Unidirectional FHPRE Scheme from Lattice for Cloud Computing

Juyan Li[1,2], Chunguang Ma[1,3], Lei Zhang[1,4], and Qi Yuan[1,5]

(Corresponding author: Chunguang Ma)

College of Computer Science and Technology, Harbin Engineering University[1]
Harbin 150001, P.R. China
College of Data Science and Technology, Heilongjiang University[2]
Harbin 150080, P.R. China
State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences[3]
Beijing 100093, P.R. China
College of Information and Electronic Technology, Jiamusi University[4]
Jiamusi 154007, P.R. China
College of Communication and Electronic Engineering, Qiqihar University[5]
Qiqihar, 161006, P.R. China
(Email: machunguang@hrbeu.edu.cn)

(Received Dec. 20, 2017; Revised and Accepted Apr. 21, 2018; First Online Feb. 26, 2019)

Abstract

With the emerging of new types of network forms, services and cloud computation, the situation has transformed from one party to many parties at least one of both communication ends, that is "one-to-many," "many-to-one," and "many-to-many" situations. Most of the existing fully homomorphic encryption schemes only allow one party to encrypt the plaintext and another party to decrypt the ciphertext without the decryption keys. This form of cryptography loses efficiency under the demands of "one-to-many," "many-to-one," and "many-to-many" scenarios. In this paper, we combine the fully homomorphic encryption with proxy re-encryption to propose the fully homomorphic proxy re-encryption scheme which can be applied to "many-to-one" scenario, that is the fully homomorphic proxy re-encryption scheme allows one party to compute arbitrary functions over encrypted data for many parties without the decryption keys. Finally, IND-CPA, KP-CPA and master secret security proof of our proposal are given.

Keywords: FHPRE; Key Privacy; Many-to-One; STP-Binary-LWE

1 Introduction

Proxy Re-Encryption (PRE), which is an extension of public key encryption, was introduced by Bleumer *et al.* at Eurocrypt 1998 [4]. A PRE scheme allows proxy (semi trusted) to transform a ciphertext for Alice (delegator) into a ciphertext for Bob (delegatee) without knowing the message. The interesting property makes PRE more applicable in many scenarios, such as encrypted email forwarding [4], vehicular ad hoc network, outsourced filtering of encrypted spam , the distributed file system [3, 9]. Fully-homomorphic encryption (FHE) marks another milestone in the history of modern cryptography. A FHE scheme allows one party to compute arbitrary functions over encrypted data for another party without the decryption key. FHE has many applications in cloud computation, such as private queries to a search engine, searching on encrypted data [8, 10, 14].

The existing FHE schemes are mostly in the form of "one-to-one" deployment situations. With the emerging of new types of network forms, services and cloud computation, the situation has transformed from one party to many parties at least one of both communication ends, that is "one-to-many," "many-to-one," and "many-to-many" situations. It's interesting to combine the concept of FHE and PRE to construct a fully homomorphic proxy re-encryption (FHPRE), which allows one party to compute arbitrary functions over encrypted data for many parties without the decryption keys, satisfying the many-to-one situation. The application of FHPRE in the cloud computation can see [13, 21, 24].

Xagawa [22] constructed the first bidirectional PRE scheme based on lattices, which is CPA secure. Aono *et al.* [1] proposed a unidirectional key-private PRE (KP-PRE) scheme based on lattices, which is CPA secure. A unidirectional scheme permits user Alice to delegate to user Bob, without permitting Alice to decrypt user

Bob's ciphertexts. A unidirectional proxy re-encryption is said to be key privacy if any adversary cannot distinguish a real re-encryption key from a random re-encryption key even if the adversary is allowed to access to the re-encryption key oracle and the re-encryption oracle which re-encrypts input ciphertexts by using the real re-encryption key [2, 18]. Ateniese *et al.* [3] introduced master secret security as another security requirement for unidirectional PRE based on lattices. Master secret security demands that it is hard for the coalition of the proxy and Bob to compute Alice's secret key.

Singh *et al.* [20] showed [1,22] is not secure under master secret security model and constructed a unidirectional multi-use PRE which is secure under master secret security model. Nishimak *et al.* [18] proposed two unidirectional KP-PRE schemes from LWE assumptions, which are CPA secure. Jiang *et al.* [11] constructed a multi-use unidirectional PRE scheme based on lattices, which is CPA secure and master secret secure. Kirshanova *et al.* [12] proposed a unidirectional proxy re-encryption scheme based on LWE problem and showed it is CCA-1 secure in the selective model. Zhang *et al.* [23] proposed Unidirectional IBPRE scheme from lattice for cloud computation, which is CPA secure.

Recently, FHE from learning with errors (LWE) assumption has attracted many attentions due to their average-case to worst-case equivalence and their conjectured resistance to quantum attacks [19]. The efficiency of FHE is one of the most concerned problems. A number of techniques are proposed and used to improve the efficiency of FHE, such as re-linearization technique, dimension modulus reduction technique [5], modulus switching technique [6]. In 2012, Brakerski [7] constructed a scale-invariant fully homomorphic encryption scheme, whose noise only grows linearly with every multiplication (before refreshing). Ma *et al.* [15] proved that STP-binary-LWE is hard when LWE is hard, and modified the scale-invariant fully homomorphic encryption scheme [7] based on STP-Binary-LWE so that it is more efficient. Furthermore, Ma *et al.* [15] can encrypt several messages at a time and achieve a balance between security and efficiency in the hierarchical encryption systems.

Unfortunately, all of the above FHE schemes are not applicable to the many-to-one situation. Zhong *et al.* [24] constructed a "many-to-one" homomorphic encryption scheme based on approximate GCD problem, which is not lattice-based scheme. The essence of the scheme [24] is a PRE scheme, and needs the trusted third party to distribute the key. Ma *et al.* [16,17] constructed a homomorphic proxy re-encryption scheme based on LWE which can only encrypt one message at a time.

In this paper, we construct a unidirectional FHPRE scheme from lattices which can be used in the "many-to-one" situation and only needs semi trusted third party. The FHPRE can encrypt two messages at a time. At last, we prove that our FHPRE is indistinguishable against chosen-plaintext attacks, and key privacy secure.

The rest of this paper is organized as follows. Section 2 is preliminaries. Section 3 describes the constructed FHPRE scheme and proves the security of FHPRE. At last, the conclusion will be given in Section 4.

2 Preliminaries

2.1 Notation

All scalars, column vectors and matrices will be denoted in the form of plain (*e.g.* x), bold lowercase (*e.g.* $\vec{x}$) and uppercase (*e.g.* X), respectively. For a real number x ($x \geq 0$), $\lceil x \rceil$, $\lfloor x \rfloor$, $\lfloor x \rceil$ denoted rounding up or down, rounding to the nearest integer. We denote $\eta = \lceil \log q \rceil$, $[x]_q = x \bmod q$, $\mathbb{Z}_q = (-\frac{q}{2}, \frac{q}{2}] \cap \mathbb{Z}$, [k] $= \{1, 2, \cdots, k\}$. The l_i norm of a vector $\vec{v}$ is denoted by $||\vec{v}||_i$. k-dimensional identity matrix is denoted by I_k. Inner product, tensor product and semitensor product are denoted by $< \vec{v}, \vec{u} >$, $P \otimes Q$, $P_{r\times kl} \ltimes Q_{l\times t} = (P(Q \otimes I_k))_{r\times kt}$, respectively.

