Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/090439

Forward-Secure Identity-based Broadcast Encryption Scheme from Lattice

Xinwen Zhang[1,2], *Shangping Wang*[3,*] *and Wenpeng Zhang*[2]

[1] School of Science, Xi'an University of Posts & Telecommunications, Xi'an, 710121, P. R. China
[2] Department of Mathematics, Northwest University, Xi'an, 710127, P. R. China
[3] Shaanxi Key Laboratory for Network Computing and Security Technolog, Xi'an University of technology, Xi'an, 710054, P. R. China

Received: 9 Nov. 2014, Revised: 9 Feb. 2015, Accepted: 10 Feb. 2015
Published online: 1 Jul. 2015

Abstract: Motivated by an identity-based broadcast encryption scheme from lattice[1] and a forward-secure identity-based encryption scheme[2], we propose a forward-secure identity-based broadcast encryption scheme from lattice by adding the forward-security mechanism on broadcast encryption scheme. Our scheme satisfies the security requirements of both the broadcast encryption scheme and forward-security scheme, that is, it is forward-secure for the secret keys used previously, and we prove that it is semantic secure based on LWE (Learning With Error)assumption[3] in the random oracle model. In addition, our construction is believed to be secure against quantum computer.

Keywords: Lattice; Identity-based broadcast encryption; Forward security; Learning with error(LWE)
Mathematics Subject Classification (2010) 68P25; 81P94; 94A60

1 Introduction

A broadcast encryption (BE) scheme is a cryptosystem that allows a sender to encrypt messages and securely distribute them to a group of users who have been authorized over a broadcast channel which is insecure. Only the chosen users can use their private keys to decrypt messages in such a system. BE can be used in pay-TV systems, DVD/CD content protection, and distribution of copyrighted material, etc. Since the first BE scheme is constructed by Fiat and Naor in 1994[4], many BE schemes have been proposed[5,6,7]. Key Encapsulation Mechanism (KEM) encryption pattern is usually used in BE schemes where broadcast ciphertext only encrypts a symmetric key used to encrypt the broadcast contents. We will also use the KEM method in our construction.

In identity-based cryptographic constructions [8,9,10,11], the public key of a user can be derived from his or her identity information, such as an email address or telephone number, while the corresponding private key is computed by a trusted authority called Key Generator Center (KGC). The conception of identity-based broadcast encryption (IBBE) was introduced by Ryuichi Sakai and Jun Furukawa[12] which incorporated identity-based cryptography into the broadcast setting. This implies that the size of the public key does not depend on the number of potential receivers, and the sender is able to transmit ciphertexts to any set of receivers who have never engaged in any setup procedure with the system. A lot of IBBE schemes have been proposed in recent years[13,14,15].

The conception of forward security was firstly proposed by C.G. Günther[16] in the key exchange protocol. It is crucial for cryptography to protect secret keys. The goal of the forward security is to protect security against the risk of exposure of keys even if the current secret key is exposed. The conception of non-interactive forward security was proposed by Anderson[17] and later formalized by Bellare and Miner[18] in 1999. The device divides the lifetime of the system into N time intervals labled as $0,1,\cdots,N$-1. The secret key on the 0-*th* time interval is stored as SK_0 and others are stored in turn. The secret key SK_{i-1} stored at interval i-1 has been deleted as soon as the device computes the secret key SK_i at interval i using the update algorithm$(SK_{i-1},\cdots)$ on a short basis. An open problem is

* Corresponding author e-mail: spwang@mail.xaut.edu.cn

that whether the construction of forward secure encryption scheme can be used in public key setting. R. Canetti, S. Halevi, and J. Katz solved the problem in 2003[19]. They constructed Binary Tree Encryption (BTE) based on the bilinear Diffi-Hellman assumption which can be easily converted into forward secure PKE scheme. Chris Peikert constructed a lattice based BTE scheme[20] which can be converted into lattice based forward PKE scheme using the technique in[19].

Our contribution. In this paper, we construct a forward-secure identity-based broadcast encryption scheme from lattices. Our scheme incorporates the forward-security mechanism into broadcast encryption scheme from lattice. It offers a higher security, at the same time it can satisfy two types of security requirements.

Firstly, our scheme offers forward-security which guarantee the security of the secret keys used previously even if the current secret key is exposed. Secondly, it can be proved semantic secure for LWE problem. In addition, our construction is believed to be secure against quantum computer.

The master public key of the KGC is a matrix $\mathbf{A}_0 \in \mathbb{Z}_q^{n\times m}$ and the corresponding secret key is a short basis $\mathbf{B}_0 \in \Lambda^{\perp}(\mathbf{A}_0)(\in \mathbb{Z}_q^{m\times m})$. We use the lattice delegation technique[21] to calculate the secret key of every receiver. And we guarantee the forward security by using the new basis delegation technique[22] which can update the secret key on progressive time intervals.

As far as we know, our construction is the *first* forward-secure identity-based broadcast encryption scheme from lattice.

Paper Outline. Our paper is organized as follows. In Section 2, we introduce basic definitions and the hard problem from lattices which insure the security. In Section 3, we describe the model of our construction and the critical algorithms we used in the paper. In Section 4, we construct a concrete forward-secure identity-based broadcast encryption scheme from lattices and prove its security. In Section 5, we extend our construction to a scheme which can encrypt multiple keys simultaneously. In Section 6, we compare the efficiency of our construction and some IBBE schemes. In Section 7, we give a conclusion.

2 Preliminaries

2.1 Notation

For a positive integer N, we define $[N]=\{1,\cdots,N\}$. For a matrix $\mathbf{A}\in\mathbb{Z}_q^{n\times m}$, let $\mathbf{A}=\{\mathbf{a}_1, \mathbf{a}_2, \cdots, \mathbf{a}_m\}$, where $\mathbf{a}_i$ denotes the *i-th* column of $\mathbf{A}$. $\|\mathbf{a}_i\|$ denotes the Euclidean norm of $\mathbf{a}_i$, $\|\mathbf{A}\|$ denotes the Euclidean norm of the longest vector in $\mathbf{A}$, i.e. $\|\mathbf{A}\|=\max_{i\in[m]}\|\mathbf{a}_i\|$.

