Lattice Forward-Secure Identity Based Encryption Scheme

Kunwar Singh*
Computer Science and Engineering Department
NIT Trichy, Tiruchirappalli, India
kunwar@nitt.edu

C. Pandurangan
Computer Science and Engineering Department
IIT Madras, India
rangan@cse.iitm.ac.in

A.K.Banerjee
Mathematics Department
NIT Trichy, Tiruchirappalli, India
banerjee@nitt.edu

Abstract

Protecting secret keys is crucial for cryptography. There are some relatively insecure devices (smart cards, mobile phones etc.) which have threat of key exposure. The goal of the forward security is to protect security of past uses of key even if the current secret key is exposed. In this paper we propose lattice based forward-secure identity based encryption scheme based on LWE assumption in random oracle model. We also propose lattice based forward-secure identity based encryption scheme in the standard model.

Keywords: lattice, identity based encryption, forward security, random oracle model, learning with error (LWE).

1 Introduction

The concept of identity-based cryptosystem was introduced by Adi Shamir in 1984 [23]. In this new paradigm users' public key can be any string which uniquely identifies the user. For example email or phone number can be public key. As a result, it significantly reduces system complexity and cost of establishing public key infrastructure. Although Shamir constructed an identity-based signature scheme using RSA function but he could not construct an identity based encryption and this became a long-lasting open problem. Only in 2001, Shamir's open problem was independently solved by Boneh and Franklin [9] and Cocks [15].

First Canetti et al [12] presented Identity-Based Encryption in standard model. They proved the security of scheme in selective-ID model. In the Selective-ID model the adversary must first declare which identity it wishes to be challenged before the global parameters are generated. Boneh and Boyen [7] then provided an efficient secure scheme in selective-ID model. Boneh and Boyen [8] described a scheme that was fully secure in the standard model, but their scheme is too inefficient for practical use. Finally, the first practical and fully secure IBE scheme was proposed by Waters [24] in the standard model under the Decisional Bilinear Diffie-Hellman assumption.

Lattice based cryptogrphy have arisen in recent years. Lattice based cryptography are attractive due to their worst case hardness assumption and their potential resistance to quantum computers. Recently Regev [22] defined the learning with errors (LWE) problem and proved that it enjoys similar worst-case hardness properties under a quantum reduction. A number of constructions of lattice identity based encryption is known [18, 13, 21, 1, 2].

Journal of Internet Services and Information Security (JISIS), volume: 2, number: 3/4, pp. 118-128
*Corresponding author: CSE Department, NIT Trichy, Tiruchirappalli-15, Tamilnadu, India, Tel: +91-043125013212, Email: kunwar2081@gmail.com

Protecting secret keys is crucial for cryptography. There are some relatively insecure devices (smart cards, mobile phones etc.) which have threat of key exposure. The goal of the forward security is to protect security of past uses of key even if the current secret key is exposed. The notion of forward secrecy was first proposed by G*ü*nther [14] in 1989 and later by Diffie et al [16] in 1992 in the contexts of key exchange protocol. A key exchange protocol is said to provide forward secrecy if compromise of long term secret keys does not compromise the secrecy of the previously generated exchange keys, which can be converted as forward secure interactive public key encryption scheme. The notion of non-interactive forward security was proposed by Anderson [4] in 1997 and later formalized by Bellare and Miner [5]. In non-interactive forward security the lifetime of the system is divided into N time interval labled $0,1,...,N-1$. The device initially stores the secret key SK_0. After that device at beginning of interval i computes secret key SK_i at interval i using update algorithm $(SK_{i-1},..,)$ and then delete secret key SK_{i-1} at interval $i-1$. A forward secure encryption scheme guarantees that exposer of secret key at interval i will not compromise on the security of system for any prior time interval. But system can not prevent the adversary from breaking the security of system for any time interval greater than i. Forward secure encryption scheme in symmetric setting was proposed by Bellare and Yee [6]. The construction of forward secure encryption scheme in public key setting was a open problem since the question was first raised by Anderson [4]. Only in 2003, Anderson's open problem was solved by Canetti et al [11]. In this paper Canetti et al [11] constructed Binary Tree Encryption (BTE) based on billinear Diffi-Hellman assumption. They have also proposed a method to convert forward secure PKE scheme from any BTE scheme. Lu and Li [20] proposed efficient forward secure PKE scheme in standard model. Two forward secure encryption scheme in identity based setting have been proposed so far [19, 25].
Chris Peikert [21] proposed lattice based BTE scheme based on Learning With Error (LWE) assumption. Using Canetti et al [11], it can be converted into lattice based forward PKE scheme.

