$

for $ID_i \in S$, choose random vector $s \in \mathbb{Z}_q^n$ and $e \in \overline{\Phi}_{\alpha}^m$ and a symmetric key $K \in \{0,1\}^m$, and compute the ciphertext (C_1, C_2) as follows:

$$\begin{aligned} C_1 &= K + M (\text{mod} 2), \\ C_2 &= \left(\sum_{i=1}^{k} Q_{ID_i} Q_{ID_i}' A_{ID_i}^{\top} \right) \left(\sum_{i=1}^{k} Q_{ID_i} Q_{ID_i}' s \right) + 2e + K) (\text{mod} Q). \end{aligned} \tag{13}$$

(iv) Decrypt $(mpk, SK_{I\,D}, I\ D)$: user with identity $I\ D$ in the broadcast set S uses his private key to decrypt ciphertext (C_1, C_2) as follows:

$$\begin{aligned} q_{ID} &= H_1(ID), \\ A_{ID} &= A_0 H_2(ID)^{-1}, \\ K &= \left(SK_{ID}^{\top}\right)^{-1} \left(SK_{ID}^{\top} (C_2 (\text{mod} q_{ID})) (\text{mod} q)\right) (\text{mod} 2) \\ &= \left(SK_{ID}^{\top}\right)^{-1} \left(SK_{ID}^{\top} \left(A_{ID}^{\top} s + 2e + K\right) (\text{mod} q)\right) (\text{mod} 2) \\ &= \left(SK_{ID}^{\top}\right)^{-1} \left(SK_{ID}^{\top} (2e + K)\right) (\text{mod} 2) \\ &= (2e + K) (\text{mod} 2), \\ M &= C_1 + K (\text{mod} 2). \end{aligned} \tag{14}$$

5. Analysis of the Proposed Anonymous IBBE Construction

5.1. Parameters and Correctness. Given the security parameter n, the analysis of parameters and correctness for our scheme is as follows.

(i) To ensure that $TrapGen\ (q,n)$ can operate, the following requirements should be met: $m > 6n \log q$ and $q = \text{poly}(n)$ [21].

(ii) To guarantee the decryption of the ciphertext, the error term should be less than $q_{ID_i}/2$, and let α, q_{ID_i}, and σ be set as [23, 47]

$$\begin{aligned} \alpha &< \frac{1}{\sigma m \omega (\log m)}, \\ q_{ID_i} &> \alpha m^{3/2} \omega (\log m), \\ \sigma &= m^{3/2} \omega\left(\log^2 n\right). \end{aligned} \tag{15}$$

(iii) Parameters q should always satisfy $q < q_{ID_i}$ and $q = m \log m$.

To ensure that decryption works, we first note that C_2 is designed according to the Chinese remainder theorem, and recall that $Q = q_{ID_1} \ldots q_{ID_n}$ and $Q_{ID_i} = Q/q_{ID_i}$; then, $Q_{ID_i} Q_{ID_i}' \equiv 1 (\text{mod} q_{ID_i})$ and $Q_{ID_i} Q_{ID_i}' \equiv 0 (\text{mod} q_{ID_j})$ for $i \neq j$. Hence, it would be valid.

$$C_2\left(\mathrm{mod}q_{ID_i}\right)=\left(\sum_{i=1}^{k}Q_{ID_i}Q'_{ID_i}A_{ID_i}^{\top}\right)\left(\sum_{i=1}^{k}Q_{ID_i}Q'_{ID_i}s\right)+2e+K\Big)\left(\mathrm{mod}q_{ID_i}\right)$$
$$=\left(A_{ID_i}^{\top}s+2e+h\right)\left(\mathrm{mod}q_{ID_i}\right). \tag{16}$$

By the properties of basis delegation, $A_{ID_i}\cdot SK_{ID_i}=0\,(\mathrm{mod}q)$, where $q<q_{ID_i}$; therefore,

$$\begin{aligned}&SK_{ID_i}^{\top}\left(\left(A_{ID_i}^{\top}s+2e+h\right)\left(\mathrm{mod}q_{ID_i}\right)\right)(\mathrm{mod}q)\\&=SK_{ID_i}^{\top}\left(A_{I\,D}^{\top}s+2e+K\right)(\mathrm{mod}q)\\&=SK_{ID_i}^{\top}\left(2e+K\right)(\mathrm{mod}q).\end{aligned} \tag{17}$$

