Lattice Based Universal Re-encryption for Mixnet

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

Mixnet (Mix Network) was proposed by David Chaum [3] for anonymous communication in 1981. A mixnet is a multistage system that accepts encrypted messages under the public keys of all intermediate mixnet nodes and outputs randomly permuted corresponding plaintexts.
In 2004, Golle et al [10] presented a new primitive called universal re-encryption based on the Elgamal public key cryptosystem. Universal mixnet based on universal re-encryption takes the input as encrypted messages under the public key of the recipients not the public key of the universal mixnet so it dispenses with the complexities of the key generation, key distribution and key maintenance. In Eurocrypt 2010 Gentry, Halevi and Vaikunthanathan [9] presented a cryptosystem which is an additive homomorphic and a multiplicative homomorphic for only one multiple. In this paper we present universal re-encryption scheme under learning with error (LWE) assumption based on [9].

Keywords: Lattice, Learning With Error (LWE), Universal Re-encryption

1 Introduction

Mixnet (mix network) was proposed by David Chaum [3] for anonymous communication in 1981. A mixnet is a multistage system that accepts encrypted messages under the public keys of all intermediate mixnet nodes and outputs randomly permuted corresponding plaintexts. Each mixnet node changes the appearance of its inputs by decrypting them (removing the layer of encryption) and permutes them before forwarding to the next node. In this way adversary will find hard to guess which input ciphertext corresponds to output ciphertext. More efficient mixnet based on decryption is proposed in [4] using the Elgamal public key cryptosystem [7].
Park et al [4] proposed another variety of mixnet known as a re-encryption mixnet based on the Elgamal public key cryptosystem [7]. A re-encryption mixnet accepts the encrypted massages under the public key of the mixnet. The private key corresponding to the public key of the mixnet is held in distributed form among all re-encryption mixnet nodes. Each re-encryption mixnet node change the appearance of input ciphertexts by re-encrypting them with random string and outputs the re-encrpted ciphertexts in random order. Ciphertext C and re-encrypted ciphertext C' both decrypt to the same plaintext. Set of ciphertexts produced by last re-encryption mixnet node is decrypted by group of t nodes using a (t,n) threshold scheme. For privacy it is required that adversary can not distinguish the ciphertext pair (C,C') from the pair (C,R) for a random ciphertext R with size same as the size of the ciphertext C'.
In 2004, Golle et al [10] presented a new primitive called universal re-encryption based on the Elgamal public key cryptosystem [7]. Universal mixnet is a mixnet based on universal re-encryption which takes

Journal of Internet Services and Information Security (JISIS), volume: 4, number: 1, pp. 1-11

*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/

the input as encrypted messages under the public key of the recipients not the public key of the universal mixnet. Even there is no term like the public key of the universal mixnet. Each universal mixnet node universally re-encrypts these ciphertext and permute them before sending to the next node. Input ciphertext to the universal mixnet node and output ciphertext of the node decrypt to the same plaintext. Finally outputs from the universal mixnet is set of universal re-encrypted ciphertexts. Potential receiver must perform to decrypt all the ciphertexts to identify messages sent for them. This is a disadvantage of the universal re-encryption. A number of constructions of universal re-encryption scheme is known [8, 5]. Advantage of universal re-encryption mixnet over the other mixnets is as follows.

- In universal mixnet, public key of the universal mixnet is not required. So it dispenses with the complexities of the key generation, key distribution and key maintenance.

- If we make assumption that universal mixnet nodes do not store the permutation of the ciphertexts and re-encryption factors used by them then universal mixnet provides perfect forward anomity.

Once quantum computer comes into reality, all the cryptosystem based on prime factorization and discrete logarithm problem can be solved in polynomial time by Shor's algorithm [14]. Lattice based hard problems are conjectured to remain secure against quantum computers. Since Ajtai's seminal result [1] on the average case / worst case equivalence, lattice based cryptogrphy has become attractive research area. Recently Regev [12] 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.