We assert $negl(n)$ is a negligible function in n if it is smaller than the inverse of any polynomial function in n for sufficiently large n. And $\omega(f(n))$ denotes the set of functions growing faster than $cf(n)$ for any $c>0$.

For a lattice basis $\mathbf{B}=\{\mathbf{b}_1,\cdots,\mathbf{b}_n\}$, $\tilde{\mathbf{B}}$ denotes its Gram-Schmidt orthogonalization. It defined as: $\tilde{\mathbf{b}}_1=\mathbf{b}_1$, $\tilde{\mathbf{b}}_i$ is the component of $\mathbf{b}_i$ orthogonal to span$(\mathbf{b}_1,\cdots,\mathbf{b}_{i-1})$ where $i=2,\cdots,n$.

2.2 Integer Lattices

Definition 1[23]. Let $\mathbf{B}=\{\mathbf{b}_1,\cdots,\mathbf{b}_n\}\in R^m$ consists of n linearly independent vectors. A m-dimensional lattice Λ generated by $\mathbf{B}$ is a discrete additive subgroup of R^m and defined as

$$\begin{aligned}\Lambda &= L(\mathbf{B}) = L(\mathbf{b}_1,\cdots,\mathbf{b}_n)\\ &= \{\mathbf{Bc} : \mathbf{c}\in\mathbb{Z}^n\}\\ &= \{\sum_{i=1}^{n} c_i\mathbf{b}_i : c_i\in\mathbb{Z}\}\end{aligned}$$

Here $\mathbf{B}$ is called a basis of the lattice $\Lambda=L(\mathbf{B})$. In this paper, we are mostly concerned on the full-rank integer lattices, i.e. $\Lambda\subseteq\mathbb{Z}^m$ with $n=m$.

2.3 Modular Lattices

Modular Lattice is a special form of integer lattices which is invariant under shifts by a primitive integer modulus q in each of the coordinates.

Definition 2[23]. Given a matrix $\mathbf{A}\in\mathbb{Z}_q^{n\times m}$ and a vector $\mathbf{u}\in\mathbb{Z}_q^n$, we define:

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

It is a lattice contains of all integer vectors which are orthogonal (mod q) to the rows of $\mathbf{A}$ and then

$$\Lambda_q^{\mathbf{u}}(\mathbf{A}) = \{\mathbf{e}\in\mathbb{Z}^m : \mathbf{Ae} = \mathbf{u} \bmod q\}$$

is a coset of $\Lambda_q^{\perp}(\mathbf{A})$ such that $\Lambda_q^{\mathbf{u}}(\mathbf{A}) = \mathbf{t}+\Lambda_q^{\perp}(\mathbf{A}) \bmod q$ for a fixed vector $\mathbf{u}\in\mathbb{Z}_q^n$, where $\mathbf{t}$ is an arbitrary solution (over $\mathbb{Z}$) of the equation $\mathbf{At}=\mathbf{u} \bmod q$.

2.4 Discrete Gaussians on Lattices

We firstly give the definition of Gaussian function used in lattice based cryptographic constructions.

Definition 3[23]. For any vector $\mathbf{c}\in R^m$ and any positive $\sigma \in \mathbb{R} > 0$, the Gaussian function centered at $\mathbf{c}$ with deviation parameter σ is defined as

$$\forall x \in \mathbb{Z}^m,\ \rho_{\sigma,\mathbf{c}}(x) = \exp(-\pi\|x-\mathbf{c}\|^2/\sigma^2)$$

and

$$\rho_{\sigma,\mathbf{c}}(\Lambda) = \sum_{x\in\Lambda}\rho_{\sigma,\mathbf{c}}(x)$$

Definition 4[23]. The discrete Gaussian distribution over m-dimensional lattice Λ is defined as

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

The distribution $D_{\Lambda,\sigma,\mathbf{c}}(x)$ is mostly defined over the lattice $\Lambda_q^{\perp}(\mathbf{A})$ for a matrix $\mathbf{A}\in\mathbb{Z}_q^{n\times m}$ or over the coset of $\Lambda_q^{\perp}(\mathbf{A})$ as $\Lambda_q^{\mathbf{u}}(\mathbf{A})$. Then

$$\forall x \in \Lambda, D_{\Lambda_q^{\mathbf{u}}(\mathbf{A}),\sigma,\mathbf{c}}(x) = \frac{\rho_{\sigma,\mathbf{c}}(x)}{\rho_{\sigma,\mathbf{c}}(\Lambda_q^{\mathbf{u}}(\mathbf{A}))}$$

2.5 Hard Problems for Lattices

Learning With Errors Assumption. To describe the learning with error (LWE) hardness assumption, we firstly introduce the following probability distribution. For a real $\alpha=\alpha(n)\in\{0,1\}$, $\alpha q > 2\sqrt{m}$, $T=R/Z$ denotes the group of reals on [0,1), we define Ψ_α as the distribution over T of a normal variable with mean 0 and standard deviation $\alpha/\sqrt{2\pi}$ then reduced modulo 1. And $\overline{\Psi}_\alpha$ denotes the distribution over qT of a normal variable with mean 0 and standard deviation $\alpha q/\sqrt{2\pi}$ then reduced modulo q.

Given a Gaussian error distributions χ and a vector $\mathbf{s} \in \mathbb{Z}_q^n$, denotes the distribution of the variable $(\mathbf{a},\mathbf{a}^\top\mathbf{s}+x)$ over $\mathbb{Z}_q^n\times\mathbb{Z}_q$, where $\mathbf{a}\in\mathbb{Z}_q^n$ is uniform and the scalar $x\in\mathbb{Z}_q$ is sampled from χ.

Definition 5[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 $\mathrm{LWE}_{q,\chi}$ is to distinguish (with non-negligible probability) between the distribution $A_{q,\chi}$ 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).

