Lattice-based Identity-Based Broadcast Encryption

Jin Wang[1], Jingguo Bi[2]

[1] Institute for Advanced Study, Tsinghua University, Beijing 100084, China
jimiwang@mail.tsinghua.edu.cn
[2] Key Laboratory of Cryptographic Technology and Information Security, Ministry of Education, Shandong University, Jinan 250100, China
jguobi@mail.sdu.edu.cn

Abstract. Motivated by the lattice basis delegation technique due to [8], we propose an adaptively secure identity-based broadcast encryption(IBBE) scheme based on the hard worst-case lattice problems. Our construction can be generalized to obtain a hierarchical IBBE (HIBBE) scheme easily. To the best of the authors' knowledge, our construction and its variants constitute the first adaptively secure IBBE schemes from lattices, which are believed secure in the post-quantum environment.

Key words: Identity-based broadcast encryption, lattices, hierarchical identity-based broadcast encryption

1 Introduction

Broadcast Encryption. Broadcast encryption (BE) schemes are cryptosystems that enable a sender encrypts messages and transmits them to a group of users over a broadcast channel such that only the chosen users can use their private keys to decrypt messages. Broadcast encryption are useful in pay-TV systems, distribution of copyrighted material, and CD/DVD content protection,etc. Since Fiat and Naor proposed the first broadcast encryption scheme[13], many BE schemes have been proposed [6,11,12,16,25]. A notable work is proposed by Boneh, Gentry and Waters [6] that achieves a desirable feature as fully collusion resistance (even if all users outside of S collude, they can obtain no information about the broadcast message). A lot of BE schemes make use of the Key Encapsulation Mechanism (KEM) encryption paradigm where the broadcast ciphertext only encrypts a symmetric key used to encrypt the broadcast contents. We will adopt the KEM method in the following.

Identity-Based Broadcast Encryption. In this paper we consider a situation where identity-based cryptography (IBC) is incorporated to the broadcast setting [12,26]. The concept of identity-based cryptography was introduced by Shamir [24] to simplify the certificate management process. As in identity-based cryptographic constructions [4,5,9,10,14], a user's public key is allowed to be derived from his/her identity information, such as an email address, while the

corresponding private key is calculated by a trusted authority called Key Generator Center (KGC). In 2007, Delerablee [12] proposed the first identity-based broadcast encryption scheme (IBBE) using the bilinear mapping, which can be seen as the generalization of identity-based encryption systems.

Motivations. Up to date, most of proposed broadcast encryption and identity-based broadcast encryption schemes rely on hard number theory problems such as integer factorization, discrete logarithm and bilinear pairings with the diffie-hellman problem. However, above underlying number theory problems will be solvable if practical quantum computers become reality, so it implies a potential security threat to these schemes. Thus, a natural question one can ask is how to design broadcast encryption systems that are secure in the quantum environment. In recent years, lattices have emerged as a possible alternative to number theories. Lattice-based cryptography began with the seminal work of Ajtai[1], who showed that it is possible to construct families of cryptographic functions in which average-case security is provably related to the worst-case complexity of hard lattice problems. Lattice-based constructions also enjoy relatively efficient implementations, as well as great simplicity. In addition, lattice-based cryptography is believed to be secure against quantum computers.

Our Contribution. Following the above discussion, in this paper, we focus on constructing a new type of identity-based broadcast encryption schemes from lattices. The idea behind our construction is based on the lattice delegation technique due to [8]. Our basic approach is as follows. In our IBBE scheme, the master public/secret key pair of the KGC is simply a matrix $\mathbf{A}_0 \in \mathbb{Z}_q^{n\times m}$ and a corresponding short basis $\mathbf{B}_0$ for lattice $\Lambda^{\perp}(\mathbf{A}_0)$. As explored in prior works[3,15], a short basis can be treated as a trapdoor for the corresponding lattice. Knowledge of such a trapdoor makes it easy to solve some seemingly hard problems relative to the lattice. Each user identity ID_i is associated with a matrix $\mathbf{A}_{ID_i} \in \mathbb{Z}_q^{n\times m}$ by taking $\mathbf{A}_{ID_i} = H_1(ID_i)$. Using the master secret key $\mathbf{B}_0$, the KGC can extract a private key (short basis) for the identity ID_i by setting $\mathbf{Q}_{ID_i} = [\mathbf{A}_0\|\mathbf{A}_{ID_i}] \in \mathbb{Z}_q^{n\times 2m}$ and running the basis delegation algorithm to generate a short basis for the lattice $\Lambda^{\perp}(\mathbf{Q}_{ID_i})$. In the broadcast approach, for the receiver set S of size k, the broadcaster constructs a public lattice related to the receiver set as $\mathbf{A}_S = [\mathbf{A}_0\|\mathbf{A}_{ID_1}\|...\|\mathbf{A}_{ID_k}]$(for $ID_i \in S, 1 \le i \le k$). Using the basis delegation technique, each member in S should be able to deduce a new decryption key (short basis) for $\Lambda^{\perp}(\mathbf{A}_S)$ from its private information. The encryption and decryption algorithms can work as in the LWE-based Dual-PKE [15]. Since the short basis for the lattice essentially functions like cryptographic trapdoors, only the users in S can decrypt the broadcast message. Our broadcast construction is provably fully collusion resistant under adaptive attacks. Moreover, our construction can be generalized to obtain a hierarchical identity-based broadcast encryption scheme easily. Finally we extend our work to achieve an IBBE with $O(\lambda\sqrt{|S|})$ size ciphertexts. In this approach we essentially perform $\sqrt{|S|}$ encryptions to $\sqrt{|S|}$ of the recipients, but share the same system parame-

ters all these encryptions.

Related Work. Our cryptographic construction is based on the hardness assumption of the *learning with error* problem (LWE)[23]. For reasonable choices of parameters, LWE is as hard as the shortest vector problem (SVP) in lattices. The first version of the LWE-based cryptosystem together with a security proof were presented by Regev [23]. Gentry, Peikert and Vaikuntanathan [15] constructed a kind of trapdoor primitives called *pre-image sampling* functions that, given a basis of a q-ary modular lattice, samples lattice points from a *Discrete Gaussian* probability distribution whose standard deviation is essentially the length of the longest *Gram-Schmidt* vector of the basis. As the application of above trapdoors, Gentry et al.[15] constructed an identity-based encryption scheme based on LWE. Another notable recent work is due to Cash et al.[8] who constructed a basis delegation technique that allows one to derive a short basis of a given lattice using a short basis of a related lattice. The mainly idea of [8], denoted as *generalized preimage sampling*, is that, given a trapdoor which allows preimage-sampling in [15], one can use this trapdoor to preimage samples under many different, but related, public keys. Using this basis delegation technique, Cash et al.[8] also constructed a hierarchical identity-based encryption (HIBE) as well as a stateless signature of lattice-based constructions. In other independent works, Peikert[22] proposed the notion of a *bonsai tree* on lattices which is technically equivalent to the basis delegation technique in [8]. Agrawal and Boyen [4] also obtained an identity-based encryption scheme without random oracles using the similar technique.

2 Preliminaries

2.1 Notation

For a positive integer d, $[d]$ denotes the set $\{1, ..., d\}$. For an $n \times m$ matrix $\mathbf{A}$, let $\mathbf{A} = [\mathbf{a}_1, ..., \mathbf{a}_m]$, where $\mathbf{a}_i$ denotes the i-th column vector of $\mathbf{A}$. We define $\|\mathbf{a}\|$ for the Euclidean norm of $\mathbf{a}$, and $\|\mathbf{A}\| = \max_{i \in [m]} \|\mathbf{a}_i\|$. We write $\omega(f(n))$ to denote the set of functions (or a particular function in that set) growing faster than $cf(n)$ for any $c > 0$.

