AN IND-CPA SECURE PKC TECHNIQUE BASED ON DIHEDRAL GROUP

Akshaykumar Meshram
Department of Applied Mathematics, Yeshwantrao Chavan College of Engineering &
Department of Mathematics, RTM Nagpur University, Nagpur, (M.S.-440001), India
akshaykjmeshram@gmail.com

Chandrashekhar Meshram
Department of Mathematics and Computer Science, R D University, Jabalpur (M.P.), India
cs_meshram@rediffmail.com

N. W. Khobragade
Department of Mathematics, RTM Nagpur University, Nagpur,(M.S.-440001), India
khobragadenw@gmail.com

Abstract - The public key cryptographic technique is one of the most important fields in computer security. It is a technique of transferring private info and data through open network communication, so only the receiver who has the secret key can read the encrypted messages which might be documents, phone conversations, images or other form of data. To implement privacy simply by encrypting the information intended to remain secret can be achieved by using methods of Public key cryptography. The information must be scrambled, so that other users will not be able to access the actual information. In this study, we propose chosen-plaintext attack secure public key cryptographic technique based on dihedral group. We demonstrated the security of proposed public key cryptographic technique in the indistinguishability chosen plaintext attack (IND-CPA) in the random oracle model.

Keywords: Public key cryptography, ring polynomial, dihedral group, IND-CPA, random oracle.

1. Introduction

In 1976, Diffie and Hellman [1] introduced the conception of public key cryptography (PKC), many PKC techniques have been proposed and broken till date. The trapdoor one-way functions play the important roles in the conception of PKC. The theoretical foundations for the cryptosystems lie in the intractability of problems closer to number theory than group theory [2]. On quantum computer, discrete log and integer factoring, as well as discrete log over elliptic curves, turned out to be efficiently solved by algorithms due to Shor [3], Kitaev [4] and Proos-Zalka [5]. Although practical quantum computers are as least 10 years away, their potential weakness will soon create doubt in current cryptographic methods [6].

Anshel et al. [7] projected a compact algebraic key establishment technique in 1999. The foundation of their method lies in the difficulty of solving equations over algebraic structure (non-commutative groups). Subsequently, Ko et al. [8] f rstly proposed new PKC technique by using braid groups in 2000. In 2001, Paeng et al. [9] published a new PKC technique built on f nite non-abelian groups. Their method is based on the discrete log in the inner automorphism group def ned via the conjugate action. Their systems was later improved to the so-called MOR techniques [10]. Meanwhile, Magliveras et al. [11] developed new approaches to design PKC technique using one-way functions and trapdoors in f nite groups. In 2002, certain homomorphic PKC techniques were constructed for the f rst time for non-abelian groups due to Grigoriev and Ponomarenko [12]. Shortly afterwards, Grigoriev and Ponomarenko [13] extended their method to arbitrary nonidentity f nite groups based on the di˜cul ty of the membership problem for groups of integer matrices. Enlightened by the idea in the arithmetic key exchange [14], in 2004, Eick and Kahrobaei [15] proposed a new PKC technique based on polycyclic groups. In 2005, Shpilrain and Ushakov [16] suggested that R. Thompson's group maybe is a good platform for constructing PKC technique. In their contribution, the key assumption is the intractability of the decomposition problem, which is more general than the conjugator search problem, def ned over R. Thompson's group, also an inf nite non-abelian group given by f nite presentation.

Recently, Meshram [17, 18, 19, 20, 21] offered new variant of PKC techniques based on discrete log and integer factoring and its generalization. Also developed some ideas for identity-based cryptography in [22, 23, 24, 25, 26, 27,28].

Organization: In this article, we propose a new ideas for designing PKC technique using the concept of dihedral group. The main idea of our purpose technique is that we can def ne polynomials and take them as the fundamental work structure for a given dihedral group. By doing so, it is much easy to implement the effective PKC technique secure under indistinguishability chosen plaintext attack (IND-CPA) in the random oracle model.

The structure of the article: This paper is organized as follows. In Section 2, preliminaries are introduced; In Section 3, we demonstrated some extension over dihedral group; In Section 4, we proposed new PKC technique using dihedral group. In Section 5, we demonstrated supporting example for proposed new PKC technique. Discussed security of proposed technique in Section 6. Finally, concluding remarks are made in Section 7.

Preliminaries

In this segment, we demonstrated required basic definition of integer coefficient ring polynomials and its properties.