Our Contribution: Idea for universal re-encryption is simple: In an additive homomorphic cryptosystem we append a second ciphertext (encryption of zero) to the ciphertext. Since in an additive homomorphic $E(M+0) = E(M) + E(0)$, so we can use the second ciphertext to re-encrypt (change the encryption factor) the first ciphertext such that the re-encrypted ciphertext and the ciphertext decrypt to the same plaintext.

In Eurocrypt 2010 Gentry, Halevi and Vaikunthanathan [9] presented a cryptosystem which is an additive homomorphic and a multiplicative homomorphic for only one multiple. To the best of our knowledge, there does not exist any lattice based universal re-encryption (URe) scheme. In this paper we propose lattice based universal re-encryption (URe) scheme under LWE assumption based on [9].

Paper Outline: Our paper is organized as follows. In section 2, we describe basic definitions, security models, results and hard problems required to understand rest of the paper. Since our scheme is based on Gentry et al scheme [9] so in section 3, we describe GHV public key cryptosystem [9]. In section 4, we describe our scheme. In section 5 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 in column form and are written using small letters, e.g. x. Matrices are written as capital letters, e.g. X. $\|S\|$ 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 Universal Re-encryption Scheme (URe)

Here definition of URe is similar to [10]. System parameters include message space M, ciphertext space $\mathbf{C}$, and set of encryption factors R. Universal Re-Encryption Scheme consists of four algorithms.

Universal KeyGen(n): On input a security parameter n, outputs the public key pk and secret key sk pair.

Universal Encryption(pk, m, r): On input public key pk, a message $m \in M$ and an encryption factor $r \in R$, and outputs a ciphertext $C \in \mathbf{C}$.

Universal Decryption(C, sk): On input a secret key sk, and a ciphertext C outputs message m.

Universal Re-Encryption(C, r): On input a ciphertext C and re-encryption factor $r \in R$, but no public key outputs ciphertext C' where $C' \in \mathbf{C}$.

2.3 Universal Semantic Security Model for Universal Re-encryption Scheme (IND-URe-CPA)

Universal semantic security model is adapted from [10]. Universal security model is variant of semantic security model. In this model, adversary is allowed to construct universal ciphertexts under randomly generated public key pk. The challenger re-encrypts the ciphertext. The goal of the adversary is to distinguish between the re-encrypted ciphertext and the random ciphertext with the same size as the size of the re-encrypted ciphertext. Here we define security model using a game that is played between the challenger and the adversary. The game proceeds as follows.

KeyGen: The challenger runs the key generation algorithm and gives public parameters to the adversary.

Challenger: The adversary submits message $m \in M$ and $r \in R$ (adversary can construct ciphertext). Challenger sets $C \leftarrow \text{Universal Encryption}(m, r, pk)$ and picks a random bit $b \in \{0, 1\}$ and a random ciphertext C with same size as size of the universal re-encrypted ciphertext. If $b = 0$ it sets the challenge ciphertext to $C^* = \text{Universal Re-encryption}(C, r')$. If $b = 1$ it sets the challenge ciphertext to $C^* = C$. Challenger sends C^* as challenge to the adversary.

Guess: The adversary outputs a guess $b' \in \{0, 1\}$, it succeeds if $b' = b$.

We refer an adversary $\mathscr{A}$ as an IND-URe-CPA adversary. We define the advantage of the adversary $\mathscr{A}$ in attacking universal re-encryption scheme ξ as $Adv_{\xi, A}(n) = |Pr[b = b'] - 1/2|$.

Definition 1. We say that universal re-encryption scheme ξ is universal semantic secure if for all IND-URe-CPA PPT adversaries A we have $Adv_{\xi, A}(n)$ is a negligible function.

2.4 Universal Semantic Security Model for Identity based Universal Re-encryption Scheme (IND-URe-ID-CPA)

Security model is similar to security model in section 2.3. In this model, adversary constructs universal ciphertext under randomly generated identity id. The challenger re-encrypts the ciphertext. The goal of the adversary is to distinguish between the re-encrypted ciphertext and random ciphertext with same size as the size of re-encrypted ciphertext. Security model is explained using following game.