Finally, we know $K\in\{0,1\}^m$,

$$\begin{aligned}&\left(SK_{ID_i}^{\top}\right)^{-1}\left(SK_{ID_i}^{\top}\left(2e+K\right)(\mathrm{mod}q)\right)(\mathrm{mod}2)\\&=\left(SK_{ID_i}^{\top}\right)^{-1}SK_{ID_i}^{\top}\left(2e+K\right)\\&=K\,(\mathrm{mod}2)\\&=K.\end{aligned} \tag{18}$$

5.2. Security

Theorem 1. *The above scheme is oAIBBE-sIND-CPA secure if the LWE problem is hard and H_2 is simulated as a random oracle.*

Proof. Suppose there exists a PPT adversary that is able to distinguish the above scheme's ciphertext from random elements with advantage ε. Then, there is a challenger $\mathscr{C}$ with advantage at least $\varepsilon+1/2$ that distinguishes (A_0,y_0) between the two distributions

$$\left\{(A_0,y_0)|y_0=A_0^ts_0+e_0\,(\mathrm{mod}q)\right\}:\ A_0\leftarrow\mathbb{Z}_q^{n\times m},s_0\leftarrow\mathbb{Z}_q^n,e_0\leftarrow\Phi_\alpha^m\Big\},$$
$$\left\{\mathrm{Unif}\left(\mathbb{Z}_q^{n\times m}\times\mathbb{Z}_q^m\right)\right\}. \tag{19}$$

(i) Init: adversary $\mathscr{A}$ outputs two different subsets $S_1^*=\{ID_1^{1*},\ldots,ID_d^{1*}\}$ and $S_2^*=\{ID_1^{2*},\ldots,ID_d^{2*}\}$ that he wants to distinguish. Challenger $\mathscr{C}$ samples $2\,d$ random matrices $R_1^*,\ldots,R_{2\,d}^*\sim\mathbb{D}_{m\times m}$ by running $R_i^*\leftarrow\mathrm{Sample}\,R\,(1^n)$ (described in Section 3.1), where all R_i^* are invertible mod q.

(ii) Setup: challenger $\mathscr{C}$ chooses two collision-intractable hash functions H_1 and H_2. H_1 is a division intractability hash function, and H_2 is simulated as a random oracle. Let Q_H be the number of H_2 queries made by $\mathscr{A}$. Let the master public key be A_0, and the master secret key is unknown to $\mathscr{C}$. The system parameters $mpk=(n,m,q,A_0,H_1,H_2)$ are given to $\mathscr{A}$.

(iii) Phase 1: adversary $\mathscr{A}$ adaptively issues queries as follows:

(iv) Random oracle hash queries: $\mathscr{A}$ may adaptively query the random oracle H_2 on any identity ID_i of its choice at any time. $\mathscr{C}$ answers the query as follows.

If $ID_i\in S_1^*\cup S_2^*$, define $H_2\,(ID_i)\leftarrow R_i^*$, return R_i^* to adversary $\mathscr{A}$, and save the tuple (ID_i,R_i^*) in a list $\mathscr{L}$.

If $ID_i\notin S_1^*\cup S_2^*$, sample a random matrix $\widetilde{R}_i\leftarrow\mathrm{Sample}\,R\,(1^n)$, where $\widetilde{R}_i$ is invertible mod q, compute $A_i=A_0\cdot(\widetilde{R}_i)^{-1}\,(\mathrm{mod}q)$, and then run sample R with basis (A_i) (described in Section 3.1) to obtain a random matrix $\widehat{R}_i\sim\mathbb{D}_{m\times m}$ and a short basis T_{B_i} for

$$\begin{aligned}B_i&=A_i\widehat{R}_i^{-1}\,(\mathrm{mod}q)\\&=A_0\cdot\widetilde{R}_i^{-1}\widehat{R}_i^{-1}\,(\mathrm{mod}q)\\&=A_0\cdot\widetilde{R}_i^{-1}\widehat{R}_i^{-1}\,(\mathrm{mod}q)\\&=A_0\cdot R_i^{-1}\,(\mathrm{mod}q).\end{aligned} \tag{20}$$

Save the tuple (ID_i,R_i,B_i,T_{B_i}) in a list $\mathscr{L}$ for future use, and return $H_2\,(ID_i)\leftarrow R_i$ to adversary $\mathscr{A}$.