2.1 Integral Coefficient Ring Polynomials

Assume that R is a ring with $(\mathrm{R},*,1)$ and $(\mathrm{R},+,0)$ as its multiple non-abelian semi-group and additive abelian group, respectively. Let us consider integral coefficient polynomials with ring assignment.

At f rst, the notion of scale multiplication over R is now close by. For $z \in \mathcal{Z}_{>0}$ and $\mathrm{r} \in \mathrm{R}$,

$$(z)\mathrm{r} \triangleq \underbrace{\mathrm{r} + \cdots \ldots \ldots \ldots + \mathrm{r}}_{z \text{ times}} \tag{1}$$

when $z \in \mathcal{Z}_{>0}$, we can define

$$(z)\mathrm{r} \triangleq (-z)(-\mathrm{r}) = \underbrace{(-\mathrm{r}) + \cdots + (-\mathrm{r})}_{-z \text{ times}} \tag{2}$$

For $z = 0$, it is natural to def ne $(z)\,\mathrm{r} = 0$.

Property 1.$(i)\mathrm{r}^a * (j)\mathrm{r}^b = (i\,j)\mathrm{r}^{a+b} = (j)\mathrm{r}^b * (i)\mathrm{r}^a,\ \forall i, j, a, b \in \mathcal{Z}$ and $\forall\, \mathrm{r} \in \mathrm{R}$.

Proof. As indicated by the def nition of the distributivity of multiplication,scale multiplication with respect to commutativity of addition and addition, this statement is finished up instantly.

Note that in general, $(i)\mathrm{r} * (j)\,\ell \neq (j)\,\ell * (i)\mathrm{r}$ when $\mathrm{r} \neq \ell$,since multiplication in R is non-commutative.

Now, let us continue to def ne positive integral coefficient ring polynomials. Assume that $s(v) = i_0 + i_1 v + \cdots + i_b v_b \in \mathcal{Z}_{>0}[v]$ is a given positive integral coefficient polynomial. We can allocate this polynomial by utilizing a component r in R and f nally get

$$s(\mathrm{r}) = \sum_{c=0}^{b}(i_c)\,\mathrm{r}^c = (i_0)1 + (i_1)\,\mathrm{r} + \cdots + (i_b)\,\mathrm{r}^b, \tag{3}$$

which is acomponent in R, obviously. Advance, in the event that we viewr as a variable in R, then $s(\mathrm{r})$ can be looked as a polynomial about variable r. The arrangement of this types of polynomials, taking over all $s(v) \in \mathcal{Z}_{>0}[v]$, can be looked the expansion of $\mathcal{Z}_{>0}$with r, indicated by $\mathcal{Z}_{>0}[\mathrm{r}]$. For comfort, we call it the arrangement of 1-ary positive integral coefficient R -polynomials.

Assume that $s(\mathrm{r}) = \sum_{c=0}^{b}(i_c)\,\mathrm{r}^c \in \mathcal{Z}_{>0}[\mathrm{r}]$, $t(\mathrm{r}) = \sum_{d=0}^{a}(j_d)\mathrm{r}^d \in \mathcal{Z}_{>0}[\mathrm{r}]$ and $b \geq a$, then

$$\left(\sum_{c=0}^{b}(i_c)\,\mathrm{r}^c\right) + \left(\sum_{d=0}^{a}(j_d)\mathrm{r}^d\right) = \left(\sum_{c=0}^{a}(i_c + j_c)\mathrm{r}^c\right) + \left(\sum_{c=a+1}^{b}(i_c)\mathrm{r}^c\right), \tag{4}$$

also, as per Property 1 and additionally the distributivity, we have

$$\left(\sum_{c=0}^{b}(i_c)\,\mathrm{r}^c\right) * \left(\sum_{d=0}^{a}(j_d)\mathrm{r}^d\right) = \left(\sum_{c=0}^{b+a}(\beta_c)\mathrm{r}^c\right)$$

Where $\beta_c = \sum_{d=0}^{c} i_d j_{c-d} = \sum_{d+k=c} i_d j_k$ and then, we can finish up instantly the following hypothesis as per Property 1.

Theorem 1. $s(\mathrm{r}) * t(\mathrm{r}) = t(\mathrm{r}) * s(\mathrm{r}),\ \forall\, s(\mathrm{r}), t(\mathrm{r}) \in \mathcal{Z}_{>0}[\mathrm{r}]$.

Remark. if x and y are two different variable, then $s(x) * t(y) \neq t(y) * s(x)$ in general.