KeyGen: The challenger runs the key generation algorithm and gives public parameters to adversary.

KeyExtrction: Adversary can make extraction query on any identity $id \neq id^*$

Challenger: The adversary submits message $m \in M$ and $r \in R$ (adversary can construct ciphertext). Challenger sets $C \leftarrow$ Universal encryption(m, r, id) and picks a random bit $b \in \{0, 1\}$ and a random ciphertext C with size same as size of universal re-encrypted ciphertext. If $b = 0$ it sets the challenge ciphertext to $C^* =$ Universal Re-encryption(C, r'). If $b = 1$ it sets the challenge ciphertext to $C^* = C$. Challenger sends C^* as challenge to the adversary.

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

Definition 2. We say that identity based universal re-encryption scheme ξ is universal semantic secure if for all IND-URe-ID-CPA PPT adversaries A we have $Adv_{\xi,A}(n)$ is a negligible function.

2.5 Integer Lattices ([6])

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 3. 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$(s_1, ..., s_i)$ where $2 \leq i \leq k$. Since $\widetilde{s_i}$ is the component of s_i so $\|\widetilde{s_i}\| \leq \|s_i\|$ for all i.
We refer to $\widetilde{\|S\|}$ as the Gram-Schmidt norm of S.

2.7 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 $t \in Z^m$.

Theorem 1 ([1, 11]) 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 $(A \in Z_q^{n \times m}, T \in Z^{n \times m})$ such that A is statistically close to a uniform matrix in $Z_q^{n \times m}$ and T is a basis for $\Lambda_q^{\perp}(A)$ satisfying

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

with all but negligible probability in n.

Lemma 1 (Lemma 7.1 of [6]) 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

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

.

2.8 The LWE Hardness Assumption ([12, 15])

The LWE (learning with error) hardness assumption is defined by Regev [12].

Definition 4. 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 5. 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 the 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 [2, 13].

Definition 6. Consider a real parameter $\beta = \beta(n) \in \{0,1\}$ and a prime q. Denote by $T = R/Z$ the group of reals [0,1) with addition modulo 1. Denote by ψ_β the distribution over T of a normal variable with mean 0 and standard deviation $\beta/\sqrt{2\pi}$ 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 $\overline{\psi}_\beta$ the discrete distribution over Z_q of the random variable $\lfloor qX \rceil$ mod q where the random variable $X \in T$ has distribution ψ_β.

Theorem 2 ([12]). 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 ([1])

SIS and ISIS hard problems were proposed by Ajtai [1] in 1996.

Definition 7. 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 8. 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 Gentry, Halevi and Vaikunthanathan (GHV) Cryptosystem ([9])

Our scheme is based on GHV cryptosystem [9] which is additive homomorphic and multiplicative homomorphic for one multiplication. We briefly describe the GHV homomorphic cryptosystem [9]. Here message space is the set of binary m-by-m matrices, i.e. $M \in Z_2^{m\times m}$ and ciphertex space is the set of m-by-m matrices, i.e. $C \in Z_q^{m\times m}$.

KeyGen(n): On input a security parameter n, we set the parameter $q =$ poly(n), $m = O(n \ log \ q)$ and a Gaussian distribution $\psi_\beta(q)_q^{m\times m}$ with Gaussian error parameter $\beta = 1/poly(n)$. We run the trapdoor sampling algorithm TrapGen of Theorem 1 to obtain a matrix $A \in Z_q^{m\times n}$ together with the trapdoor $T \in Z^{m\times m}$. The public key is A and the secret key is T.

Encrypt$(A, M \in \{0,1\}^{m\times m})$**:** To encrypt message $M \in \{0,1\}^{m\times m}$, do the following.