Our Contribution: To the best of our knowledge, there does not exist any lattice based forward-secure identity based encryption (fs-IBE) scheme. In this paper we propose lattice based fs-IBE scheme in random oracle model based on LWE assumption. We also propose lattice based fs-IBE scheme in standard model. Our schemes are based on lattice based hierarchical identity based encryption (HIBE) scheme proposed by Cash et al [13].

2 Preliminaries

2.1 Forward Secure IBE

Here definition of IBE is similar to [11, 19]. Forward secure IBE consists of five algorithms.

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

Extract(mpk,msk,id): On input master public key mpk, a master secret key msk, and an identity id $\in \{0,1\}^*$ outputs private key corresponding to an identity id.

Update(mpk,SK$_{id||i}$,$id||i$): On input master public key mpk, secret key SK$_{id||i}$ at i^{th} time period outputs secret key SK$_{id||(i+1)}$ at $(i+1)^{th}$ time period.

Encrypt($mpk,id||i$,M): On input master public key mpk, $id||i$ and a message M outputs ciphertext C.

Decrypt(C,mpk,SK$_{(id||i)}$): On input master public key mpk, a private key $SK_{id||i}$, and a ciphertext C outputs message M.

2.2 Selective-ID Security Model for Forward-Secure IBE

Security model is adapted from [11]. We define adaptive-ID security model using a game that the challenge ciphertext is indistinguishable from a random element in the ciphertext space. This property implies both semantic security and recipient anonymity. The game proceeds as follows.

Init: The adversary submits a target identity id^*.

Setup: The challenger runs Setup($1^n, N$) and gives the master public parameters (mpk) to adversary and keeps master secret key (msk) to itself.

Query Phase:

- Hash query: The adversary can issue hash query for any identity id. Adversary can repeat this polynomial number of times for different identities adaptively.
- Extraction query: The adversary can issue a query for a private key $SK_{id||0}$ corresponding to identity $id||0$. Adversary can repeat this polynomial number of times for different identities($id \neq id^*$) adaptively.

Attack: The adversary issues one breakin(j) query and challenge(i,b) query, in either order, subject to $0 \leq i < j \leq N$. These queries are answered as follows:

- On query breakin(j), secret key $SK_{id||j}$ is computed and return to the adversary.
- On query challenge(i,b), the challenger picks a random bit $r \in \{0,1\}$ and a random ciphertext C. If $r = 0$ it sets the challenge ciphertext to $C^* = \text{Encrypt}(mpk, id^*||i, b)$. If $r = 1$ it sets the challenge ciphertext to $C^* = C$. It returns C^* as challenge to the adversary.

Guess: The adversary outputs a guess $r' \in \{0,1\}$, it succeeds if $r' = r$.
We refer an adversary A as an IND-sID-CPA adversary. We define the advantage of the adversary A in attacking fs-IBE scheme ξ as $Adv_{\xi,A}(n) = |Pr[r = r'] - 1/2|$.

Definition 1. We say that forward-secure IBE scheme ξ is selective-ID, indistinguishable from random if for all IND-sID-CPA PPT adversaries A we have $Adv_{\xi,A}(n)$ is a negligible function.

2.3 Integer Lattices

A lattice is defined as the set of all integer combinations

$$L(b_1, ..., b_n) = \left\{ \sum_{i=1}^{n} x_i b_i : x_i \in Z \text{ for } 1 \leq i \leq n \right\}$$

of n linearly independent vectors $b_1, ..., b_n \in R^n$. The set of vectors $\{b_1, ..., b_n\}$ is called a basis for the lattice. A basis can be represented by the matrix $B = [b_1, ..., b_n] \in R^{n \times n}$ having the basis vectors as columns. Using matrix notation, the lattice generated by a matrix $B \in R^{n \times n}$ can be defined as $L(B) = \{Bx : x \in Z^n\}$, where Bx is the usual matrix-vector multiplication. The determinant of a lattice is the absolute value of the determinant of the basis matrix $det(L(B)) = |det(B)|$.