2.2 Dihedral Group

For regular polygon with w sides has $2w$ different symmetric w rotation symmetric and w reflection symmetric. The associated rotation and reflections make up the dihedral group

$$\mathcal{D}_w = \{1, g, g^2, \dots, g^{w-1}, e, ge, \dots, g^{w-1}e\}.$$

The group presentation for the dihedral group is

$$\mathcal{D}_w = \{g, e / g^2 = 1, e^w = 1, (g, e)^2 = 1\}.$$

The matrix representation of elements of the group $\mathcal{D}_w$ are

$$g_\rho = \begin{pmatrix} \cos\frac{2\pi\rho}{w} & -\sin\frac{2\pi\rho}{w} \\ \sin\frac{2\pi\rho}{w} & \cos\frac{2\pi\rho}{w} \end{pmatrix} \text{ and } e_\rho = \begin{pmatrix} \cos\frac{2\pi\rho}{w} & \sin\frac{2\pi\rho}{w} \\ \sin\frac{2\pi\rho}{w} & -\cos\frac{2\pi\rho}{w} \end{pmatrix}$$

For $w = 4$, we get

$$g_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, g_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, g_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, g_3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$
$$e_0 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, e_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, e_2 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, e_3 = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$$

3 Extension over Dihedral Group

The technique portrayed in the above subsection 2.1 is suite for general non-commutative rings. In similar way, we can transfer these outcomes to general dihedral group.

Now, given a dihedral group $(\mathcal{D}_w, *, 1_{\mathcal{D}_w})$. Suppose that there is a ring $(\mathbb{R}, +, *, 1_{\mathbb{R}})$ and a monomorphism $\varsigma : (\mathcal{D}_w, *, 1_{\mathcal{D}}) \to (\mathbb{R}, +, *, 1_{\mathbb{R}})$. Then, the inverse map $\varsigma^{-1} : \varsigma(\mathcal{D}_w) \to \mathcal{D}_w$ is also a well-def ned monomorphism and for $i, j \in \mathcal{D}_w$, if $\varsigma(i) + \varsigma(j) \in \varsigma(\mathcal{D}_w)$, we can assign a new element $\alpha \in \mathcal{D}_w$ as

$$\alpha \triangleq \varsigma^{-1}(\varsigma(i) + \varsigma(j)), \tag{5}$$

and call α as the quasi-sum of i and j, denoted by $\alpha = i \oplus j$. Similarly, for $l \in \mathbb{R}$ and $i \in \mathcal{D}_w$, if $l * \varsigma(i) \in \varsigma(\mathcal{D}_w)$, then we can assign a new element $\beta \in \mathcal{D}_w$ as

$$\beta \triangleq \varsigma^{-1}(l * \varsigma(i)), \tag{6}$$

and call β as the l quasi-multiple of i, denoted by $\beta = l \otimes i$.

Then, we can see that the monomorphism ς is linear in sense of that the following equalities hold

$$\begin{aligned} \varsigma(l \otimes i \oplus j) &= \varsigma((l \otimes i) \oplus j) \\ &\overset{\beta \leftarrow (l \otimes i)}{=} \varsigma(v \oplus j) \\ &= \varsigma(\varsigma^{-1}(\varsigma(\beta) + \varsigma(j))) \\ &= \varsigma(\varsigma^{-1}(\varsigma(\varsigma^{-1}(l * \varsigma(i))) + \varsigma(j))) \\ &= \varsigma(\varsigma^{-1}(l * \varsigma(i) + \varsigma(j))) \\ &= l * \varsigma(i) + \varsigma(j). \end{aligned}$$

For $i, j \in \mathcal{D}_w$ and $l * \varsigma(i) + \varsigma(j) \in \varsigma(\mathcal{D}_w)$.

Further, for $s(v) = z_0 + z_1 v + \cdots + z_a v^a \in \mathcal{Z}[v]$ and $i \in \mathcal{D}_w$ if $s(\varsigma(i)) = z_0 * 1_{\mathbb{R}} + z_1 * \varsigma(i) + \cdots + z_n * \varsigma(i)^a \in \varsigma(\mathcal{D}_w)$, then we can assign a new element $\gamma \in \mathcal{D}_w$ as

$$\gamma \triangleq \varsigma^{-1}(s(\varsigma(i))) = \varsigma^{-1}(z_0 * 1_{\mathbb{R}} + z_1 * \varsigma(s) + \cdots + z_a * \varsigma(i)^a), \tag{7}$$

and call w as the quasi-polynomial of h on s, denoted by $w = h(s)$.