(i) Secret key queries: $\mathscr{A}$ makes interactive key extraction queries on arbitrary identity ID_i. $\mathscr{C}$ answers a query on ID_i as follows:

If $ID_i\in S_1^*\cup S_2^*$, $\mathscr{C}$ aborts and fails.
If $ID_i\notin S_1^*\cup S_2^*$, $\mathscr{C}$ retrieves the saved tuple (ID_i,R_i,B_i,T_{B_i}) from the hash oracle query list $\mathscr{L}$; else, it runs the random oracle hash query on ID_i. Let $B_i=A_0\cdot R_i^{-1}\,(\mathrm{mod}q)$ and T_{B_i} be a short basis for $\Lambda q^{\perp}\,(B_i)$, and return T_{B_i} to adversary $\mathscr{A}$.

Notice that B_i is exactly the encryption matrix for ID_i, and therefore, T_{B_i} is a trapdoor for $\Lambda_q^{\perp}\,(B_i)$.

Challenge: adversary $\mathscr{A}$ chooses two equal-length messages $M_1,M_2\in\{0,1\}^m$ and sends to challenger $\mathscr{C}$. Challenger $\mathscr{C}$ chooses at random a symmetric key $K\in\{0,1\}^m$ and a random bit $\beta\in\{0,1\}$; challenger $\mathscr{C}$ computes $Q^{\beta*}=q_{ID^{\beta*}}\cdots q_{ID^{\beta*}}$, where $q_{ID^{\beta*}}=H_1\,(ID_j^{\beta\,*})$ and $j\in S_\beta^*$, and then returns the challenge ciphertext to adversary $\mathscr{A}$.

$$\begin{aligned}C_1&=M_\beta+K\,(\mathrm{mod}2),\\C_2&=2y_0+K\left(\mathrm{mod}Q^{\beta*}\right).\end{aligned} \tag{21}$$

(ii) Phase 2: adversary $\mathscr{A}$ adaptively issues queries as Phase 1.

(iii) Guess: adversary $\mathscr{A}$ outputs a guess bit β', and $\mathscr{A}$ wins the game if $\beta=\beta'$.

(iv) Analysis: in the following, we analyse the correctness of the challenge ciphertext.

(v) On the one hand, if y_0 is a uniformly random matrix, then the challenge ciphertext is also

uniformly random, regardless of the choice of β. Hence, in this case, $\mathscr{C}$ outputs 1 with probability at most 1/2.

(vi) On the other hand, if $y_0 = A_0 s_0 + e_0 \pmod{q}$, then the challenge ciphertext is $2y_0 + K \pmod{Q} = 2(A_0 s_0 + e_0) + K \pmod{Q}^{\beta*} = 2 \quad (A_{ID_i^{\beta*}} \cdot R_i^* \cdot s_0 + e_0) + K \pmod{Q^{\beta*}} = 2(A_{ID_i^{\beta*}} \cdot R_i^* \cdot s_0 + e_0) + K \pmod{Q^{\beta*}} = (A_{ID_i^{\beta*}} \cdot 2R_i^* \cdot s_0 + 2e_0 + K) \pmod{Q^{\beta*}} = (A_{ID_i^{\beta*}} \cdot s' + 2e_0 + K) \quad \pmod{Q^{\beta*}} = (\sum_{i=1}^{k} Q_{ID_i^{\beta*}} Q_{ID_i^{\beta*}}{}' A_{ID_i^{\beta*}}) \quad (\sum_{i=1}^{k} Q_{ID_i^{\beta*}} Q_{ID_i^{\beta*}}{}' s') + 2e_0 + K) \pmod{q_{ID_i^{\beta*}}} = (\sum_{i=1}^{k} Q_{ID_i^{\beta*}} Q_{ID_i^{\beta*}}{}' A_{ID_i^{\beta*}})(\sum_{i=1}^{k} Q_{ID_i^{\beta*}} Q_{ID_i^{\beta*}}{}' s') + 2e_0 + K) \pmod{Q^{\beta*}}$.

