Lattice Based Identity Based Proxy Re-Encryption Scheme

Kunwar Singh[1]*, C. Pandu Rangan[2], and A.K.Banerjee[1]
[1]National Institute of Technology Tiruchirappalli, India
{kunwar, banerjee}@nitt.edu
[2]Indian Institute of Technology Madras
Chennai, Tamil Nadu, India
rangan@cse.iitm.ac.in

Abstract

At Eurocrypt 1998, Blaze, Bleumer and Strauss (BBS) presented a new primitive called proxy re-encryption. This new primitive allows semi trusted proxy to convert a ciphertext for Alice into a ciphertext for Bob without underlying message. Till now all the identity based proxy re-encryption schemes are based on the number theoretic assumptions like prime factorization, discrete logarithm problem etc. In this paper we propose a lattice based identity based proxy re-encryption scheme in the random oracle model for the single bit as well as for the multi-bit. Both of our schemes are anonymous, bidirectional and multi use. In these schemes, we have used Micciancio and Peikert's strong trapdoor [20] and this strong trapdoor is shown to be very efficient [6].

Keywords: Lattice, Identity Based Encryption, Proxy Re-encryption, Random Oracle Model, Learning With Error (LWE).

1 Introduction

The concept of identity-based cryptosystem was introduced by Adi Shamir in 1984 [24]. In this new paradigm a user's public key can be any string which uniquely identifies the user. For example an email or phone number can be a 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 [8] and Cocks [12].
Lattice based cryptogrphy have bloomed in recent years because of the following advantages.

- Number-theoretic hard problems like prime factorization and discrete logarithm problem can be solved in polynomial time by Shor's algorithm [25]. But till now there is no polynomial time quantum algorithm for lattice hard problems.
- Security of the cryptosystem depends on the hardness of the problem in the average case. Ajtai in his seminal result [3] has shown that lattice based cryptosystems are secure on the assumption of lattice based hard problems in the worst case. It gives strong hardness guarantee.
- Lattice based cryptosystems are efficient and parallelizable.
- Almost all the fully homomorphic encryption are based on lattice hard problems.

Journal of Internet Services and Information Security (JISIS), volume: 3, number: 3/4, pp. 38-51

*Corresponding author: Computer Science and Engineering Department, National Institute of Technology, Trichy, Tiruchirappalli-15, Tamilnadu, India, Tel: +91-43125013212, Web: `http://www.nitt.edu/home/academics/departments/cse/faculty/kunwar/`

Drawback of lattice based cryptosystem is that it has large key size and ciphertext size. Recently Regev [23] defined the learning with error (LWE) problem and proved that it also enjoys similar average case / worst case equivalence hardness properties under a quantum reduction. A number of constructions of lattice based identity based encryption is known [15, 10, 21, 1, 2].

At Eurocrypt 1998, Blaze, Bleumer and Strauss [7] presented a new primitive called proxy re-encryption. This new primitive allows semi trusted proxy to convert a ciphertext for Alice into a ciphertext for Bob without underlying message. This primitive have many useful applications. For example, Director can authorize his secretary (proxy) to convert encrypted mail for Director into encrypted mail for Dean whenever he is on leave. Then Dean can decrypt the encrypted mail using his secret key. Green and Ateniese [16] presented first proxy re-encryption scheme in the identity based setting. There are some other proxy re-encryption schemes [5, 9, 11, 19, 14, 17] in the context of public key encryption and identity based encryption. There is only one lattice based proxy re-encryption scheme [26] based on LWE assumption in the context of public key encryption.

Our Contribution: To the best of our knowledge, there does not exist any lattice based identity based proxy re-encryption (IB-PRE) scheme. In this paper we construct a lattice based identity based proxy re-encryption scheme in the random oracle model for the single bit as well as for the multi-bit. Our scheme satisfies the following properties of proxy re-encryption.

- Anonymous: In anonymous scheme ciphertext does not reveal anything about the identity of the receiver.
- Bidirectional: Bidirectional scheme permits proxy to convert a ciphertext for Alice to a ciphertext for Bob and vice-versa without knowing the underlying message.
- Multi use: A multi use scheme permits the proxy to perform multiple re-encryptions on a single ciphertext, e.g., re-encrypt from A to B, then re-encrypt the result from B to C, etc.

In this scheme, we have used Micciancio and Peikert's strong trapdoor [20] which is simpler, tighter, faster and smaller than trapdoor used for lattices like in [15]. Micciancio and Peikert's strong trapdoor is shown to be very efficient in [6].

Paper Outline: Our paper is organized as follows. In section 2, we describe basic definitions, security models, results and hard problems required to understand the rest of the paper. In section 3, we briefly describe Micciancio and Peikert's strong trapdoor for lattices [20]. In section 4, we describe our scheme for single bit and in section 5, we describe our scheme for multi bit. In section 6 we give conclusion and related open problems.

2 Preliminaries

2.1 Notation

We denote $[j] = \{0,1,...,j\}$, set of real numbers by R and the integers by Z. We assume vectors to be written in column form. $||S||$ denotes the Euclidean norm of the longest (maximum euclidean norm) vector in matrix S, i.e. $||S|| := max_i||s_i||$ for $1 \leq i \leq k$.
We say that *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.

