AN ADAPTIVELY SECURE NIPE SCHEME BASED ON DCR ASSUMPTION

Haiying Gao and Chao Ma

Information Engineering University, Zhengzhou, China

ABSTRACT

Non-zero inner product encryption provides fine-grained access control to private data, but the existing non-zero inner product encryption schemes are mainly constructed based on the problem of bilinear groups and lattices without homomorphism. To meet the needs of users to control private data and cloud servers to directly process ciphertexts in a cloud computing environment, this paper designs a non-zero inner product encryption scheme based on the DCR assumption. Specifically, the access control policy is embedded in the ciphertext by a vector $\boldsymbol{y}$*, and the user attribute vector* $\boldsymbol{x}$ *is embedded in the secret key. If the inner product of the policy vector* $\boldsymbol{y}$ *of the encryptor and the attribute vector* $\boldsymbol{x}$ *of the decryptor is not zero, the decryptor can decrypt correctly. This scheme has additive homomorphism in the plaintext-ciphertext space, and it can be proved to be additive homomorphic and adaptively secure.*

KEYWORDS

Non-Zero Inner Product Encryption, Adaptive secure, Decision Composite Residuosity.

1. INTRODUCTION

With the rapid development of cloud computing and big data technology, the protection of cloud data has attracted more and more attention. ABE (Attribute-based Encryption) is a new type of Function Encryption (FE), which can simultaneously support sensitive data protection and access control [1, 2, 3]. For example, it can be used for fine-grained access control to cloud-encrypted data and support conditional information sharing in the cloud computing environment. In a inner product attribute encryption scheme, the policy vector $\boldsymbol{y}$ and the attribute vector $\boldsymbol{x}$ is embedded in the ciphertext or secret key. If the inner product of the decrypted user's attribute vector $\boldsymbol{x}$ and the policy vector $\boldsymbol{y}$ is equal to the preset value, the decryption algorithm can output plaintext. A scheme is called Zero Inner Product Encryption (ZIPE) scheme if the preset value is zero, otherwise, it will be called a Non-zero Inner Product Encryption (NIPE) scheme. This paper studies the design of a NIPE scheme.

The existing NIPE schemes are mainly constructed based on the difficult problems of bilinear groups and lattices, unfortunately, they do not have homomorphism. To meet the needs of users to control the private data in the cloud computing environment and the direct processing of ciphertext by the cloud server, this paper proposes a NIPE scheme based on the Decision Composite Residuosity (DCR) assumptio. Specifically, the policy vector $\boldsymbol{y}$ is embedded in the ciphertext in the form of a vector by modular multiplication and the user attribute vector $\boldsymbol{x}$ is embedded in the secret key by calculating the inner product of the attribute vector and the master secret key. The NIPE scheme can be used for ciphertext access control. As shown in Figure 1, the goal of the encryptor Alice is: Bob can decrypt correctly if his attribute w not belongs to the set $\Omega = \{w_1, w_2, ..., w_{n-1}\}$. The NIPE scheme can be used for this purpose and the specific description

David C. Wyld et al. (Eds): AIAPP, NLPML, DMA, CRIS, SEC, CoSIT, SIGL - 2022
pp. 169-183, 2022. CS & IT - CSCP 2022 DOI: 10.5121/csit.2022.120914

is as follows.

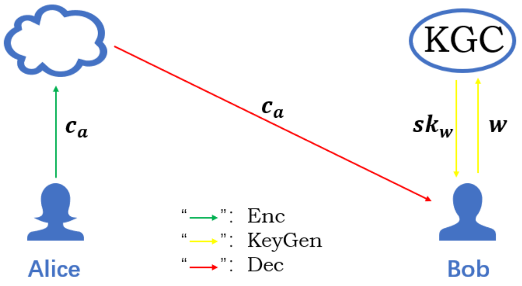

Figure 1. A NIPE scheme for ciphertext access control

Encryption. Alice constructs the polynomial $\phi(x)=(x-w_1)(x-w_2)...(x-w_{n-1})=a_0+a_1x+...+a_{n-1}x^{n-1}$ cording to the above set Ω, then embeds the policy vector $\boldsymbol{a}=(a_0,a_1,...,a_{n-1})$ to the ciphertext c_a.

Key Generation. Bob sends his attribute vector $\boldsymbol{w}=(1,w,...,w^{n-1})$ to Key Generation Center (KGC), then KGC generates a secret key sk_w and sends it to Bob securely.

Decryption. Bob downloads the ciphertext c from the cloud server to the local machine and he can decrypt it correctly if $\langle \boldsymbol{a},\boldsymbol{w}\rangle \neq 0$ (ie $\boldsymbol{w}\notin\Omega$).

Through the above scheme, Alice realizes the encryption and access control of the message at the same time.

Homomorphic Encryption. The homomorphic encryption scheme allows anyone to directly process the ciphertext without knowing the plaintext. And the effect is equivalent to operating on the plaintext first and then encrypting the result. Homomorphic encryption can be widely used in secret voting, bidding and so on [4]. According to the type of homomorphic mapping [5], homomorphic encryption schemes can be divided into additive homomorphism and multiplicative homomorphism. For example, RSA and ElGamal encryption belongs to multiplicative homomorphism, while Paillier encryption belongs to additive homomorphism [6, 7, 8].

This paper studies the NIPE scheme with additive homomorphism, which supports the direct operation of the cloud server on the ciphertext and realizes the access control of the encrypted user to the ciphertext at the same time. To illustrate the practical application of NIPE with additive homomorphism, Figure 2 shows an example of this type of scheme applied to confidential data query and the example is described as follows:

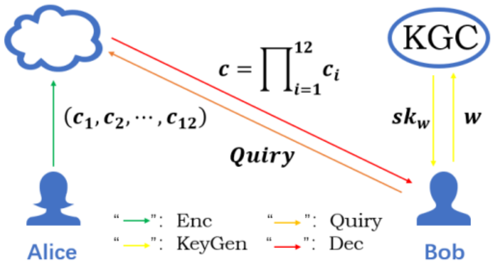

Figure 2. A NIPE scheme for querying average salary.