Clearly, for arbitrary $i, j \in \mathcal{D}_w, l \in \mathbb{R}$ and $s(v) \in \mathcal{Z}[v]$, $i \oplus j$, $l \otimes i$ and $s(i)$ are not always well-def ned. But, we can prove that the following theorem holds.

Theorem 2. For some $i \in \mathcal{D}_w$ and some $s(v), t(v) \in \mathcal{Z}[v]$, if $s(i)$ and $t(i)$ are well-def ned, then

(i) $\varsigma(s(i)) = s(\varsigma(i))$;

(ii) $s(i) * t(i) = t(i) * s(i)$.

Proof. At f rst, (i) is apparent according to the def nition of quasi-polynomial. Next, we have,

$$\begin{aligned} s(i) * t(i) &= \varsigma(\varsigma^{-1}(s(i))) * \varsigma(\varsigma^{-1}(t(i))) \\ &= \varsigma\left(\varsigma^{-1}(s(i)) * \varsigma^{-1}(t(i))\right) \\ &= \varsigma(\varsigma^{-1}(s(i) * t(i))) \end{aligned}$$

$$= \varsigma(\varsigma^{-1}(t(i) * s(i)))$$
$$= \varsigma(\varsigma^{-1}(t(i)) * \varsigma^{-1}(s(i)))$$
$$= \varsigma\left(\varsigma^{-1}\left(t(i)\right)\right) * \varsigma\left(\varsigma^{-1}\left(s(i)\right)\right)$$
$$= t(i) * s(i).$$

3.1 Symmetrical Decomposition Problem (SDP):

For given $(u, \varphi) \in \mathcal{D}_w \times \mathcal{D}_w$ and $b, a \in \mathcal{Z}$, find $z \in \mathcal{D}_w$ such that $\varphi = z^b u z^a$.

3.2 Polynomial Diffie-Hellman (PDH) Problem over Dihedral group: Suppose that $(\mathcal{D}_w, *)$ is a dihedral group. For any arbitrarily selected component $c \in \mathcal{D}_w$, we define a set $\beta_c \subseteq \mathcal{D}_w$ by

$$\beta_c \triangleq \{t(c): t(u) \in \mathcal{Z}_{>0}[u]\}.$$

Then, let we consider the new versions of computational Diffie-Hellman problem over $(\mathcal{D}_w, *)$ with respect to its subset β_c, it is known as polynomial Diffie-Hellman (PDH) problem and define by. For given u, u^{z_1} and u^{z_2}, we compute $u^{z_1 z_2}$ (or $u^{z_2 z_1}$), where $u \in \mathcal{D}_w$, $z_1, z_2 \in \beta_c$.

Accordingly, the PDH cryptographic assumption says that PDH, problem over $(\mathcal{D}_w, *)$ is intractable, i.e., there does not exist probabilistic polynomial time algorithm which can solve PDH, problem over $(\mathcal{D}_w, *)$ with non-negligible accuracy with respect to problem scale.

4. Propose An IND-CPA Secure PKC Technique

In this section, we described new PKC Technique as following:

Setup:

1. We assume that SDP on $\mathcal{D}_w$ for a given dihedral group $(\mathcal{D}_w, *)$.
2. Select two random integers $b, a \in \mathcal{Z}$ and components h and f from $\mathcal{D}_w$.
3. Let $\mathfrak{h}$ be the cryptographic hash function define as $\mathfrak{h}: \mathcal{D}_w \to \acute{M}$.

The public parameters of the technique is given by the tuple $\{\mathcal{D}_w, h, f, b, a, \acute{M}, \mathfrak{h}\}$.

Key generation: Each user selects an arbitrary polynomial $s(v) \in \mathcal{Z}[v]$ such that $s\left(\varsigma(h)\right) \in \varsigma(\mathcal{D}_w)$, then takes $s(h)$ as his/her private key and calculates $\varphi = s(h)^b f s(h)^a$ and publishes his/her public key (h, f, φ).

Encryption: For a given message $\mathfrak{m} \in \acute{M}$ and receiver's key (h, f, φ), the sender adopt the below procedure

1. Selects random polynomial $t(v) \in \mathcal{Z}[v]$ such that $t\left(\varsigma(h)\right) \in \varsigma(\mathcal{D}_w)$ and then takes $t(h)$as salt.
2. Calculates $\psi = t(h)^b * f * t(h)^a$ and $\chi = \mathfrak{h}(t(h)^b * f * t(h)^a) \oplus \mathfrak{m}$.
3. Finally the cipher text is given by $\acute{C} = (\psi, \chi) \in \mathcal{D}_w \times \acute{M}$.