Definition 2. For q prime, $A \in Z_q^{n\times m}$ and $u \in Z_q^n$, define:

$$\Lambda_q(A) := \{e \in Z^m \ \ s.t. \ \exists s \in Z_q^n \ where \ A^T s = e \ (mod \ q)\}$$

$$\Lambda_q^{\perp}(A) := \{e \in Z^m \ \ s.t. \ \ Ae = 0 \ (mod \ q)\}$$

$$\Lambda_q^{u}(A) := \{e \in Z^m \ \ s.t. \ \ Ae = u \ (mod \ q)\}$$

2.4 The Gram-Schmidt Norm of a Basis

Let S be a set of vectors S = $\{s_1, ..., s_k\}$ in R^m. We use the following notation:

- $|S|$ denotes the L_2 length of the longest vector in S, i.e. $\|S\| := max_i|s_i|$ for $1 \leq i \leq k$.
- $\widetilde{S} := \{\widetilde{s_1}, ..., \widetilde{s_k}\} \subset R^m$ denotes the Gram-Schmidt orthogonalization of the vector $s_1, ..., s_k$ taken in that order.

We refer to $\widetilde{\|S\|}$ as the Gram-Schmidt norm of S.

2.5 Discrete Gaussians

Let L be a subset of Z^m. For any vector $c \in R^m$ and any positive parameter $\sigma \in R > 0$, define:
$\rho_{\sigma,c}(x) = exp(-\pi \frac{\|x-c\|}{\sigma^2})$: a Gaussian-shaped function on R^m with center c and parameter σ,
$\rho_{\sigma,c}(L) = \sum_{x\in L} \rho_{\sigma,c}(x)$: the (always converging) $\rho_{\sigma,c}$ over L,
$D_{L,\sigma,c}$: the discrete Gaussian distribution over L with parameters σ and c,

$$\forall y \in L \ , \ D_{L,\sigma,c} = \frac{\rho_{\sigma,c}(y)}{\rho_{\sigma,c}(L)}$$

The distribution $D_{L,\sigma,c}$ will most often be defined over the Lattice $L = \Lambda_q^{\perp}$ for a matrix $A \in Z_q^{n\times m}$ or over a coset $L = t + \Lambda_q^{\perp}(A)$ where $t \in Z^m$.

Lemma 1 ([[17],Lemma 7.1]). Let Λ be an m-dimensional lattice. There is a deterministic polynomial-time algorithm ToBasis(S,s) that, given an arbitrary basis of Λ and a full-rank set $S = \{s_1, ..., s_m\}$ in Λ, returns a basis T of Λ satisfying

$$\|\widetilde{T}\| \leq \|\widetilde{S}\| \ \ and \ \ \|T\| \leq \|S\|\sqrt{m}/2$$

.

RandBasis(S, s) ([[21]]) Randomized algorithm RandBasis(S, s) takes a basis S of some m-dimensional lattice $\wedge$ and a parameter $s \geq \|\widetilde{S}\|\sqrt{(\log n)}$, and outputs a new basis S of lattice $\wedge$, generated as follows.

1. For $i = 1, ..., m$:
   (a) Choose $v \leftarrow$ SampleBasis(S, s). If v is linearly independent of $\{v_1, ..., v_{i1}\}$, then let $v_i = v$ and go to the next value of i; otherwise, repeat this step.
2. Output $S' =$ ToBasis(V, S)

Lemma 2 ([[21],Lemma 3.3]). With overwhelming probability, $S' \leftarrow \text{RandBasis}(S,s)$ repeats Step 1a at most $O(m^2)$ times, and $||\widetilde{S'}|| \leq s\sqrt{m}$. Moreover,for any two bases S_0 , S_1 of the same lattice and any $s \geq ||\widetilde{S_i}||\sqrt{(log\ n)}$ for $i = \{0,1\}$ RandBasis(S_0,s) and RandBasis(S_1,s) are within negl(n) statistical distance.

Theorem 1 ([[3], Theorem 3.2]). Let $q \geq 3$ be odd and $m := \lceil 6n\log q \rceil$.
There is probabilistic polynomial-time algorithm TrapGen(q,n) that outputs a pair ($A \in Z_q^{n\times m}, S \in Z^{n\times m}$) such that A is statistically close to a uniform matrix in $Z_q^{n\times m}$ and S is a basis for $\Lambda_q^{\perp}(A)$ satisfying

$$\|\widetilde{S}\| \leq O(\sqrt{n\log q}) \ \ and \ \ \|S\| \leq O(n\log q)$$

with all but negligible probability in n.