1. Choose a uniformly random matrix $S \leftarrow Z_q^{n\times m}$ and an error matrix $X \leftarrow \psi_\beta(q)_q^{m\times m}$.
2. Output the ciphertext
$$C = AS + 2X + M \ (mod\ q)$$

Decrypt$(T, C:)$ To decrypt C, do the following.

1. Set $E = TCT^t\ mod\ q$.
2. Output the matrix $B = T^{-1}E(T^t)^{-1}\ mod\ q$.

Correctness: Since $T.A = 0$ therefore $E = TCT^t = T(2X+M)T^t\ mod\ q$. Now if $T(2X+M)T^t\ mod\ q$ is equal to $T(2X+M)T^t$ then $T^{-1}ET\ mod\ q = M$. So for correct decryption one has to set the parameter β small enough so that all the entries of $T(2X+M)T^t$ are smaller than $q/2$ with high probability.

Additive Homomorphic: Let $C_1 = AS_1 + 2X_1 + M_1$ and $C_2 = AS_2 + 2X_2 + M_2$ be ciphertexts for messages M_1 and M_2 under public key A. Then

$$C = C_1 + C_2 = A(S_1+S_2) + 2(X_1+X_2) + M_1 + M_2$$

would be decrypted to $M_1 + M_2$ as long as all the entries in $T(2(X_1+X_2)+M_1+M_2)T^t$ are smaller than $q/2$.

Multiplicative Homomorphic: The product of C_1 and C_2 is

$$\begin{aligned} C &= C_1.C_2^t \\ &= (AS_1 + 2X_1 + M_1).(AS_2 + 2X_2 + M_2)^t \\ &= A.(S_1C_2^t) + 2.(X_1(2X_2+M_2) + M_1X_2^t) + M_1M_2^t + (2X_1+M_1)S_2^t.A^t \end{aligned}$$

Product ciphertext C has the form $AS + 2X + M + S'A^t$. Ciphertext would be decrypted to $M_1.M_2$ as long as all the entries in $T(2X+M)T^t$ are smaller than $q/2$.

Theorem 3([9]) For the security parameter n and any $c = c(n) > 0$. Let q, m, β be set as

$$\begin{aligned} q &> 2^{20}(c+4)^3 n^{3c+4} Log^5\ n,\ \ q \text{ is a prime} \\ m &= \lfloor 8n\ log\ q \rfloor \\ \beta &= \frac{1}{27n^{1+(3c/2)} log\ n\ log\ q\ \sqrt{qm}} \end{aligned}$$

Then the encryption scheme from above with parameters n, m, q, β supports n^c additions and one multiplication (in any order) over the matrix ring $Z_2^{m\times m}$.

For our scheme we will use variant of GHV cryptosystem which is only additive homomorphic. For this variant decryption algorithm will not have right multiplication of T^t.

4 Universal Re-encryption

Our scheme is based on GHV cryptosystem which is explained in section 3.1.
Idea for universal re-encryption is to append second ciphertext (encryption of zero) to GHV cryptosystem ciphertext. Since GHV public key cryptosystem is additive homomorphic i.e. $(E(M+0) = E(M) + E(0))$ so we can use the second ciphertext to re-encrypt (change the encryption factor) the first ciphertext such that re-encrypted ciphertext and ciphertext decrypt to same plaintext.

Universal KeyGen(n): On input a security parameter n, we set the parameter $q = \text{poly}(n)$, $m = O(n\ log\ q)$ and a Gaussian distribution $\psi_\beta(q)_q^{m\times m}$ with Gaussian error parameter $\beta = 1/poly(n)$. We run the trapdoor sampling algorithm TrapGen of Theorem 1 to obtain a matrix $A \in Z_q^{m\times n}$ together with the trapdoor $T \in Z^{m\times m}$. The public key is A and the secret key is T.

Universal Encryption(A, M): To encrypt message $M \in \{0,1\}^{m\times m}$, we do the following.