The next **Lemma** will be used to prove the correctness of our forward-secure identity-based broadcast encryption scheme from lattices.

Lemma 2.1(**Lemma 3.9** in [26]): Let $\mathbf{e}$ be some vector in $\mathbb{Z}^m$ and let $\mathbf{y}\leftarrow\overline{\Psi}_\alpha^m$. Then the quantity $|\langle\mathbf{e},\mathbf{y}\rangle|$ when treated as an integer in $(-q/2,q/2]$ satisfies

$$|\langle\mathbf{e},\mathbf{y}\rangle| \le \|\mathbf{e}\|q\alpha\cdot\omega(\sqrt{\log m}) + \|\mathbf{e}\|\sqrt{m}/2$$

3 Model of Our Scheme and Requirements of Security

3.1 Trapdoor and Basis Delegation Functions

In our paper, we need make use of the following algorithm:
——**TrapGen**$(1^n,1^m,q)$(Lemma 3.1 in [21])-generating a function with trapdoor: For integers n, q, m with $q\ge2$ and $m\ge5n\lg q$, **TrapGen**(1^n) outputs a pair (**A**,**B**) such that $\mathbf{A}\in\mathbb{Z}_q^{n\times m}$ is statistically close to uniform on $\mathbb{Z}_q^{n\times m}$ and **B** is a short basis of $\Lambda_q^{\perp}(\mathbf{A})$ such that $\|\tilde{\mathbf{B}}\|\le m\cdot\omega(\sqrt{\log m})$ with all but $n^{\omega(1)}$ probability.

——**SampleDom**(1^n)(Definition in [23])-domain sampling with uniform output: **SampleDom**(1^n) samples x (possibly non-uniform) from some distribution $D_{Z^m,r}$.

——**SampleBasis**(**A**, $\mathbf{B}_S$, S, L) (Theorem 3.3 in [21]): For integers n, q, m, k with $q\ge2$ and $m\ge5n\lg q$, on input of $\mathbf{A}=(\mathbf{A}_1,\mathbf{A}_2,\cdots,\mathbf{A}_k)\in\mathbb{Z}_q^{n\times km}$, a set $S\subseteq[k]$, a basis $\mathbf{B}_S$ of $\Lambda_q^{\perp}(\mathbf{A}_S)$, and an integer $L\ge\|\tilde{\mathbf{B}}_S\|\cdot\sqrt{km}\cdot\omega(\sqrt{\log km})$, the PPT algorithm **SampleBasis**(**A**, $\mathbf{B}_S$, S, L) outputs **B** as a basis of $\Lambda_q^{\perp}(\mathbf{A})$ such that $\|\tilde{\mathbf{B}}\|\le L$ with an overwhelming probability.

——**GenSamplePre**(**A**, $\mathbf{A}_S$, $\mathbf{B}_S$, **y**, r)(Theorem 3.4 in [21])-In this paper we use algorithm **GenSamplePre**(**A**, $\mathbf{A}_S$, $\mathbf{B}_S$, **y**, r) to extend the basis of lattice. Given positive the integers n, q, m, k with $q\ge2$ and $m\ge2n\lg q$, on input of $\mathbf{A}=(\mathbf{A}_1,\mathbf{A}_2,\cdots,\mathbf{A}_k)\in\mathbb{Z}_q^{n\times km}$, a set $S\subseteq[k]$, a basis $\mathbf{B}_S$ of $\Lambda_q^{\perp}(\mathbf{A}_S)$, a vector $\mathbf{y}\in\mathbb{Z}_q^n$ and an integer $r\ge\|\tilde{B_S}\|\cdot\omega(\sqrt{\log km})$, the PPT algorithm **GenSamplePre**(**A**, $\mathbf{A}_S$, $\mathbf{B}_S$, **y**, r) outputs a vector **e** such that the conditional distribution of **e** is within the negligible statistical distance of $D_{\Lambda_q^{\mathbf{y}}(\mathbf{A}),r}$ for an overwhelming fraction of $\mathbf{A}\in\mathbb{Z}_q^{n\times km}$.

——**ToBasis**(**B**,**S**)(Lemma 1 in [25])-Given an arbitrary basis **B** of an m-dimensional lattice Λ and a full rank set $\mathbf{S}\subset\Lambda$, a deterministic polynomial time algorithm **ToBasis**(**B**,**S**) returns a basis **T** of Λ such that

$$\|\tilde{\mathbf{T}}\| \le \|\tilde{\mathbf{S}}\|$$

——**RandBasis**(**S**, σ)[20]-Given a basis **S** of an m-dimensional lattice Λ and a parameter

$\sigma \geq \|\tilde{\mathbf{S}}\| \cdot \omega(\sqrt{\log m})$, the randomized algorithm **RandBasis**(**S**,σ) outputs a new basis $\mathbf{S}'$ of Λ, generated as follows.

1. For i=1,2,$\cdots$,m:

(a)Choose $\mathbf{v} \leftarrow$**SampleDom**(**S**, σ). If **v** is linearly independent of $\{\mathbf{v}_1,\cdots,\mathbf{v}_{i-1}\}$, then let $\mathbf{v}_i$=**v** and go to the next value of i; otherwise, repeat this step.

2. Output $\mathbf{S}'$=**ToBasis**(**V**, **S**) for $\mathbf{V}=\{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_m\}$.

——**NewBasisDel**(**A**, **R**, $\mathbf{T_A}$, σ)([2])-it works as follows.

1. Run **TrapGen**($1^n, 1^m, q$) to output $\mathbf{T_A} \in \Lambda_q^{\perp}(\mathbf{A})$, and calculate $\mathbf{T}_\mathbf{B}' = \mathbf{R}\mathbf{T_A}$.

2. Run **ToBasis**($\mathbf{T}_\mathbf{B}'$, **S**) to convert the short basis $\mathbf{T}_\mathbf{B}'$ into a shorter basis $\mathbf{T}_\mathbf{B}''$.