Theorem 2 ([[13], Lemma 3.3]). Let $A = [A_1,...,A_k]$, where each $A_i \in Z_q^{n\times m}$. For $S \subseteq [k]$, $S = \{i_1,...,i_j\}$, we write $A_S = [A_{i_1},...,A_{i_j}]$. Let n,q,m,k be positive integers with $q \geq 2$ and $m \geq 2n\ log\ q$. There exists a PPT algorithm ExtendBasis, that on input of $A \in Z_q^{n\times km}$, a set $S \subseteq [k]$, a basis B_S for $\Lambda_q^{\perp}(A_S)$, and an integer $L \geq \|\widetilde{B_S}\|.\sqrt{km}.w(\sqrt{km})$ outputs $B \leftarrow \text{ExtendBasis}(A,B_S,S,L)$. With overwhelming probability B is a basis of $\Lambda_q^{\perp}(A)$ with $\|\widetilde{B}\| \leq L$.

2.6 The LWE Hardness Assumption

The LWE (learning with error) hardness assumption is defined by Regev [22].

Definition 3. Consider a prime q, a positive integer n, and a distribution χ over Z_q, typically taken to be normal distribution. The input is a pair (A,v) from an unspecified challenge oracle $\bigcirc$, where $A \in Z_q^{m\times n}$ is chosen uniformly. v is chosen uniformly from Z_q^m or chosen to be $As+e$ for a uniformly chosen $s \in Z_q^n$ and a vector $e \in Z_q^m$. When v is chosen to be $As+e$ for a uniformly chosen $s \in Z_q^n$ and a vector $e \in Z_q^m$ an unspecified challenge oracle $\bigcirc$ is a noisy pseudo-random sampler $\bigcirc_s$. When v is chosen uniformly an unspecified challenge oracle $\bigcirc$ is a truly random sampler $\bigcirc_\$$.
Goal of the adversary is to distinguish with some non-negligible probability between these two cases.
Or we say that an algorithm A decides the (Z_q,n,χ)-LWE problem if $|Pr[A^{\bigcirc_s} = 1] - Pr[A^{\bigcirc_\$} = 1]|$ is non-negligible for a random $s \in Z_q^n$.

Definition 4. Consider a real parameter $\alpha = \alpha(n) \in \{0,1\}$ and a prime q. Denote by $T = R/Z$ the group of reals [0,1) with addition modulo 1. Denote by ψ_α the distribution over T of a normal variable with mean 0 and standard deviation $\alpha/\sqrt{2\pi}$ then reduced modulo 1. Denote by $\lfloor x \rceil = \lfloor x + \frac{1}{2} \rfloor$ the nearest integer to the real $x \in R$. We denote by $\overline{\psi}_\alpha$ the discrete distribution over Z_q of the random variable $\lfloor qX \rceil \bmod q$ where the random variable $X \in T$ has distribution ψ_α.

Theorem 3 ([22]). If there exists an efficient, possibly quantum, algorithm for deciding the $(Z_q,n,\overline{\psi_\alpha})$-LWE problem for $q > 2\sqrt{n}/\alpha$ then there exists an efficient quantum algorithm for approximating the SIVP and GapSVP problems, to within $O(n/\alpha)$ factors in the l_2 norm, in the worst case.

3 Lattice Based Forward Secure IBE Scheme

Our scheme is similar to scheme of [13] and [21]. Now we describe our new forward secure-IBE scheme as follows.

Setup(n,N): On input a security parameter n, we set the parameters q,m accordingly. Let $H:\{0,1\}^* \rightarrow Z_q^{n\times m}$ be hash function. Next we do the following.

1. Use algorithm TrapGen(q,n) to generate a matrix $A \in Z_q^{n\times m}$ and a short basis T_A for $\Lambda_q^{\perp}(A)$ such that $\|\widetilde{T_A}\| \leq O(\sqrt{n\log q})$.
2. For each $j \in [N] = \{0,1,2,...,N\}$ and an arbitary identity id we define the associated parity check matrix $A_{id,[j]}$
   $A_{id,[j]} = [A, A_{id,0}, A_{id,1}, ..., A_{id,j}] \in Z_q^{n\times(j+2)m}$, where $A_{id,i} = H(id||i) \in Z_q^{n\times m}$
3. We choose $y \leftarrow Z_q^n$ uniformly.
4. Output the master public key and master secret key,
   mpk = (A,y), msk = T_A.