2.2 Lattices

Lattices. Let $\mathbf{B} = \{\mathbf{b}_1, ..., \mathbf{b}_n\} \in \mathbb{R}^n$ consist of n linearly independent vectors. A n-dimensional lattice Λ generated by $\mathbf{B}$ is defined as

$$\Lambda = \mathcal{L}(\mathbf{B}) = \{\mathbf{Bc} : \mathbf{c} \in \mathbb{Z}^n\}$$

Here $\mathbf{B}$ is called a *basis* of the lattice $\Lambda = \mathcal{L}(\mathbf{B})$. For a basis $\mathbf{B} = \{\mathbf{b}_1, ..., \mathbf{b}_n\}$, let $\widetilde{\mathbf{B}}$ denote its *Gram-Schmidt orthogonalization*, defined iteratively as follows: $\widetilde{b_1} = b_1$, and for $i = 2, ..., n$, $\widetilde{b_i}$ is the component of b_i orthogonal to $\text{span}(b_1, ..., b_n)$.

Modular Lattices. In this paper our cryptographic construction will build on

a special form of integer lattices denoted as *Modular Lattice*, which is invariant under shifts by a primitive integer modulus q in each of the coordinates. We will work with two kinds of m-dimensional modular lattices defined by Ajtai [3]. Given a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ for some integers q, m, n, the first lattice contains of all integer vectors that are orthogonal (modulo q) to the rows of $\mathbf{A}$ and is defined as:

$$\Lambda^{\perp}(\mathbf{A}) = \{\mathbf{e} \in \mathbb{Z}^m : \mathbf{A}\mathbf{e} = 0 \bmod q\}$$

The second lattice is generated by the rows of $\mathbf{A}$:

$$\Lambda(\mathbf{A}) = \{\mathbf{y} \in \mathbb{Z}^m : \mathbf{y} = \mathbf{A}^T\mathbf{w} \bmod q, \text{ for some } \mathbf{w} \in \mathbb{Z}^n\}$$

Discrete Gaussians on Lattices. Here we review Gaussian functions used in lattice based cryptographic constructions. For any $r > 0$ the Gaussian function on $\mathbb{R}^n$ centered at $\mathbf{c}$ with deviation parameter r is defined as

$$\forall\, \mathbf{x} \in \mathbb{R}^n, \rho_{r,\mathbf{c}}(x) = \exp(-\pi\|\mathbf{x} - \mathbf{c}\|^2/r^2)$$

For any $\mathbf{c} \in \mathbb{R}^n$, $r > 0$ and n-dimensional lattice Λ, the discrete gaussian distribution over Λ is defined as

$$\forall\, \mathbf{x} \in \Lambda, D_{\Lambda_{r,\mathbf{c}}}(x) = \frac{\rho_{r,\mathbf{c}}(\mathbf{x})}{\rho_{r,\mathbf{c}}(\Lambda)}$$

For a fixed vector $\mathbf{y} \in \mathbb{Z}_q^n$ in the span of a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, define the coset of $\Lambda^{\perp}(\mathbf{A})$ as $\Lambda_y^{\perp}(\mathbf{A}) = \{\mathbf{e} \in \mathbb{Z}^m : \mathbf{A}\mathbf{e} = \mathbf{y} \bmod q\} = \mathbf{t} + \Lambda^{\perp}(\mathbf{A}) \bmod q$; where $\mathbf{t}$ is an arbitrary solution (over $\mathbb{Z}$) of the equation $\mathbf{A}\mathbf{t} = \mathbf{y} \bmod q$. The Gaussian on $\Lambda_y^{\perp}(\mathbf{A})$, which is the conditional distribution of $D_{\mathbb{Z}^m,r}$ on $\mathbf{A}\mathbf{e} = \mathrm{y} \bmod q$, is given by

$$\forall\, \mathbf{x} \in \Lambda, D_{\Lambda_y^{\perp}(\mathbf{A}),r}(\mathbf{x}) = \frac{\rho_{r,c}(\mathbf{x})}{\rho_{r,c}(\mathbf{t} + \Lambda^{\perp}(\mathbf{A}))}$$

Micciancio and Regev[19] proposed a lattice quantity called the *smoothing parameter*:

Definition 1. *For any n-dimensional lattice Λ and positive real $\epsilon > 0$, the smoothing parameter $\eta_\epsilon(\Lambda)$ is the smallest real $r > 0$ such that $\sum_{0\neq\mathbf{x}\in\Lambda^*} \rho_{1/r,0}(\mathbf{x}) \leq \epsilon$.*

2.3 Hard Problems for Modular Lattice

We recall the *small integer solution* (SIS) and *learning with errors* (LWE) problems, which may be seen as average-case problems related to the family of modular lattices.

Small Integer Solution Problem The most well known computational problem on lattices is the *shortest vector problem* (SVP), in which given a basis of a lattice Λ and the goal is to find the shortest vector $v \in \Lambda\backslash\{0\}$. There is a special version of the SVP for the modular lattices, named *small integer solution* problem (SIS).

Definition 2. *The small integer solution problem* SIS *(in the Euclidean l_2 norm) is as follows: given an integer q, a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, and a real β, find a nonzero integer vector $\mathbf{e} \in \mathbb{Z}^m$ such that $\mathbf{Ae} = 0 \bmod q$ and $\|\mathbf{e}\|_2 \leq \beta$*

For functions $q(n)$, $m(n)$, and $\beta(n)$, $\mathsf{SIS}_{q,m,\beta}$ is the ensemble over instances $(q(n), \mathbf{A}, \beta(n))$, where $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ is uniformly random. For $\beta \geq \sqrt{m}$ and $m \geq 2n \lg q$, with overwhelming probability over the choice of $\mathbf{A}$, there exists an $\mathbf{e} \in \{0,1\}^m$ such that $\mathbf{Ae} = \mathbf{y} \bmod q$ for any $\mathbf{y} \in \mathbb{Z}_q^n$[15].

Learning With Errors Problem To describe the *learning with error* (LWE) hardness assumption, the following probability distribution is needed. For any $\alpha > 0$, the continuous Gaussian distribution D_α has density function $\exp(-\pi x^2/\alpha^2)$ for all $x \in \mathbb{R}$. For a positive integer q, define Ψ_α to be the distribution on $\mathbb{Z}_q$ obtained by taking a sample from $D_{q\cdot\alpha}$, rounding to the nearest integer, and reducing modulo q. For a dimension parameter $n \in \mathbb{Z}$, an integer $q = q(n) > 2$, a Gaussian error distributions χ and a vector $\mathbf{s} \in \mathbb{Z}_q^n$; the distribution of the variable $(\mathbf{a}, \mathbf{a}^T\mathbf{s} + x)$ over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ is denoted as $A_{\mathbf{s},\chi}$, where the vector $\mathbf{a} \in \mathbb{Z}_q^n$ is uniform and the scalar $x \in \mathbb{Z}_q$ is sampled from χ [19]. The l*earning with errors* problems is defined as follows [23]:

Definition 3. *For an integer $q = q(n)$ and a Gaussian error distributions χ on $\mathbb{Z}_q$, the goal of the (average-case) learning with error problem* $\mathsf{LWE}_{q,\chi}$ *is to distinguish (with non-negligible probability) between the distribution $A_{\mathbf{s},\chi}$ for some random secret $\mathbf{s} \in \mathbb{Z}_q^n$ and the uniform distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$(via oracle access to the given distribution)*

We write $\mathsf{Adv}^{\mathrm{sis}}_{q,\beta,\mathcal{A}}(k)$ and $\mathsf{Adv}^{\mathrm{lwe}}_{q,\chi,\mathcal{A}}(k)$ to denote the success probability and distinguishing advantage of an algorithm $\mathcal{A}$ for the SIS and LWE problems, respectively. Using Gaussian techniques, Micciancio and Regev[19] showed that for any poly-bounded m, $\beta = poly(n)$ and for any prime $q \geq \beta \cdot \omega(\sqrt{n \log n})$, the average-case problem $\mathsf{SIS}_{q,m,\beta}$ is as hard as approximating the SIVP problem (a variant of SVP) in the worst case to within a factor $\tilde{O}(\beta \cdot \sqrt{n})$. Regev[23] showed that, for any prime $q \geq (1/\alpha) \cdot (\omega(\sqrt{n \log n}))$ and a Gaussian Error Distributions $\chi = \Psi_\alpha$, the decisional $\mathrm{LWE}_{q,\chi}$ problem is as hard as approximating the SIVP and GapSVP (a variant of SVP) problems in the worst case to within $\tilde{O}(n/\alpha)$ factors using a quantum algorithm.