Encryption. Alice uses the NIPE scheme with additive homomorphism to encrypt the everyone's salary $m_1, m_2, ..., m_{12}$ in a department and obtains the ciphertext sequence $c_1, c_2, ..., c_{12}$, which is embedded with the same policy vector. Then upload the ciphertext sequence to the cloud server.

Key generation. Bob sends his attribute vector $\boldsymbol{w} = \left(1, w, ..., w^{n-1}\right)$ to KGC, then KGC generates a secret key and sends it to Bob securely.

Query. Bob wants to know the average salary in this department, so he sends a request to the cloud server to "Query the average salary".

Operation. The cloud server calculates $c = c_1 + c_2 + ... + c_{12}$ and sends c Bob.

Decryption. Bob can get $ave = \left(m_1 + m_2 + ... + m_{12}\right)/12$ if his attribute vector and the policy vector in ciphertext c meet the conditions $\langle \boldsymbol{a}, \boldsymbol{w} \rangle \neq 0$.

To design the NIPE scheme with additive homomorphism, we need to consider both the IPE schemes and the design method of the FE schemes with additive homomorphism. The following introduces and analyzes the current research status. Katz et al. proposed the first IPE scheme based on composite-order bilinear groups, which only achieves selective security and the length of the ciphertext is linearly related to the dimension of the policy vector [9]. Attrapadung and Libert constructed ZIPE and NIPE schemes with constant-size ciphertexts, but only the zero inner product encryption scheme can be proved to be adaptively secure [10]. Okamoto and Takashima proposed two adaptively secure NIPE schemes based on the DLIN assumption, one of which has a constant-size ciphertext and the other has a constant-size secret key [11]. Later, they first proposed an adaptively secure IPE scheme with constant-size public parameters. The dimension of the policy vector and the number of attributes are not restricted by public parameters [12]. In 2014, Chen and Wee first proposed the NIPE scheme based on the DBDH assumption which can be used for identity revocation, but only has selective security [13]. To resist quantum attacks, designing public-key cryptographic schemes based on difficult problems on the lattice has become a research hotspot. Agrawal et al. first proposed an inner product function encryption scheme based on Learning with Errors (LWE) assumption in a lattice group, which has weak attribute hiding but only selective security [14]. The above schemes are all constructed on bilinear groups or lattices without additive homomorphism and multiplicative homomorphism so that they are not suitable for dense state computing of cloud data. In 2016, Agrawal et al. constructed a FE scheme on the Paillier group based on the DCR assumption, which provided us with ideas for designing an additive homomorphic NIPE scheme [15]. Table 1 shows the characteristics of our scheme and previous schemes.

Our contribution. Considering that the public key encryption scheme constructed based on the DCR assumption has additive homomorphism, we decided to learn from the advantages of the existing IPE schemes to design a NIPE scheme based on this assumption. Katsuma and Yamada presented an adaptively secure NIPE scheme based on lattice and a framework for transforming from FE to NIPE [16]. Using this framework, this paper designs a NIPE scheme with additive homomorphism based on the DCR assumption. It can not only realize the access control to ciphertext data but also is suitable for ciphertext calculation so that it has a wider application prospect. In terms of the security, we prove that the scheme is adaptively secure based on the DCR assumption with a series of indistinguishable game sequences. In short, the scheme given in this article has the following two characteristics.

1. It can be widely used in attribute revocation, blacklist management, secret voting, etc.
2. It has additive homomorphism and can be used for ciphertext retrieval, etc.

Organization. Section 2 provides the basic knowledge and symbols that need to be explained in this article. Section 3 introduces our scheme and its security proof. Section 4 gives the performance analysis.

Table 1. Comparison of previous works about IPE

Paper	Type	Homomorphism	Assumption	Security
[9]	ZIPE	No	Subgroup Decision	Selective
[10]	ZIPE	No	DLIN	Adaptive
	NIPE			Selective
[11]	NIPE	No	DLIN	Adaptive
[12]	ZIPE	No	DLIN	Adaptive
[13]	NIPE	No	DBDH	Selective
[14]	FE	No	LWE	Selective
Our	NIPE	Addition	DCR	Adaptive

2. FORMAT GUIDE

Notation. Let Z denote the set of integers. Let Z_N^* denote the reduced residues system of modulo N. We represent a vector $(x_1,\ldots,x_l)\in \mathrm{Z}_p^l$ with lowercase boldface characters $\boldsymbol{x}$, and represent its infinite norm with $\|\boldsymbol{x}\|_\infty$. Let$[a,b]=$ $\{a,a+1,..,b\}$ for natural numbers a and b if $a<b$. In particular, $[a,b]$ will be written as $[b]$ if $a=1$. Let natural number λ denotes the standard security parameter. Let $negl(\lambda)$ denotes a negligible function which is less than $1/\mathrm{p}(\lambda)$ for a polynomial function $\mathrm{p}(\lambda)$.

Definition 1. (s-DCR Assumption [4, 17]). Given $N=pq$ and p,q are two large prime numbers. Define the s-DCR (with integer $s>0$) assumption as follows: For any Probability Polynomial Time (PPT) adversary A, the advantage of distinguishing the following two distributions is negligible.

$$D_0=\left\{z=z_0^{N^s} \bmod N^{s+1}, z_0\in \mathrm{Z}_N^*\right\},\ D_1=\left\{z\in \mathrm{Z}_{N^{s+1}}^*\right\}.$$

Note. We set $D_0=\left\{z=z_0^N \bmod N^2, z_0\in \mathrm{Z}_N^*\right\}$, $D_1=\left\{z\in \mathrm{Z}_{N^2}^*\right\}$ in 1-DCR problem.

Definition 2. (Formal Definition of the NIPE Scheme).

$\boldsymbol{Setup}\left(1^{\lambda},1^{l}\right)\rightarrow mpk,msk$: First input the security parameters $\left(\lambda,\ l\right)$, then output the master public key mpk and master secret key msk .