Extract(mpk,T,id): PKG generates the secret key for a user identity $id \in \{0,1\}^*$ by calling the function RandBasis(SampleBasis(A,T,$A_{id,0}$)) (theorem 2 and lemma 2). Output of function $SK_{id||0}$ is the secret key of this user.

Update(mpk,$\mathbf{SK}_{id||i}$,$id||i$): Given secret key at i^{th} time period $\mathrm{SK}_{id||i}$ user can find secret key at $i+1^{th}$ time period as follows.
$SK_{id||i+1}$ = RandBasis(ExtBasis($\mathrm{SK}_{id||i}, A_{id,[i+1]}$)) by theorem 2 and lemma 2.
Output $\mathrm{SK}_{id||i+1}$.

Encrypt(mpk,$id||i$,b): To encrypt a bit $b \in \{0,1\}$, we do the following.

1. We compute $A_{id,[i]} = [A, A_{id,0}, A_{id,1}, ..., A_{id,i}] \in Z_q^{n\times(i+2)m}$, where $A_{id,i} = H(id||i) \in Z_q^{n\times m}$.
2. we choose $s \leftarrow Z_q^n$ uniformly.
3. Compute $p = A_{id,[i]}^T s + e \in Z_q^{m(i+2)}$, where $e \leftarrow \chi^{m(i+2)}$. Here $\chi^{m(i+2)}$ is error (gaussian) distribution.
4. Compute $c = y^T s + b\lfloor\frac{q}{2}\rfloor + \overline{e}$, where $\overline{e} \leftarrow \chi$. Here χ is error (gaussian) distribution.
5. Output the ciphertext $C = (p,c)$.

Decrypt(C,mpk,$\mathbf{SK}_{(id||i)}$): To decrypt $C = (p,c)$, we do the following.

1. $s \leftarrow \mathrm{invert}(mpk, \mathrm{SK}_{(id||i)}, p)$.
2. Now we compute $b' = c - y^T s$.
3. If b' is closer to 0 than $\lfloor\frac{q}{2}\rfloor$ mod q output 0 otherwise output 1.

It is required that above forward secure IBE scheme has the correctness property, i.e, for any index $i \in [0,N]$ and secret key $\mathrm{SK}_{id||i}$ and any message bit b we have $b = \mathrm{Decryption}(mpk, \mathrm{SK}_{id||i}, \mathrm{Encryption}(mpk, id||i, \mathrm{b}))$.

Theorem 4. If hash function H is modeled as random oracle, then our lattice forward-secure IBE is IND-sID-CPA (semantic) secure assuming the $LWE_{q,\chi}$ is hard or $Adv_{B,LWE_{q,\chi}}(n) = \frac{1}{N} Adv_{\chi,A}(n)$.

Proof: Here proof is similar to proof of theorem 4.1 of [13].
We now show semantic security of fs-IBE in the random oracle model. We will show that if there exist a PPT adversary A that breaks fs-IBE scheme with non-negligible probability then there must exist a PPT adversary B that solves LWE hard problem by simulating views of A. We assume that

- For each $i \in [N]$, A always makes polynomial number of Q_H different H-queries of interval i.
- Whenever A makes an H-query of interval i, we assume that it has queried H-query of interval $j < i$.
- Whenever A submits a user secret key query, we assume that it has made all relevant H queries beforehand.

Adversary A declares an identity ID^* that it intends to attack. Adversary B(works as challenger for adversary A) first pick $i^* \in [N]$. Here i^* is a guess for the i of challenge (i,b) query. Now B obtains $(i^*+2)(m+1)$ LWE samples, which get parsed as
$(A_i^*, p_i^*) \in Z_q^{n \times m} \times Z_q^n$ $(0 \leq i \leq j^*)$ and $(y^*, c^*) \in Z_q^m \times Z_q$.