2.2 Identity-Based Bidirectional Proxy Re-Encryption Scheme (IB-BPRE)

IB-BPRE consists of six algorithms.

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

Extract(PP, msk, id): On input public parameters PP, a master secret key msk, and an identity id, this algorithm outputs private key sk_{id} corresponding to an identity id.

Encrypt(PP, id, M): On input public parameters PP, an identity id, and a message m, this algorithm outputs ciphertext C_{id}.

RKGen(PP, sk_{id_i}, sk_{id_j}): On input a secret key sk_{id_i} and a secret key sk_{id_j}, this algorithm outputs a re-encryption key $rk_{i,j}$.

Re-encryption($PP, rk_{i,j}, C_{id_i}$): On input a ciphertext C_{id_i} under identity id_i and re-encryption key $rk_{i,j}$, this algorithm outputs a re-encrypted ciphertext C_{id_j} for an identity id_j.

Decrypt(PP, sk_{id}, C_{id}): On input public parameters PP, a private key $sk_{id} = e_{id}$ and a ciphertext C_{id}, this algorithm outputs message m.

Correctness. Identity Based Proxy Re-encryption is correct if suppose $C_{id_i} \leftarrow Encrypt(PP, id_i, m)$, $rk_{i,j} \leftarrow RKGen(PP, sk_{id_i}, skid_j)$ and $C_{id_j} \leftarrow$ Re-encryption($PP, rk_{i,j}, C_{id_i}$), then the following equation holds.

- Decrypt $(PP, sk_{id_i}, C_{id_i}) = m$.
- Decrypt $(PP, sk_{id_j}, C_{id_j}) = m$.

2.3 Adaptive-ID Security Model for IB-BPRE Scheme (IND-pID-CPA) [16, 11]

We define adaptive-ID security model using a game that is played between the challenger and the adversary. This property implies both semantic security and recipient anonymity. The game proceeds as follows.

Setup: The challenger runs Setup (1^n) and gives the public parameters PP to adversary and keeps master secret key msk to itself. Here CU denote set of users for which adversary has made private key query (corrupted users) and HU denote set of users for which adversary has not made private key query (honest users).

Phase 1: The adversary can make following queries.

- The adversary can issue a private key query on the identity id, challenger runs the $extract$ algorithm and returns private key query d_{id} to adversary $\mathscr{A}$. Adversary can repeat this polynomial times for different identities adaptively.

- The adversary can issue re-encryption key query $rk_{i,j}$ corresponding to identities id_i and id_j such that either $id_i, id_j \in HU$ or $id_i, id_j \in CU$. Adversary can repeat this polynomial times for different pair of identities adaptivly.

- The adversary can issue re-encryption query corresponding to identities id_i and id_j such that either $id_i, id_j \in HU$ or $id_i, id_j \in CU$. Challenger runs $RKGen$ algorithm to obtain $rk_{i,j}$ corresponding to identities id_i and id_j then challenger generates ciphertext C_{id_j} by running $Re-encryption$ algorithm.

Challenge: The adversary submits identity id^* and message m. Identity id^* should belong to set HU. Challenger picks a random bit $r \in \{0,1\}$ and a random ciphertext C. If $r = 0$ it sets the challenge ciphertext to C^* :=Encrypt(PP, id^*, m). If $r = 1$ it sets the challenge ciphertext to $C^* := C$. It sends C^* as challenge to the adversary.

Phase 2: Phase 1 is repeated except that for private key query on the identity $id \neq id^*$ should not be part of re-encryption key query and re-encryption query of phase 1.

Guess: Finally, the adversary outputs a guess $r' \in \{0,1\}$ and wins if $r = r'$.

We refer an adversary $\mathscr{A}$ as an IND-pID-CPA adversary. We define the advantage of the adversary $\mathscr{A}$ in attacking an IB-PRE scheme ξ as

$$Adv_{\xi,A}(\lambda) = |Pr[r = r'] - 1/2|$$

Definition 1. We say that an IB-PRE scheme is IND-pID-CPA if for all probabilistic polynomial time algorithm A and negligible function ε, $Adv_{\xi,A}(\lambda) \leq \varepsilon$.

2.4 Adaptive-ID Security Model for IB-UPRE Scheme (IND-pID-CPA)

In the above security model if we allow re-encryption query $rk_{i,j}$ corresponding to identities id_i and id_j such that $id_i \in CU$ and $id_j \in HU$ then it will be security model for identity based unidirectional proxy re-encryption scheme.

2.5 Integer Lattices ([13])

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:

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

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

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

2.6 Gram Schmidt Orthogonalization:

$\widetilde{S} := \{\widetilde{s_1}, ..., \widetilde{s_k}\} \subset R^m$ denotes the Gram-Schmidt orthogonalization of the set of linearly independent vectors $S = \{s_1, ..., s_k\} \subset R^m$. It is defined as follows: $\widetilde{s_1} = s_1$ and $\widetilde{s_i}$ is the component of s_i orthogonal to span$\underline{(s_1, ..., s_i)}$ where $2 \le i \le k$. Since $\widetilde{s_i}$ is the component of s_i so $\|\widetilde{s_i}\| \le \|s_i\|$ for all i.
We refer to $\widetilde{\|S\|}$ as the Gram-Schmidt norm of S.