Decryption: Upon receiving a ciphertext $\acute{C}$, the receiver, by using his private key $s(h)$, estimates the plaintext $\mathfrak{m}$ as following

$$\mathfrak{m} = \mathfrak{h}\left(s(h)^b * \psi * s(h)^a\right) \oplus \chi$$

5. Concrete Examples:

In this segment, we illustrate example for supporting our proposed new public key cryptographic technique using integral coefficient ring polynomial based on dihedral group.

At first, we have to define the message space $\acute{M}$ as well as cryptographic hash functions $\mathfrak{h}$ for the purpose technique. For simplicity, we assume that $\acute{M} \triangleq \mathfrak{m}_2(\mathcal{Z}_N)$ for the technique, while

$$\mathfrak{h}: \mathfrak{m}_2(\mathcal{Z}_N) \to \acute{M} = \mathfrak{m}_2(\mathcal{Z}_N), m_{ij} \mapsto 2^{m_{ij}} \bmod N,$$

Suppose that $\mathfrak{V} = \begin{pmatrix} d & 0 \\ 0 & 0 \end{pmatrix} \in \mathfrak{m}_2(\mathcal{Z}_N)$. Form above definition, we estimate $\mathfrak{V}^2 = \begin{pmatrix} d^2 \bmod N & 0 \\ 0 & 0 \end{pmatrix} \in \mathfrak{m}_2(\mathcal{Z}_N)$ without knowing the factoring of N.

Next, let $N = 3.7 = 21$ for example. Suppose that the system parameters are listed below

$$b = 2, a = 3, h = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, f = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}.$$

5.1 Encryption and Decryption Process

Suppose that the polynomial $s(v) = 8v^3 + 2v^2 + 5v + 2$ picked by sender

Then, sender's private key is

$$\mathcal{s}(\mathcal{h}) = 8\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}^3 + 2\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}^2 + 5\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix} + 2\mathrm{I} = \begin{pmatrix}26 & 0\\ 0 & 26\end{pmatrix},$$

Then, the corresponding public key would be

$$\varphi \triangleq \mathcal{s}(\mathcal{h})^2 \mathcal{f} \mathcal{s}(\mathcal{h})^3 = \begin{pmatrix}26 & 0\\ 0 & 26\end{pmatrix}^2 \begin{pmatrix}0 & -1\\ -1 & 0\end{pmatrix}\begin{pmatrix}26 & 0\\ 0 & 26\end{pmatrix}^3 = \begin{pmatrix}0 & 4\\ 4 & 0\end{pmatrix}$$

Let us pick a message randomly, say $\mathfrak{m} = \begin{pmatrix}5 & 8\\ 3 & 2\end{pmatrix}$. Suppose the salt polynomial we picked randomly is coincide to $t(\mathcal{v})$. Then, the salt matrix from

$t(\mathcal{v}) = 7\mathcal{v}^5 + 3\mathcal{v} + 1$ and computes

$$t(\mathcal{h}) = 7\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}^5 + 3\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix} + \mathrm{I} = \begin{pmatrix}5 & 0\\ 0 & 5\end{pmatrix}$$

Now, let us compute the ciphertext (ψ, χ) as follows:

$$\psi = t(\mathcal{h})^2 * \mathcal{f} * t(\mathcal{h})^3 = \begin{pmatrix}5 & 0\\ 0 & 5\end{pmatrix}^2 \begin{pmatrix}0 & -1\\ -1 & 0\end{pmatrix}\begin{pmatrix}5 & 0\\ 0 & 5\end{pmatrix}^3 = \begin{pmatrix}0 & 25\\ 25 & 0\end{pmatrix},$$

and

$$\begin{aligned}\chi &= \mathfrak{h}(t(\mathcal{h})^2 * \varphi * t(\mathcal{h})^3) \oplus \mathfrak{m}\\ &= \mathfrak{h}\left(\begin{pmatrix}5 & 0\\ 0 & 5\end{pmatrix}^2 \begin{pmatrix}0 & 4\\ 4 & 0\end{pmatrix}\begin{pmatrix}5 & 0\\ 0 & 5\end{pmatrix}^3\right) \oplus \begin{pmatrix}5 & 8\\ 3 & 2\end{pmatrix}\\ &= \mathfrak{h}\left(\begin{pmatrix}0 & 5\\ 5 & 0\end{pmatrix}\right) \oplus \begin{pmatrix}5 & 8\\ 3 & 2\end{pmatrix}\\ &= \left(\begin{pmatrix}2^0 & 2^5\\ 2^5 & 2^0\end{pmatrix} \bmod \mathrm{N}\right) \oplus \begin{pmatrix}5 & 8\\ 3 & 2\end{pmatrix}\\ &= \begin{pmatrix}1 & 32\\ 32 & 1\end{pmatrix} \oplus \begin{pmatrix}5 & 8\\ 3 & 2\end{pmatrix}\\ &= \begin{pmatrix}4 & 40\\ 35 & 3\end{pmatrix}\end{aligned}$$