Setup: Adversary B sets master public key to be $mpk = A = A_0^*$ (m samples from LWE oracle). Next Adversary B simulates the view of A as follows:

- Hash H Queries: A's hash query on $id^*||0$, adversary B returns $A_1 \in Z_q^{m \times n}$ (samples obtained from LWE oracle). Similarly on A's hash query on $id^*||1, ..., id^*||N$, adversary B returns $A_2, A_3, ..., A_N$ respectively. For A's hash query on identity $id \neq id^*$, adversary B run the trapdoor algorithm TrapGen to generate $A \in Z_q^{n \times m}$ with corresponding trapdoor $T \in Z^{m \times m}$. Adversary B returns matrix A and stores the tuple (id, A, T) in list H.
- Extraction Queries: When adversary A asks for the secret key for the identity $id \neq id^*$. As we have assumed that before extraction query adversary A would have made hash query for it, so adversary B will check the list H and returns the corresponding T to adversary A.

Attack:

- Challenge(i,b): When adversary A queries challenge (i,b), the adversary B picks a random bit $r \in \{0,1\}$ and a random ciphertext C. If $r = 0$ it returns challenge ciphertext to be (p^*, C^*) else it returns random ciphertext C.
- Breakin(j): When adversary A queries breakin(j), if $i \leq j \leq i^*$ then adversary B outputs a random bit and game abort (since B can not answer extraction queries for $j \leq i^*$). Otherwise adversary B run the trapdoor algorithm TrapGen to generate $A_j \in Z_q^{n \times m(j+1)}$ with corresponding trapdoor $T_j \in Z_q^{m(j+1) \times m(j+1)}$ and then returns T_j.

When adversary A terminates with some output, adversary B terminates with same output. Since form of ciphertext is same as form of LWE problem, so if adversary A breaks the scheme then there exist adversary B which solves LWE hard problem.
Since probability that $i = i^*$ is $\frac{1}{N}$, so the probability that B does not abort during simulation is $\frac{1}{N}$. $Adv_{B,LWE_{q,\chi}}(n) = \frac{1}{N} Adv_{\chi,A}(n)$. Hence our scheme is semantic secure.

4 Lattice Based Forward Secure IBE Scheme in the Standard Model

Cryptographic schemes which are secure in random oracle model does not mean that these schemes will be secure when the random oracle model is instantiated by real hash function. Therefore constructing schemes in standard model is an important goal [10]. Our scheme is similar to HIBE scheme in selective model of [13]. Now we describe our new lattice based forward secure IBE scheme in standard model as follows.

Setup(n,N)**:** On input a security parameter n, we set the parameters q,m accordingly. Let $H:\{0,1\}^* \rightarrow \{0,1\}^\lambda$ be real. $H(id||i) = (t_1||t_2||...||t_\lambda)$ where $t_i \in \{0,1\}$. Next we do following.

1. Use algorithm TrapGen(q,n) to generate a matrix $A \in Z_q^{n\times m}$ and a short basis T_A for $\Lambda_q^\perp(A)$ such that $\|\widetilde{T_A}\| \leq O(\sqrt{n\log q})$.

2. For $0 \leq i \leq N,\ 1 \leq u \leq \lambda$ and $b \in \{0,1\}$ sample the matrices $C_{i,u,b} \in Z_q^{n\times m}$ uniformly and independently and also sample $y \in Z_q^n$ uniformly. For each $j \in [N] = \{0,1,2,...,N\}$ and an arbitary identity id we define the associated parity check matrix $A_{id,[j]}$ as
   $A_{id,[j]} = [A, A_{id,0}, A_{id,1}, ..., A_{id,j}] \in Z_q^{n\times((j+1)\lambda+1)m}$,
   where $A_{id,j} = [C_{j,1,t_1}, ..., C_{j,\lambda,t_\lambda}] \in Z_q^{n\times\lambda m}$
   for $H(id||j) = (t_1||t_2||...t_\lambda) \in \{0,1\}^\lambda$

3. Output the master public key and master secret key,

$$mpk = (A, y, (C_{i,u,b})_{\substack{0\leq i\leq N \\ 1\leq u\leq\lambda \\ b\in\{0,1\}}}),\ msk = T_A$$

Extract(mpk,T,id), Update(mpk,$SK_{id||i}, id||i$), Encrypt(mpk,$id||i$,b) and Decrypt(C,mpk,$SK_{(id||i)}$) function is same as Extract, Update, Encrypt and Decrypt function of section 3 lattice based forward-secure IBE scheme.