2.7 Discrete Gaussian

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 (Lemma 7.1 of [13]). Let Λ be an m-dimensional lattice. There is a deterministic polynomial-time algorithm ToBasis(S,B) that, given an arbitrary basis B of Λ and a full-rank set $S = \{s_1, ..., s_m\}$ in Λ, returns a basis T of Λ satisfying

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

.

2.8 The LWE Hardness Assumption ([23, 1])

The LWE (learning with error) hardness assumption is defined by Regev [23].

Definition 3. **LWE:** Consider a prime q, a positive integer n, and a Gaussian distribution χ^m over Z_q^m. Given $(A, As + x)$ where matrix $A \in Z_q^{m\times n}$ is uniformly random and $x \in \chi^m$.
LWE hard problem is to find s with non-negligible probability.

Definition 4. **Decision LWE:** Consider a prime q, a positive integer n, and a Gaussian distribution χ^m over Z_q^m. The input is a pair (A, v) from an unspecified challenge oracle O, where $A \in Z_q^{m\times n}$ is chosen uniformly. An unspecified challenge oracle O is either a noisy pseudo-random sampler O_s or a truly random sampler $O_\$$. It is based on how v is chosen.

1. When v is chosen to be $As+e$ for a uniformly chosen $s \in Z_q^n$ and a vector $e \in \chi^m$, an unspecified challenge oracle O is a noisy pseudo-random sampler O_s.

2. When v is chosen uniformly from Z_q^m, an unspecified challenge oracle O is a truly random sampler $O_\$$.

Goal of the adversary is to distinguish between above two cases with non-negligible probability.
Or we say that an algorithm A decides the (Z_q, n, χ)-LWE problem if $|Pr[A^{O_s} = 1] - Pr[A^{O_\$} = 1]|$ is non-negligible for a random $s \in Z_q^n$.

Above decision LWE is also hard even if s is chosen from the Gaussian distribution rather than the uniform distribution [4, 18].

Definition 5. 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 1 ([23]). 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/α) factors in the l_2 norm, in the worst case.

2.9 Small Integer Solution (SIS) Assumption

SIS and ISIS hard problems were proposed by Ajtai [3] in 1996.

Definition 6. Given an integer q, a matrix $A \in Z_q^{n\times m}$ and real β, find a *short* nonzero integer vector $x \in Z_q^m$ such that $Ax = 0 \ mod \ q$ and $x \leq \beta$.
OR find a nonzero integer vector $x \in Z_2^m$ such that $Ax = 0 \ mod \ q$.

2.10 Inhomogeneous Small Integer Solution (ISIS) Assumption

Definition 7. Given an integer q, a matrix $A \in Z_q^{n\times m}$, a syndrome $u \in Z_q^n$ and real β, find a *short* nonzero integer vector $x \in Z_q^m$ such that $Ax = u \ mod \ q$ and $x \leq \beta$.
OR find a nonzero integer vector $x \in Z_2^m$ such that $Ax = u \ mod \ q$.

3 Strong Trapdoors for Lattices

We briefly describe Micciancio and Peikert's strong trapdoor for lattices which are simpler, tighter, faster and smaller [20]. In this method, there is a gadget matrix G for which inversion (f_G^{-1} and g_G^{-1}) is easy. We know that f_A^{-1} and g_A^{-1} are hard without trapdoor as short basis. In this method strong trapdoor is matrix R not the short basis. So to invert using strong trapdoor matrix R first f_A^{-1} and g_A^{-1} are converted to f_G^{-1} and g_G^{-1} for gadget matrix G and then we know that f_G^{-1} and g_G^{-1} are easy. Detail description is as follows.

3.1 Gadget G and Inversion(f_{HG}^{-1} and g_{HG}^{-1}) Algorithms

Let $q \geq 2$ be an integer modulus and $k \geq 1$ be an integer dimension. Vector $g = (g_1,...,g_k) \in Z_q^k$ is called primitive vector if $gcd(g_1,...,g_k,q) = 1$. Let matrix $S_k \in Z_q^{k\times k}$ is a basis of lattice $\Lambda^{\perp}(g^t)$, i.e, $g^t.S_k = 0 \in Z_k^{1\times k}$. A matrix G is a primitive matrix if its columns generate all of Z_q^n i.e. $G.Z^m = Z_q^n$. Matrix $G = I_n \otimes g^t \in Z_q^{n\times nk}$ and basis of $\Lambda^{\perp}(G)$ $S = I_n \otimes S_k \in Z^{nk\times nk}$. Matrix G, basis of $\Lambda^{\perp}(G)$ i.e. S are the direct sums of n copies of g^t and S_k respectively. Let $g_G(s,\varepsilon) = s^tG + e^t$ and $f_G(x) = Gx \ mod \ q$. g_G and f_G can be inverted in polynomial time. These inversions are parallelizable and offline. Inverting the functions g_G and f_G are summarized in the following theorem.