$s' = R_i^* \cdot 2s_0 \pmod{q_{ID_i^{\beta*}}}$ is uniformly distributed (since Q and 2 are relatively prime). This is identical to the output distribution of the real ciphertext.

Hence, if adversary $\mathscr{A}$ succeeds in guessing the right M_β and S_β with probability $1/2 + \varepsilon$, then challenger $\mathscr{C}$ will correctly guess the nature of the LWE oracle with probability at least $1/2 + \varepsilon/2$. This concludes the proof of the security reduction.

Remark. The above scheme cannot achieve the anonymity for the insider attacker. Because any authorized receiver can obtain the private information *s, e*, and *K*, he/she uses *s, e*, and *K* to decrypt C_2. The decryption process is similar to Thrapdoor Sampling Algorithm of Section 2.1 Therefore, in order to ensure whether or not *ID* is an authorized receiver, adversary $\mathscr{A}$ only needs to calculate whether $C_2 \pmod{H_1(ID)}$ and $(A_{I\ D}^{\top} s + 2e + h) \pmod{H_1(ID)}$ are equal. If yes, *ID* is an authorized receiver; otherwise, *ID* is not an authorized receiver.

6. Conclusions

We propose a lattice-based anonymous IBBE scheme employing the Chinese remainder theorem and lattice basis delegation in fixed dimensions. Our scheme achieves chosen-plaintext security in the random oracle model and is with multiple attractive properties, such as constant-size private/public key and ciphertext and constant encryption/decryption overhead.

Data Availability

All the data included in this study are available upon request by contact with the corresponding author.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was partially supported by the National Science Foundation of China (NSFC) (Grant nos.61902067 and 62102166), Foundation for Young Innovative Talents in Ordinary Universities of Guangdong (2018KQNCX255), Opening Project of Guangdong Province Key Laboratory of Information Security Technology (Grant no.2020B1212060078), Dongguan Science and Technology of Social Development Program (2020507140146), Dongguan University of Technology (2021KTSCX134), Key-Area Research and Development Program of Guangdong Province (Grant no. 2020B0101360001), Guangdong Basic and Applied Basic Research Foundation (Grant no. 2020A1515111175), and Guangdong Natural Science Key Field Project (2019KZDZX1008).

References

[1] A. Lekbich, A. Belfqih, C. Zedak, J. Boukherouaa, and F. El Mariami, "A secure wireless control of remote terminal unit using the internet of things in smart grids," in *Proceedings of the 6th International Conference on Wireless Networks and Mobile Communications, WINCOM 2018*, pp. 1–6, IEEE, Marrakesh, Morocco, October 2018.

[2] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying iot security: an exhaustive survey on iot vulnerabilities and a first empirical look on internet-scale iot exploitations," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019.

[3] A. Fiat and M. Naor, "Broadcast encryption," in *Proceedings of the Advances in Cryptology - CRYPTO '93, 13th Annual International Cryptology Conference*, pp. 480–491, Santa Barbara, CA, USA, August 1993.

[4] X. Du, Y. Wang, J. Ge, and Y. Wang, "An id-based broadcast encryption scheme for key distribution," *IEEE Transactions on Broadcasting*, vol. 51, no. 2, pp. 264–266, 2005.

[5] B. Malek and M. Ali, "Adaptively secure broadcast encryption with short ciphertexts," *International Journal Network Security*, vol. 14, no. 2, pp. 71–79, 2012.

[6] C Delerablée, P. Pascal, and D. Pointcheval, "Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys," in *Proceedings of the Pairing-Based Cryptography - Pairing 2007, 1st International Conference*, pp. 39–59, Tokyo, Japan, July 2007.

[7] X. Xiaodong Lin, X. Xiaoting Sun, P.-H. Pin-Han Ho, and X. Xuemin Shen, "GSIS: a secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456, 2007.