2.4 Trapdoor and Basis Delegation Functions for Modular Lattices

It was shown in [15] that if $\mathsf{SIS}_{q,m,2r\sqrt{m}}$ is hard, $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ defines a one-way function $f_{\mathbf{A}} : D_n \to \mathbb{Z}_q^n$ with $f_{\mathbf{A}}(\mathbf{e}) = \mathbf{Ae} \bmod q$, where $D_n = \{\mathbf{e} \in \mathbb{Z}^m : \|\mathbf{e}\| \leq r\sqrt{m}\}$. The input distribution is $D_{\mathbb{Z}^m,r}$. A short basis for $\Lambda^\perp(\mathbf{A})$ can be used as a trapdoor to sample from $f_A^{-1}(y)$. Knowledge of such a trapdoor makes it easy to solve some hard problems relative to the lattice, such as LWE and SIS problems. Here we briefly introduce such a set of one-way pre-image sampleble functions (defined in [15]), denoted as TrapGen, SampleDom, SamplePre , which will be used as building blocks in our cryptographic construction. The following

functions take the Gaussian smoothing parameter $r \geq \|\tilde{\mathbf{B}}\| \cdot \omega(\sqrt{\lg m})$ as a parameter:

- *Generating a function with trapdoor*: Let n, q, m be integers with $q \geq 2$, $m \geq 2n\lg q$, $\mathsf{TrapGen}(1^n)$ outputs a pair $(\mathbf{A}, \mathbf{T})$ such that $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ is statistically close to uniform on $\mathbb{Z}_q^{n\times m}$ and $\mathbf{B}$ is a good basis of $\Lambda^{\perp}(\mathbf{A})$ such that $\|\widetilde{\mathbf{B}}\| \leq m \cdot \omega(\sqrt{\log m})$ with all but $n^{\omega(1)}$ probability.
- *Domain sampling with uniform output*: $\mathsf{SampleDom}(1^n)$ samples x from distribution $D_{\mathbb{Z}^m,r}$.
- *Preimage sampling with a trapdoor*: $\mathsf{SamplePre}(\mathbf{A}, \mathbf{B}, \mathbf{y}, r)$ on input of $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, a good basis $\mathbf{B}$ for $\Lambda^{\perp}(\mathbf{A})$ as the trapdoor, a vector $\mathbf{y} \in \mathbb{Z}_q^n$ and r; the conditional distribution of the output $\mathbf{e}$ is within negligible statistical distance of $D_{\Lambda_y^{\perp}(\mathbf{A}),r}$.

We now recall the method proposed in [8] which uses a good basis of a lattice Λ to generate another good basis for a higher-dimensional lattice Λ' which contains a sublattice isomorphic to Λ . Let $\mathbf{A} \in \mathbb{Z}_q^{n\times km}$ and write $\mathbf{A} = [\mathbf{A}_1, ..., \mathbf{A}_k]$, where each $\mathbf{A}_i \in \mathbb{Z}_q^{n\times m}$. For $S' \subseteq [k]$, $S' = \{i_1, ..., i_j\}$, let $\mathbf{A}'_S = [\mathbf{A}_{i_1}, ..., \mathbf{A}_{i_j}]$, i.e., the components of $\mathbf{A}$ are selected according to S', when $\mathbf{A}'$ is viewed as a vector over $\mathbb{Z}_q^{n\times m}$. The mainly result of [8] is the theorem as follows.

Theorem 1. Let n, q, m, k be positive integers with $q \geq 2$ and $m \geq 2n \lg q$. There exists a PPT algorithm $\mathsf{SampleBasis}$, that on input of $\mathbf{A} \in \mathbb{Z}_q^{n\times km}$, a set $S' \subseteq [k]$, a basis $\mathbf{B}_{S'}$ for $\Lambda^{\perp}(\mathbf{A}_{S'})$, and an integer $L \geq \|\tilde{\mathbf{B}}_{S'}\| \cdot \sqrt{km} \cdot \omega(\sqrt{\log km})$ outputs $\mathbf{B} \leftarrow \mathsf{SampleBasis}(\mathbf{A}, \mathbf{B}_{S'}, S', L)$ such that, for an overwhelming fraction of $\mathbf{A} \in \mathbb{Z}_q^{n\times km}$, $\mathbf{B}$ is a basis of $\Lambda^{\perp}(\mathbf{A})$ with $\|\tilde{\mathbf{B}}\| \leq L$ (with overwhelming probability). Furthermore, up to a statistical distance the distribution of the basis $\mathbf{B}$ only depends on $\mathbf{A}$ and L.

To prove the above theorem, a sampling algorithm $\mathsf{GenSamplePre}$ is proposed which allows to preimage sampling of the function $f_{\mathbf{A}}(\mathbf{e}) = \mathbf{Ae} \bmod q$ given a short basis $\mathbf{B}_{S'}$ for $\Lambda^{\perp}(\mathbf{A}_{S'})$, and the output is within negligible statical distance of $D_{\Lambda_y^{\perp}(\mathbf{A}),r}$, where $r \geq \|\tilde{\mathbf{B}}_R\| \cdot \omega(\sqrt{\log km})$. Assume without loss of generality that $S = [k]$ for some $s \in [l]$. Let $S_c = [k]/S$,

The algorithm $\mathsf{SampleBasis}(\mathbf{A}, \mathbf{B}_{S'}, S', L)$ works as follows. It draws $O((km)^2)$ samples by running $\mathsf{GenSamplePre}(\mathbf{A}, \mathbf{B}_{S'}, S', \mathrm{y} = 0; s = L/\sqrt{km})$ times. These samples contain km linearly-independent vectors and have length at most $r \cdot \sqrt{km} = L$. The algorithm then applies the deterministic algorithm PT from [21] to process the samples into a basis of $\Lambda^{\perp}(\mathbf{A})$ without increasing the length of their Gram-Schmidt vectors.

2.5 Identity-Based Broadcast Encryption

An identity-based broadcast encryption scheme IBBE with security parameter λ and maximal size l of the target set, is made up of four algorithms:

- $\mathsf{Setup}(\lambda, l)$: Takes as input the security parameter λ and the maximal size l of the receivers set, and outputs a list of system parameters PK and the master key MSK for the KGC.
- $\mathsf{Extract}(\mathrm{MSK}, \mathrm{ID})$: Takes as input a user's identity string $ID_i \in \{0,1\}^*$ $(1 \leq i \leq l)$ and the master key of the KGC. It outputs a user private key sk_{ID_i}.
- $\mathsf{Enc}(S, \mathrm{PK})$: Takes as input system parameters, a set of receiver identities $S = \{ID_1, ..., ID_k\}$ with $k \leq l$, and outputs a pair (Hdr, K), where Hdr is called the header and $K \in \mathcal{K}$. Here $\mathcal{K}$ is a set of keys for the symmetric encryption algorithm.
  Let $M \in \{0,1\}^*$ be a message to be broadcast to users in S .Choose a symmetric encryption scheme E_{sym} with key-space $\mathcal{K}$ and algorithms SymEnc and SymDec. The broadcaster generates $(\mathrm{Hdr}, K) \leftarrow \mathrm{Enc}(S, PK)$, and computes the encryption of M as $C_M \leftarrow \mathsf{SymEnc}(K, M)$. The broadcast message to users in S consists of (Hdr, S, C_M).
- Dec $(S, \mathrm{ID}, sk_{ID_i}, \mathrm{Hdr}, \mathrm{PK})$: Takes as input system parameters, a receiver subset $S = \{ID_1, ..., ID_k\}$ with $k \leq l$, an identity ID_i and the corresponding private key sk_{ID_i}, a header Hdr, and the public key PK. If $ID_i \in S$, the algorithm outputs the message encryption key K which is then used to decrypt C_M and obtain M.

For consistency purposes, we of course require that for all $S \subseteq \{ID_1, ..., ID_l\}$ and all $ID_i \in S$, if $<\mathrm{PK}, \mathrm{MSK}> \xleftarrow{R} \mathsf{Setup}(\lambda, l)$, $sk_{ID_i} \xleftarrow{R} \mathsf{KeyGen}(ID_i, \mathrm{MSK})$, and $<\mathrm{Hdr}, K> \xleftarrow{R} \mathsf{Enc}(S, PK)$, then $\mathsf{Dec}(S, ID_i, sk_{ID_i}, \mathrm{Hdr}, PK) = K$.