- We choose uniformly random matrices $S_1, S_2 \leftarrow Z_q^{n\times m}$ and error matrices $X_1, X_2 \leftarrow \psi_\beta(q)_q^{m\times m}$.
- Compute $C_1 = AS_1 + 2X_1 + M \in Z_q^{m\times m}$ and $C_2 = AS_2 + 2X_2 + 0^{m\times m}(\text{zero matrix}) \in Z_q^{m\times m}$.
- Output the ciphertext $C = (C_1, C_2)$.

Universal Decryption($T, C = (C_1, C_2)$): To decrypt C, we do the following.

- Set $E_1 = TC_1$.
- Compute $M_1 = T^{-1}E_1\ mod\ 2$.
- Similarly set $E_2 = TC_2$.
- Compute $M_2 = T^{-1}E_2\ mod\ 2$.
- If $(M_2 = 0^{m\times m})$ then output message $M = M_1$. Otherwise decryption fails and output is $\perp$.

Universal Re-encryption($C = (C_1, C_2)$): To re-encrypt ciphertext $C = (C_1, C_2)$ without using public key, we do the following.

- Choose two matrices $R_1, R_2 \leftarrow \psi_\beta(q)_q^{m\times m}$. We also choose error matrices $X_3, X_4 \leftarrow \psi_\beta(q)_q^{m\times m}$.
- Compute

$$\begin{aligned} C_1' &= C_1 + C_2R_1 + 2X_3 \\ &= (AS_1 + 2X_1 + M) + (AS_2 + 2X_2 + 0^{m\times m})R_1 + 2X_3 \\ &= A(S_1 + S_2R_1) + (2(X_1 + X_2R_1) + 2X_3) + M \end{aligned}$$

- Compute

$$\begin{aligned} C_2' &= C_2R_2 + 2X_4 \\ &= (AS_2 + 2X_2 + 0^{m\times m})R_2 + 2X_4 \\ &= AS_2R_2 + 2X_2R_2 + 0^{m\times m} + 2X_4 \end{aligned}$$

- Output the ciphertext $C' = (C_1', C_2')$.

It is required that above universal re-encryption scheme has the correctness property, i.e, decryption of C' and decryption of C gives the same message M. It is only possible when all the entries in $T2(X_1 + X_2R_1) + 2X_3 + M$ and $2X_2R_2 + 2X_4 + 0^{m\times m}$ are less than $q/2$. Since X_1, X_2, X_3, X_4, R_1 and R_2 are small, so we can set parameter β small enough so that with the high probability all the entries in $T2(X_1 + X_2R_1) + 2X_3 + M$ and $2X_2R_2 + 2X_4 + 0^{m\times m}$ are less than $q/2$.

Theorem 4. Lattice based universal re-encryption scheme is IND-URe-CPA (semantic) secure assuming the $LWE_{q,\chi}$ is hard or $Adv_{B,LWE_{q,\chi}}(n) = Adv_{\chi,A}(n)$.

Proof: We now show universal semantic security of the universal re-encryption scheme. We will show that if there exists a PPT adversary $\mathscr{A}$ that breaks universal re-encryption scheme with non-negligible probability then there must exist a PPT challenger $\mathscr{B}$ that solves decision LWE hard problem with non-negligible probability by simulating views of A.

Adversary $\mathscr{A}$ constructs the ciphertext $C = (C_1, C_2)$ for message m and sends to the challenger $\mathscr{B}$. Since ciphertext C_2 is statistically close to uniform, so challenger $\mathscr{B}$ obtains m LWE samples (for vector r_1), m LWE samples (for vector r_2),...,m LWE samples (for vector r_m) where vectors $r_1, r_2, \ldots, r_m$ are from Gaussian (error) distribution ψ^m and matrix $R_1 = [r_1 \ldots r_m]$. It parsed as $C_2R_1 + 2X_3$ then challenger computes $C'_1 = C_2R_1 + 2X_3 + C_1$. Similarly Challenger again obtains m LWE samples (for vector r'_1), m LWE samples (for vector r'_2) ... m LWE samples (for vector r'_m) where vectors $r'_1, r'_2, \ldots, r'_m$ are from Gaussian (error) distribution ψ^m and matrix $R_2 = [r'_1 \ldots r'_m]$. It parsed as $C_2R_2 + 2X_4$ then challenger assigns $C'_2 = C_2R_2 + 2X_4$. Here matrices $X_3, X_4 \leftarrow \psi_\beta(q)_q^{m\times m}$.