Theorem 2 (Theorem 4.1 of [20]) For any integers $q \leq 2$, $n \leq 1$, $k = log_2 q$ and $m = nk$, there is a primitive matrix $G \in Z_q^{n\times m}$ such that

- The lattice $\Lambda^{\perp}(G)$ has a known basis $S \in Z^{m\times m}$ with $\|\widetilde{S}\| \leq \sqrt{5}$ and $\|\widetilde{S}\| \leq max\{\sqrt{5}, \sqrt{k}\}$. Moreover, when $q = 2^k$, we have $\widetilde{S} = 2I$ (so $\|\widetilde{S}\| = 2$) and $\|S\| = \sqrt{5}$.
- Both G and S require little storage. In particular, they are sparse (with only $O(m)$ nonzero entries) and highly structured.
- Inverting $g_G(s,\varepsilon) = s^tG + e^t$ can be performed in quasilinear $O(n.log^c\ n)$ time for any $s \in Z_q^n$ and any $e \in P_{1/2}(q.B{-}t)$, where B can denote either S or $\widetilde{S}$. Moreover, the algorithm is perfectly parallelizable, running in polylogarithmic $O(log^c\ n)$ time in n processors. When $q = 2^k$, the polylogarithmic term $O(log^c\ n)$ is essentially just the cost of k additions and shifts on k-bit integers.
- Preimage sampling for $f_G(x) = Gx \ mod \ q$ with Gaussian parameter $s \geq \|\widetilde{S}\|.w\sqrt{(log\ n)}$ can be performed in quasilinear $O(nlog^c\ n)$ time, or parallel polylogarithmic $O(log^c n)$ time using n processors. When $q = 2^k$, the polylogarithmic term is essentially just the cost of k additions and shifts on k-bit integers, plus the (offline) generation of about m random integers drawn from $D_{Z,s}$.

3.2 $G \leftrightarrow A$

First matrix G is converted into semirandom matrix $A' = [\overline{A}|HG]$, where $\overline{A} \in Z_q^{n\times\overline{m}}$ is chosen at random and $H \in Z_q^{n\times n}$ is the desired tag. Now this semi random matrix A' is converted into random matrix A by applying random unimodular transformation $T = \begin{pmatrix} I & -R \\ O & I \end{pmatrix}$ where matrix $R \in Z^{\overline{m}\times w}$ is ”short” trapdoor matrix which is chosen from Gaussian distribution D.

$A = [\overline{A}|HG]\begin{pmatrix} I & -R \\ O & I \end{pmatrix} = [\overline{A}|HG - \overline{A}R]$

Definition 8. Let $A \in Z_q^{n\times m}$ and $G \in Z_q^{n\times w}$ be matrices $m \geq w \geq n$. A G-trapdoor for A is a matrix $R \in Z^{m-w)\times w}$ such that $A\begin{pmatrix} R \\ I \end{pmatrix} = HG$ for some invertible matrix $H \in Z_q^{n\times n}$. Matrix H is referred as the tag of the trapdoor.

3.3 f_A^{-1}, g_A^{-1} to f_{HG}^{-1}, g_{HG}^{-1}:

g_A^{-1} to g_{HG}^{-1}: Given a trapdoor of R for $A \in Z_q^{n\times m}$ and an LWE instance $b^t = s^tA + e^t \ mod \ q$ for some short error vector $e \in Z^m$. We compute $\widehat{b}^t = b^t\begin{pmatrix} R \\ I \end{pmatrix} = s^tA\begin{pmatrix} R \\ I \end{pmatrix} + e^t\begin{pmatrix} R \\ I \end{pmatrix} = s^t(HG) + e^t\begin{pmatrix} R \\ I \end{pmatrix}$.

If $e^t \begin{pmatrix} R \\ I \end{pmatrix}$ is in $[-q/4, q/4)$ then g_A^{-1} is reduced to g_{HG}^{-1}.

f_A^{-1} to f_{HG}^{-1}: For f_A^{-1}, given syndrome $u \in Z_q^n$, we sample a Gaussian z from $\Lambda_u^{\perp}(G)$ such that $HGz = u$. Now $A \begin{pmatrix} R \\ I \end{pmatrix} z = u$ and $\begin{pmatrix} R \\ I \end{pmatrix} z$ lies in $\Lambda_u^{\perp}(A)$. Since $G = A \begin{pmatrix} R \\ I \end{pmatrix}$ so $A \begin{pmatrix} R \\ I \end{pmatrix} z = u$ and $y = \begin{pmatrix} R \\ I \end{pmatrix} z$ lie in $\Lambda_u^{\perp}(A)$. However the distribution of y is non-spherical. This leaks information about the trapdoor R. This is corrected using convolution technique from Peikert [22]. Specifically, a Gaussian perturbation $p \in Z^m$ having covariance $s^2 - \begin{pmatrix} R \\ I \end{pmatrix} \sum_G [R^t I]$. Syndrome $v = u - Ap$ is adjusted. For this syndrome v, Gaussian z is sampled from $\Lambda_u^{\perp}(G)$ such that $Gz = v$. Now $A \begin{pmatrix} R \\ I \end{pmatrix} z = v$ and $y = \begin{pmatrix} R \\ I \end{pmatrix} z \in \Lambda_u^{\perp}(A)$. Distribution of y is non-spherical but distribution of $x = y + p$ is spherical and $Ax = u$. Output x.