$[X|Y] \in \mathbb{Z}_q^{m\times(n+l)}$ is the concatenation of the columns of $X \in \mathbb{Z}_q^{m\times n}, Y \in \mathbb{Z}_q^{m\times l}$. $[X;Y] \in \mathbb{Z}_q^{(n+l)\times m}$ is the concatenation of the rows of $X \in \mathbb{Z}_q^{n\times m}, Y \in \mathbb{Z}_q^{l\times m}$. We set

$$\begin{aligned} BD\left(\vec{x}^T\right) &= \left(\vec{u}_1^T|\cdots|\vec{u}_\eta^T\right) \in \{0,1\}^{n\eta}; \\ P2\left(\vec{x}\right) &= \left(1, 2, \cdots, 2^{\eta-1}\right)^T \otimes \vec{x} \\ &= \left(1\vec{x}; 2\vec{x}; \cdots; 2^{\eta-1}\vec{x}\right)^T \in \mathbb{Z}_q^{n\eta}, \end{aligned}$$

where $\vec{x} \in \mathbb{Z}_q^n$, $\vec{x}^T = \sum_{k=1}^{\eta} 2^{k-1}\vec{u}_k^T$. When A is a matrix, let $P2(A), BD(A)$ be the matrix formed by applying the operation to each column of A.

Concerning a probability distribution D, we record it as $\vec{x} \leftarrow D$, which means that $\vec{x}$ is sampled according to D. So for a set S, we record it as $y \leftarrow S$, which means that y is sampled uniformly from S. Two random variables X and Y are said to be statistically (and computationally) indistinguishable, denoted by $X \approx_s Y$ ($X \approx_c Y$).

2.2 $STP - Binary - LWE_{n,q,\chi^k}$ and Key Switching

Ma *et al.* [15] proved that STP-binary-LWE is hard and showed the Key Switching functions by semitensor product.

Theorem 1. *([15]) For an integer $q = q(n) \geq 2$ and a distribution χ on $\mathbb{Z}_q$, an integer dimension $n = n' log(logn') \in \mathbb{Z}^+$, where n' is the dimension of LWE problem. The $STP-Binary-LWE_{n,q,\chi^k}$ problem, which is to distinguish the following two distributions: In the first distribution, one samples $(\vec{a}; b_1, \cdots, b_k)$ uniformly from $\mathbb{Z}_q^{n+k}$. In the second distribution, one first draws $\vec{s} \leftarrow \mathbb{Z}_2^{n/k}$ and then samples $(\vec{a}, b_1, \cdots, b_k) \in \mathbb{Z}_q^{n+k}$ by independently sampling $\vec{a} \leftarrow \mathbb{Z}_q^n$, $e_i \leftarrow \chi, i \in [k]$, and setting $(b_1, \cdots, b_k) = \vec{a}^T \ltimes \vec{s} + (e_1, \cdots, e_k)$, is hard.*

In the following, we can without loss of generality let that $k = 2$. We show the Key Switching functions which can switch ciphertexts under S into ciphertexts under $(1;\vec{t})$. Let q be an integer and χ be a distribution over $\mathbb{Z}$.

- $\mathrm{SwitchKeyGen}_q(S,\vec{t})$: Input $S \in \mathbb{Z}^{n_s\times 2}$, $\vec{t} \in \mathbb{Z}^{\frac{n_t}{2}}$, $A_{s:t} \leftarrow \mathbb{Z}_q^{\hat{n}_s\times n_t}$ and $X \leftarrow \chi^{\hat{n}_s\times 2}$, where $\hat{n}_s = n_s \cdot \lceil logq \rceil$. Output $P_{s:t} = [B_{s:t}|| - A_{s:t}] \in \mathbb{Z}_q^{\hat{n}_s\times(n_t+2)}$, where $B_{s:t} := [A_{s:t} \ltimes \vec{t} + X_{s:t} + PowersOf2_q(S)]_q \in \mathbb{Z}_q^{\hat{n}_s\times 2}$.
- $\mathrm{SwitchKey}_q(P_{s:t},\vec{c_s})$: Input $P_{s:t}$ and ciphertext $\vec{c_s}$ under S. Output ciphertext $\vec{c_t} := [P_{s:t}^T \cdot BitDecomp_q(\vec{c_s})]_q$ under $(1;\vec{t})$.

Lemma 1. *([15]) (correctness). Let $S \in \mathbb{Z}^{n_s\times 2}, \vec{t} \in \mathbb{Z}^{n_t/2}$ and $\vec{c_s} \in \mathbb{Z}_q^{n_s}$ be any vectors. Let $P_{s:t} \leftarrow SwitchKeyGen_q(S,\vec{t})$ and set $\vec{c_t} \leftarrow SwitchKey_q(P_{s:t},\vec{c_s})$. Then*

$$\vec{c_s}^T \ltimes S = \vec{c_t} \ltimes (1;\vec{t}) - BitDecomp_q(\vec{c_s})^T X_{s:t}(modq).$$

Lemma 2. *([15]) (security). Let $S \in Z^{n_s\times 2}$ be any vector, $\vec{t} \leftarrow \mathbb{Z}^{n_t/2}$, $P_{s:t} \leftarrow$ SwitchKeyGen$(S, \vec{t})$, then P is computationally indistinguishable from uniform over$\mathbb{Z}_q^{\hat{n}_s\times(n_t+2)}$, assuming STP-Binary-DLWE$_{n,q,\chi^k}$.*

2.3 Syntax of FHPRE and Security Model

The FHPRE compromises FHE and PRE, the Syntax of FHPRE is as follows.

Definition 1. *(Unidirectional FHPRE Scheme)*

A single-hop unidirectional FHPRE scheme consists of the following 7 algorithms:

1) *Setup$(1^k, 1^L) \to pp$: Given the security parameter k, the upper bound on the maximal multiplicative depth $L \in \mathbb{N}$ that the scheme can homomorphically evaluate, output the public parameters pp.*
2) *Gen$(pp, i, L) \to \left(ek^i, dk^i, evk^i\right)$: Given pp, L and a user identity i, output an encryption/decryption key pair $\left(ek^i, dk^i\right)$, eval keys $evk^i = \{evk^i_{(l-1):l}\}_{l\in[L]}$, and decryption keys dk^i_l at level l of the circuit, $l \in [L]$.*
3) *Enc$(pp, ek^i, \mu) \to ct$: Given pp, ek^i and a message μ , output a ciphertext ct^i_0 at level 0 of the circuit.*
4) Eval$(pp, evk^i_{(l-1):l}, c^i_{l-1,1}, c^i_{l-1,2}) \to c^i_l$: *Given $pp, evk^i_{(l-1):l}$, and ciphertexts $c^i_{l-1,1}, c^i_{l-1,2}$ at level $l-1$ of the circuit, output a ciphertext c^i_l at level l of the circuit, $l \in [L]$.*
5) *Dec$\left(pp, dk^i, ct^i_L\right) \to \mu$: Given dk^i and ct^i_L at level L of the circuit, output a plaintext μ or an error symbol $\perp$.*
6) Rekey $\left(pp, dk^i_l, \mathrm{ek}^j\right) \to rk^{i\to j}_{l\to 0}$: *Given a decryption key dk^i_l of user i at level l of the circuit and ek^j of user j, output a re-encryption key $rk^{i\to j}_{l\to 0}$, $l = 0, 1, \cdots, L$.*
7) *ReEnc$\left(pp, rk^{i\to j}_{l\to 0}, ct^i_l\right) \to ct^j_0$: Given the re-encryption key $rk^{i\to j}_{l\to 0}$ and ct^i_l for the user i at level l of the circuit, output a ciphertext ct^j_0 for the user j at level 0 of the circuit.*

Correctness: Three requirements are needed:

$$\begin{aligned} Dec\left(pp, dk^i_l, ct^i_l\right) &= \mu; \\ Dec\left(pp, dk^i, ct^i_L\right) &= \mu; \\ \mathrm{Dec}\left(pp, dk^j_l, ReEnc\left(pp, rk^{i\to j}_{l\to 0}, ct^i_l\right)\right) &= \mu, \end{aligned}$$

where $l \in [L]$. Now we define the security model of an FHPRE scheme.