Theorem 5: Our lattice based forward-secure IBE is IND-sID-CPA (semantic) secure assuming the $LWE_{q,\chi}$ is hard or $Adv_{B,LWE_{q,\chi}}(n) = \frac{1}{N} Adv_{\chi,A}(n)$.

Proof: Here proof is same as proof of theorem 4 except how adversary B sets the matrix $A_{id||j}$.
Adversary A declares an identity ID^* that it intends to attack. Adversary B first pick $i^* \in [N]$. Here i^* is a guess for the i of challenge(i,b) query. Now B obtains $2^\lambda(i^*+1)(m\lambda+1)$ LWE samples, which get parsed as
$(C_{j,i,t_i}, p_i) \in Z_q^{n\times m} \times Z_q^n$ for $(0 \leq j' \leq i^*, 1 \leq u \leq \lambda, t_i \in \{0,1\})$ and $(y^*, c^*) \in Z_q^n \times Z_q$. Adversary B sets master public key to be $mpk = A = A_0^*$ (m samples from LWE oracle). Based on hash value $H(id||j) = (t_1, t_2, ..., t_\lambda) \in \{0,1\}^\lambda$, adversary B sets the matrix $A_{id||j}$.
This proof differs from proof of theorem 4 by number of LWE samples required for adversary B. Number of LWE samples required in this proof is approximately equal to 2^λ times LWE samples required in proof of the previous theorem 4.

5 Conclusion

We have proved our schemes to be semantically secure based on LWE assumption. Our schemes may be improved by adapting them to ideal lattices. Construction of CCA secure lattice-based forward-secure IBE scheme is open problem. Another open problem is to construct lattice-based forward-secure HIBE scheme .

References

[1] S. Agrawal, D. Boneh, and X. Boyen. Efficient lattice (H)IBE in the standard model. In *Proc. of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'10), French Riviera, LNCS*, volume 6110, pages 553–572. Springer-Verlag, May - June 2010.

[2] S. Agrawal and X. Boyen. Identity-based encryption from lattices in the standard model. Manuscript, July 2009. Available at `http://www.cs.stanford.edu/~xb/ab09/`.

[3] J. Alwen and C. Peikert. Generating Shorter Bases for Hard Random Lattices. In *Proc. of the 26th International Symposium on Theoretical Aspects of Computer Science (STACS '09), Freiburg, Germany*, pages 75–86, February 2009.

[4] R. Anderson. Two remarks on public key cryptology. Invited Lecture, ACM-CCS, 1997. Available at `http://www.cl.cam.ac.uk/users/rja14`.

[5] M. Bellare and S. Miner. A forward-secure digital signature scheme. In *Proc. of the 19th International Conference on Cryptology (CRYPTO '99), Santa Barbara, California, USA, LNCS*, volume 1666, pages 431–448. Springer-Verlag, August 1999.

[6] M. Bellare and B. Yee. Forward security in private-key cryptography. Technical Report 035, Cryptology ePrint Archive, 2000.

[7] D. Boneh and X. Boyen. Efficient selective-ID secure identity-based encryption without random oracles. In *Proc. of the 23th International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'04), Interlaken, Switzerland, LNCS*, volume 3027, pages 223–238. Springer-Verlag, May 2004.

[8] D. Boneh and X. Boyen. Secure identity based encryption without random oracles. In *Proc. of the 24th International Conference on Cryptology (CRYPTO'04), Santa Barbara, California, USA, LNCS*, volume 3152, pages 443–459. Springer-Verlag, June 2004.

[9] D. Boneh and M. K. Franklin. Identity based encryption from the weil pairing. In *Proc. of the 21th International Conference on Cryptology (CRYPTO'01), Santa Barbara, California, USA, LNCS*, volume 2139, pages 213–229. Springer-Verlag, August 2003.

[10] R. Canetti, O. Goldreich, and S. Halevi. The random oracle methodology, revisited. In *Proc. of the 30th Proceedings of the thirtieth annual ACM symposium on Theory of computing (STOC'98), New York, USA*, pages 209–218. ACM, May 1998.

[11] R. Canetti, S. Halevi, and J. Katz. A forward-secure public-key encryption scheme. In *Proc. of the 23th International Conference on the Theory and Applications of Cryptographic Techniques (CRYPTO'03), Warsaw, Poland, LNCS*, volume 2729, pages 255–271. Springer-Verlag, May 2003.