$\boldsymbol{KeyGen}\ (msk,\boldsymbol{x})\rightarrow sk$: First input an attribute vector $\boldsymbol{x}$, then compute the secret key sk and retain it.
$\boldsymbol{Enc}(mpk,m\cdot\boldsymbol{y})\rightarrow c$: First input the message m and vector $\boldsymbol{y}$, then output the ciphertext c .
$\boldsymbol{Dec}\left(mpk,\left(\boldsymbol{x},sk\right),\left(\boldsymbol{y},c\right)\right)\rightarrow m$: First input the $\left(\boldsymbol{x},sk\right)$ and $\left(\boldsymbol{y},c\right)$, then output the message m if $\left\langle\boldsymbol{x},\boldsymbol{y}\right\rangle\neq 0$.

Definition 3. (Adaptive Security Model of the NIPE Scheme).

This model is described by a series of games between adversary A and challenger Bł.

Setup. The challenger Bł runs the ***Setup***, then sends mpk to the adversary A .

Phase 1. The adversary A adaptively chooses an attribute vector $\boldsymbol{x}'$ for a secret key query. Then the challenger Bł runs ***KeyGen*** and returns $sk_{x'}$.

Challenge Phase. The adversary A submits two equal-length messages (m_1 and m_2) and the challenge vector $\boldsymbol{y}$ to the challenger B (Any challenge attribute vector $\boldsymbol{x}'$ and vector $\boldsymbol{y}$ satisfy $\left\langle\boldsymbol{x}',\boldsymbol{y}\right\rangle=0$). Then challenger B samples $b\in\left\{0,1\right\}$, runs ***Enc*** and returns c to the adversary A .

Phase 2. The adversary A may do more secret key queries, the specific steps are as Phase 1.

Guess. Finally, the adversary A outputs a guess b' about $b\in\left\{0,1\right\}$ and A win the game if $b'=b$. Now we let Adv_i denote the advantage of a PPT adversary A wins in the $Game_i$. If $Adv_{\mathrm{A}}\left(\lambda\right)$ is a negligible function for any PPT adversary A , we say it is adaptively secure.

3. ADAPTIVELY SECURE NIPE SCHEME BASED ON DCR ASSUMPTION

In this section, we propose our NIPE scheme based on DCR assumption. Sect.3.1, Sect.3.3 and Sect.3.4 show a specific description of its construction, security and homomorphism proof.

3.1. Construction

We first show our scheme by four PPT algorithms.

```
Algorithm 1  Setup$\left(1^{\lambda},1^{l}\right)$
Input: Security parameter $\lambda$ and vector dimension $l$ .
Output: Master public key $mpk$ and master secret key $msk$ .
1.  Pick two prime numbers $p$ and $q$ of the form $p=2p'+1$ (random prime numbers
    $p',q'>2^{\mathrm{p}(\lambda)}$ ).
```

```
2. Let $N = pq$.
3. Sample $g' \in \mathbb{Z}_{N^2}^*$ and compute $g = g'^{2N} \bmod N^2$.
4. Sample $s_i \in \{-2^{\lambda-1}N^4, -2^{\lambda-1}N^4+1, ..., 2^{\lambda-1}N^4\}$ and compute $h_i = g^{s_i} \bmod N^2$.
5. Return $mpk = \left(N, g, \{h_i\}_{i\in[l]}\right)$, $msk = \{s_i\}_{i\in[l]}$.
```

```
Algorithm 2 KeyGen $(msk, \boldsymbol{x})$
Input: Master secret key $msk$ and attribute vector $\boldsymbol{x}$.
Output: Secret key $sk$.
1. Select the attribute vector $\boldsymbol{x} = (x_1, x_2, ..., x_l) \in \mathbb{Z}^l$ and $0 \le x_i < N^{1/4} l^{-1/2}$.
2. Compute $sk = \sum_{i=1}^{l} s_i \cdot x_i \in \mathbb{Z}$.
3. Return $sk$.
```

```
Algorithm 3 Enc$(mpk, m \cdot \boldsymbol{y})$
Input: Message $0 < m < N^{1/2}$, vector $\boldsymbol{y} = (y_1, y_2, ..., y_l) \in \mathbb{Z}^l$ and $0 \le y_i < N^{1/4} l^{-1/2}$.
Output: Ciphertext $c$.
1. Pick $r \in \{0, \ldots, \varphi(N)/2\}$ randomly and compute
       $c = \left\{ \begin{array}{l} c_0 = g^r \bmod N^2 \\ \left\{c_i = (1 + m \cdot y_i N) \cdot h_i^r \bmod N^2\right\}_{i\in[l]} \end{array} \right\}$.
2. Return the ciphertext $c$.
```

```
Algorithm 4 Dec$(mpk, (\boldsymbol{x}, sk), (\boldsymbol{y}, c))$
Input: $(\boldsymbol{x}, sk)$ and $(\boldsymbol{y}, c)$
Output: message $m$
1. Compute
       $\hat{c} = \prod_{i=1}^{l} c_i^{x_i} \cdot c_0^{-sk} \bmod N^2$, $z = \begin{cases} (\hat{c} - 1) \bmod N^2 / N, & if \langle \boldsymbol{x}, \boldsymbol{y} \rangle > 0 \\ ((\hat{c} - 1) \bmod N^2 - N^2)/N, & if \langle \boldsymbol{x}, \boldsymbol{y} \rangle < 0 \end{cases}$.
2. Return the message $m = z / \langle \boldsymbol{x}, \boldsymbol{y} \rangle$.
```

3.2. Correctness

The correctness of the decryption algorithm is given by the following formula.