Definition 2. *(IND-CPA security) Let UniFH-PRE=(Setup, Gen, Enc, Eval, Dec, ReKey, ReEnc) be a single-hop, unidirectional PRE Scheme, k a security parameter. Suppose that there exists a PPT algorithm RandEnc which takes pp as input and outputs a random ciphertext at output side. Let $H = H(k)$ and $C = C(k)$ be polynomials of k, which stands for the number of honest users and corrupted users, respectively. Consider the following game, denoted by $Expt^{IND-CPA}_{A,UniFHPRE}(k)$, between challenger and adversary.*

Initialization: *Given security parameter k and coin $b \in \{0,1\}$, run $pp \leftarrow Setup(1^k, 1^L)$. Initialize $CU \leftarrow \{H+1, \cdots, H+C\}$, which denote the set of corrupted users. For $i = 0, \cdots, H+C$, generate key pairs $\left(ek^i, dk^i, evk^i\right) \leftarrow \mathrm{Gen}\left(\mathrm{pp}, 1^i, 1^L\right)$. Run the adversary on input pp, key pairs of corrupted users $\left(ek^i, dk^i, evk^i\right)\}_{i=H+1,\cdots,H+C}$, and public keys of honest users $\left(ek^i, evk^i\right)\}_{i=0,\cdots,H}$.*

Learning Phase: *For $\forall l \in [L]\cup\{0\}$, the adversary could issue queries to the following oracles in any order and many times:*

Oracle REKEY receives two indices $i, j \in \{0, 1, \cdots, H+C\}$. If $i = j$ then it returns $\perp$; if $(i = 0) \cap (j \in CU)$ then the oracle returns $\perp$; otherwise, returns $rk^{i\to j}_{l\to 0} \leftarrow Rekey\left(pp, dk^i_l, \mathrm{ek}^j\right)$.

Oracle REENC receives two indices $i, j \in \{0, 1, \cdots, H+C\}$ and ciphertext ct^i_l. If $i = j$ then returns $\perp$; if $(i = 0) \cap (j \in CU)$ then the oracle returns $\perp$; otherwise, it queries (i, j) to REKEY, obtains $rk^{i\to j}_{l\to 0}$, and returns $ct^j_0 \leftarrow ReEnc\left(pp, rk^{i\to j}_{l\to 0}, ct^i_l\right)$.

Oracle CHALLENGE, which can be queried only once, receives μ. If $(b = 0)$, it returns $ct \leftarrow RandEnc(pp)$. If $(b = 1)$, it returns $ct \leftarrow Enc(pp, ek^0, \mu)$.

Eventually. The adversary halts after it and outputs its decision $b' \in \{0, 1\}$.

Finalization: *Output 1 if $b' = b$. Otherwise, output 0.*

We define the advantage of the adversary as

$$\begin{aligned}&Adv_{A,UniFHPRE}^{Ind-CPA}(k)\\ = &\left|\begin{array}{c}\Pr\left[Expt_{A,UniFHPRE}^{Ind-CPA}(k)\rightarrow 1\,|b=1\right]\\ -\Pr\left[Expt_{A,UniFHPRE}^{Ind-CPA}(k)\rightarrow 1\,|b=0\right]\end{array}\right|\end{aligned}$$

We say that UniFHPRE is IND-CPA secure if $Adv_{A,UnFHiPRE}^{Ind-CPA}(\cdot)$ is negligible for every PPT adversary.

Definition 3. *(KP-CPA security) Let UniFHPRE=(Setup, Gen, Enc, Eval, Dec, ReKey, ReEnc) be a single-hop, unidirectional FHPRE Scheme, k a security parameter. Suppose that there exists a PPT algorithm RandRekey which takes pp as input and outputs a random re-encryption key rk. Let $H = H(k)$ and $C = C(k)$ be polynomials of k, which stands for the number of honest users and corrupted users, respectively. Consider the following game, denoted by $Expt_{A,UniFHPRE}^{KP-CPA}(k)$, between challenger and adversary.*

Initialization: *Given security parameter k and coin $b \in \{0,1\}$, run $pp \leftarrow Setup\left(1^k, 1^L\right)$. Initialize $T \leftarrow \phi$ which is a table containing the re-encryption keys and shared among oracles. For $i = -1, 0, \cdots, H+C$, generate key pairs $\left(ek^i, dk^i, evk^i\right) \leftarrow \mathrm{Gen}\left(\mathrm{pp}, 1^i, 1^L\right)$. Run adversary with pp, the public keys and eval keys of honest users $\{(ek^i, evk^i)\}_{i=0,\cdots,H}$, the key pairs of corrupted users $\{(ek^i, dk^i, evk^i)\}_{i=H+1,\cdots,H+C}$.*

Learning Phase: *For $\forall l \in L$, adversary could issue queries to the following oracles in any order and many times except for the constraint in oracle CHALLENGE.*

Oracle REKEY receives two indices $i, j \in \{-1, 0, \cdots, H + C\}$. If $i = j$ then it returns $\perp$; if $(i, j) = (0, -1)$, then it returns $\perp$; if there already exists the re-encryption key from user i at level l of the circuit to user j, i.e. *$\left(i, l, j, rk_{l\rightarrow 0}^{i\rightarrow j}\right) \in T$, then it returns $rk_{l\rightarrow 0}^{i\rightarrow j}$, otherwise, it generates $rk_{l\rightarrow 0}^{i\rightarrow j} \leftarrow \mathrm{Rekey}\left(pp, dk_l^i, \mathrm{ek}^j\right)$, updates $T \leftarrow T \cup \left\{\left(i, l, j, rk_{l\rightarrow 0}^{i\rightarrow j}\right)\right\}$, and returns $rk_{l\rightarrow 0}^{i\rightarrow j}$.*

Oracle REENC receives two indices $i, j \in \{-1, 0, \cdots, H + C\}$ and a ciphertext ct_l^i. if $i = j$ then it returns $\perp$; if there exists no re-encryption key $rk_{l\rightarrow 0}^{i\rightarrow j}$ in the table T, it generates $rk_{l\rightarrow 0}^{i\rightarrow j} \leftarrow Rekey\left(pp, dk_l^i, ek^j\right)$, and updates $T \leftarrow T \cup \left\{\left(i, j, rk_{l\rightarrow 0}^{i\rightarrow j}\right)\right\}$, it finally returns $ct_0^j \leftarrow ReEnc\left(pp, rk_{l\rightarrow 0}^{i\rightarrow j}, ct_l^i\right)$.