4 Lattice Based Identity Based Proxy Re-Encryption Scheme in the Random Oracle Model

Our scheme is the extension of lattice based identity based encryption scheme of Gentry et al [15] and scheme of Xagawa et al [26].

Setup(n): On input a security parameter n, we set the parameters $q = poly(n)$ and $k = O(log\ q) = O(log\ n)$ accordingly. We choose one hash function $K : \{0,1\}^* \to Z_q^n$. We choose a Gadget matrix $G \in Z_q^{n \times m}$ with tag $H \in Z_q^{n \times n}$. Gadget matrix G is converted into random matrix $A \in Z_q^{n \times m}$ by $A = [\overline{A} | HG - \overline{A}R]$, where $\overline{A} \in Z_q^{n \times m}$ is chosen at random and R is "short" trapdoor matrix chosen from Gaussian distribution D. So master public key $mpk = A$ and master secret key $msk = R$.

Extract(mpk, R, id): Let $u = K(id_i)$ then return $sk_{id_i} =$ short vector $x \in \{0,1\}^{m \times 1}$ such that $Ax = u\ mod\ q$ (or $x \leftarrow f_A^{-1}(u)$).

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

- We choose $s \leftarrow Z_q^n$ uniformly.
- Compute $p = A^T s + e$, where $e \leftarrow \chi^m$. Here χ^m is error (Gaussian) distribution.
- Compute $c_{id_i} = u^T s + b\lfloor \frac{q}{2} \rfloor + \overline{e}$, where $\overline{e} \leftarrow \chi$. Here χ is error (Gaussian) distribution.
- Output the ciphertext $C_{id_i} = (p, c_{id_i}) \in (Z_q^m \times Z_q)$.

RKGen(PP, sk_{id_i}, sk_{id_j}): Outputs $rk_{i,j} = sk_{id_i} - sk_{id_j}$.

Re-Encrypt($PP, rk_{i,j}, C_{id_i}$): $(p, c_{id_i}) = C_{id_i}$. We compute

$$\begin{aligned} c_{id_j} &= c_{id_i} - rk_{i,j}^T p \\ &= u_{id_i}^T s + b\lfloor \frac{q}{2} \rfloor + \overline{e} - (sk_{id_i}^T - sk_{id_j}^T)(A^T s + e) \\ &= u_{id_j}^T s + b\lfloor \frac{q}{2} \rfloor + \overline{e}' \end{aligned}$$

where $\overline{e}' = \overline{e} - (sk_{id_i}^T - sk_{id_j}^T)e$.
New error $\overline{e}'$ may be greater than $\overline{e}$ but error after decrypting C_{id_j} will be around same as error after decrypting C_{id_i}.

Decrypt(PP, x_{id_j}, C_{id_j}): To decrypt $C_{id_j} = (p, c_{id_j})$, we do the following.

- We compute $b' = c_{id_j} - sk_{id_j}^T p$.
- If b' is closer to 0 than $\lfloor \frac{q}{2} \rfloor$ mod q output 0 otherwise output 1.

Correctness: $c_{id_j} - sk_{id_j}^T p = b\lfloor \frac{q}{2} \rfloor + \overline{e} - sk_{id_j}^T e$ and $c_{id_i} - sk_{id_i}^T p = b\lfloor \frac{q}{2} \rfloor + \overline{e}' - sk_{id_i}^T e$
Or $c_{id_j} - sk_{id_j}^T p = b\lfloor \frac{q}{2} \rfloor + \text{error}_1$ and $c_{id_i} - sk_{id_i}^T p = b\lfloor \frac{q}{2} \rfloor + \text{error}_2$. Since $\overline{e}, \overline{e}'$ and sk_{id} are short vectors so with proper choice of the parameters one can make error$_1$ and error$_2$ less than $q/4$ with high probability. Hence the above IB-PRE scheme is correct.

Above scheme can be extended to encrypt $k = poly(n)$ bits by the following two ways.

1. We can repeat the encryption for k bits. In this case for k different bits, we will have k different s values but with same public key u. Size of ciphertext $= O(k(mlog\ n + log\ n)) = \tilde{O}(km)$[1] and size of public key $= O(mlog\ n) = \tilde{O}(m)$.
2. We can include k independent syndroms $u_1, ..., u_k$ in the public key. Now we can use same s for encryption of all $k-$ bits. In this case size of the ciphertext $= O(mlog\ n + klog\ n) = \tilde{O}(k+m)$ and size of public key $= O(kmlog\ n) = \tilde{O}(km)$[15]. Based on this, we present multi-bit proxy re-encryption scheme in next section.

So there is trade-off between size of the ciphertext and size of the public key to encrypt multi bit.

Theorem 3. If hash function K is modeled as random oracle, then lattice based identity based proxy scheme is IND-pID-CPA (semantic) secure assuming the $LWE_{q,\chi}$ is hard or $Adv_{B,LWE_{q,\chi}}(n) = Adv_{\chi,A}(n)$.