[12] R. Canetti, S. Halevi, and J. Katz. Chosen-ciphertext security from identity-based encryption. In *Proc. of the 23th International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw (EUROCRYPT'04), Poland, LNCS*, volume 3027, pages 207–222. Springer-Verlag, May 2004.

[13] D. Cash, D. Hofheinz, and E. Kiltz. How to delegate a lattice basis. Technical Report 351, Cryptology ePrint Archive, 2009.

[14] C.G.Gunther. An identity-based key-exchange protocol. In *Proc. of the 8th Workshop on the Theory and Application of Cryptographic Techniques Houthalen (EUROCRYPT'89), Belgium, LNCS*, volume 434, pages 29–37. Springer-Verlag, April 1989.

[15] C. Cocks. An identity based encryption scheme based on quadratic residues. In *Proc. of the 8th IMA International Conference Cirencester (IMA '01), Cirencester, UK, LNCS*, volume 2260, pages 360–363.

Springer-Verlag, December 2001.

[16] W. Diffie, P. Van-Oorschot, and M. Weiner. Authentication and authenticated key exchanges. *Designs, Codes and Cryptography*, 2(2):107–125, June 1992.

[17] D.Micciancio and S.Goldwasser. *Complexity of Lattice Problems: A Cryptographic Perspective*. Kluwer Academic Publishers, 2002.

[18] C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proc. of the 40th Annual ACM symposium on Theory of computing (STOC'08), NewYork, USA*, pages 197–206. ACM, August 2008.

[19] H. Li, H. Yang, and F. Li. Identity-based encryption with forward security. In *Proc. of the International Conference on Communications, Circuits and Systems (ICCCAS'09), San Jose, California, USA*, pages 287–290. IEEE, July 2009.

[20] Y. Lu and J. Li. An efficient forward-secure public-key encryption scheme without random oracles. In *ISECS*, pages 376–379, July 2010.

[21] C. Peikert. Bonsai trees (or, arboriculture in lattice-based cryptography). Technical Report 359, Cryptology ePrint Archive, 2009.

[22] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proc. of the 37st ACM annual ACM symposium on Theory of computing (STOC'05), New York, USA*, pages 84–93. ACM, September 2005.

[23] A. Shamir. Identity-based cryptosystems and signature schemes. In *Proc. of the 4th CRYPTO(CRYPTO '84), Santa Barbara, California, USA, LNCS*, pages 47–53. Springer-Verlag, August 1984.

[24] B. R. Waters. Efficient identity-based encryption without random oracles. Technical Report 180, Cryptology ePrint Archive, 2004.

[25] D. Yao, N. Fazio, Y. Dodis, and A. Lysyanskaya. Id-based encryption for complex hierarchies with applications to forward security and broadcast encryption. In *Proc of the 11th ACM conference on Computer and communications security(CCS '04), NewYork, USA*, pages 354–363. ACM, August 2004.

Kunwar Singh received the M.Tech degree in Computer Science and Engineering from Jawaharlal University, New Delhi, India in 2003. Currently he is pursuing PhD degree in computer science and engineering from IIT Madras. He is an Assistant Professor in Computer Science and Engineering Department at NIT Trichy, India since 2006. Before that he worked in AEC Agra, Uttar Pradesh from 2004 to 2006. His research interest includes Public Key Cryptography, Identity-Based Encryption and Lattice Based Cryptography.

C.Pandu Rangan is a Professor in the department of computer science and engineering of Indian Institute of Technology - Madras, Chennai, India. He heads the Theoretical Computer Science Lab in IIT Madras. His areas of interest are in theoretical computer science mainly focusing on Cryptography, Algorithms and Data Structures, Game Theory, Graph Theory and Distributed Computing.

A.K.Banerjee received the B.Sc. degree with distinction, and the M.Sc. degree with first class in Mathematics from Ranchi University in 1967, 1970 respectively. He received PhD degree in Mathematics Department from IIT Mumbai, India in 1977. From 1978 to 1980, he was a Lecturer in Mathematics Department at NIT Trichy, India. From 1980 to 1996, he was an Assistant Professor in Mathematics Department at NIT Trichy, India. Since 1996, he is Professor in Mathematics Department at NIT Trichy, India. His research interest includes Fluid Mechanics and Cryptology. He is the member of Advisory Editorial Board of 'SCIENTIA IRANICA' an International Journal of Science and Technology and the International Journal of Computer Science and Engineering.