Oracle CHALLENGE can be queried only once. On the query, the oracle searches the table T for $\left(0, l, -1, rk_{l\rightarrow 0}^{0\rightarrow -1}\right)$, if such key does not exist, it generates $rk_{l\rightarrow 0}^{0\rightarrow -1} \leftarrow \mathrm{Re}Key\left(pp, dk_l^0, ek^{-1}\right)$ and updates $T \leftarrow T \cup \left\{\left(0, l, -1, rk_{l\rightarrow 0}^{0\rightarrow -1}\right)\right\}$. If $b = 0$ then it returns a random re-encryption key $rk \leftarrow FakeReKey(pp)$, which is not contained in T. If $b = 1$, then it returns the real re-encryption key $rk_{l\rightarrow 0}^{0\rightarrow -1}$ contained in T.

Eventually. Adversary halts after it outputs its decision $b' \in \{0,1\}$.

Finalization: *Output 1 if $b' = b$. Otherwise, output 0.*

The advantage of Adversary is

$$\begin{aligned}&Adv_{A,UniFHPRE}^{KP-CPA}(k)\\ = &\left|\begin{array}{c}\Pr\left[Expt_{A,UniFHPRE}^{KP-CPA}(k)\rightarrow 1\,|b=1\right]\\ -\Pr\left[Expt_{A,UniFHPRE}^{KP-CPA}(k)\rightarrow 1\,|b=0\right]\end{array}\right|\end{aligned}$$

We say that UniFHPRE is KP-CPA secure if $Adv_{A,UniFHPRE}^{KP-CPA}(\cdot)$ is negligible for every polynomial-time adversary.

3 Unidirectional FHPRE Scheme

In this section, we constructed a single-hop unidirectional FHPRE scheme based on [15] and proved the scheme is IND-CPA and KP-CPA security.

3.1 Our Construction

A single-hop unidirectional FHPRE scheme consists of the following 7 algorithms.

1) Setup$(1^k, 1^L)$: Sample $A \leftarrow \mathbb{Z}_q^{N\times n}$, where $N \triangleq (n+2)\cdot(logq + O(1))$, $n = n'log(logn') \in \mathbb{Z}^+$, n' is the dimension of LWE problem. Output $pp = \left(1^k, 1^n, q, \chi, L, A\right)$.

2) Gen(pp, i): Sample $s_l^i, t_l^i \leftarrow \mathbb{Z}_2^{n/2}$, $l = 0, 1, \cdots, L$, and compute $B_0^i = [A \ltimes \vec{s}_0^{\,i} + X_0^i]_q$, where $X_0^i \leftarrow \chi^{N\times 2}$. Let $P_0^i = [B_0^i \parallel -A] \in \mathbb{Z}_q^{N\times(n+2)}$. For $\forall l \in [L]$, define

$$\widetilde{S}_{l-1}^i = (\alpha||\beta) \in \mathbb{Z}_2^{(n+2)^2\lceil logq\rceil^2\times 2},$$

where

$$\alpha = BD((1;\vec{s}_{l-1}^{\,i})\otimes(1;0))\otimes BD((1;\vec{s}_{l-1}^{\,i})\otimes(1;0)),$$

$$\beta = BD((1;\vec{s}_{l-1}^{\,i})\otimes(0;1))\otimes BD((1;\vec{s}_{l-1}^{\,i})\otimes(0;1)),$$

and compute $P_{(l-1):l}^i \leftarrow SwitchKeyGen(\widetilde{S}_{l-1}^i, \vec{s}_{l-1}^{\,i})$. Output

$$\begin{aligned}\left(ek^i, dk^i\right) &= \left(P_0^i, \vec{s}_L^{\,i}\right)\\ dk_l^i &= \vec{s}_l^{\,i}, l \in [L]\\ evk^i &= \{evk_{(l-1):l}^i\}_{l\in[L]}\\ &= \{P_{(l-1):l}^i\}_{l\in[L]}.\end{aligned}$$

3) Enc$(pp, ek^i = P_0^i, (m_1, m_2))$: Compute

$$\vec{c}_0^{\,i} = \left[P_0^{iT}\cdot\vec{r} + \left\lfloor\frac{q}{2}\right\rfloor\vec{m}\right]_q \in \mathbb{Z}_q^{(n+2)},$$

where $\vec{r} \leftarrow \{0,1\}^N$, $\vec{m} = (m_1, m_2, 0\cdots,0)^T \in \mathbb{Z}_2^{(n+2)}$. Output $ct_0^i = \vec{c}_0^{\,i}$.

4) Eval($\bullet$): Suppose the homomorphic addition and multiplication over GF(2) be enable to evaluate depth L arithmetic circuits in a gate-by-gate manner. For any $i \in [L]$, a gate at level i of the circuit is that the operand ciphertexts can be decrypted using $\vec{s}_{i-1}$, and the output of the homomorphic operation can be decrypted using $\vec{s}_i$.

   - Add$(pp, evk^i_{(l-1):l}, c^i_{l-1,1}, c^i_{l-1,2})$: Input ciphertexts $c^i_{l-1,1} = \vec{c}^i_{l-1,1}$, $c^i_{l-1,2} = \vec{c}^i_{l-1,2}$ under secret key $\vec{s}^i_{l-1}$, and compute

$$\vec{c}^i_{l-1,add} = P2(\vec{c}^i_{l-1,1}+\vec{c}^i_{l-1,2}) \otimes P2(1,1,0,\cdots,0),$$

$$\vec{c}^i_{l,add} \leftarrow Switchkey(P^i_{(l-1):l}, \vec{c}^i_{l-1,add}) \in \mathbb{Z}_q^{n+2}.$$

   Output $c^i_{add,l} = \vec{c}^i_{l,add}$.

   - Mult$(pp, evk^i_{(l-1):l}, c^i_{l-1,1}, c^i_{l-1,2})$: Input ciphertexts $c^i_{l-1,1} = \vec{c}^i_{l-1,1}, c^i_{l-1,2} = \vec{c}^i_{l-1,2}$ under secret key $\vec{s}^i_{l-1}$, and compute

$$\tilde{\vec{c}}^j_{l-1,mult} = \lfloor \frac{2}{q}(P2(\vec{c}_1) \otimes P2(\vec{c}_2)) \rceil,$$

$$\vec{c}^i_{l,mult} \leftarrow SwitchKey(P^i_{(l-1):l}, \tilde{\vec{c}}^j_{l-1,mult}) \in \mathbb{Z}_q^{n+2}.$$

   Output $c^i_{mult,l} = \vec{c}^i_{l,mult}$.

5) Dec$\big(pp, dk^i = \vec{t}^i_L, ct^i_L = \vec{c}^i_L\big)$: Input ciphertext ct^i_L under secret key $dk^i (= \vec{s}^i_L)$ and $\vec{s}^i_L$. Output

$$(m_1, m_2) = \left[\left\lfloor 2 \cdot \frac{\left[c_L^T \ltimes (1; \vec{s}_L)\right]_q}{q} \right\rceil\right]_2$$

6) Rekey$\Big(pp, dk^i_{l-1} = \vec{s}^i_{l-1}, \mathrm{ek}^j = P^j_0\Big)$: Compute

$$\begin{aligned} M^{i\to j}_{l\to 0} &\in \mathbb{Z}_q^{(n+2)\lceil \log q\rceil \times (n+2)} \\ &\leftarrow R^{i\to j}_{l\to 0} P^j_0 + P2\left((1; \vec{s}^i_l) \otimes I_2 || 0\right) \\ N^j_0 &\in Z_q^{N\times(n+2)} \leftarrow R^j_0 P^j_0, \end{aligned}$$

where $0 \in \{0\}^{(n+2)\times n}$, $R^{i\to j}_{l\to 0} \in Z_2^{(n+2)\lceil \log q\rceil \times N}$, $R^j_0 \in Z_2^{N\times N}$. Output $rk^{i\to j}_{l\to 0} = (M^{i\to j}_{l\to 0}, N^j_0)$.