[8] Y. Jung, Y. Nam, J. Kim, W. Jeon, H. Lee, and D. Won, "Key management scheme using dynamic identity-based broadcast encryption for social network services," *Lecture Notes in Electrical Engineering*, vol. 279, pp. 435–443, 2014.

[9] D. Naor, M. Naor, and J. Lotspiech, "Revocation and tracing schemes for stateless receivers," in *Proceedings of the Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference*, pp. 41–62, Santa Barbara, CA, USA, August 2001.

[10] Y. Dodis and N. Fazio, "Public key broadcast encryption for stateless receivers," in *Proceedings of the Security And Privacy In Digital Rights Management, ACM CCS-9 Workshop, DRM 2002*, pp. 61–80, Springer, Washington, DC, USA, November 2002.

[11] D. Boneh, G. Craig, and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," in *Proceedings of the Advances in Cryptology - CRYPTO 2005:*

25th Annual International Cryptology Conference, pp. 258–275, Santa Barbara, CA, USA, August 2005.

[12] B. Adam, D. Boneh, and B. Waters, "Privacy in encrypted content distribution using private broadcast encryption," in *Proceedings of the Financial Cryptography and Data Security, 10th International Conference, FC 2006*, pp. 52–64, Anguilla, West Indies, February 2006.

[13] G. Craig and B. Waters, "Adaptive security in broadcast encryption systems (with short ciphertexts)," in *Proceedings of the Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 171–188, Cologne, Germany, April 2009.

[14] W. Peter, "Shor. Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pp. 124–134, Santa Fe, NM, USA, November 1994.

[15] R. Bendlin, "Lattice-based cryptography," *Lecture Notes in Computer Science*, vol. 4117, no. 1-2, pp. 131–141, 2013.

[16] M. Ajtai, "Generating hard instances of lattice problems (extended abstract)," in *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing*, pp. 99–108, Philadelphia, PA, USA, May 1996.

[17] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in *Proceedings of the 37th Annual ACM Symposium on Theory of Computing*, pp. 84–93, Baltimore, MD, USA, May 2005.

[18] D. Micciancio and S. Goldwasser, "Complexity of lattice problems: a cryptographic perspective," *Kluwer International Series in Engineering and Computer Science*, Kluwer Academic Publishers, Boston, MA, USA, 2002.

[19] B. Libert, K. G. Paterson, and E. A. Quaglia, "Anonymous broadcast encryption: adaptive security and efficient constructions in the standard model," in *Proceedings of the Public Key Cryptography - PKC 2012 - 15th International Conference on Practice and Theory in Public Key Cryptography*, pp. 206–224, Darmstadt, Germany, May 2012.

[20] F. Wang, A. Wang, and C. Wang, "Lattice-based dynamical and anonymous broadcast encryption scheme," in *Proceedings of the 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 3PGCIC 2015*, pp. 853–858, Krakow, Poland, November 2015.

[21] S. Agrawal, D. Boneh, and X. Boyen, "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*, pp. 553–572, Monaco, French Riviera, May 2010.

[22] R. Gennaro, S. Halevi, and T. Rabin, "Secure hash-and-sign signatures without the random oracle," in *Proceedings of the Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques*, J. Stern, Ed., Springer, Prague, Czech Republic, pp. 123–139, May 1999.

[23] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, "Bonsai trees, or how to delegate a lattice basis," in *Proceedings of the Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 523–552, French Riviera, France, May 2010.

[24] Adi Shamir, "Identity-based cryptosystems and signature schemes," *Lecture Notes in Computer Science*, vol. 196, no. 2, pp. 47–53, 1985.

[25] G. Craig, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proceedings of the 40th Annual ACM Symposium on Theory of Computing*, pp. 197–206, Victoria, Canada, May 2008.

[26] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *Journal of the ACM*, vol. 56, no. 6, pp. 1–40, 2009.

[27] M. Ajtai, "Generating hard instances of the short basis problem," in *Proceedings of the Automata, Languages and Programming, 26th International Colloquium, ICALP'99*, pp. 1–9, Prague, Czech Republic, July 1999.