$$
\begin{aligned}
\tilde{c} &= \prod_{i=1}^{l} c_i^{x_i} \cdot c_0^{-sk} \bmod N^2 \\
&= \prod_{i=1}^{l} \left(1 + N \cdot m \cdot y_i\right)^{x_i} \cdot h_i^{r \cdot x_i} \cdot g^{-r \cdot sk} \bmod N^2 \\
&= \prod_{i=1}^{l} \left(1 + N \cdot m \cdot x_i \cdot y_i\right) \cdot g^{r \cdot s_i \cdot x_i} \cdot g^{-r \sum_{i=1}^{l} s_i \cdot x_i} \bmod N^2 \\
&= \prod_{i=1}^{l} \left(1 + N \cdot m \cdot x_i \cdot y_i\right) \bmod N^2 \\
&= 1 + m \cdot N \sum_{i=1}^{l} x_i \cdot y_i \bmod N^2 \\
&= 1 + m \cdot N \cdot \langle \boldsymbol{x}, \boldsymbol{y} \rangle \bmod N^2
\end{aligned}
$$

$z = (\tilde{c} - 1) \bmod N^2 / N = m \cdot \langle \boldsymbol{x}, \boldsymbol{y} \rangle$ if $\langle \boldsymbol{x}, \boldsymbol{y} \rangle > 0$ and $z = \left((\tilde{c} - 1) \bmod N^2 - N^2\right) / N = m \cdot \langle \boldsymbol{x}, \boldsymbol{y} \rangle$ if not, so there must be $m = z / \langle \boldsymbol{x}, \boldsymbol{y} \rangle$.

Note. A few notes about the process of decryption.

(1). Regarding the calculation of $c_0^{-sk} \bmod N^2$. We first need to calculate $c_0^{sk} \bmod N^2$ if $sk > 0$, and then use the extended Euclidean algorithm to calculate $\left(c_0^{sk} \bmod N^2\right)^{-1} \bmod N^2$. The following analysis that $c_0^{sk} \bmod N^2$ must be reversible. And $c_0^{sk} \bmod N^2$ can be written as $(g')^{w} \bmod N^2$ because of $c_0 = g'^{2Nr} \bmod N^2$ and $g' \in \mathrm{Z}_{N^2}^{*}$. If $(N\varphi(N)) \mid w$, then the inverse element of $c_0^{sk} \bmod N^2$ is 1. Otherwise, $u^{w} \bmod N^2 = (g')^{-w} \bmod N^2$ and $u = (g')^{-1} \bmod N^2$.

(2) According to the parameter setting, we have

$$
\left| m \cdot \langle \boldsymbol{x}, \boldsymbol{y} \rangle \right| < \left| N^{1/2} \cdot \sum\nolimits_{i=1}^{l} x_i y_i \right| < N^{1/2} \cdot l \cdot N^{1/4} l^{-1/2} \cdot N^{1/4} l^{-1/2} = N .
$$

That is, if the attribute vector $\boldsymbol{x}$ satisfies $\langle \boldsymbol{x}, \boldsymbol{y} \rangle \neq 0$, the decryption algorithm can output the message m.

To facilitate the understanding of the above scheme, specific examples are given below to illustrate the specific operation process of the scheme.

Setup: Set the number of attributes $l = 2$, "safe" parameters $\lambda = 2,\ \mathrm{p}(\lambda) = \lambda = 2$, two isometric prime numbers $(p,\ q) = (11,\ 13)$. Compute $N = 143,\ N^2 = 20449,\ 2 < N^{1/4} l^{-1/2} < 3$. Select $g' = 3,\ g = g'^{2N} = 9441 \bmod N^2,\ (s_1, s_2) = (2,3)$, and compute $(h_1, h_2) = (15739,\ 9465)$. Output $mpk = (143, 9441, \{15739,\ 9465\}),\ msk = \{2,3\}$ 。

KeyGen: Let the attribute vector $\boldsymbol{x} = (2,2)$, output the secret key $sk = s_1 x_1 + s_2 x_2 = 10$.

The following shows the corresponding encryption and decryption operations for embedding two different vectors $\boldsymbol{y}$ in the ciphertext.

1. If the vector $\boldsymbol{y}$ selected in the encryption algorithm satisfies $\langle \boldsymbol{x},\boldsymbol{y}\rangle > 0$.

Enc: Input $m=5,\ \boldsymbol{y}=(1,2),\ r=2$ and output as follows.

$$\left\{\begin{array}{l} c_0 = 9441^2 \bmod 20449 = 15739 \\ c_1 = (1+5\times 1\times 143)\times 15739^2 \bmod 20449 = 13952 \\ c_2 = (1+5\times 2\times 143)\times 9465^2 \bmod 20449 = 19176 \end{array}\right\}$$

Dec: At this point, we have $\langle \boldsymbol{x},\boldsymbol{y}\rangle = 6 > 0$. Firstly, calculate $c_0{}^{sk} = 19119 \bmod N^2,\ c_0{}^{-sk}$. $=19119^{-1} = 10286 \bmod N^2$ and $\hat{c} = c_1{}^{x_1}\cdot c_2{}^{x_2}\cdot c_0{}^{-sk} = 7723 \bmod N^2$. Compute $z=(\hat{c}-1)/N=30$ because of $\langle \boldsymbol{x},\boldsymbol{y}\rangle > 0$. Finally, output the message $m = z/\langle \boldsymbol{x},\boldsymbol{y}\rangle = 5$.

2. If the vector $\boldsymbol{y}$ selected in the encryption algorithm satisfies $\langle \boldsymbol{x},\boldsymbol{y}\rangle < 0$.

Enc: Input $m=5,\ \boldsymbol{y}=(1,-2),\ r=2$ and output as follows.

$$\left\{\begin{array}{l} c_0 = 15739,\ c_1 = 13952 \\ c_2 = (1+5\times(-2)\times 143)\times 9465^2 \bmod 20449 = 20034 \end{array}\right\}$$

Dec: At this point, we have $\langle \boldsymbol{x},\boldsymbol{y}\rangle = -2 < 0$. Firstly, calculate $c_0{}^{sk} = 19119 \bmod N^2,\ c_0{}^{-sk}$. $=19119^{-1} = 10286 \bmod N^2$ and $\hat{c} = c_1{}^{x_1}\cdot c_2{}^{x_2}\cdot c_0{}^{-sk} = 19020 \bmod N^2$. Then because of $\langle \boldsymbol{x},\boldsymbol{y}\rangle < 0$, $z=(\hat{c}-1-N^2)/N=-10$. Finally, output the message as $m = z/\langle \boldsymbol{x},\boldsymbol{y}\rangle = 5$.