7) ReEnc$\Big(pp, rk^{i\to j}_{l\to 0} = (M^{i\to j}_{l\to 0}, N^j_0), ct^i_l = \vec{c}^i_l\Big)$: Output

$$ct^j_0 = \vec{c}^j_0 = SwitchKey_q\left(M^{i\to j}_{l\to 0}, \vec{c}^i_l\right) + {N^j_0}^T \vec{r}^j_0,$$

where $\vec{r}^j_0 \in \mathbb{Z}_2^N$.

We show the correctness of the FHPRE scheme below.

Lemma 3. *([15]) Let $\vec{s} \in Z_2^{n/2}$, $\vec{c} \in Z_q^{n+2}$ be such that $\vec{c}^T \ltimes (1, \vec{s}) = \lfloor \frac{q}{2} \rfloor \cdot (m_1, m_2) + X(modq)$, where $m_1, m_2 \in \{0,1\}$ and $||X||_\infty \le \lfloor \frac{q}{2} \rfloor /2$. Then $Dec(\vec{c}) = (m_1, m_2)$.*

proposition 1. *Let $q, n, |\chi| \le B, L$ be parameters for FHPRE, and let ciphertexts $c^i_l = \vec{c}^i_l$ and secret key $\vec{s}^i_l$ be such that*

$$\vec{c}^{i\,T}_l \ltimes (1; \vec{s}^i_l) = \left\lfloor \frac{q}{2} \right\rfloor (m_1, m_2) + X^i_l (modq),$$

where $m_1, m_2 \in \{0,1\}$ and $||X^i_l||_\infty \le E < \lfloor \frac{q}{2} \rfloor /2$. Define $\vec{c}^j_0 \leftarrow ReEnc\Big(pp, rk^{i\to j}_{l\to 0}, \vec{c}^i_l\Big)$. Then

$$\vec{c}^{j\,T}_0 \ltimes \Big(1; \vec{s}^j_0\Big) = \left\lfloor \frac{q}{2} \right\rfloor (m_1, m_2) + X(modq),$$

where $||X||_\infty \le E + N(n+2)\lceil \log q\rceil B^2 + N^2 B$.

Proof. Suppose $\vec{c}^{i\,T}_l \ltimes \big(1; \vec{s}^i_l\big) = \lfloor \frac{q}{2} \rfloor (m_1, m_2) + X^i_l (modq)$, where $|X^i_l||_\infty \le E < \lfloor \frac{q}{2} \rfloor /2$. To decrypt the re-encrypted ciphertext $ct^j_0 = \vec{c}^j_0 = SwitchKey\left(M^{i\to j}_{l\to 0}, \vec{c}^i_l\right) + {N^j_0}^T \vec{r}^j_0$ with $\Big(1; \vec{s}^j_0\Big)$, where $\vec{r}^j_0 \in \mathbb{Z}_2^N$, $M^{i\to j}_{l\to 0} = R^{i\to j}_{l\to 0} Q^j_0 + P2\left((1; s^i_l) \otimes I_2 || 0\right)$, $R^{i\to j}_{l\to 0} \in \mathbb{Z}_2^{(n+2)\lceil \log q\rceil \times N}$, $N^j_0 = R^j_0 Q^j_0$, $R^j_0 \in \mathbb{Z}_2^{N\times N}$, one computes

$$\begin{aligned} & \vec{c}^{j\,T}_0 \ltimes \Big(1; \vec{s}^j_0\Big) \\ = \;& SwitchKey\Big(M^{i\to j}_{l\to 0}, \vec{c}^i_l\Big)^T \ltimes \Big(1; \vec{s}^j_0\Big) \\ & + N^{j\,T}_0 \vec{r}^j_0 \ltimes \Big(1; \vec{s}^j_0\Big) \,(\mathrm{mod} q) \\ = \;& BD\big(\vec{c}^i_l\big)^T R^{i\to j}_{l\to 0} Q^j_0 \ltimes \Big(1; \vec{s}^j_0\Big) \\ & + BD\big(\vec{c}^i_l\big)^T P2\left(\big(1; \vec{s}^i_l\big) \otimes I_2 || 0\right) \ltimes \Big(1; \vec{s}^j_0\Big) \\ & + \vec{r}^{j\,T}_0 R^j_0 Q^j_0 \ltimes \Big(1; \vec{s}^j_0\Big) \,(\mathrm{mod} q) \\ = \;& \left\lfloor \frac{q}{2} \right\rfloor (m_1, m_2) + X^i_l + BD\big(\vec{c}^i_l\big)^T R^{i\to j}_{l\to 0} Y^j_0 \\ & + \vec{r}^{j\,T}_0 R^j_0 Y^j_0 (\mathrm{mod} q). \end{aligned}$$

Let $X = X^i_l + BD\big(\vec{c}^i_l\big)^T R^{i\to j}_{l\to 0} Y^j_0 + {\vec{r}^j_0}^T R^j_0 Y^j_0$, we have

$$\begin{aligned} & \left\| X^i_l + BD\big(\vec{c}^i_l\big)^T R^{i\to j}_{l\to 0} Y^j_0 + {\vec{r}^j_0}^T R^j_0 Y^j_0 \right\|_\infty \\ \le \;& \|X^i_l\|_\infty + \left\| BD\big(\vec{c}^i_l\big)^T R^{i\to j}_{l\to 0} Y^j_0 \right\|_\infty + \left\| {\vec{r}^j_0}^T R^j_0 Y^j_0 \right\|_\infty \\ < \;& E + N(n+2)\lceil \log q\rceil B^2 + N^2 B. \end{aligned}$$

□

Lemma 4. *([15]) Let $q, n, |\chi| \le B, L$ be parameters for FHPRE, and let $(pk, evk, dk) \leftarrow Gen\ (1^L, 1^n)$. Let $\vec{c}_1, \vec{c}_2$ be such that*

$$\vec{c}^T_1 \ltimes (1, \vec{s}_{i-1}) = \left\lfloor \frac{q}{2} \right\rfloor (m_1, m_2) + X_1 (\mathrm{mod}\ q),$$

$$\vec{c}^T_2 \ltimes (1, \vec{s}_{i-1}) = \left\lfloor \frac{q}{2} \right\rfloor (m_1^{'}, m_2^{'}) + X_2 (\mathrm{mod}\ q),$$

with $||X_1||_\infty, ||X_2||_\infty \le E \le \lfloor \frac{q}{2} \rfloor /2$. Define

$$\vec{c}_{add} \leftarrow HE.Add_{evk}(\vec{c}_1, \vec{c}_2),$$

$$\vec{c}_{mult} \leftarrow HE.Mult_{evk}(\vec{c}_1, \vec{c}_2).$$

Then

$$\vec{c}_{add}^{T} \ltimes (1, \vec{s}_i) = \left\lfloor \frac{q}{2} \right\rfloor [(m_1+m_1^{'}, m_2+m_2^{'})]_2 + X_{add}(\bmod\ q),$$

$$\vec{c}_{mult}^{T} \ltimes (1, \vec{s}_i) = \left\lfloor \frac{q}{2} \right\rfloor (m_1 m_1^{'}, m_2 m_2^{'}) + X_{mult}(\bmod\ q),$$

where $||X_{add}||_\infty, ||X_{mult}||_\infty \leq O(n) \cdot max\{E, nlog^3 q \cdot B\}$.