3. Run **RandBasis**($\mathbf{T}_\mathbf{B}''$, σ) to randomize $\mathbf{T}_\mathbf{B}''$ to a new basis $\mathbf{T_B}$.

3.2 The model of a Forward-Secure Identity-Based Broadcast Encryption

We define the forward-secure identity based broadcast encryption scheme consists of the following five phase.

Setup( ): On input a security parameter n, the algorithm outputs the master public key *mpk* and the master secret key *msk*.

Extract( ): On input the master public key *mpk*, the master secret key *msk*, and an identity $ID_i\|0 \in \{0,1\}^*$ at the initial condition of the valid user i, the algorithm outputs the corresponding private key.

Update( ): On input the master public key *mpk* and the secret key $\mathbf{B}_{ID_i\|j}$ of the user i at the j-*th* time period, the algorithm outputs the secret key $\mathbf{B}_{ID_i\|j+1}$ at the $j+1$-*th* time period.

Encrypt( ): On input a set of broadcast message receivers S and a message encryption key K, the algorithm outputs the header **Hdr**.

Decrypt( ): On input a set of broadcast message receivers S, a header **Hdr**, the private key $\mathbf{B}_{ID_i\|j}$ of the user i and the public key $\mathbf{A}_{ID_i\|j}$ of all the users, the algorithm outputs the message encryption key K which is then used to decrypt ciphertext C_M and obtain the broadcast message M.

3.3 The Requirements of Security

There are two types of security requirements for our forward-secure identity-based broadcast encryption schemes.

1. As For a forward-secure encryption scheme, we require that an attacker would not obtain the secret key previously used even if it gets the current secret key.

2. As a broadcast encryption scheme, we require that the outsiders who are not in the group of receivers and only have public information would by no means infer information about the broadcast message even if all users that are not in S collude, i.e. our scheme is of semantic security.

4 Our Construction and Security Proof

4.1 Our forward-secure IBBE scheme

Let k, l, m, n, q be positive integers with $q > \frac{5}{2}\sqrt{km}[\omega(\sqrt{\log km})+1]\cdot(1+r\sqrt{km})$, $q\alpha > \frac{\sqrt{km}}{2}$ and $m \geq 2n\lg q$. Let $k \leq l$, where l is the maximum number of the receivers. The whole time period of the system is divided into N time intervals labeled as 0,1,$\cdots$,N-1.

Setup:

1. Choose a hash function $H : \{0,1\}^* \rightarrow \{0,1\}^{m\times m}$. H will be viewed as a random oracle in the security analysis.

2. Choose $\mathbf{v} \in \mathbb{Z}_q^n$ uniformly at random.

3. Run the trapdoor generation algorithm **TrapGen**(1^n) to generate a pair ($\mathbf{A}_0$,$\mathbf{B}_0$) such that $\mathbf{A}_0 \in \mathbb{Z}_q^{n\times m}$ is statistically close to uniform on $\mathbb{Z}_q^{n\times m}$ and $\mathbf{B}_0 \in \mathbb{Z}_q^{m\times m}$ is a short basis of $\Lambda^{\perp}(\mathbf{A}_0)$ such that $\|\mathbf{B}_0\| \leq L$ where $L \geq m\cdot\omega(\sqrt{\log m})$.

4. Output the master public key mpk=($\mathbf{A}_0$,**v**), and the master secret key msk=$\mathbf{B}_0$.

Extract(msk, $ID_{i\|0}$):

1. For an arbitrary $ID_i \in \{0,1\}^*$, define the associated matrix $\mathbf{A}_{ID_i\|0}$ as

$$\mathbf{A}_{ID_i\|0} = \mathbf{A}_0(\mathbf{R}_{ID_i\|0})^{-1}, \mathbf{A}_{ID_i\|0} \in \mathbb{Z}_q^{n\times m}$$

where $\mathbf{R}_{ID_i\|0} = H(ID_i\|0)$ such that $\mathbf{R}_{ID_i\|0} \in \mathbb{Z}_q^{m\times m}$.

2. To construct users secret key, run the basis delegation algorithm **SampleBasis**($\mathbf{A}_{ID_i\|0}$, $\mathbf{B}_0$, S, L') and generate $\mathbf{B}_{ID_i\|0}$ such that $\|\mathbf{B}_{ID_i\|0}\| \leq L'$ where $L' \geq \sqrt{km^3}\cdot\omega(\log m)$. The secret key for ID_i on the 0-*th* time period is $\mathbf{B}_{ID_i\|0}$.

Update(mpk, $\mathbf{B}_{ID_i\|j}$, $ID_i\|j$):

Given the secret key $\mathbf{B}_{ID_i\|j}$ at the j-*th* time period, the user i can find the secret key $\mathbf{B}_{ID_i\|j+1}$ at the j+1-*th* time period as follows:

1. Let

$$\begin{aligned}\mathbf{R}_{ID_i\|j+1} &= H\ (ID_i\|\mathbf{B}_{ID_i\|j}\|j+1)\mathbf{R}_{ID_i\|j}\\ &= H\ (ID_i\|\mathbf{B}_{ID_i\|j}\|j+1)\\ &\quad H\ (ID_i\|\mathbf{B}_{ID_i\|j-1}\|j)\\ &\quad \cdots H(ID_i\|0)\end{aligned}$$

where $\mathbf{R}_{ID_i\|j+1} \in \mathbb{Z}_q^{m\times m}$ and

$$\begin{aligned}\mathbf{A}_{ID_i\|j+1} &= \mathbf{A}_0(\mathbf{R}_{ID_i\|j+1})^{-1}\\ &= \mathbf{A}_{ID_i\|j}H^{-1}(ID_i\|\mathbf{B}_{ID_i\|j}\|j+1)\end{aligned}$$

such that $\mathbf{A}_{ID_i\|j+1} \in \mathbb{Z}_q^{n\times m}$.