There are two types of security requirements for identity-based broadcast encryption schemes: security against outsiders who only have public information (denoted as Collision-Resistance) and security against insiders who hold legitimate secret keys but are malicious to broadcasters. Considering the former type as collusion resistance of the scheme, Gentry and Waters[15] define adaptive security for IBBE systems under a chosen identity attack. In this model the adversary is allowed to adaptively chose the identity it wishes to attack. More precisely, adaptive security model is defined using the following game between an adversary $\mathcal{A}_1$ and a challenger. Both $\mathcal{A}_1$ and the challenger are given l, the maximal size of a set of receivers S as input.

Setup: The challenger runs $\mathsf{Setup}(\lambda, l)$ to obtain a public key PK, which is then given to $\mathcal{A}_1$.

Key Query Phase : The adversary $\mathcal{A}_1$ adaptively issues extraction queries on ID_i $(1 \leq i \leq l)$. The challenger responds by running algorithm $\mathsf{Extract}$ to generate the private key corresponding to ID_i and returns the resulting key to $\mathcal{A}_1$.

Challenge: Once the adversary $\mathcal{A}_1$ decides that the key query phase is over, $\mathcal{A}_1$ specifies a challenge set $S^* = \{ID_1^*, ..., ID_k^*\}$ that it wants to attack (with $k \leq l$). The challenger sets $(\mathrm{Hdr}^*, K_0) = \mathsf{Enc}(S^*, PK)$ and K_1 to be a random value in $\mathcal{K}$. The challenger picks a random $b \leftarrow \{0,1\}$ and returns (Hdr^*, K_b) to $\mathcal{A}_1$.

Guess: The adversary $\mathcal{A}_1$ outputs a guess $b' \in \{0,1\}$ and wins the game if $b' = b$

We denote by q_E the total number of extraction queries. Viewing q_E, l as attack parameters, we denote by $\mathsf{Adv}^{ibbe}_{l,q_E}(\mathcal{A}_1) = |2 \times \Pr[b' = b] - 1|$

Definition 4. *Let* $\mathsf{Adv}_{IBBE}(l, q_E) = \max_{\mathcal{A}_1} \mathsf{Adv}^{ibbe}_{l,q_E}(\mathcal{A}_1)$ *where the maximum is taken over all probabilistic algorithms* $\mathcal{A}_1$ *running in time* $\mathrm{poly}(\lambda)$*, an identity-based broadcast encryption scheme* $\mathcal{IBBE}$ *is said to be* (l, q_E) *adaptively secure if* $\mathsf{Adv}_{IBBE}(l, q_E) = \mathrm{negl}(\lambda)$

The above game models an attack where all users outside of the set S collude to try and expose a broadcast message intended for authorized users in S. In the second type of attacks,the game could be described as follows: the attacker $\mathcal{A}_2$ holds legitimate secret keys for some authorized users in S and targets on another user $ID_{i^*} \in S$ in order to find its private key.Here we define a strong adversary that $\mathcal{A}_2$ may collude with all $k-1$ users in S and get their secret keys except for the target user ID_{i^*} . If for all poly-time algorithms $\mathcal{A}_2$ the probability that $\mathcal{A}_2$ successfully forge a secret key for ID_{i^*} is negligible, we say the scheme is secure against insider attack.

3 Identity-Based Broadcast Encryption Scheme from Lattices

In this section, we describe our identity-based broadcast encryption system using the lattice basis delegation technique. We start with a slight variant of the generalized sampling algorithm $\mathsf{GenSamplePre}$(in [8]), which differs only in the structure of the extended lattice. The original algorithm enables the growth of extended matrices in a tree form. In our approach, we will handle with another extension policy better suited for our IBBE scheme given later.

3.1 Generalized Preimage Sampling Algorithm

Assume without loss of generality that $S = [k]$, for some $k \in [l]$. Let k_1, k_2, k_3, k_4 be positive integers and $k = k_1+k_2+k_3+k_4$. We write $\mathbf{A}_S = [\mathbf{A}_{S_1} \| \mathbf{A}_{S_2} \| \mathbf{A}_{S_3} \| \mathbf{A}_{S_4}] \in \mathbb{Z}_q^{n \times km}$, where $\mathbf{A}_{S_1} \in \mathbb{Z}_q^{n \times k_1 m}$, $\mathbf{A}_{S_2} \in \mathbb{Z}_q^{n \times k_2 m}$, $\mathbf{A}_{S_3} \in \mathbb{Z}_q^{n \times k_3 m}$, $\mathbf{A}_{S_4} \in \mathbb{Z}_q^{n \times k_4 m}$. Let $\mathbf{A}_R = [\mathbf{A}_{S_1} \| \mathbf{A}_{S_3}] \in \mathbb{Z}_q^{n \times (k_1+k_3)m}$. Given a short basis $\mathbf{B}_R$ for $\Lambda^{\perp}(\mathbf{A}_R)$ and an integer $r \geq \|\mathbf{B}_R\| \cdot \omega(\sqrt{\log km})$, the algorithm $\mathsf{GenSamplePre}$ allows to sample a preimage of the function $f_{\mathbf{A}_S}(\mathbf{e}) = \mathbf{A}_S \mathbf{e} \bmod q$. $\mathsf{GenSamplePre}(\mathbf{A}_S, \mathbf{A}_R, \mathbf{B}_R, \mathbf{y}, r)$ proceeds as follows:

1 Sample $\mathbf{e}_{S_2} \in \mathbb{Z}^{k_2 m}$ from the distribution $D_{\mathbb{Z}^{k_2 m}, r}$ and sample $\mathbf{e}_{S_4} \in \mathbb{Z}^{k_4 m}$ from the distribution $D_{\mathbb{Z}^{k_4 m}, r}$. Parse $\mathbf{e}_{S_2} = [\mathbf{e}_{k_1+1}, ..., \mathbf{e}_{k_1+k_2}] \in (\mathbb{Z}^m)^{k_2}$ and $\mathbf{e}_{S_4} = [\mathbf{e}_{k-k_4+1}, ..., \mathbf{e}_k] \in (\mathbb{Z}^m)^{k_4}$.

2 Let $\mathbf{z} = \mathbf{y} - \mathbf{A}_{S_2}\mathbf{e}_{S_2} - \mathbf{A}_{S^4}\mathbf{e}_{S_4}$. Run $\mathbf{e}_R \leftarrow \mathsf{SamplePre}(\mathbf{A}_R, \mathbf{B}_R, \mathbf{z}, r)$ to sample a vector $\mathbf{e}_R \in \mathbb{Z}^{(k_1+k_3)m}$ from the distribution $D_{\Lambda^{\perp}_{\mathbf{y}}(\mathbf{A}_S), r}$. Parse $\mathbf{e}_R = [\mathbf{e}_1, ..., \mathbf{e}_{k_1}, \mathbf{e}_{k_1+k_2+1}, ..., \mathbf{e}_{k-k_4}] \in (\mathbb{Z}^m)^{k_1+k_3}$ and let $\mathbf{e}_{S_1} = [\mathbf{e}_1, ..., \mathbf{e}_{k_1}] \in (\mathbb{Z}^m)^{k_1}$, $\mathbf{e}_{S_3} = [\mathbf{e}_{k_1+k_2+1}, ..., \mathbf{e}_{k-k_4}] \in (\mathbb{Z}^m)^{k_3}$

3 Output $\mathbf{e} \in \mathbb{Z}^{km}$, as $\mathbf{e} = [\mathbf{e}_1, ..., \mathbf{e}_k]$

Note that by construction, we have $\mathbf{A}_{S_1}\mathbf{e}_{S_1} + \mathbf{A}_{S_3}\mathbf{e}_{S_3} = \mathbf{A}_R\mathbf{e}_R = \mathbf{z} \bmod q$. Thus $\mathbf{A}_S\mathbf{e} = \sum_{i=1}^{4} \mathbf{A}_{S_i}\mathbf{e}_{S_i} = \mathbf{y} \bmod q$, and the output vector $\mathbf{e}$ of $\mathsf{GenSamplePre}$ is contained in $\Lambda_y^{\perp}(\mathbf{A}_S)$. For the analyze of output distribution, we have the following algorithm.