Proof: Here proof is similar to proof of theorem 7.2 of [15] and proof of theorem 15.3.3 of [26].
We now show semantic security of IB-PRE in the random oracle model. We will show that if there exist a PPT adversary $\mathscr{A}$ that breaks IB-PRE scheme with non-negligible probability then there must exist a PPT challenger $\mathscr{B}$ that solves LWE hard problem with non-negligible probability by simulating views of $\mathscr{A}$. Here CU denotes set of users for which adversary has made private key query (corrupted users) and HU denotes set of users for which adversary has not made private key query (honest users). For our proof, we make following assumptions.

1. We assume that for CU, adversary will directly ask (not like hash then private key query) private key query and challenger will return private key with hash of the identity of the user.
2. For HU, adversary will ask only hash query of the identity of the user.

Challenger (adversary $\mathscr{B}$) sets the master public key $mpk = A$ and a public key $u^* \in Z_q^*$ for IB-PRE. Challenger $\mathscr{B}$ chooses an index $i \leftarrow [Q_{hash}]$ uniformly at random and simulates the views of $\mathscr{A}$ as follows.

[1] A function $g(n)$ is in $\tilde{O}(f(n))$ if there exist constants $a, c \geq 0$ such that $g(n) \leq af(n)log^c f(n)$ for all sufficiently large n

- Hash Queries: We describe how challenger $\mathscr{B}$ answers the hash queries of the adversary for honest users. When adversary asks first hash query on id_1, challenger generates $h_1 \leftarrow Z_q^n$ uniformly. Adversary returns h_1 to the adversary and stores (id_1, h_1) in a hash table (UHT). Now challenger generates re-encryption key $r_{1\to j} \in Z_q^m$ for $j = 2, ..., Q$ and stores in re-encryption table. When adversary asks second hash query on id_2, challenger will return $h_2 = h_1 - Ar_{1\to 2}$ and store (id_2, h_2) in UHT. Subsequently when adversary asks i^{th} hash query, challenger will return $h_i = h_1 - Ar_{1\to i}$ and stores (id_i, h_i) in UHT.

- Whenever A submits a user secret key query for identity $id_j \in CU$, challenger $\mathscr{B}$ randomly choose a short vector e_j from Gaussian distribution D and computes $u_j = Ae_j$. Challenger $\mathscr{B}$ returns e_j as secret key and u_j as hash value of the identity id_j and stores the tuple (id_j, u_j, e_j) in key table (KT).

- Challenger $\mathscr{B}$ answers the re-encryption key query for the the identities in two ways.

  1. Whenever A submits a re-encryption key query for the the identities id_j and id_k such that $id_j, id_k \in HU$, challenger $\mathscr{B}$ retrieves the values $r_{1\to i}$ and $r_{1\to j}$ from re-encryption table and returns $r_{i\to j} = r_{1\to j} - r_{1\to i}$ to adversary $\mathscr{A}$.
  2. Whenever A submits a re-encryption key query for the the identities id_j and id_k such that $id_j, id_k \in CU$, challenger $\mathscr{B}$ retrieves the values e_j and e_k from table KT and return $e_j - e_k$ to the adversary $\mathscr{A}$.

Challenge ciphertext: Now adversary $\mathscr{A}$ produces a challenge identity id^* and message m. Challenger $\mathscr{B}$ will retrieve the hash value u^* of challenge identity id^* from table UHT. Since matrix A and vector u^* are statistically close to uniform, so $(A, p = A^T s + x)$ simply consists of m samples from LWE and $c^* = u^* s + \bar{x}$ is one LWE sample.
Challenger $\mathscr{B}$ obtains the m LWE samples from LWE oracle for matrix A and which is parsed as $(A, p = A^T s + x)$. Similarly $\mathscr{B}$ again obtains the *one* LWE sample from LWE oracle for matrix u^* and is parsed as $(u^*, c = u^* s + x)$. Now challenger $\mathscr{B}$ computes $c^* = c + b\lfloor \frac{q}{2} \rfloor$ and sends $C^* = (p, c^*)$ to adversary $\mathscr{A}$.

Phase 2: Adversary can ask query with some restriction same as in phase one.

Now adversary $\mathscr{A}$ outputs that challenged ciphertext is a valid ciphertext then challenger will output that oracle O as pseudo-random LWE oracle. If adversary $\mathscr{A}$ outputs random ciphertext then adversary will output random LWE oracle. In other words if adversary $\mathscr{A}$ terminates with some output then challenger $\mathscr{B}$ terminates with same output and ends the simulation. So if adversary $\mathscr{A}$ breaks the scheme then there exists challenger $\mathscr{B}$ which solves LWE hard problem.
$Adv_{B, LWE_{q,\chi}}(n) = Adv_{\chi, A}(n)$. Hence our scheme is semantically secure.

5 Lattice Based Identity Based Multi-bit Proxy Re-encryption Scheme in the Random Oracle Model

We can include l independent syndroms $u_1, \ldots, u_l$ in the public key. Now we can use same s for encryption of all l- bits. In this way size of the ciphertext is less than l times the size of the ciphertext for single bit but size of the public key is l-times size of the public key for single bit.