Theorem 2. *([15]) The scheme HE with parameters* $n, q, |\chi| \leq B, L$ *for which* $q/B \geq (O(n))^{L+O(1)}$, *is L-homomorphic.*

3.2 Security

We show the security of the FHPRE scheme in this section which includes IND-CPA and KP-CPA security.

proposition 2. *Under the* $STP-Binary-LWE_{n,q,\chi^k}$ *assumption, the FHPRE scheme is IND-CPA secure.*

Proof. We consider the following games for $b \in \{0,1\}$.

Game$_0^b$**:** This is the real game $Expt_{A,UniFHPRE}^{Ind-CPA,I}(k)$ with b. Suppose the target public key is $ek^0 = P_0^0$, where $P_0^0 = [B_0^0 \parallel -A]$, $B_0^0 = [A \ltimes \vec{s}_0^0 + X_0^0]_q$, $X_0^0 \leftarrow \chi^{N\times 2}$. The other public keys of honest users are $\left\{ek^i\right\}_{i=1,\cdots,H} = \left\{P_0^i\right\}_{i=1,\cdots,H}$, where $P_0^i = [B_0^i \parallel -A]$, $B_0^i = [A \ltimes \vec{s}_0^i + X_0]_q$, $X_0^i \leftarrow \chi^{N\times 2}$. The challenger computes the re-encryption key from user 0 at level l to user $i \in [H]$ at level 0 of the circuit as $M_{l\to 0}^{0\to i} \leftarrow R_{l\to 0}^{0\to i} P_0^i + P2\left(\left(1;\vec{s}_l^0\right) \otimes I_2 || 0\right)$, $N_0^i \leftarrow R_0^i P_0^i$, where $0 \in \{0\}^{(n+2)\times n}$, $R_{l\to 0}^{0\to i} \in \mathbb{Z}_2^{(n+2)\lceil \log q \rceil \times N}$, $R_0^i \in \mathbb{Z}_2^{N\times N}$. The challenger computes the target ciphertext on query (m_1, m_2) as follows:

- If $(b = 0)$, it returns $ct \leftarrow \mathbb{Z}_q^{n+2}$.
- If $(b = 1)$, it returns $ct \leftarrow \left[{P_0^0}^T \cdot \vec{r} + \left\lfloor \frac{q}{2} \right\rfloor \vec{m}\right]_q \in \mathbb{Z}_q^{(n+2)}$, where $\vec{r} \leftarrow \{0,1\}^N$, $\vec{m} = (m_1, m_2, 0 \cdots, 0)^T \in \mathbb{Z}_2^{(n+2)}$.

The adversary finally outputs its guess $b' \in \{0,1\}$.

Game$_1^b$**:** We replace P_0^i, $P_{(l-1):l}^i$ with ${P_0^i}^+ \leftarrow \mathbb{Z}_q^{N\times 2}$, ${P_{(l-1):l}^i}^+ \leftarrow \mathbb{Z}_q^{(n+2)^2\lceil logq \rceil^3 \times (n+2)}$ for $i \in [H]$. The challenger computes a re-encryption key from user 0 at level l to user i ($i \in [H]$) at level 0 of the circuit by using $\mathbf{s}_l^0$ and ${P_0^i}^+$ as Game$_0^b$. The others are the same as in Game$_0^b$.

Since in the two games, the challenger does not require the secret $\vec{s}_0^i$, there is $P_0^i \approx_c {P_0^i}^+$ under the $STP-Binary-LWE_{n,q,\chi^k}$ assumption. It follows from lemma 2, we have $P_{(l-1):l}^0 \approx_c {P_{(l-1):l}^0}^+$. Furthermore, Game$_0^b \approx_c$Game$_1^b$.

Game$_2^b$**:** We replace $M_{l\to 0}^{0\to i}$, N_0^i with $M_{l\to 0}^{0\to i^+} \leftarrow \mathbb{Z}_q^{(n+2)\lceil \log q \rceil \times (n+2)}$, $N_0^{i+} \leftarrow \mathbb{Z}_q^{N\times (n+2)}$. The others are the same as in Game$_1^b$.

It follows from the leftover hash lemma, we have $M_{l\to 0}^{0\to i} \approx_s M_{l\to 0}^{0\to i^+}$ and $N_0^i \approx_s N_0^{i+}$. Furthermore, Game$_1^b \approx_s$Game$_2^b$.

Game$_3^b$**:** We replace $ct_0^j \leftarrow ReEnc\left(pp, rk_{l\to 0}^{i\to j}, ct_l^i\right)$ with $ct_0^{j+} \leftarrow \mathbb{Z}_q^{n+2}$. The others are the same as in Game$_2^b$.
It follows from the leftover hash lemma, we have $ct_0^{j+} \approx_s ct_0^j$. Furthermore,

$$\text{Game}_2^b \approx_s \text{Game}_3^b$$

.

Finally, we have that Game$_3^0 \approx_s$Game$_3^1$ from the leftover hash lemma. Combining the above indistinguishability, we have shown that Game$_0^0 \approx_c$Game$_0^1$. This completes the proof. □

Theorem 3. *Under the* $STP-Binary-LWE_{n,q,\chi^k}$ *assumption, the homomorphic PRE scheme is KP-CPA secure.*

Proof. We start with the original game with b = 1.

Game$_0$**:** This is the game $Expt_{A,UniFHPRE}^{KP-CPA}(k)$ with b = 1. The challenger runs the adversary with input pp, public keys $\left\{ek^i\right\}_{i=0,\cdots,H}$ and eval keys $\left\{evk^i\right\}_{i=0,\cdots,H}$ for honest users and key pairs $\left\{ek^i, dk^i\right\}_{i=H+1,\cdots,H+C}$, $\left\{evk^i\right\}_{i=H+1,\cdots,H+C}$ for corrupted users. The challenger generates the real re-encryption key $M_{l\to 0}^{0\to -1} \leftarrow R_{l\to 0}^{0\to -1} P_0^{-1} + P2\left(\left(1;\vec{s}_l^0\right) \otimes I_2 || 0\right)$, $N_0^{-1} \leftarrow R_0^{-1} P_0^{-1}$, where $0 \in \{0\}^{(n+2)\times n}$, $R_{l\to 0}^{0\to -1} \in \mathbb{Z}_2^{(n+2)\lceil \log q \rceil \times N}$, $R_0^{-1} \in \mathbb{Z}_2^{N\times N}$. On the re-encryption query (0, l, -1, $ct = c_l^o$), it re-encrypts the ciphertext with the real re-encryption key, that is, it returns $ct_0^{-1} = c_0^{-1} = SwitchKey\left(M_{l\to 0}^{0\to -1}, \vec{c}_l^0\right) + {N_0^{-1}}^T \vec{r}_0^{-1}$, where $\vec{r}_0^{-1} \in \mathbb{Z}_2^N$. We summarize the input and the answers to the adversary as follows:

RealPK: P_0^{-1};
Challenge: $M_{l\to 0}^{0\to -1}, N_0^{-1}$;
Table: $M_{l\to 0}^{0\to -1}, N_0^{-1}$;
ReEnc: $ct_0^{-1} = \vec{c}_0^{-1} = SwitchKey_q\left(M_{l\to 0}^{0\to -1}, \vec{c}_l^0\right) + {N_0^{-1}}^T \vec{r}_0^{-1}$.

After the learning phase, the adversary outputs its guess $b' \in \{0,1\}$.