3.3. Security

Our security proof relies on a series of games which are detailed below. Table 2 shows some parameters in these four games.

Games.

Game$_0$. The original system generates the sk and ciphertext c.

Game$_1$. Same as $Game_0$, but the range of $\{s_i\}_{i\in[l]}$ is changed. Specifically, the challenger B reduces the upper bound of $\{s_i\}_{i\in[l]}$ such as $|s_i| < 2^{\lambda-1}N^4 - (N^4/2)$.

Note that the upper bound of the value of $\{s_i\}_{i\in[l]}$ is reduced in Game_1, and the upper bound of the value is restored to $2^{\lambda-1}N^4$ by a special parameter setting method in the proof of $Game_3$. This step is to prepare for finding equivalent parameters in $Game_3$.

$Game_2$. Compare to $Game_1$, modify the challenge ciphertext $c=(c_0,c_1,...,c_l)$. Specifically, the challenger B computes

$$c=\begin{Bmatrix} c_0=z^2=\left(z_0{}^N\right)^2 \bmod N^2, z=z_0{}^N \bmod N^2,\ z_0\in \mathrm{Z}_N^* \\ \left\{c_i=\left(1+m_b\cdot y_iN\right)\cdot c_0{}^{s_i} \bmod N^2\right\}_{i\in[l]} \end{Bmatrix}.$$

The modification is to connect the attack scheme with the 1-DCR assumption.

$Game_3$. Modify the first item of the challenge ciphertext

$$c_0=z^2 \bmod N^2, z\in \mathrm{Z}_{N^2}^*.$$

Then compute c_i as $Game_2$

$$c_i=\left(1+m_b\cdot y_iN\right)\cdot c_0{}^{s_i} \bmod N^2, i\in[l].$$

Note that $Game_3$ is designed to make the ciphertext of m_0 under one set of parameters, from the algebraic expression, equivalent to the ciphertext of m_1 under another set of parameters. And the adversary cannot distinguish between the two sets of parameters, so the adversary's attack advantage is almost zero.

Table 2. Master secret key and ciphertext in four games.

Game	$\boldsymbol{Game_0}$	$\boldsymbol{Game_1}$	$\boldsymbol{Game_2}$	$\boldsymbol{Game_3}$
c_0	g^r	g^r	$z_0^{2N}, z_0\in \mathrm{Z}_N^*$	$z^2, z\in \mathrm{Z}_{N^2}^*$
c_i	$(1+m\cdot y_iN)\cdot h_i^r$	$(1+m\cdot y_iN)\cdot h_i^r$	$(1+m\cdot y_iN)\cdot c_0{}^{s_i}$	$(1+m\cdot y_iN)\cdot c_0{}^{s_i}$
$\lvert s_i\rvert$	$2^{\lambda-1}N^4$	$2^{\lambda-1}N^4-\left(N^4/2\right)$	$2^{\lambda-1}N^4-\left(N^4/2\right)$	$2^{\lambda-1}N^4-\left(N^4/2\right)$

Lemma 1 ($Game_0 \approx Game_1$). The advantage of the adversary As in $Game_0$ and $Game_1$ satisfies $|Adv_0-Adv_1|\le l/2^{\lambda}$.

Proof. We first analyze the differences about various parameters and focus on $\{h_i\}_{i\in[l]}$. Obviously, relative to $Game_0$, $Game_1$ only changes the bound of $\{s_i\}_{i\in[l]}$. Consequently, $|Adv_0-Adv_1|\le l\cdot\left(N^4/2^{\lambda}N^4\right)=l/2^{\lambda}$.

Lemma 2 ($Game_1 \approx Game_2$). The advantage of the adversary A in $Game_1$ or $Game_2$ satisfies $|Adv_1-Adv_2|<1/2^{\mathrm{p}(\lambda)}$.

Proof. We conclude that $g^r \approx_c z^2 \bmod N^2$ based on that they are both $(2N)$th residuals in $\mathrm{Z}_{N^2}^*$, which means that the ciphertext in $Game_1$ and $Game_2$ have the same distribution. That is, As can't determine whether the ciphertext distribution belongs to $Game_1$ or $Game_2$. Consequently,

$\left|Adv_1 - Adv_2\right| \le 1/2^{\mathrm{p}(\lambda)}$.

Lemma 3 ($Game_2 \approx Game_3$). There exists a challenger B_1 who can solve 1-DCR problem with a non-negligible advantage if the adversary A can determine c in $Game_2$ or $Game_3$. That is, $\left|Adv_2 - Adv_3\right| \le Adv_{\mathrm{B}_1}^{1-DCR}(\lambda)$.

Proof. From 1-DCR assumption, let

$$\mathrm{D}_0 = \left\{ z = z_0^{2N} \bmod N^2, z_0 \in \mathrm{Z}_N^* \right\},\ \ \mathrm{D}_1 = \left\{ z^2, z \in \mathrm{Z}_{N^2}^* \right\}.$$