[28] G. Craig and Alice Silverberg, "Hierarchical id-based cryptography," in *Proceedings of the Advances in Cryptology - ASIACRYPT 2002, 8th International Conference on the Theory and Application of Cryptology and Information Security*, pp. 548–566, Queenstown, New Zealand, December 2002.

[29] J. Horwitz and B. Lynn, "Toward hierarchical identity-based encryption," in *Proceedings of the Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 466–481, Amsterdam, The Netherlands, April 2002.

[30] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, "Bonsai trees, or how to delegate a lattice basis," in *Advances in Cryptology –EUROCRYPT*, pp. 523–552, Springer Berlin Heidelberg, Berlin, Germany, 2010.

[31] D. B. Shweta Agrawal and X. Boyen, "Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE," in *Proceedings of the Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference*, pp. 98–115, Santa Barbara, CA, USA, August 2010.

[32] S. Amit and B. Waters, "Fuzzy identity-based encryption," in *Proceedings of the Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, R. Cramer, Ed., Springer, Aarhus, Denmark, pp. 457–473, May 2005.

[33] X. Boyen, "Attribute-based functional encryption on lattices," in *Theory of Cryptography*, S. Amit, Ed., in *Proceedings of the Theory Of Cryptography - 10th Theory Of Cryptography Conference, TCC 2013*, pp. 122–142, Springer, Tokyo, Japan, March 2013.

[34] C. . Delerablée, "Identity-based broadcast encryption with constant size ciphertexts and private keys," in *Proceedings of the Advances in Cryptology - ASIACRYPT 2007, 13th International Conference on the Theory and Application of Cryptology and Information Security*, Kuching, Malaysia, December 2007.

[35] D. Boneh, B. Waters, and M. Zhandry, "Low overhead broadcast encryption from multilinear maps," *Proceedings, Part I*, in *Proceedings of the Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference*, Santa Barbara, CA, USA, August 2014.

[36] J. Jongkil Kim, W. Susilo, and J. Seberry, "Adaptively secure identity-based broadcast encryption with a constant-sized ciphertext," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 679–693, 2015.

[37] B. Dan and M. Zhandry, "Multiparty key exchange, efficient traitor tracing, and more from indistinguishability obfuscation," *Algorithmica*, vol. 8616, no. 4, pp. 1–53, 2016.

[38] N. Fazio and I. Milinda Perera, "Outsider-anonymous broadcast encryption with sublinear ciphertexts," in *Proceedings of the Public Key Cryptography - PKC 2012 - 15th International Conference on Practice and Theory in Public Key Cryptography*, Darmstadt, Germany, May 2012.

[39] K. He, J. Weng, M. H. Au, Y. Mao, R. H. Deng, and Deng, "Generic anonymous identity-based broadcast encryption with chosen-ciphertext security," in *Information Security and*

Privacy, pp. 207–222, Springer International Publishing, Berlin, Germany, 2016.

[40] J. Wang and J. Bi, "Lattice-based identity-based broadcast encryption scheme," *IACR Cryptology ePrint Archive*, vol. 288, 2010.

[41] A. Georgescu, "Anonymous lattice-based broadcast encryption," in *Proceedings of the Information and Communicatiaon Technology - International Conference, ICT-EurAsia 2013*, Yogyakarta, Indonesia, March 2013.

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

[43] D. Boneh, G. Craig, S. Gorbunov et al., "Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits," in *Proceedings of the Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques*, P. Q. Nguyen and E. Oswald, Eds., , Copenhagen, Denmark, May 2014.

[44] S. Agrawal and S. Yamada, "Optimal broadcast encryption from pairings and LWE," in *Proceedings of the Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, A. Canteaut and Yuval Ishai, Eds., , Zagreb, Croatia, May 2020.

[45] D. Micciancio and S. Goldwasser, "Complexity of lattice problems - a cryptograhic perspective," *Kluwer International Series in Engineering and Computer Science*, Springer, Berlin, Germany, 2002.

[46] W. Mao, *Modern Cryptography: Theory and Practice*, Prentice Hall, Hoboken NJ, USA, 2003.

[47] G. Craig, S. Halevi, and V. Vaikuntanathan, "A simple bgn-type cryptosystem from lwe," in *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 506–522, French Riviera, France, June 2010.