Setup(n): On input a security parameter n, we set the parameters $q = poly(n)$ and $k = O(log\ q) = O(log\ n)$ accordingly. We choose one hash function $K : \{0,1\}^* \to Z_q^{n\times l}$ where l is the message length. We choose a Gadget matrix $G \in Z_q^{n\times m}$ with tag $H \in Z_q^{n\times n}$. Gadget matrix G is converted into random matrix $A \in Z_q^{n\times m}$ by $A = [\overline{A}|HG - \overline{A}R]$, where $\overline{A} \in Z_q^{n\times m}$ is chosen at random and R is "short" trapdoor matrix chosen from Gaussian distribution D. So master public key $mpk = A$ and master secret key $msk = R$.

Extract(mpk, R, id): Let $U = (u_1,\dots,u_l) = K(id_i) \in Z_q^{n\times l}$ then secret key SK_{id} corresponding to the identity id is collection of l short column vector x_i's such that $Ax_i = u_i\ mod\ q$ for all $1 \le i \le l$ (or $x \leftarrow f_A^{-1}(u_i)$). Return $SK_{id} \in Z_q^{m\times l}$.

Encrypt(mpk, id_i, b): To encrypt a message $m \in \{0,1\}^l$, we do the following.

- We choose $s \leftarrow Z_q^n$ uniformly.
- Compute $p = A^T s + e$, where $e \leftarrow \chi^m$. Here χ^m is error (Gaussian) distribution.
- Compute $c_{id_i} = U^T s + m\lfloor \frac{q}{2} \rfloor + \overline{e}$, where $\overline{e} \leftarrow \chi^l$. Here χ^l is error (Gaussian) distribution.
- Output the ciphertext $C_{id_i} = (p, c_{id_i}) \in (Z_q^m \times Z_q^l)$.

RKGen(PP, SK_{id_i}, SK_{id_j}): Outputs $RK_{i,j} = SK_{id_i} - SK_{id_j}$.

Re-Encrypt($PP, RK_{i,j}, C_{id_i}$): $(p, c_{id_i}) = C_{id_i}$. We compute

$$\begin{aligned} c_{id_j} &= c_{id_i} - RK_{i,j}^T p \\ &= U_{id_i}^T s + m\lfloor \frac{q}{2} \rfloor + \overline{e} - (SK_{id_i}^T - SK_{id_j}^T)(A^T s + e) \\ &= U_{id_j}^T s + m\lfloor \frac{q}{2} \rfloor + \overline{e}' \end{aligned}$$

where $\overline{e}' = \overline{e} - (SK_{id_i}^T - SK_{id_j}^T)e$.
New error $\overline{e}'$ may be greater than $\overline{e}$ but error after decrypting C_{id_j} will be around same as error after decrypting C_{id_i}.

Decrypt(PP, SK_{id_j}, C_{id_j}): To decrypt $C_{id_j} = (p, c_{id_j})$, we do the following.

- We compute $b = c_{id_j} - SK_{id_j}^T p \in Z_q^{1\times l}$. We parse b as $b_1,\dots,b_l$.
- If b_i is closer to 0 than $\lfloor \frac{q}{2} \rfloor$ mod q then $b_i = 0$ else $b_i = 1$.
- Output $b = b_1,\dots,b_l$.

Theorem 4. If hash function K is modeled as random oracle, then lattice based identity based multi-bit proxy scheme is IND-pID-CPA (semantic) secure assuming the $LWE_{q,\chi}$ is hard or $Adv_{B,LWE_{q,\chi}}(n) = Adv_{\chi,A}(n)$.

Proof: Here proof is similar to proof of previous theorem 3.

6 Conclusion

In some cases adversary already may have private keys of users ID's of his choice. So security must be strengthened a bit. Security must allow the adversary to obtain the private key associated with any identity ID of his choice then adversary can declare the identity to be challenged. The scheme which is secure against this kind of attack is called adaptive-ID (IND-pID-CPA) secure scheme [8]. We have proved our scheme to be semantically secure in adaptive-ID (IND-pID-CPA). Construction of adaptively secure lattice-based unidirectional proxy re-encryption scheme in the context of public key encryption as well as in the identity based encryption is an open problem.

Acknowledgments.

We would like to thank anonymous reviewers for their useful comments.

References

[1] Shweta Agrawal, Dan Boneh, and Xavier Boyen. Efficient Lattice (H)IBE in the Standard Model. In *Proc. of the 29th Annual international conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT'10), French, Riviera, LNCS*, volume 6110, pages 553–572. Springer-Verlag, May-June 2010.

[2] Shweta Agrawal and Xavier Boyen. Identity-Based Encryption from Lattices in the Standard Model. `http://www.cs.stanford.edu/~xb/ab09/`, July 2009.

[3] Miklos Ajtai. Generating hard instances of lattice problems (extended abstract). In *Proc. of the 28th Annual ACM symposium on Theory of computing (STOC'96), Philadelphia, Pennsylvania, USA*, pages 99–108. ACM, May 1996.

[4] Benny Applebaum, David Cash, Chris Peikert, and Amit Sahai. Fast Cryptographic Primitives and Circular-Secure Encryption Based on Hard Learning Problems. In *Proc. of the 29th Annual International Cryptology Conference (CRYPTO'09), Santa Barbara, California, USA, LNCS*, volume 5677, pages 595–618. Springer-Verlag, August 2009.

[5] Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage. *ACM Transactions on Information and System Security (TISSEC)*, 9(1):1–30, February 2006.