T is the input of the challenger Bþ. To determine T belongs to D_0 or D_1, Bþ performs as the following algorithm.

```
Algorithm 3.5
Setup:
    1. $\mathrm{B}_1$ runs algorithm ***Setup***.
    2. $\mathrm{B}_1$ samples
           $s_i \in \left\{ -2^{\lambda-1}N^4 + \left(N^4/2\right), -2^{\lambda-1}N^4 + 1, ..., 2^{\lambda-1}N^4 - \left(N^4/2\right) \right\}$ .
    3. $\mathrm{B}_1$ sends $mpk$ to the adversary $\mathrm{A}$ .
Phase 1:
    1. $\mathrm{A}$ adaptively choose an attribute vector $\boldsymbol{x}' = \left(x_1', x_2', ..., x_l'\right) \in \mathrm{Z}^l$ .
    2. $\mathrm{B}_1$ runs the *KeyGen* and sends $sk_{x'}$ to adversary $\mathrm{A}$ .
Challenge:
    1. $\mathrm{A}$ submits two equal-length messages ( $m_1$ and $m_2$ ) and the challenge vector $\boldsymbol{y}$
    to $\mathrm{B}_1$ (Any challenge attribute vector $\boldsymbol{x}'$ and vector $\boldsymbol{y}$ satisfy $\left\langle \boldsymbol{x}', \boldsymbol{y} \right\rangle = 0$ ).
    2. $\mathrm{B}_1$ samples $b \in \{0,1\}$ , runs the algorithm *Enc* and returns $c$ to the adversary
    $\mathrm{A}$ .
           $c = \left\{ c_0 = T \bmod N^2, \left\{ c_i = \left(1 + m_b \cdot y_i N\right) \cdot T^{s_i} \bmod N^2 \right\}_{i \in [l]} \right\}$
Phase 2: $\mathrm{A}$ may do more secret key queries, the specific steps are as Phase 1.
Guess: $\mathrm{A}$ outputs a guess $b' \in \{0,1\}$ and $\mathrm{A}$ wins the game if $b' = b$ .
```

Note: If $T \in \mathrm{D}_0$, we have

$$c = \left\{ c_0 = z_0^{2N} \bmod N^2, \left\{ c_i = \left(1 + m_b \cdot y_i N\right) \cdot z_0^{2Ns_i} \bmod N^2 \right\}_{i \in [l]} \right\},$$

If $T \in \mathrm{D}_1$, we have

$$c = \left\{ c_0 = z^2 \bmod N^2, \left\{ c_i = \left(1 + m_b \cdot y_i N\right) \cdot c_0^{s_i} \bmod N^2 \right\}_{i \in [l]} \right\}.$$

That is, B_1 can solve the 1-DCR problem if A can distinguish $Game_2$ from $Game_3$. So we conclude $\left|Adv_2 - Adv_3\right| \le Adv_{\mathrm{B}_1}^{1-DCR}(\lambda)$.

Lemma 4 $\left|Adv_3 - 1/2\right| < 1/2^{\mathrm{p}(\lambda)}$.

Proof. We sample $\alpha_z \in \mathrm{Z}_N$, $r_z \in \mathrm{Z}_{p'q'}$ and modify $c_0 = \left(1+\alpha_z N\right)\cdot g^{r_z} \bmod N^2$. This is the same as the expression $c_0 = z^2 \bmod N^2$ because it is also the square residue in $\mathrm{Z}^*_{N^2}$ (This is due to $c_0 = \left(1+\alpha_z N\right)\cdot g^{r_z} = \left(\left(\left(\alpha_z N\cdot\left(N+1\right)/2\right)+1\right)\cdot g'^{N\cdot r_z}\right)^2 \bmod N^2$). Then we have

$$\begin{aligned} c_i &= \left(1+m_b\cdot y_i N\right)\cdot\left(1+\alpha_z N\right)^{s_i}\cdot g^{r_z\cdot s_i} \bmod N^2 \\ &= \left(1+m_b\cdot y_i N\right)\cdot\left(1+s_i\alpha_z N\right)\cdot g^{r_z\cdot s_i} \bmod N^2 \\ &= \left(1+m_b\cdot y_i N+\alpha_z s_i N\right)\cdot g^{r_z\cdot s_i} \bmod N^2,\ i\in[l] \end{aligned}.$$

We observe that the integer $\alpha_z \in \mathrm{Z}_N$ is invertible with the probability $1-\left(p+q-1\right)/pq$ which is close to 1. So there must be an integer $\mu \in \mathrm{Z}$, $|\mu| < N$ which causes $\mu\cdot p'q' \equiv 1 \bmod N$ based on the fact $\gcd\left(p'q', N\right)=1$. Besides, define

$$\left\{s_i' = s_i + \left(a_z^{-1} \bmod N\right)\cdot\left(m_b - m_{1-b}\right)\cdot y_i\cdot\left(\mu\cdot p'q'\right)\in \mathrm{Z}\right\}_{i\in[l]},$$

which shows

$$\left\{\begin{array}{l} s_i' = s_i + \left(a_z^{-1} \bmod N\right)\cdot\left(m_b - m_{1-b}\right)\cdot y_i \bmod N \\ s_i' = s_i \bmod p'q' \end{array}\right\}_{i\in[l]}\text{、}$$

and

$$\begin{aligned} c_i &= \left(1+m_{1-b}\cdot y_i N\right)\cdot c_0^{s_i'} \bmod N^2 \\ &= \left(1+m_{1-b}\cdot y_i N\right)\cdot\left(\left(1+\alpha_z N\right)\cdot g^{r_z}\right)^{s_i'} \bmod N^2 \\ &= \left(1+m_{1-b}\cdot y_i N+\alpha_z s_i' N\right)\cdot g^{r_z\cdot s_i'} \bmod N^2 \end{aligned}.$$

Besides, we show $s_i' \in \left\{-2^{\lambda-1}N^4, -2^{\lambda-1}N^4+1, \ldots, 2^{\lambda-1}N^4\right\}$ due to the following inequation:

$$\left|\left(a_z^{-1} \bmod N\right)\cdot\left(m_b - m_{1-b}\right)\cdot y_i\cdot\left(\mu\cdot p'q'\right)\right| \le N\cdot 2N^{1/2}\cdot N^{1/4}l^{-1/2}\cdot N\cdot\frac{N}{4} < \frac{N^4}{2}.$$

According to $\left\langle \boldsymbol{x}', \boldsymbol{y}\right\rangle = 0$, we get $\sum_{i=1}^{l} s_i\cdot x_i' = \sum_{i=1}^{l} s_i'\cdot x_i'$, which means that the adversary A is blind for these two master secret keys. That is, the adversary A cannot determine what the message is m_0 or m_1 because these two ciphertexts have the same distribution. That is, the advantage of the adversary A satisfies

$$\left|Adv_3 - 1/2\right| \le \left(p+q-1\right)/pq < 1/2^{\mathrm{p}(\lambda)} .$$

Theorem 1. From the 1-DCR assumption, our NIPE scheme over Z is adaptively secure.