Game$_1$**:** The challenger replaces P_0^{-1} with $P_0^{-1+} \leftarrow \mathbb{Z}_q^{N\times(n+2)}$, and the re-encryption keys in challenge and the table is constructed from P_0^{-1+} and $\vec{s}_l^0$. The other parts are the same as *Game*$_0$. The challenger re-encrypts a given ciphertext with the re-encryption key in the table. The challenger answers the queries from user 0 at level l to user -1 at level 0 as follows:

RealPK: P_0^{-1+};

Challenge: $M_{l\to 0}^{0\to -1}, N_0^{-1}$;

Table: $M_{l\to 0}^{0\to -1}, N_0^{-1}$;

ReEnc: $ct_0^{-1} = \vec{c}_0^{-1} = SwitchKey_q\left(M_{l\to 0}^{0\to -1}, \vec{c}_l^0\right) + {N_0^{-1}}^T \vec{r}_0^{-1}$.

It is easy to verify that $P_0^{-1} \approx_c P_0^{-1+}$ under the $STP-Binary-LWE_{n,q,\chi^k}$ assumption, since we do not need to know $\vec{s}_0^{-1}$. Furthermore, we have $Game_0 \approx_c Game_1$ by the leftover hash lemma.

$Game_2$**:** The challenger replaces $M_{l\to 0}^{0\to -1}, N_0^{-1}$ with $M_{l\to 0}^{0\to -1+} \leftarrow \mathbb{Z}_q^{(n+2)\lceil \log q\rceil \times (n+2)}$, $N_0^{-1+} \leftarrow Z_q^{N\times(n+2)}$. The other parts are not changed from the previous game: the challenger re-encrypts a given ciphertext with the random re-encryption key in the table. The challenger answers the queries from user 0 at level l to user -1 at level 0 as follows:

RealPK: P_0^{-1+};

Challenge: $M_{l\to 0}^{0\to -1+}, N_0^{-1+}$;

Table: $M_{l\to 0}^{0\to -1+}, N_0^{-1+}$;

ReEnc: $ct_0^{-1} = \vec{\tilde{c}}_0^{-1} = SwitchKey_q\left(M_{l\to 0}^{0\to -1+}, \vec{c}_l^0\right) + {N_0^{-1+}}^T \vec{r}_0^{-1}$.

It follows from the leftover hash lemma, we have $M_{l\to 0}^{0\to -1} \approx_s M_{l\to 0}^{0\to -1+}$ and $N_0^{-1} \approx_s N_0^{-1+}$. Furthermore, $Game_1 \approx_s Game_2$.

$Game_3$**:** If the query is (0,l -1, $ct = \vec{c}_l^0$), then it returns $\vec{c}_0^{-1+} \leftarrow \mathbb{Z}^{n+2}$. The other parts are not changed from the previous game: The challenger answers the queries from user 0 to -1 as follows: The challenger answers the queries from user 0 at level l to user -1 at level 0 as follows:

RealPK: P_0^{-1+};

Challenge: $M_{l\to 0}^{0\to -1+}, N_0^{-1+}$;

Table: $M_{l\to 0}^{0\to -1+}, N_0^{-1+}$;

ReEnc: $ct_0^{-1} = \vec{c}_0^{-1+}$.

It follows from the leftover hash lemma, we have $\vec{c}_0^{-1+} \approx_s \vec{\tilde{c}}_0^{-1}$. Furthermore, $Game_2 \approx_s Game_3$.

$Game_4$**:** The challenger additionally generates another random re-encryption key $M_{l\to 0}^{0\to -1++} \leftarrow \mathbb{Z}_q^{(n+2)\lceil \log q\rceil \times (n+2)}$, $N_0^{-1++} \leftarrow \mathbb{Z}_q^{N\times(n+2)}$ and uses it in the re-encryption oracle. The other parts are not changed from the previous game: As a summary, the challenger answers the queries from user 0 at level l to user -1 at level 0 as follows:

RealPK: P_0^{-1+};

Challenge: $M_{l\to 0}^{0\to -1+}, N_0^{-1+}$;

Table: $M_{l\to 0}^{0\to -1++}, N_0^{-1++}$;

ReEnc:

$$
\begin{aligned}
ct_0^{-1} &= \vec{c}_0^{-1++} \\
&= SwitchKe_q y\left(M_{l\to 0}^{0\to -1++}, \vec{c}_l^0\right) \\
&\quad + {N_0^{-1++}}^T \vec{r}_0^{-1}.
\end{aligned}
$$

We note that the adversary does not know the alternative fake re-encryption key $M_{l\to 0}^{0\to -1++}, N_0^{-1++}$, directly. Even if the adversary knows the alternative, it cannot distinguish the two games since the re-encrypted ciphertext, which is almost uniformly at random in the ciphertext space from the leftover hash lemma. Hence, we have $Game_3 \approx_s Game_4$.

$Game_5$**:** We again modify the re-encryption key in the table and the re-encryption oracle. The challenger additionally generates a fake re-encryption key $M_{l\to 0}^{0\to -1*} \leftarrow R_{l\to 0}^{0\to -1*} P_0^{-1+} + P2\left((1;\vec{s}_l^0) \otimes I_2 || 0\right)$, $N_0^{-1*} \leftarrow R_0^{-1*} P_0^{-1+}$, where $0 \in \{0\}^{(n+2)\times n}$, $R_{l\to 0}^{0\to -1*} \in \mathbb{Z}_2^{(n+2)\lceil \log q\rceil \times N}$, $R_0^{-1*} \in \mathbb{Z}_2^{N\times N}$ In the re-encryption oracle, the oracle uses the additional fake-re-encryption key. The other parts are not changed from the previous game: As a summary, the challenger answers the queries from user 0 at level l to user -1 at level 0 as follows:

RealPK: P_0^{-1+};

Challenge: $M_{l\to 0}^{0\to -1+}, N_0^{-1+}$;

Table: $M_{l\to 0}^{0\to -1*}, N_0^{-1*}$;

ReEnc: $ct_0^{-1} = \vec{c}_0^{-1*} SwitchKey_q\left(M_{l\to 0}^{0\to -1*}, \vec{c}_l^0\right) + {N_0^{-1*}}^T \vec{r}_0^{-1}$.

It follows from the leftover hash lemma, we have $M_{l\to 0}^{0\to -1+} \approx_s M_{l\to 0}^{0\to -1*}$, $N_0^{-1+} \approx_s N_0^{-1*}$, $\vec{c}_0^{-1++} \approx_s \vec{c}_0^{-1*}$. Furthermore, $Game_4 \approx_s Game_5$.

$Game_6$**:** This is a final game. We replace the fake public key $P_0^{-1+}$with the real public key P_0^{-1} . The other parts are not changed from the previous game: As a summary, the challenger answers the queries from user 0 at level l to user -1 at level 0 as follows:

RealPK: P_0^{-1};

Challenge: $M_{l\to 0}^{0\to -1+}, N_0^{-1+}$;

Table: $M_{l\to 0}^{0\to -1*}, N_0^{-1*}$;

ReEnc: $ct_0^{-1} = \vec{c}_0^{-1*} SwitchKey_q\left(M_{l\to 0}^{0\to -1*}, \vec{c}_l^0\right) + {N_0^{-1*}}^T \vec{r}_0^{-1}$.