Theorem 2. Let n, q, m, k be positive integers with $q \geq 2$ and $m \geq 2n \lg q$. There exists a PPT algorithm $\mathsf{GenSamplePre}$, that on input of $\mathbf{A}_S \in \mathbb{Z}_q^{n \times km}$, a set $R \subseteq [k]$, a basis $\mathbf{B}_R$ for $\Lambda^{\perp}(\mathbf{A}_R)$, a vector $\mathbf{y} \in \mathbb{Z}_q^n$ and an integer $r \geq \|\tilde{\mathbf{B}}_R\| \cdot \omega(\sqrt{\log km})$ outputs $\mathbf{e} \leftarrow \mathsf{GenSamplePre}(\mathbf{A}_S, \mathbf{A}_R, \mathbf{B}_R, \mathbf{y}, r)$ such that, for an overwhelming fraction of $\mathbf{A}_S \in \mathbb{Z}_q^{n \times km}$, is within negligible statical distance of $D_{\Lambda_y^{\perp}(\mathbf{A}_S), r}$

Proof: The algorithm differs from the original one only in the structure of the extension matrix, so the proof can be deduced directly from [8] and therefore it is omitted.

3.2 Our Construction

Let k, l, m, n, q, t be positive integers with $q \geq 2$ and $m \geq 2n\log q$. Let $k \leq l$, where l is the maximum number of the receivers. The IBBE scheme shares parameter functions $L(k)$, $r(k)$, $\alpha(k)$ defined in [8] as follows:

- $L \geq m \cdot \omega(\sqrt{\log n}); L(k) \geq L \cdot m^{k/2} \cdot \omega(\log^{k/2} m)$: The size of user's secret basis.
- $r(k) \geq L(k-1) \cdot \omega(\sqrt{\log m})$: Gaussian parameter for generating the short basis.
- $\alpha(k) \leq 1/(r(k) \cdot \sqrt{km+1} \cdot \omega(\sqrt{\log n}))$: Gaussian parameter for adding noise to the ciphertext.

Setup: Choose a hash function $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_q^{n \times m}$. The security analysis will view H_1 as a random oracle. Choose $\mathbf{v} \in \mathbb{Z}_q^{n \times t}$ uniformly at random, where t is the length of the message encryption key. Then run the trapdoor generation algorithm $\mathsf{TrapGen}$ (described in section 2.4) to generate $\mathbf{A}_0 \in \mathbb{Z}_q^{n \times m}$ with a short basis $\mathbf{B}_0 \in \mathbb{Z}_q^{m \times m}$ ($\|\mathbf{B}_0\| \leq L$) for $\Lambda^{\perp}(\mathbf{A}_0)$. Output $\mathtt{PK} =< \mathbf{A}_0, H_1, \mathbf{v} >$ and the master key $\mathtt{MSK} = \mathbf{B}_0$.

$\mathsf{Extract}(\mathtt{MSK}, ID_i)$: For an arbitrary identity $ID_i \in \{0,1\}^*$, define the associated matrix $\mathbf{Q}_{ID_i}$ as

$$\mathbf{Q}_{ID_i} = [\mathbf{A}_0 \| \mathbf{A}_{ID_i}] \in \mathbb{Z}_q^{n \times 2m}$$

where $\mathbf{A}_{ID_i} = H_1(ID_i) \in \mathbb{Z}_q^{n \times m}$. To construct user's secret key, run the basis delegation algorithm $\mathsf{SampleBasis}$ (described in section 2.4) and generate $\mathbf{B}_{ID_i} \leftarrow \mathsf{SampleBasis}(\mathbf{Q}_{ID_i}, \mathbf{B}_0, S_0 = \{1\}, L(1))$, which is a short basis for $\Lambda^{\perp}(\mathbf{Q}_{ID_i})$. Note that by Theorem 1 we have $\|\widetilde{\mathbf{B}}_{ID_i}\| \leq L(1)$. The secret key for ID_i is $\mathbf{B}_{ID_i}$.

$\mathsf{Enc}(S, PK)$: Assume for notational simplicity that $S = \{ID_1, ..., ID_k\}$ with $k \leq l$. The broadcaster does the following:

- Let $\mathbf{A}_S = [\mathbf{A}_0 \| \mathbf{A}_{ID_1} \| ... \| \mathbf{A}_{ID_k}] \in \mathbb{Z}_q^{n \times (k+1)m}$ where $\mathbf{A}_{ID_i} = H_1(ID_i) \in \mathbb{Z}_q^{n \times m} (1 \leq i \leq k)$. Define a label lab_S that contains information about how $\mathbf{A}_S$ is associated with the sequence of the receivers $\{ID_1, ..., ID_k\}$.
- Choose a vector $\mathbf{u} \in \mathbb{Z}_q^n$ uniformly at random, and compute $\mathbf{p} = \mathbf{A}_S^T \mathbf{u} + \mathbf{x}_1 \in \mathbb{Z}_q^{(k+1)m}$, where $\mathbf{x}_1 \leftarrow \chi^{(k+1)m}$ and $\chi = \Psi_{\alpha(k+1)}$.
- Choose a message encryption key $K \in \{0,1\}^t$. For $1 \leq j \leq t$, let $b_j = bit_j(K)$ be the j-th bit of K. Compute $\mathbf{c} = \mathbf{v}^T \mathbf{u} + \mathbf{x}_2 + K \cdot \lfloor q/2 \rfloor \in \mathbb{Z}_q^t$ where $\mathbf{x}_2 \leftarrow \chi^t$.
- Output Hdr $=< \mathbf{p}, \mathbf{c}, lab_S >$.

$\mathsf{Dec}(\mathrm{Hdr}, \mathbf{B}_{ID_i})$: In order to retrieve the message key, an authorized receiver with identity $ID_i \in S$ and the private key $\mathbf{B}_{ID_i}$ does the following:

- By the information in lab_S, set $\mathbf{A}_S = [\mathbf{A}_0 \| \mathbf{A}_{ID_1} \| ... \| \mathbf{A}_{ID_k}] \in \mathbb{Z}_q^{n \times (k+1)m}$ where $\mathbf{A}_{ID_i} = H_1(ID_i) \in \mathbb{Z}_q^{n \times m} (\ 1 \leq i \leq k)$.
- Parse $\mathbf{v} = [\mathbf{v}_1, ..., \mathbf{v}_t] \in (\mathbb{Z}_q^n)^t$. For $1 \leq j \leq t$, run the generalized preimage sampling algorithm $\mathsf{GenSamplePre}$ and generate $\mathbf{e}_j \leftarrow \mathsf{GenSamplePre}(\mathbf{A}_S, \mathbf{A}_{ID_i}, \mathbf{B}_{ID_i}, \mathbf{v}_j, r(k+1)) \in \mathbb{Z}^{(k+1)m}$. Note that $\mathbf{e}_j$ is distributed according to $D_{\Lambda_{\mathbf{v}_j}^{\perp} \mathbf{A}_S, r(k+1)}$.
- Parse $\mathbf{c}$ as $[c_1, ..., c_t] \in \mathbb{Z}_q$. For $1 \leq j \leq t$, compute $b'_j = c_j - \mathbf{e}_j^T \mathbf{p} \in \mathbb{Z}_q$, let $b_j = 0$ if b'_j is closer to 0 than to $\lfloor q/2 \rfloor \in \mathbb{Z}_q$; otherwise $b_j = 1$.
- Output $K = [b_1, ..., b_t]$.

3.3 Correctness

The scheme's correctness is inherited by LWE-PKE [23] and the properties of the trapdoor functions [15]. In the encryption process, authorized users in S construct a one-way function $f_{A_S} : D_S \rightarrow \mathbb{Z}_q^n$ as $f_{\mathbf{A}_S}(\mathbf{e}) = \mathbf{A}_S \mathbf{e} \bmod q$, where $D_S = \{\mathbf{e} \in \mathbb{Z}^{(k+1)m} : \|\mathbf{e}\| \leq r(k+1)\}$ with the following properties:

Correct Distributions: By Lemma 5.1 in [15], the distribution of the syndrome $\mathrm{v}_j = \mathbf{A}_S \mathbf{e}_j \bmod q$ is within statistical distance 2ϵ of uniform over $\mathbb{Z}_q^n$. By the Theorem 2, algorithm $\mathsf{GenSamplePre}(\mathbf{A}_S, \mathbf{A}_{ID_i}, \mathbf{B}_{ID_i}, \mathrm{v}_j, r(k+1))$ samples an element $\mathbf{e}_j \in D_S$ from distribution within negligible statistical distance of $D_{\Lambda_{\mathbf{v}_j}^{\perp}(\mathbf{A}_S), r(k+1)}$.