Proof. We can determine the advantage of the adversary A in *Game₀* by lemma 1~4.

$$\left|Adv_0 - 1/2\right| \le \left|Adv_0 - Adv_1\right| + \left|Adv_1 - Adv_2\right| + \left|Adv_2 - Adv_3\right| + \left|Adv_3 - 1/2\right|$$
$$\le l/2^{\lambda} + 1/2^{\mathrm{p}(\lambda)-1} + Adv_{\mathrm{B}_0}^{1-DCR}(\lambda)$$

3.4. Homomorphism

The following shows that the scheme in this chapter has additive homomorphism, where $m_1, m_2, ..., m_k$ represents k plaintexts and $m = \sum_{j=1}^{k} m_j < \sqrt{N}$. $E\left(m_j\right) = \left\{c_0^j, c_1^j, ..., c_l^j\right\}$ represents a ciphertext obtained by encrypting the plaintext m_j and $E\left(m_j\right)_i = c_i^j$.

$$\begin{aligned}
&\left\{\prod_{j=1}^{k} E\left(m_j\right)_0, ..., \prod_{j=1}^{k} E\left(m_j\right)_i, ...\right\} \\
&= \left\{\prod_{j=1}^{k} c_0^j, ..., \prod_{j=1}^{k} c_i^j, ...\right\} \\
&= \left\{\prod_{j=1}^{k} g^{r_j} \bmod N^2, ..., \prod_{j=1}^{k} \left(1 + m_j \cdot y_i N\right) \cdot g^{s_i \cdot r_j} \bmod N^2, ...\right\} \\
&= \left\{g^{\sum_{j=1}^{k} r_j} \bmod N^2, ..., \prod_{j=1}^{k} (1+N)^{m_j \cdot y_i} \cdot g^{s_i \cdot r_j} \bmod N^2, ...\right\} \\
&= \left\{g^{\sum_{j=1}^{k} r_j} \bmod N^2, ..., (1+N)^{y_i \cdot \sum_{j=1}^{k} m_j} \cdot g^{s_i \cdot \sum_{j=1}^{k} r_j} \bmod N^2, ...\right\} \\
&= \left\{g^{\sum_{j=1}^{k} r_j} \bmod N^2, ..., (1+N)^{y_i \cdot m} \cdot g^{s_i \cdot \sum_{j=1}^{k} r_j} \bmod N^2, ...\right\} \\
&= \left\{E\left(m\right)_0, ..., E\left(m\right)_i, ...\right\}
\end{aligned}$$

To better illustrate the additive homomorphism of the scheme in this chapter, an example is given below, in which the number of plaintexts is $k = 2$.

Setup: Set the number of attributes $l = 2$, "safe" parameters $\lambda = 2,\ \mathrm{p}\left(\lambda\right) = \lambda + 1 = 3$, two isometric prime numbers $p = 11,\ q = 13$. So $N = 143,\ N^2 = 20449,\ 2 < N^{1/4} l^{-1/2} < 3$. Select $g' = 3$ and compute $g = g'^{2N} = 9441 \bmod N^2,\ \left(s_1, s_2\right) = \left(2, 3\right),\ \left(h_1, h_2\right) = \left(15739, 9465\right)$. Finally, output

$$mpk = \left(143, 9441, \left\{15739, 9465\right\}\right),\ msk = \left\{2, 3\right\}$$

KeyGen: Let the attribute vector $\boldsymbol{x} = \left(2, 2\right)$, output the secret key $sk = s_1 x_1 + s_2 x_2 = 10$.

Enc: Input $\left(m_1, m_2\right) = \left(4, 5\right),\ \boldsymbol{y} = \left(1, 2\right),\ \left(r_1, r_2\right) = \left(2, 3\right)$, then compute and output as follows.

$$\left\{c_0^1 = 15739,\ c_1^1 = 2369,\ c_2^1 = 15172\right\},\ \left\{c_0^2 = 9465,\ c_1^2 = 9166,\ c_2^2 = 15965\right\}$$

Query: A user B sends a "query request" for $m = m_1 + m_2$ to the cloud server.

Compute: The cloud server calculates the new ciphertext as follows and send it to B.

$$\left\{ c_0 = c_0^1 \cdot c_0^2 = 19119 \bmod N^2,\ c_1 = c_1^1 \cdot c_1^2 = 17865 \bmod N^2,\ c_2 = c_2^1 \cdot c_2^2 = 2575 \bmod N^2 \right\}$$

Dec: User B first calculates $c_1^{x_1} \cdot c_2^{x_2} \bmod N^2 = 14257 \bmod N^2$ and $c_0^{sk} = 19119 \bmod N^2$ after receiving the ciphertext, then $c_0^{-sk} = 19119^{-1} = 10286 \bmod N^2$. Secondly, he calculates $\hat{c} = c_1^{x_1} \cdot c_2^{x_2} \cdot c_0^{-sk} = 7723 \bmod N^2$ and $z = (\hat{c} - 1)/N$. Finally outputs the message as follows.

$$m = z / \langle \boldsymbol{x}, \boldsymbol{y} \rangle = 9 (= m_1 + m_2)$$

4. Performance Analysis

This paper constructs an adaptively secure NIPE scheme with additive homomorphism based on DCR assumption. Table 3 shows the parameter comparison between our scheme and the existing NIPE scheme, where l represents the number of attributes, $|G|$ and $|G_T|$ represents the order of the group G and G_T. B, E, D represents the time complexity of bilinear pairing, exponential, and division operations in group G.

Table 3. Parameter length and comparison of existing NIPE schemes.