2. Run the basis delegation algorithm **NewBasisDel** to compute the secret key $\mathbf{B}_{ID_i\|j+1} \leftarrow$ **NewBasisDel** ($\mathbf{A}_{ID_i\|j+1}$, $\mathbf{R}_{ID_i\|j+1}$, $\mathbf{B}_{ID_i\|j}$, σ) where $\sigma \geq m\cdot\omega(\log m)$.

Public the $\mathbf{A}_{ID_i\|j}, j = 1,2,\cdots$. The algorithm **Update**(mpk, $\mathbf{B}_{ID_i\|j}$, $ID_i\|j$) can insure the forward-security of our IBBE scheme.

Encrypt(mpk, S, b):

Assume that $S = \{ID_1, ID_2, \cdots, ID_k\}$ is the set of broadcast message receivers where $k \leq l$. To encrypt a bit $b \in \{0,1\}$, the broadcaster does the following.

1. Compute $\mathbf{A}_{S\|j} = [\mathbf{A}_{ID_1\|j}\|\mathbf{A}_{ID_2\|j}\|\cdots\|\mathbf{A}_{ID_k\|j}] \in \mathbb{Z}_q^{n\times km}$. Define a label lab_S that contains information about how $\mathbf{A}_{S\|j}$ is associated with the sequence of the receivers $\{ID_1, ID_2, \cdots, ID_k\}$ at the *j-th* time period.

2. Choose $\mathbf{u} \in \mathbb{Z}_q^n$ uniformly at random.

3. Compute $\mathbf{p} = \mathbf{A}_{S\|j}^\top\mathbf{u} + \mathbf{e} \in \mathbb{Z}_q^{km}$, where $\mathbf{e} \leftarrow \chi^{km}$ and $\chi = \Psi_\alpha$.

4. Compute $c = \mathbf{v}^\top\mathbf{u} + \bar{e} + b\lfloor\frac{q}{2}\rfloor \in \mathbb{Z}_q$, where $\bar{e} \leftarrow \chi$ and $\chi = \Psi_\alpha$.

Output **Hdr**$= \langle \mathbf{p}, c, lab_S\rangle$.

Decrypt(**Hdr**, $\mathbf{B}_{ID_i\|j}$):

To decrypt $\mathbf{p}$ and c, the user whose identity is ID_i does the following

1. Run the generalized preimage sampling algorithm and generate

$$\mathbf{y} \leftarrow \textbf{GenSamplePre}(\mathbf{A}_{S\|j}, \mathbf{A}_{ID_i\|j}, \mathbf{B}_{ID_i\|j}, \mathbf{v}, r) \in \mathbb{Z}_q^{km}$$

Note that $\mathbf{y}$ is distributed according to $D_{\Lambda_q^{\mathbf{v}}\mathbf{A}_{S\|j},r}$ where $r \geq m\cdot\omega(\log m)$.

2. Compute $b' = c - \mathbf{y}^\top\mathbf{p} \in \mathbb{Z}_q$. Let $b = 0$ if b' is closer to 0 than to $\lfloor\frac{q}{2}\rfloor \in \mathbb{Z}_q$; otherwise $b = 1$.

4.2 Correctness

Theorem 1: Our forward-secure identity-based broadcast encryption scheme from lattice is correct if the preimage sampling algorithm **GenSamplePre** is correct.

Proof: for the preimage sampling algorithm **GenSamplePre**($\mathbf{A}_{S\|j}, \mathbf{A}_{ID_i\|j}, \mathbf{B}_{ID_i\|j}, \mathbf{v}, r$), we have

$$\begin{aligned}&\mathbf{A}_{S\|j}\mathbf{y} = \mathbf{v}\\ &\mathbf{y}^\top\mathbf{p} = \mathbf{y}^\top(\mathbf{A}_{S\|j}^\top\mathbf{u} + \mathbf{e})\\ &\quad = (\mathbf{A}_{S\|j}\mathbf{y})^\top\mathbf{u} + \mathbf{y}^\top\mathbf{e}\\ &\quad = \mathbf{v}^\top\mathbf{u} + \mathbf{y}^\top\mathbf{e}\end{aligned}$$

Then

$$b' = c - \mathbf{y}^\top\mathbf{p} = \bar{e} - \mathbf{y}^\top\mathbf{e} + b\lfloor\frac{q}{2}\rfloor$$

According **Lemma 2.1**,

$$\begin{aligned}\|\bar{e} - \mathbf{y}^\top\mathbf{e}\| &\leq \|\bar{e}\| + \|\mathbf{y}^\top\mathbf{e}\|\\ &\leq [q\alpha\cdot\omega(\sqrt{\log m}) + \frac{1}{2}]\\ &\quad + \|\mathbf{y}\|[q\alpha\cdot\omega(\sqrt{\log km}) + \frac{\sqrt{km}}{2}]\end{aligned}$$

because $\mathbf{y} \leftarrow \overline{\Psi}_\alpha^{km}$, then $\|\mathbf{y}\| \leq r\sqrt{km}$ such that $r \geq km\cdot\omega(\log km)$

Then the above formula satisfies

$$\begin{aligned}\|\bar{e} - \mathbf{y}^\top\mathbf{e}\| &\leq [q\alpha\cdot\omega(\sqrt{\log m}) + \frac{1}{2}]\\ &\quad + r\sqrt{km}[q\alpha\cdot\omega(\sqrt{\log km}) + \frac{\sqrt{km}}{2}]\\ &\leq [q\alpha\cdot\omega(\sqrt{\log km}) + \frac{\sqrt{km}}{2}]\\ &\quad + r\sqrt{km}[q\alpha\cdot\omega(\sqrt{\log km}) + \frac{\sqrt{km}}{2}]\\ &= q\alpha[\omega(\sqrt{\log km}) + 1](1 + r\sqrt{km})\end{aligned}$$

Because $q > \frac{5}{2}\sqrt{km}[\omega(\sqrt{\log km}) + 1]\cdot(1 + r\sqrt{km})$ and $q\alpha > \frac{\sqrt{km}}{2}$, then $\|\bar{e} - \mathbf{y}^\top\mathbf{e}\| \leq \frac{q}{5}$. So our forward-secure identity-based broadcast encryption scheme is correct.