One-Wayness Without Trapdoors: By Theorem 5.9 in [15], inverting a random function $f_{\mathbf{A}_S}$ on a uniform output is equivalent to solving the *inhomogeneous small integer solution* problem ISIS(a variant of SIS) as $\mathsf{ISIS}_{q,(k+1)m,r(k+1)}$.

In the broadcast approach, the size of the trapdoor basis $L(k)$ and the Gaussian parameter $r(k)$ of the decryption key increase geometrically with k, the the number of the receivers in S. To ensure correct decryption, the inverse noise parameter $1/\alpha(k)$ in the associated LWE problem also must grow with the receiver number in S.

3.4 Security

As mentioned earlier, an IBBE scheme should be secure against two types of attacks: attacks by an outsider (adversary $\mathcal{A}_1$) and attacks by authorized receivers (adversary $\mathcal{A}_2$).
In the former type, an IBBE scheme is said to be fully collusion resistant when, even if all users that are not in S collude, they can by no means infer information about the broadcast message. In the following theorem we will show that our scheme is adaptively secure for any collusion of non-authorized users.

Theorem 3. *Let $q \geq 5r(l)(m+1)$ and $m \geq 2n \lg q$. If H_1 is modeled as random oracles, the IBBE system above is adaptively secure against collusion of outsiders assuming that $\mathsf{LWE}_{q,\chi}$ is hard, where $\chi = \Psi_{\alpha(l+1)}$*

Proof. To simplify the analysis, we consider the situation of encrypting a single bit of the symmetric message key in the scheme. Assume that there exists an adaptive adversary $\mathcal{A}_1$ breaking our scheme with distinguish advantage $\mathsf{Adv}^{ibbe}_{l,q_E}(\mathcal{A}_1)$. We now construct an adversary $\mathcal{B}$ that has advantage $\mathsf{Adv}^{lwe}_{q,\chi}(\mathcal{B})$ in attacking the LWE problem where

$$\mathsf{Adv}^{\mathrm{lwe}}_{q,\chi}(\mathcal{B}) \geq \frac{\mathsf{Adv}^{ibbe}_{l,q_E}(\mathcal{A}_1)}{l q_{H_1}^{l-1}} - \mathrm{negl}$$

Both the adversary and the challenger are given as input l, the maximal size of a broadcast recipient group, q_E and q_{H_1}, the total number of extraction queries and random oracle queries on H_1, that can be issued by the adversary $\mathcal{A}_1$. $\mathcal{B}$ interacts with $\mathcal{A}_1$ as follows:

Setup : $\mathcal{B}$ first uniformly picks $k^* \in [l]$. (k^* is a guess for the size of the challenge receiver set). $\mathcal{B}$ then obtains $(k^*+1)m+1$ samples $(a_j, b_j) \in \mathbb{Z}_q^n \times \mathbb{Z}_q (1 \leq j \leq (k^*+1)m+1)$ from the LWE oracle where all $a_j \in \mathbb{Z}_q^n$ are random, and either all $b_j \in \mathbb{Z}_q$ are also random or all are equal to $a_j^T s + x_j$ for a uniform secret $s \in \mathbb{Z}_q^n$ and independent Gaussian noises x_j drawn from χ. Next $\mathcal{B}$ parses these LWE samples $(a_j, b_j) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ $(1 \leq j \leq (k^*+1)m)$ as $(\mathbf{A}_i^*, p_i^*) \in (\mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^m)$ $(0 \leq i \leq k^*)$ and $(y^*, c^*) = (a_{(k^*+1)m+1}, b_{(k^*+1)m+1}) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$. $\mathcal{B}$ chooses $\mathbf{v} \in \mathbb{Z}_q^n$ uniformly at random. It sets the master public key as $mpk = \mathbf{A}_0 = \mathbf{A}_0^*$, the master secret key (a short basis for $\Lambda^{\perp}(\mathbf{A}_0)$) is unknown to $\mathcal{B}$. The system parameters are given to $\mathcal{A}_1$. To respond to $\mathcal{A}_1$'s hash queries in the random oracle, $\mathcal{B}$ will maintain a list H_1, which is initialized to be empty and will store tuples of values. $\mathcal{A}_1$ also chooses a random vector $t^* = \{t_1^*, ..., t_{k^*}^*\} \in \{1, ..., Q_{H_1}\}^{k^*}$.

Query Phase: $\mathcal{A}_1$ issues following queries as it wants:

1. *Queries to H_1.* On $\mathcal{A}_1$'s *j-th* query ID_i to H_1, if $j = t_i^*$, $\mathcal{B}$ returns $\mathbf{A}_i^*$ to $\mathcal{A}_1$. Otherwise, $\mathcal{B}$ runs the algorithm $\mathsf{TrapGen}$ to generate $\mathbf{A}_i \in \mathbb{Z}_q^{n \times m}$ with the corresponding trapdoor $\mathbf{B}_i \in \mathbb{Z}_q^{m \times m}$. $\mathcal{B}$ returns $\mathbf{A}_i$ to $\mathcal{A}_1$ and stores the tuple $\langle ID_i, \mathbf{A}_i, \mathbf{B}_i \rangle$ in list $\mathcal{H}_1$. Note that according to [3], $\mathbf{A}_i$ is statically close to uniform over $\mathbb{Z}_q^{n \times m}$.

2. *Queries to Ext.* When $\mathcal{A}_1$ asks for a user's secret key for ID_i, we assume that $\mathcal{A}_1$ has made a H_1 query on ID_i. If $\langle ID_i, \mathbf{A}_i, \mathbf{B}_i \rangle$ is contained in list H_1, $\mathcal{B}$ can compute a properly distributed basis $\mathbf{B}_{ID_i}$ corresponding to ID_i's public key $\mathbf{A}_{ID_i} = [\mathbf{A}_0 \| \mathbf{A}_i]$ by running $\mathbf{B}_{ID_i} \leftarrow \mathsf{SampleBasis}(\mathbf{A}_{ID_i}, \mathbf{B}_i, S_0 = \{1\}, L(1))$. If the generation is successful, then $\mathcal{B}$ returns $\mathbf{B}_{ID_i}$. Otherwise $\mathcal{B}$ aborts.

Challenge : $\mathcal{A}_1$ specifies a target receiver set $S^* = \{ID_1^*, ..., ID_{k'}^*\}$ with $k' \leq l$. Assume that $\mathcal{A}_1$ has already made all relevant queries to H_1 that defines $\mathbf{A}_{S^*}$. If $k' \neq k^*$, $\mathcal{B}$ aborts and returns a random bit. Otherwise, if one of $ID_i^* \in S^*$ is contained in list H_1, $\mathcal{B}$ aborts and returns a random bit. Otherwise we have $\mathbf{A}_{S^*} = [\mathbf{A}_0^* \| \mathbf{A}_1^* \| ... \| \mathbf{A}_{k^*}^*]$. $\mathcal{B}$ sets a challenge $C^* = (p^*, c^*)$ for a random bit $b^* \in \{0, 1\}$ as $p^* = (p_0^*, ..., p_k^*)$ and c^* chosen in the Setup phase.

Guess: Finally, the adversary $\mathcal{A}_1$ outputs a guess $b' \in \{0, 1\}$, $\mathcal{B}$ returns genuine if $b' = b^*$, or random if $b' \neq b^*$ as its answer for the LWE instances.