Challenger $\mathscr{B}$ sends $C^* = (C'_1, C'_2)$ to the adversary $\mathscr{A}$.

When Oracle O is a pseudo-random LWE oracle then C^* is a valid universal re-encryption of ciphertext C. When Oracle O is a random oracle then C^* is a uniform.

Finally adversary $\mathscr{A}$ terminates with some output, challenger $\mathscr{B}$ terminates with same output and ends the simulation. So if adversary $\mathscr{A}$ breaks the scheme then there exist challenger $\mathscr{B}$ which solves decision LWE hard problem.

$Adv_{B,LWE_{q,\chi}}(n) = Adv_{\chi,A}(n)$. Hence our scheme is universal semantic secure.

5 Conclusion

We have proved our scheme to be universal semantically secure. In our scheme receiver has to decrypt all the ciphtexts to identify message for him. A lattice based universal re-encryption scheme improving this cost in receiver side is an open problem.

Acknowledgments

We would like to thank one of the anonymous reviewers for pointing out a mistake in our scheme.

References

[1] M. 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 Press, January 1996.

[2] B. Applebaum, D. Cash, C. Peikert, and A. Sahai. Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In *Proc. of the 29th Annual International Cryptology Conference*

on Advances in Cryptology (CRYPTO'09), California, USA, LNCS, volume 5677, pages 595–618. Springer-Verlag, August 2009.

[3] D. Chaum. Untraceable electronic mail,return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–88, February 1981.

[4] K. K. Choonsik Park, Kouichi Itoh. Efficient anonymous channel and all/nothing election scheme. 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.

[5] G. Danezis. Breaking four mix-related schemes based on universal re-encryption. In *Proc. of the 9th International Conference of Information Security (ISC'06), Samos Island, Greece, LNCS*, volume 4176, pages 46–59. Springer-Verlag, August–September 2006.

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

[7] T. Elgamal. A public-key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4):469–472, July 1985.

[8] P. Fairbrother. An improved construction for universal re-encryption. In *Proc. of the 4th international conference on Privacy Enhancing Technologies (PET'04), Toronto, Canada, LNCS*, volume 3424, pages 79–87. Springer-Verlag, January 2004.

[9] V. Gentry, Halevi. A simple bgn-type cryptosystem from lwe. In *Proc. of the 29th Annual international conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT'10), French Riviera, LNCS*, volume 6110, pages 506–522. Springer-Verlag, January 2010.

[10] P. Golle, M. Jakobsson, A. Juels, and P. F. Syverson. Universal re-encryption for mixnets. In *Proc. of The Cryptographers' Track at the RSA Conference 2004 (CT-RSA'04), San Francisco, USA, LNCS*, volume 2964, pages 163–178. Springer-Verlag, February 2004.

[11] C. P. Joel Alwen. 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. IBFI Schloss Dagstuhl, February 2009.

[12] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proc. of the The 37th ACM Symposium on Theory of Computing (STOC'05), Baltimore, USA*, pages 84–93. ACM Press, May 2005.

[13] C. P. Richard Lindner. Better key sizes (and attacks) for lwe-based encryption. In *Proc. of The Cryptographers' Track at the RSA Conference 2011 (CT-RSA'11), San Francisco, CA, USA, LNCS*, volume 6558, pages 319–339. Springer-Verlag, January 2011.

[14] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, October 1997.

[15] X. B. Shweta Agrawal, Dan Boneh. 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.

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.