4.3 Security Proof

Theorem 2: Our forward-secure identity-based broadcast encryption scheme from lattice is IND-sID-CPA semantic secure in random oracle model assuming the LWE is hard or

$$Adv_{LWE}(n) = \frac{1}{N}Adv_{fs-IBBE}(n)$$

here hash function H is modeled as random oracle.

Proof: we now prove the semantic security of our forward-secure identity-based broadcast encryption scheme in the random oracle model. We will prove that if there exists a PPT adversary $\mathscr{A}$ breaking our fs-IBBE scheme with non-negligible advantage $Adv_{fs-IBBE}(n)$, then there must exist a PPT adversary $\mathscr{B}$ can solve the LWE hard problem with non-negligible advantage $Adv_{LWE}(n)$ by simulating views of $\mathscr{A}$. We assume that

1) For each $j \in [N]$, $\mathscr{A}$ always makes q_H (polynomial number) different H-queries on interval j.

2) Whenever $\mathscr{A}$ makes a H-queries on interval j, we assume that $\mathscr{A}$ has queried relevant H-queries on interval $t < j$.

3) Whenever $\mathscr{A}$ issues a users secret key query, we assume that $\mathscr{A}$ has made all relevant H-queries beforehand.

Adversary $\mathscr{A}$ declares that it intends to attack an identity $ID^* \in S$. Adversary $\mathscr{B}$ (works as challenger for adversary $\mathscr{A}'$ s view) firstly picks $j^* \in \{0,1,\cdots,N-1\}$.

Here j^* is a guess for the j of challenge(j,b) query and the accuracy of the guess is $\frac{1}{N}$. Now $\mathscr{B}$ obtains $km+1$ LWE samples which get parsed as $(\mathbf{a}_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ $(0 \le i \le km)$.

Setup: Adversary $\mathscr{B}$ runs the trapdoor algorithm **TrapGen**( ) to generate $\mathbf{A}_0 \in \mathbb{Z}_q^{n\times m}$ with corresponding trapdoor $\mathbf{B}_0 \in \mathbb{Z}_q^{m\times m}$. Then $\mathscr{B}$ sets master public key to be $mpk = \mathbf{A}_0$ and master secret key to be trapdoor $\mathbf{B}_0$.

Query: Next adversary $\mathscr{B}$ interacts with $\mathscr{A}$ as follows:

H-Queries:

1) $\mathscr{A}'$s hash query on $ID^*\|j^*$: Adversary $\mathscr{B}$ returns $\mathbf{A}_{j^*}$ is m-samples (a matrix which is composed of n vectors $\mathbf{a}_i$ where $(1 \le i \le m)$) from LWE oracle, i.e. $\mathbf{A}_{j^*} = (\mathbf{a}_1, \mathbf{a}_2, \cdots, \mathbf{a}_m) \in \mathbb{Z}_q^{n\times m}$.

2) $\mathscr{A}'$s hash query on any $ID_{i\|0}$: Adversary $\mathscr{B}$ will choose a low norm matrix $\mathbf{R}_{ID_{i\|0}} \in \mathbb{Z}_q^{m\times m}$ uniformly and calculate matrix $\mathbf{A}_{ID_{i\|0}} = \mathbf{A}_0(\mathbf{R}_{ID_i\|0})^{-1} \in \mathbb{Z}_q^{n\times m}$. Then $\mathscr{B}$ runs the algorithm **SampleBasis**( ) to generate basis $\mathbf{B}_{ID_{i\|0}}$ of $\Lambda_q^{\perp}(\mathbf{A}_{ID_{i\|0}})$. Adversary $\mathscr{B}$ returns $\mathbf{A}_{ID_{i\|0}}$ as an answer to hash query and stores the tuple $(ID_{i\|0}, \mathbf{A}_{ID_{i\|0}}, \mathbf{B}_{ID_{i\|0}})$ in list H.

3) $\mathscr{A}'$s hash query on any $ID_{i\|j}$ $(ID_i \ne ID^*)$ where $j > 0$: Since we have assumed above that $\mathscr{A}$ would have made hash query on $ID_{i\|j-1}$, adversary $\mathscr{B}$ will choose low norm matrix $\mathbf{R}_{ID_{i\|0}} \in \mathbb{Z}_q^{m\times m}$ uniformly and run algorithm **NewBasisDel**$(\mathbf{A}_{ID_i\|j-1}, \mathbf{R}_{ID_i\|j}, \mathbf{B}_{ID_i\|j-1}, \sigma)$ to generate matrix $\mathbf{A}_{ID_i\|j}$ and short basis $\mathbf{B}_{ID_i\|j}$ of $\Lambda_q^{\perp}(\mathbf{A}_{ID_{i\|j}})$. Adversary $\mathscr{B}$ returns the matrix $\mathbf{A}_{ID_i\|j}$ as an answer to hash query and stores the tuple $(ID_{i\|j}, \mathbf{A}_{ID_{i\|j}}, \mathbf{B}_{ID_{i\|j}})$ in list H.

4) $\mathscr{A}'$s hash query on any $ID^*\|j$ where $0 < j < j^*$: Adversary $\mathscr{B}$ will choose a low matrix $\mathbf{R}_{ID^*\|j} \in \mathbb{Z}_q^{m\times m}$ uniformly and returns $\mathbf{A}_{ID^*\|j} = \mathbf{A}_0(\mathbf{R}_{ID^*\|j})^{-1} \in \mathbb{Z}_q^{n\times m}$ to adversary $\mathscr{A}$.

5) $\mathscr{A}'$s hash query on $ID^*\|j^*+1$: Adversary $\mathscr{B}$ runs the trapdoor algorithm **TrapGen**( ) to generate $\mathbf{A}_{ID^*\|j^*+1} \in \mathbb{Z}_q^{n\times m}$ with corresponding trapdoor $\mathbf{B}_{ID^*\|j^*+1} \in \mathbb{Z}_q^{m\times m}$ and returns matrix $\mathbf{A}_{ID^*\|j^*+1}$ and stores the tuple $(ID^*\|j^*+1, \mathbf{A}_{ID^*\|j^*+1}, \mathbf{B}_{ID^*\|j^*+1})$ in list H.