Scheme	Homomo-rphism	Master public-key	Ciphertext	Decryption complexity	Assump-tion	Security
[18]	No	$6l\|G\|$	$5l\|G\|$	$9B$	DLIN	Adaptive
[13]	No	$(l^2+3l+1)\|G\|$ $+\|G_T\|$	$(2l+3)\|G\|$ $+\|G_T\|$	$9B+D$	DBDH	Selective
[15]	No	$(l+1)\|G\|$	$9\|G\|+\|G_T\|$	$3B+D$	DLIN	Selective
Our	Additive	$(l+1)\|G\|$	$(l+1)\|G\|$	$(n+1)E+D$	DCR	Adaptive

Compared with the existing NIPE schemes, the scheme in this paper has additive homomorphism, which facilitates the processing of ciphertext data in the cloud. The scale of the public parameters of the scheme is the same as that of the scheme [15], but this scheme is adaptively secure, and its security intensity is far greater than the selectively secure. Compared with the same security scheme [18], its number of ciphertexts has advantages.

5. Conclusions

This paper proposes a NIPE scheme with additive homomorphism. Based on DCR assumption, it is proved that the scheme is adaptively secure. In terms of whether it has homomorphism, this scheme selects composite-order residual class rings to replace the bilinear group used in the previous NIPE schemes, which makes the scheme have additive homomorphism and is more suitable for dense state calculation of cloud private data. But it needs to be specially pointed out that the parameter range is expanded. And how to design an adaptively secure NIPE scheme with additive homomorphism in a small parameter range is a new challenge.

ACKNOWLEDGEMENTS

This research was supported by the National Natural Science Foundation of China (No. 61902428).

REFERENCES

[1] Dan Boneh, Amit Sahai & Brent Waters, (2011) “Functional encryption: Definitions and challenges”, TCC 2011: Theory of Cryptography, LNCS 6597, pp 253-273.

[2] Adam O'Neill, (2010) “Definitional Issues in Functional Encryption”, Cryptology ePrint Archive, Report 2010/556. https://eprint.iacr.org/2010/556.pdf

[3] Amit Sahai & Brent Waters, (2005) “Fuzzy Identity-Based Encryption”, Cryptology – EUROCRYPT 2005, LNCS 3494, pp 457-473.

[4] Ronald L. Rivest, Len Adleman & Michael L. Dertouzos, (1978) “On Data Banks and Privacy Homomorphisms”, Foundations of Secure Computation, vol. 4, pp 169-179.

[5] T. W. Hungerford, (1982) “ALGEBRA: (Graduate Texts in Mathematics, 73)”, Bulletin of the London Mathematical Society, vol. 14, pp 158-159.

[6] Pascal Paillier, (1999) “Public-Key Cryptosystems Based on Composite Degree Residuosity Classes”, Advances in Cryptology - EUROCRYPT ’99, LNCS 1592, pp 223-238.

[7] R.L. Rivest, A. Shamir & L. Adleman, (1983) “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”, Communications of the ACM 26, pp 96–99.

[8] T. Elgamal, (1984) “A Public-Key Cryptosystems and a Signature Scheme Based on Discrete Logarithms”, IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469-472.

[9] J. Katz, A. Sahai & B. Waters. (2013) “Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products”, Journal of Cryptology 26, pp 191–224.

[10] N. Attrapadung & B. Libert, (2010) “Functional Encryption for Inner Product: Achieving Constant-Size Ciphertexts with Adaptive Security or Support for Negation,” Public Key Cryptography – PKC 2010, LNCS 6056, pp 384-402.

[11] T. Okamoto & K. Takashima, (2009) “Hierarchical Predicate Encryption for Inner-Products”, Advances in Cryptology – ASIACRYPT 2009, LNCS 5912, pp 214-231.

[12] T. Okamoto & K. Takashima, (2012) “Fully Secure Unbounded Inner-Product and Attribute-Based Encryption”, Advances in Cryptology – ASIACRYPT 2012, LNCS 7658, pp 349-366.

[13] J. Chen & H. Wee, “Doubly spatial encryption from DBDH”, Theoretical Computer Science. 543, pp 79-89.

[14] S. Agrawal, D. M. Freeman & V. Vaikuntanathan, (2011) “Functional Encryption for Inner Product Predicates from Learning with Errors,” Advances in Cryptology – ASIACRYPT 2011, LNCS 7073, pp 21-40.

[15] S. Agrawal, B. Libert & D. Stehle, (2016) “Fully Secure Functional Encryption for Inner Products, from Standard Assumptions”, Advances in Cryptology – CRYPTO 2016, LNCS 9816, pp 333-362

[16] S. Katsumata & S. Yamada, (2019) “Non-zero Inner Product Encryption Schemes from Various Assumptions: LWE, DDH and DCR”, Public-Key Cryptography – PKC 2019, LNCS 11443, pp 158-188.

[17] I. Damgard & M. Jurik, (2001) “A Generalisation, a Simplification and Some Applications of Paillier's Probabilistic Public-Key System”, Public Key Cryptography- 2001, LNCS 1992, pp 119-136.

[18] T. Okamoto & K. Takashima, (2011) “Achieving short ciphertexts or short secret-keys for adaptively secure general inner-product encryption”, Cryptology and Network Security, LNCS 7092, pp 138-159.

[19] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, B. Waters & H. Gilbert, (2010) “Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption”, Advances in Cryptology – EUROCRYPT 2010, LNCS 6110, pp 62-91.

AUTHORS

Haiying Gao

Female, born in 1978, from Zhoukou City, Henan Province, China. In 2006, she received a PhD degree from Beijing University of Posts and Telecommunications. Now she is a professor and doctoral supervisor at the Information Engineering University, and her research direction is design and analysis of cryptographic algorithm.

Chao Ma

Male, born in 1995, from Zhengzhou City, Henan Province, China. In 2021, he received a master's degree from the University of Information Engineering. The research direction is the design and analysis of public key cryptographic algorithms.