Since $M_{l\to 0}^{0\to -1+}, N_0^{-1+}$ is distributed uniformly at random, this game is equivalent to $Expt_{A,UniFHPRE}^{KP-CPA}(k)$ with $b = 0$. It follows from the $STP-Binary-LWE_{n,q,\chi^k}$ assumption, we have $P_0^{-1} \approx_c P_0^{-1+}$. Furthermore, $Game_5 \approx_c Game_6$.

Above all, we know $Game_0 \approx_c Game_6$, that is $Expt_{A,UniFHPRE}^{KP-CPA}(k)$ with $b = 0$ and $Expt_{A,UniFHPRE}^{KP-CPA}(k)$ with $b = 1$ are computationally indistinguishable under $STP-Binary-LWE_{n,q,\chi^k}$ assumption. This completes the proof. □

3.3 Comparison

Compared with the homomorphic proxy re-encryption scheme of Ma *et al.* [16, 17], our scheme can encrypt two messages at a time under the same computation complexity , and has the same security of IND-CPA and KP-CPA under LWE. The comparison results in Table 1.

4 Conclusion

In this paper, we adopt the scheme of Ma *et al.* to construct a FHPRE scheme which allows one party to compute arbitrary functions over encrypted data for many parties without the decryption keys. That is, the FHPRE scheme satisfies the "many-to-one" situation. We also prove that our FHPRE scheme is IND-CPA, KP-CPA and master secret secure. We will be devoted to improving the computation efficiency in our future work, so as to make our FHPRE schemes more practical.

Acknowledgments

The authors thank the anonymous referees for their helpful comments. This work was supported by the National Natural Science Foundation of China (61472097) and the Open Fund of the State Key Laboratory of Information Security(2016-MS-10).

References

[1] Y. Aono, X. Boyen, L. Wang, "Key-private proxy re-encryption under LWE," in *The 14th International Conference on Cryptology*, pp. 1-18, 2013.

[2] G. Ateniese, K. Benson, S. Hohenberger, "Key-private proxy re-encryption," in *Cryptographers Track at the RSA Conference*, pp. 279-294, 2009.

[3] G. Ateniese, K. Fu, M. Green, S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," *ACM Transactions on Information and System Security (TISSEC'06)*, vol.9, no. 1, pp.1-30, 2006.

[4] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in *Advances in Cryptology (EUROCRYPT'98)*, pp. 127-144, 1998.

[5] Z. Brakerski, V. Vaikuntanathan, "Efficient fully homomorphic encryption from (Standard) LWE," in *The 52nd Annual IEEE Symposium on Foundations of Computer Science (FOCS'11)*, pp. 97-106, 2011.

[6] Z. Brakerski, C. Gentry, V. Vaikuntanathan, "(leveled) Fully homomorphic encryption without bootstrapping," in *The 3rd Innovations in Theoretical Computer Science Conference (ITCS'12)*, pp. 309-325, 2012.

[7] Z. Brakerski, "Fully homomorphic encryption without modulus switching from classical GapSVP," in *The 32nd Annual Cryptology Conference (CRYPTO'12)*, pp. 868-886, 2012.

[8] Z. Cao, L. Liu, Y. Li, "Ruminations on fully homomorphic encryption in client-server computing scenario," *International Journal of Electronics and Information Engineering*, vol. 8, no. 1, pp. 32-39, 2018.

[9] P. Chung, C. Liu, M. Hwang, "A study of attribute-based proxy re-encryption scheme in cloud environments," *International Journal of Network Security*, vol.16, no.1, pp. 1-13, 2014.

[10] C. Gentry, "A fully homomorphic encryption scheme," *ACM Digital Library*, 2009. ISBN: 978-1-109-44450-6

[11] M. M. Jiang, Y. P. Hu, B. C. Wang, *et al.*, "Lattice-based multi-use unidirectional proxy re-encryption," *Security and Communication Networks*, vol. 18, no. 8, pp. 3796-3803, 2015.

[12] E. Kirshanova "Proxy re-encryption from lattices," in *International Workshop on Public Key Cryptography*, pp. 77-94, 2014.

[13] C. Lan, H. Li, S. Yin, *et al.*, "A new security cloud storage data encryption scheme based on identity proxy re-encryption," *International Journal of Network Security*, vol. 19, no. 5, pp. 804-810, 2017.

[14] L. Liu, Z. Cao, "Analysis of two confidentiality-preserving image search schemes based on additive homomorphic encryption," *International Journal of Electronics and Information Engineering*, vol. 5, no. 1, pp. 1-5, 2016.

[15] C. Ma, J. Li, G. Du, "A flexible fully homomorphic Encryption," *Wireless Personal Communications*, vol. 95, no. 2, pp. 761-772, 2017.

[16] C. Ma, J. Li, W. Ouyang, "A homomorphic proxy re-encryption from Lattices," in *10th International Conference*, pp.353-372, 2016.

[17] C. Ma, J. Li, W. Ouyang, "Lattice-based identity-based homomorphic conditional proxy re-encryption for secure big data computing in cloud environment," *International Journal of Foundations of Computer Science*, vol. 28, no. 6, pp. 645-660, 2017.

[18] R. Nishimaki, K. Xagawa, "Key-private proxy re-encryption from lattices, revisited," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 98, no. 1, pp. 100-116, 2015.

[19] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in *The 37th Annual ACM Symposium on Theory of Computing (STOC'05)*, pp. 84-93, 2005.

[20] K. Singh, C. P. Rangan, A. K. Banerjee, "Cryptanalysis of unidirectional proxy re-encryption scheme," in *Information and Communication Technology-EurAsia Conference*, pp. 564-575, 2014.

[21] Y. Wang, D. Yan, F. Li, X. Hu, "A key-insulated proxy Re-encryption Scheme for data sharing in a cloud environment," *International Journal of Network Security*, vol. 19, no. 4, pp. 623-630, 2017.

[22] K. Xagawa, *Cryptography with Lattices*, PhD thesis, Tokyo Institute of Technology, Tokyo, 2010.

Table 1: Comparison

Cryptosystem	Computation complexity	Message	INC-CPA	KP-CPA	LWE	Many-to-one
The scheme of [16, 17]	$O(n^2)$	1	YES	YES	YES	YES
The proposed scheme	$O(n^2)$	2	YES	YES	YES	YES

[23] M. Zhang, L. Wu, X. Wang, X. Yang, "Unidirectional IBPRE scheme from lattice for cloud computation," *Journal of Ambient Intelligence and Humanized Computing*, vol. 7, pp. 623-631, 2016.

[24] H. Zhong, J. Cui, R. Shi, C. Xia, "Many-to-one homomorphic encryption scheme," *Security and Communication Networks*, vol. 9, pp. 1007-1015, 2015.

Biography

Juyan Li is currently a Ph.D. candidate at Harbin Engineering University, Harbin, China. Currently his researches focus on cryptography and information security. His email address is lijuyan587@163.com

Chunguang Ma is a full professor in the Harbin Engineering University. He received his BSc, MSc and PhD in 1996, 2002 and 2005 respectively. His current research interests include post-quantum cryptography, distributed cryptographic protocol, cloud computing security and privacy, AI and security, block chain technology and application, etc. He published many papers and his research is funded by Natural Science Foundation of China, Natural Science Foundation of Heilongjiang. He is the corresponding author of this work and his email address is machunguang@hrbeu.edu.cn.

Lei Zhang is currently a Ph.D. candidate at Harbin Engineering University, Harbin, China. Currently his researches focus on cryptography and information security.

Qi Yuan is currently a Ph.D. candidate at Harbin Engineering University, Harbin, China. Currently her researches focus on cryptography and information security.