6) $\mathscr{A}'$s hash query on any $ID^*\|j$ where $j > j^*+1$: Since we have assumed that $\mathscr{A}$ would have made hash query on $ID^*\|j-1$, Adversary $\mathscr{B}$ will choose a low matrix $\mathbf{R}_{ID^*\|j} \in \mathbb{Z}_q^{m\times m}$ uniformly and run algorithm **NewBasisDel**$(\mathbf{A}_{ID^*\|j^*-1}, \mathbf{R}_{ID^*\|j}, \mathbf{B}_{ID^*\|j^*-1}, \sigma)$ to generate matrix $\mathbf{A}_{ID^*\|j^*}$ and short basis $\mathbf{B}_{ID^*\|j^*}$ of $\Lambda_q^{\perp}(\mathbf{A}_{ID^*\|j})$. Adversary $\mathscr{B}$ returns $\mathbf{A}_{ID^*\|j^*}$ as an answer to hash query and stores the tuple $(ID^*\|j, \mathbf{A}_{ID^*\|j}, \mathbf{B}_{ID^*\|j})$ in list H.

Extraction Queries:

When adversary $\mathscr{A}$ asks for the secret key for any identity ID_i where $ID_i \ne ID^*$, as we have assumed above that adversary $\mathscr{A}$ has made all relevant hash query for it before the extraction query, adversary $\mathscr{B}$ looks up the list H and returns the corresponding $\mathbf{B}_{ID_i\|j}$ to adversary $\mathscr{A}$.

Attack:

1) challenge(j,b): When adversary $\mathscr{A}$ initiates query of challenge(j,b), the adversary $\mathscr{B}$ picks a random bit $r \in \{0,1\}$ and a random ciphertext C. If $r = 0$ it returns $(\mathbf{p}^*, c^*)$ as challenge ciphertext, otherwise it returns random ciphertext C.

2) Breakin(t): When adversary $\mathscr{A}$ queries breakin(t), if $j < t \le j^*$ adversary B outputs a random bit and game aborts (Now $\mathscr{B}$ can not answer extraction queries for the secret keys on interval $t \le j^*$ are not stored on list H). Otherwise adversary $\mathscr{B}$ looks up the list H and returns the corresponding $\mathbf{B}_{ID_i\|j}$ to adversary $\mathscr{A}$.

Now adversary $\mathscr{B}$ operates as follows:

1) Set

$$\mathbf{p}^* = \begin{pmatrix} b_1 \\ \vdots \\ b_{km} \end{pmatrix} \in \mathbb{Z}_q^{km}$$

2) Blind the message bit b by $c^* = b_0 + b\lfloor \frac{q}{2} \rfloor$.

3) Set $C = (\mathbf{p}^*, c^*)$ and send it to adversary $\mathscr{A}$.

If Oracle $\mathscr{O}$ is a pseudo-random LWE oracle, i.e. the samples are **genuine**, then $c^* = b_0 + b\lfloor \frac{q}{2} \rfloor = \mathbf{a}_0^{\top}\mathbf{y} + x + b\lfloor \frac{q}{2} \rfloor$ for some $\mathbf{y} \in \mathbb{Z}_q^n$ and noise x. Similarly

$$\mathbf{p}^* = \begin{pmatrix} b_1 \\ \vdots \\ b_{km} \end{pmatrix} = \mathbf{A}_{ID^*\|j^*}^{\top}\mathbf{y} + x_1$$

for some $\mathbf{y} \in \mathbb{Z}_q^n$ and noise x_1. So $C = (\mathbf{p}^*, c^*)$ is a valid encryption of b on $ID^*\|j^*$. If Oracle $\mathscr{O}$ is a random oracle, i.e. the samples are **random**, then b_0, b_1 are uniform and therefore $C = (\mathbf{p}^*, c^*)$ is uniform too.

Guess: Finally adversary $\mathscr{A}$ terminates the game with some output which is a guess about whether the ciphertext is random or not, then adversary $\mathscr{B}$ terminates with the same output to decide whether the LWE instances are genuine or not. So if adversary $\mathscr{A}$ can break our scheme, then there must exist adversary $\mathscr{B}$ can solve the LWE hard problem.

Since probability that $j = j^*$ is $\frac{1}{N}$, that is, the probability of adversary $\mathscr{B}$ not aborting during the simulation is $\frac{1}{N}$, then $Adv_{LWE}(n) = \frac{1}{N}Adv_{fs-IBBE}(n)$.

Hence our scheme is semantic secure in the random oracle model assuming the LWE is hard.

Table 1: Comparison of some IBBE schemes

	Hdr size	public-key size	private-key size	security
IBBE in[7]	$O(\|S\|)$	$O(l)$	$O(1)$	Adaptively Secure Non-ROM
IBBE in[1]	$O(\|S\|)$	$O(1)$	$O(1)$	Adaptively Secure in ROM
Our Work	$O(\|S\|)$	$O(1)$	$O(1)$	IND-sID-CPA in ROM

5 Extension

We can extend our construction to encrypt on t bits message simultaneously. The previous steps are the same as the first scheme. The difference is that we choose $\mathbf{v} \in Z_q^{n\times t}$ uniformly at random, where t is the length of the message encryption key.

On the encryption phase, we choose a message key $K \in \{0,1\}^t$. For $1 \le j \le t$, let b_j be the j-th bit of K. Compute

$$\mathbf{c} = \mathbf{v}^\top \mathbf{u} + \bar{\mathbf{e}} + K\lfloor \frac{q}{2} \rfloor \in \mathbb{Z}_q^t$$

where $\bar{\mathbf{e}} \leftarrow \chi^m$.