In the view of $\mathcal{A}_1$, the behavior of $\mathcal{B}$ is statistically close to the one provided by the real adaptive security experiment. In particular, A_{S^*} is created using the LWE instances and has a uniform distribution whether the LWE instances are genuine or not. It is easy to see that the probability of an abort during the challenge query is $1 - \frac{1}{lq_{H_1}^{k^*-1}}$. Implementing a straightforward additional artificial abort step, this probability of an abort can be raised to $1 - \frac{1}{lq_{H_1}^{l-1}}$. If $\mathcal{B}$ does not abort in the query phase, then the distribution of its answers is statistically close to the one from the real adaptive security environment. For the challenge ciphertext, if the LWE instances are genuine, the components of C^* will have the same distribution as in the LWE game: whereas, if the LWE instances are random, so will be the components of C^*. If $\mathcal{A}_1$ exhibit a different success probability in either case, $\mathcal{B}$ will have successfully distinguished between $(k^*+1)m+1$ genuine and random instances of the LWE problem. The proof can be easily generalized to the multi-bit encryption, because each syndrome $\mathbf{c}^*$ is independent and statistically close to uniform.

In the second type of attacks, for coalition of authorized users, the security can be referred to the following insider attack problem. Assume, for contradiction, that there is an adversary $\mathcal{A}_2$ colluding with all $k-1$ users in S and getting their secret keys except for the challenge user ID_{i^*}. The target of $\mathcal{A}_2$ is trying to find the private key of the challenge user $ID_{i^*} \in S$. By Theorem 5.9 of [15], each authorized user ID_i in S constructs a one-way function $f_{ID_i} : D_{2m} \rightarrow \mathbb{Z}_q^n$ as $f_{ID_i}(\mathrm{e}) = \mathbf{Q}_{ID_i}\mathrm{e} \bmod q$, where $D_{2m} = \{\mathrm{e} \in \mathbb{Z}^m : \|\mathrm{e}\| \leq r(2)\}$ and the short basis $\mathbf{B}_i$ for $\Lambda^{\perp}(\mathbf{Q}_{ID_i})$ is its trapdoor. The above insider attack problem can be reduced to breaking the collision-resistant one-way function $f_{ID_{i^*}}$ defined by the challenge user ID_{i^*}.

Theorem 4. *The IBBE system above is secure against coalition of authorized users under chosen message attack assuming that* $\mathsf{SIS}_{q,m,\sigma\sqrt{m}}$ *is hard.*

Proof: Let $\mathcal{A}_2$ be an adversary that breaks the unforgeability on the insider attack of the IBBE scheme with probability $\epsilon = \epsilon(n)$. We construct a poly-time

adversary $\mathcal{B}_2$ that solves $\mathsf{SIS}_{q,m,\sigma\sqrt{m}}$ with probability negligibly close to ϵ.
In the Init phase the adversary $\mathcal{A}_2$ chooses a target set S^* and a challenge $ID_{i^*} \in S^*$. $\mathcal{B}$ obtains the system parameters and gives them to $\mathcal{A}_1$. In the attack game $\mathcal{A}_2$ issues private key queries on $ID_i \in S/\{ID_{i^*}\}$ and preimage quires $\mathbf{y}_i \in \mathbb{Z}_q^n$ on $\mathbf{Q}_{ID_{i^*}} = \mathbf{A}_0 \| \mathbf{A}_{i^*}$. As mentioned in [15], the answer for the preimage query $\mathbf{y}_i$ can be treated as the signature for $\mathbf{y}_i$ under $f_{ID_{i^*}}$. So it can be reduced to the chosen message attack on $f_{ID_{i^*}}$. $\mathcal{B}_2$ answers the key queries in a similar way as in Theorem 3 and the preimage queries as in the proof of Theorem 6.1 in [15]. The full proof can be deduced from the combination of the techniques that are used in Theorems 3 and Theorem 6.1 in [15], and therefore, it is omitted.

3.5 Efficiency

Our construction involves nothing but additions and multiplications modulo q. It achieves $O(1)$-size public keys, $O(k)$-size ciphertexts and constant size private keys. Note that ciphertext is linear in the size of S, the efficiency cost is similar to the adaptively secure IBBE scheme in [15]. We remark that the resulting IBBE scheme is not very practical. Comparing with pairing based IBBE constructions, our scheme is however does serve as a lattice-based IBBE supported by the adaptive security.

4 Variants and Extensions

4.1 Hierarchical IBBE Scheme

The concept of hierarchical IBBE scheme (HIBBE) was proposed by Boneh and Hamburg in [7]. In a hierarchical IBBE scheme there is a tree-like hierarchy of identities and private keys as in HIBE [17]. An broadcaster picks a set S of nodes in the hierarchy and encrypts a message to this set if the number of distinct path prefixes in S is less than the maximal size of a receiver set. Building upon the lattice basis delegation structure, Cash et. al's proposed a hierarchical identity-based encryption scheme (HIBE)[8]. Note that we could easily obtain a hierarchical IBBE scheme by representing user's identity and corresponding matrices in a tree structure. The four algorithms of HIBBE: Setup, $\mathsf{Extract}$, Enc, Dec have similar functions to that of IBBE scheme except for the following characteristics:

- For a d-depth identity: $ID_i|d = (ID_{i1}, ..., ID_{id}) \in \{0,1\}^*$, let $\mathbf{A}_{ID_i|d} = [\mathbf{A}_0 \| \mathbf{A}_{ID_{i1}} \| ... \| \mathbf{A}_{ID_{id}}] \in \mathbb{Z}_q^{n \times (d+1)m}$ where $\mathbf{A}_{ID_{ij}} = H_1(ID_{ij}) \in \mathbb{Z}_q^{n \times m}$, $1 \leq j \leq d$.
- The $\mathsf{Extract}$ algorithm in HIBBE will generate the private key for a given identity of a lower level user. For a user $ID_i|d-1 = (ID_{i1}, ..., ID_{id-1})$ of depth $d-1$, it uses its private key $\mathbf{B}_{ID_i|d-1}$ to generate the private key for a user $ID_i|d = (ID_{i1}, ..., ID_{id}) \in \{0,1\}^*$ (where the first $d-1$ elements of $ID_i|d$ are those in $ID_i|d-1$) by running $\mathbf{B}_{ID_i|d} \leftarrow \mathsf{SampleBasis}(\mathbf{A}_{ID_i|d}, \mathbf{B}_{ID_i|d-1},$

$S_0 = \{1, ..., d\}, L(d))$. Note that $\mathbf{B}_{ID_i|d}$ is a short basis for $\Lambda^{\perp}(\mathbf{A}_{ID_i|d})$ and by Theorem 1 we have $\|\widetilde{\mathbf{B}}_{ID_i|d}\| \leq L(d)$.

– For the receiver set S, the matrix $\mathbf{A}_S$ is constructed as following: for $1 \leq i \leq k(k = |S|)$, let j $(0 \leq j \leq d)$ be the minimal number such that $\mathbf{A}_{ID_{ij}}$ is not contained in $\mathbf{A}_S$, set $\mathbf{A}_i = [\mathbf{A}_{i-1}\|\mathbf{A}_{ID_{ij}}\|...\|\mathbf{A}_{ID_{id}}]$. Finally let $\mathbf{A}_S = \mathbf{A}_k$. Note that in the decryption approach, the receiver can set $\mathbf{A}_S$ from the information in lab_S.

4.2 IBBE Scheme with Sublinear-Size Ciphertexts

Below,we describe a system that builds on the initial IBBE system to obtain sublinear size ciphertexts. The idea behind our construction is based on the parallel method proposed in [6]. We essentially divide $l(= l_1 \cdot l_2)$ users into l_1 subsets in which each set has at most l_2 users. This approach allows one to encrypt to a set S with $|S| = |k_1 \cdot k_2|$, $(k_1 \leq l_1, k_2 \leq l_2,)$

Setup: As in the basic scheme. In addition, Let l_1 be a positive integer dividing $l(= l_1 \cdot l_2)$, the maximal number of users in the receiver set.The choice of l_1 would depend on the concrete application.

Extract($\mathtt{MSK}, ID$): As in the basic scheme.