[6] Rachid El Bansarkhani and Johannes Buchmann. Improvement and Efficient Implementation of a Lattice-based Signature Scheme. In *Proc. of Selected Areas in Cryptography 2013 (SAC'13), Simon Fraser University, Burnaby, British Columbia, Canada*, August 2013.

[7] Mate Blaze, G. Bleumer, and M. Strauss. Divertible protocols and atomic proxy cryptography. In *Proc. of the 1998 International Conference on the Theory and Application of Cryptographic Techniques (Eurocrypt'98), Espoo, Finland, LNCS*, volume 1403, pages 360–363. Springer-Verlag, May-June 1998.

[8] Dan Boneh and Matthew K. Franklin. Identity Based Encryption From the Weil Pairing. In *Proc. of the 21st Annual International Cryptology Conference on Advances in Cryptology (CRYPTO'01), Santa Barbara, California, USA, LNCS*, volume 2139, pages 213–229. Springer-Verlag, August 2001.

[9] Ran Canneti and Susan Hohenberger. Chosen-Ciphertext Secure Proxy Re-Encryption. In *Proc. of the 14th ACM conference on Computer and communications security (ACM CCS'07), Alexandria, Virginia, USA*, pages 185–194. ACM, October-November 2007.

[10] David Cash, Dennis Hofheinz, and Eike Kiltz. How to Delegate a Lattice Basis. Cryptology ePrint Archive, Report 2009/351, 2009. `http://eprint.iacr.org/`.

[11] Cheng-Kang Chu and Wen-Guey Tzeng. Identity-Based Proxy Re-Encryption Without Random Oracles. In *Proc. of the 10th International Conference on Information Security (ISC'07), Valparaíso, Chile, LNCS*, volume 4779, pages 189–202. Springer-Verlag, October 2003.

[12] Clifford Cocks. An Identity Based Encryption Scheme Based on Quadratic Residues. In *Proc. of the 8th IMA International Conference on Cryptography and Coding, Cirencester, UK, LNCS*, volume 2260, pages 360–363. Springer-Verlag, December 2001.

[13] D.Micciancio and S.Goldwasser. *Complexity of Lattice Problems: A Cryptographic Perspective*, volume 671. Kluwer Academic Publishers, 2002.

[14] Yevgenity Dodis and Anca Ivan. Proxy cryptography revisited. In *Proc. of the 10th Annual Network and Distributed System Security Symposium (NDSS'03), San Diego, California, USA*. The Internet Society, February 2003.

[15] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proc. of the 40th annual ACM symposium on Theory of computing (STOC'08), Victoria, British Columbia, Canada*, pages 197–206. ACM, May 2008.

[16] Matthew Green and Giuseppe Ateniese. Identity-Based Proxy Re-Encryption. In *Proc. of the 5th international conference on Applied Cryptography and Network Security (ACNS'07), Zhuhai, China, LNCS*, volume 4521, pages 288–306. Springer-Verlag, June 2007.

[17] Xiaoming Hu, Xu Chen, and Shangteng Huang. Fully Secure Identity Based Proxy Re-Encryption Schemes in the Standard Model. In *Proc. of the 2008 International Conference on Computer Science and Information Technology (ICCSIT'08), Singapore, Singapore)*, pages 53–57. IEEE, August-September 2008.

[18] Richard Lindner and Chris Peikert. Better key sizes (and attacks) for LWE-based encryption. In *Proc. of the 11th International Conference on Topics in Cryptology (CT-RSA'11), San Francisco, California, USA, LNCS*, volume 6558, pages 319–339. Springer-Verlag, February 2011.

[19] Toshihiko Matsuo. Proxy Re-encryption Systems for Identity-Based Encryption . In *Proc. of The 1st International Conference on Pairing-based Cryptography (Pairing'07), Tokyo, Japan, LNCS*, volume 4575, pages 247–267. Springer-Verlag, July 2007.

[20] Daniele Micciancio and Chris Peikert. Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller. In *Proc. of the 21st Annual Eurocrypt Conference (Eurocrypt'02), Amsterdam, The Netherlands, LNCS*, volume 7237, pages 700–718. Springer-Verlag, April-May 2012.

[21] Chris Peikert. Bonsai Trees (or, Arboriculture in Lattice-Based Cryptography). Cryptology ePrint Archive, Report 2009/359, 2009. `http://eprint.iacr.org/`.

[22] Chris Peikert. An efficient and parallel gaussian sampler for lattices. In *Proc. of the 30th annual Aonference on Advances in Cryptology (CRYPTO'10), Santa Barbara, California, USA, LNCS*, pages 80–92. Springer-Verlag, August 2010.

[23] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proc. of the 37th annual ACM symposium on Theory of computing (STOC'05), Baltimore, Maryland, USA*, pages 84–93. ACM, May 2005.

[24] Adi Shamir. How to share a secret. 22(11):612–613, November 1979.

[25] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. 26(5):1484–1509, October 1997.

[26] Keita Xagawa. *Cryptography with Lattices*. PhD thesis, Department of Mathematical and Computing Sciences, Tokyo Institute of Technology, 2010.

Author Biography

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 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 is a Professor in the 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.