Then at the decryption phase, parse $\mathbf{v}$=$[v_1, \cdots, v_t] \in (Z_q^n)^t$. For $1 \le j \le t$, run the generalized preimage sampling algorithm **GenSamplePre**( ) and generate $\mathbf{y}_j \leftarrow$ **GenSamplePre**$(\mathbf{A}_{S\|j}, \mathbf{A}_{ID_i\|j}, \mathbf{B}_{ID_i\|j}, \mathbf{v}_j, r) \in \mathbb{Z}^{km}$. Note that $\mathbf{y}_j$ is distributed according to $D_{\Lambda_q^{v_j}\mathbf{A}_{S\|j},r}$.

Parse $\mathbf{c} = [c_1, \cdots, c_t] \in (\mathbb{Z}_q)^t$. For $1 \le j \le t$, compute

$$b_j^{'} = c_j - \mathbf{y}_j^\top \mathbf{p} \in \mathbb{Z}_q$$

Let $b_j = 0$ if $b_j^{'}$ is closer to 0 than to $\lfloor \frac{q}{2} \rfloor \in \mathbb{Z}_q$; otherwise $b_j = 1$.

Output $K = [b_1, \cdots, b_t]$.

6 Efficiency

In our construction, we realize $O(1)$-size of public keys and private keys, $O(k)$-size of ciphertexts and $O(|S|)$-size of Hdr. Compared with the construction in[1], we improve the security for our construction satisfies the forward security. But we do not pay the cost of efficiency even the size of public keys is shorter than that in[1]. The comparison of efficiency with some IBBE schemes is shown in the following Table 1.

7 Conclusion

In this paper, we propose a forward-secure identity-based broadcast encryption scheme from lattices by adding the forward-security on broadcast encryption scheme. Our scheme satisfies the security requirements of both the broadcast encryption and forward-security schemes. And our construction is believed secure in the post-quantum environment as it is based on lattice problem.

References

[1] Jin Wang, Jingguo Bi, Cryptology ePrint Archive, Report 2010/288, 2010.
[2] Kunwar Singh, C. Pandurangan, Journal of Internet Services and Information Security (JISIS), 3(1/2): 5-19(2013).
[3] Oded Regev, Journal of the ACM (JACM), 2009, 56(6): 34.
[4] Fiat, Amos, Moni Naor, Advances in CryptologyłCRYPTO93, 480-491(1994).
[5] Dan Boneh, Craig Gentry, Brent Waters, Advances in Cryptology CCRYPTO 2005, 3621: 258-275(2005).
[6] Yevgeniy Dodis, Nelly Fazio, Digital Rights Management, 61-80(2003).
[7] Craig Gentry, Brent Waters, Advances in Cryptology-EUROCRYPT 2009, 171-188(2009).
[8] Dan Boneh, Matt Franklin, Advances in Cryptology CRYPTO 2001, 213-229(2001).
[9] Clifford Cocks, Cryptography and Coding, 360-363(2001).
[10] Craig Gentry, Advances in Cryptology-EUROCRYPT 2006, 445-464(2006).
[11] Joël Alwen, Chris Peikert C, Theory of Computing Systems, 48(3): 535-553(2011).
[12] Ryuichi Sakai, Jun Furukawa, IACR Cryptology ePrint Archive, 217(2007).
[13] Dan Boneh, Xavier Boyen, Eu-jin Goh, Advances in Cryptology CEUROCRYPT 2005, 440-456(2005).
[14] Craig Gentry, Advances in Cryptology-EUROCRYPT 2006, 445-464(2006).
[15] Dan Boneh, Michael Hamburg, Advances in Cryptology-ASIACRYPT 2008, 455-470(2008).
[16] Christoph G Günther, Advances in Cryptology-Eurocrypt 89, 29-37(1990).
[17] Ross Anderson, Unpublished. Available from http://www.cl. cam. ac. uk/users/rja14, 1997.
[18] Mihir Bellare, Sara K. Miner, Advances in Cryptology-CRYPTO 99, 431-448(1999).
[19] Canetti Ran, Shai Halevi, Jonathan Katz, Advances in Cryptology-Eurocrypt 2003, 255-271(2003).
[20] Chris Peikert, IACR Cryptology ePrint Archive, 359(2009).
[21] David Cash, Dennis Hofheinz, Eike Kiltz, IACR Cryptology ePrint Archive, 351(2009).
[22] Shweta Agrawal, Dan Boneh, Xavier Boyen, Advances in Cryptology CCRYPTO 2010, 98-115(2010).
[23] Craig Gentry, Chris Peikert, Vinod Vaikuntanathan, Proceedings of the 40th annual ACM symposium on Theory of computing. ACM, 197-206(2008).
[24] Daniele Micciancio, Shafi Goldwasser, Kluwer Academic Publishers, 2002.
[25] David Cash, Hofheinz D, Kiltz E, et al, Journal of cryptology, 25(4): 601-639(2012).
[26] Agrawal, S., Freeman, D.M., Vaikuntanathan, V, ASIACRYPT 2011,7073: 21-40(2012).

Xinwen Zhang is a lecturer in XI'an University of Posts & Telecommunications. She received her phD degree in Northwest University in 2015. Her main research interests are cryptography.

Shangping Wang received his B.S. degree in mathematics in 1982 from Xi'an University of Technology, Xi'an, China,. He received his M.S. degree in applied mathematics in 1989 from Xi'an Jiaotong University, Xi'an, China, and earned his phD degree in cryptology in 2003 from Xi'an University, Xian, China. Currently, he is a professor in Xi'an University of Technology. His current research interests are cryptography and information security.

Wenpeng Zhang is a professor of mathematics in Northwest University. He received his phD degree in Shandong University in 1988. He is the director of Chinese Mathematical Society, editor in chief of Scientia Magna, and the Deputy editor of Pure and Applied Mathematics. His main research interests are: Dirichilet L - function, Hurwitz zeta - function, Lehmer problems, the mean value of Dedekind sums, Kloosterman sums, and combinatorial identities of famous sequences in number theory.