Enc(S, PK): Partition S into $k_1 \leq l_1$ sets $< S_1, ..., S_{k_1} >$ of size $k_2 \leq l_2$ with $k = |k_1 \cdot k_2|$. Let $S_i = \{ID_{i1}, ..., ID_{ik_2}\}$ $(1 \leq i \leq k_1)$. Define a label lab_S that contains information about how $S_i (1 \leq i \leq k_2)$ is associated with receivers in S. The broadcaster chooses a message encryption key $K \in \{0,1\}^t$ and for $1 \leq i \leq k_1$, does the following:

- Let $\mathbf{A}_{S_i} = [\mathbf{A}_0\|\mathbf{A}_{ID_{i1}}\|...\|\mathbf{A}_{ID_{ik_2}}] \in \mathbb{Z}_q^{n\times(k_2+1)m}$ where $ID_{ij} \in S_i$ $(1 \leq j \leq k_2)$ and $\mathbf{A}_{ID_{ij}} = H_1(ID_{ij}) \in \mathbb{Z}_q^{n\times m}$.
- Choose a vector $\mathbf{u}_i \in \mathbb{Z}_q^n$ uniformly at random, and compute $\mathbf{p}_i = \mathbf{A}_{S_i}^T\mathbf{u}_i + \mathbf{x}_{i1} \in \mathbb{Z}_q^{(k_2+1)m}$, where $\mathbf{x}_{i1} \leftarrow \chi^{(k_2+1)m}$ and $\chi = \Psi_{\alpha(k_2)}$.
- Compute $\mathbf{c}_i = \mathbf{v}^T\mathbf{u}_i + \mathbf{x}_{i2} + K \cdot \lfloor q/2 \rfloor \in \mathbb{Z}_q^t$ where $\mathbf{x}_{i2} \leftarrow \chi^t$
- Set $\mathrm{Hdr}_i =< \mathbf{p}_i, \mathbf{c}_i, S_i >$

The broadcaster outputs $\mathrm{Hdr} =< \mathrm{Hdr}_1, ..., \mathrm{Hdr}_{k_1} >$

Dec($\mathrm{Hdr}, \mathbf{B}_{ID_{ij}}$): Parse Hdr as $\mathrm{Hdr}_1, ..., \mathrm{Hdr}_{k_1}$. In order to retrieve the message key, an authorized receiver with identity $ID_{ij} \in S_i$ and the corresponding privet key $\mathbf{B}_{ID_{ij}}$ does the following:

- Following the information in lab_S, set $\mathbf{A}_{S_i} = [\mathbf{A}_0\|\mathbf{A}_{ID_{i1}}\|...\|\mathbf{A}_{ID_{ik_2}}] \in \mathbb{Z}_q^{n\times(k_2+1)m}$ where $ID_{ij} \in S_i (1 \leq j \leq k_2)$ and $\mathbf{A}_{ID_{ij}} = H_1(ID_{ij}) \in \mathbb{Z}_q^{n\times m}$.
- Parse $\mathbf{v} = [\mathbf{v}_1, ..., \mathbf{v}_t] \in (\mathbb{Z}_q^n)^t$. For $1 \leq d \leq t$, compute $\mathbf{e}_{id} =$ GenSamplePre($\mathbf{A}_{S_i}$, $\mathbf{A}_{ID_{ij}}, \mathbf{B}_{ID_{ij}}, \mathbf{v}_d, r(k_2+1)) \in \mathbb{Z}^{(k_2+1)m}$.
- Parse $\mathbf{c}_i$ as $[c_{i1}, ..., c_{it}] \in \mathbb{Z}_q$. Using Lab_S, find appropriate Hdr_i. For $1 \leq d \leq t$, compute $b'_d = \mathbf{c}_{id} - \mathbf{e}_{id}^T\mathbf{p}_i \in \mathbb{Z}_q$, let $b_d = 0$ if b'_d is closer to 0 than to $\lfloor q/2 \rfloor \in \mathbb{Z}_q$. Otherwise $b_d = 1$.

- Output $K = [b_1, ..., b_t]$.

It is easy to observe that in the case where $|S|$ is expressed as a product $k_1 \cdot k_2$ with $k_1, k_2 = O(\sqrt{|S|})$, the overall size of the ciphertext is $O(\lambda \cdot \sqrt{|S|})$. One can prove the security of this encryption by a method similar to the proof of Theorem 3.

5 Conclusion

In this paper, we have presented a new type of identity-based broadcast encryption schemes from modular lattices. The idea behind our construction is based on the lattice delegation method due to [8]. Our construction and its variants constitute the first adaptively secure IBBE schemes from lattices, which are believed secure in the post-quantum environment.

References

1. Ajtai, M.: Generating hard instances of lattice problems. Quaderni di Matematica 13, 1-32 (2004); Preliminary version in STOC 1996
2. Ajtai, M., Dwork, C.: A public-key cryptosystem with worst-case/average-case equivalence. In: STOC, pp. 284-293 (1997)
3. Ajtai, M.: Generating hard instances of the short basis problem. In: Wiedermann, J., Van Emde Boas, P., Nielsen, M. (eds.) ICALP 1999. LNCS, vol. 1644, pp. 1-9. Springer, Heidelberg (1999)
4. Agrawal, S.,Boyen, S. Identity-based encryption from lattices in the standard model. In manuscript, 2009.
5. Boneh, D., Franklin, M.K.: Identity-based encryption from the weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213-229. Springer, Heidelberg (2001)
6. Boneh, D., Gentry, C., Waters, B.: Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 258-275. Springer, Heidelberg (2005)
7. Boneh, D., Hamburg, M.: Generalized Identity-based and Broadcast Encryption Schemes. In: Pieprzyk, J. (ed.) Asiacrypt'08. LNCS, vol. 5350, pp. 455-470. Springer, Heidelberg (2008)
8. Cash, D.,Hofheinz,D.,Kiltz,E.: How to delegate a lattice basis.In: Halevi, S. (ed.) CRYPTO rumption (2009). Cryptology ePrint Archive, Report 2009/351 (2009), http://eprint.iacr.org/2009/351
9. Cha, J.C., Cheon, J.H.: An identity-based signature from gap Diffie-Hellman groups. In: Desmedt, Y.G. (ed.) PKC 2003. LNCS, vol. 2567, pp. 18-30. Springer, Heidelberg (2002)
10. Cocks, C.: An identity based encryption scheme based on quadratic residues. In: IMA Int. Conf., pp. 360-363 (2001)
11. Dodis, Y., Fazio, N.: Public Key Broadcast Encryption for Stateless Receivers. In: Feigenbaum, J. (ed.) DRM 2002. LNCS, vol. 2696, pp. 61C80. Springer, Heidelberg (2003)

12. Delerabl'ee, C.: Identity-Based Broadcast Encryption with Constant Size Ciphertexts and Private Keys. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 200-215. Springer, Heidelberg (2007)
13. Fiat, A., Naor, M.: Broadcast Encryption. In: Stinson, D.R. (ed.) CRYPTO 1993. LNCS, vol. 773, pp. 480-491. Springer, Heidelberg (1994)
14. Gentry, C.: Practical Identity-Based Encryption Without Random Oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 445-464. Springer, Heidelberg (2006)
15. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: STOC, pp. 197-206 (2008)
16. Gentry, C., Waters, B.: Adaptive Security in Broadcast Encryption Systems (with Short Ciphertexts).In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 171-188. Springer, Heidelberg (2009)
17. Gentry, C., Silverberg, A.: Hierarchical ID-Based Cryptography. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 548C566. Springer, Heidelberg (2002)
18. Kawachi, A., Tanaka, K., Xagawa, K.: Multi-bit cryptosystems based on lattice problems. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 315-329. Springer, Heidelberg (2007)
19. Micciancio, D., Regev, O.:Worst-case to average-case reductions based on Gaussian measures. SIAM J. Comput. 37(1), 267-302 (2007); Preliminary version in FOCS 2004
20. Micciancio, D., Regev, O.: Lattice-based cryptography. In: Post Quantum Cryptography, pp. 147-191. Springer, Heidelberg (2009)
21. Micciancio, D., Goldwasser,S.: Complexity of Lattice Problems: a cryptographic perspective.:The Kluwer International Series in Engineering and Computer Science. Kluwer Academic Publishers,vol.671 Boston, Massachusetts, 2002.
22. Peikert, C.: Bonsai Trees:Arboriculture in Lattice-Based Cryptography. In manuscript, 2009.
23. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: STOC, pp. 84-93 (2005)
24. Shamir, A.: Identity-Based Cryptosystems and Signature Schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47-53. Springer, Heidelberg (1985)
25. Sakai, R., Furukawa, J.: Identity-Based Broadcast Encryption. Eprint 2007/217
26. Wagner, D.: A generalized birthday problem. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 288-303. Springer, Heidelberg (2002)