Now, let us check the decryption process:

$$\begin{aligned}\mathfrak{m}' &= \mathfrak{h}(\mathcal{s}(\mathcal{h})^2 * \psi * \mathcal{s}(\mathcal{h})^3 \oplus \chi\\ &= \mathfrak{h}\left(\begin{pmatrix}26 & 0\\ 0 & 26\end{pmatrix}^2 \begin{pmatrix}0 & 25\\ 25 & 0\end{pmatrix}\begin{pmatrix}26 & 0\\ 0 & 26\end{pmatrix}^3\right) \oplus \begin{pmatrix}4 & 40\\ 35 & 3\end{pmatrix}\\ &= \mathfrak{h}\left(\begin{pmatrix}0 & 5\\ 5 & 0\end{pmatrix}\right) \oplus \begin{pmatrix}4 & 40\\ 35 & 3\end{pmatrix}\\ &= \left(\begin{pmatrix}2^0 & 2^5\\ 2^5 & 2^0\end{pmatrix} \bmod \mathrm{N}\right) \oplus \begin{pmatrix}4 & 40\\ 35 & 3\end{pmatrix}\\ &= \begin{pmatrix}1 & 32\\ 32 & 1\end{pmatrix} \oplus \begin{pmatrix}4 & 40\\ 35 & 3\end{pmatrix}\\ &= \begin{pmatrix}5 & 8\\ 3 & 2\end{pmatrix}\\ &= \mathfrak{m}.\end{aligned}$$

6. Security examination

Theorem 3: Let $\mathfrak{h}$ be a random oracle and $\mathfrak{F}$ be an IND-CPA foe that has advantage against the purpose fundamental technique inside $\mathcal{k}$ iterations. Assume that$\mathfrak{F}$ makes a $q_{\mathfrak{h}}$ total of inquiries to $\mathfrak{h}$. Then there is aprocedure $\mathcal{A}$ that resolves polynomial Diffie-Hellman problem over $\mathcal{D}_w$with advantage at least ϵ' within $\mathcal{k}'$iterations, where

$$\epsilon' = \frac{2\epsilon}{q_{\mathfrak{h}}}, \mathcal{k}' = O(\mathcal{k}).$$

Proof: Procedure $\mathcal{A}$ is given as input tuple $(c, u, \varphi_1, \varphi_2)$ with $\varphi_i = u^{z_i} = {z_i}^{b} u {z_i}^{a}$ for unknown $z_i \epsilon$ ß$_c, i =$ 1,2, an instance of polynomial Diffie-Hellman problem. Let $\varphi = u^{z_1 z_2}$ denote the solution to polynomial Diffie-Hellman problem on this instance.

Setup. At f rst, the algorithm $\mathcal{A}$ sets the framework parameters to be $<$ Ɍ$, b, a,$ Ḿ$,$ ħ $>$ and forms a public key (c, u, φ_1). Framework parameters and the public key ought to be accessible to the foe Ƒ.

H-queries. Then, $\mathcal{A}$ keeps up a ħ^{list} which contains two f elds (d_j, t_j) and is initialized with empty. At whatever point the foe Ƒ creates a ħ-inquiry with info d, $\mathcal{A}$ looks at whether there exists the combine (d, t) in ħ^{list}. Provided that this is true, returns t as the response to Ƒ; Otherwise, arbitrarily selects $t \in$ Ḿ, includes the combine (d, t) into ħ^{list} and returns t as the response to Ƒ. Unmistakably, the simulation on ħ is faultless.

Challenge. When Ƒ yields messages ɱ$_1$and ɱ$_2$ on which it wanted to be challenged. $\mathcal{A}$ selects arbitrary a string $\chi \in$ Ḿ and def nes ciphertext pair Ć $= (\varphi_2, \chi)$. It then provides Ć to Ƒ as the challenge. See that, by def nition, the decryption of Ć is $\chi \oplus$ ħ $(u^{(log_u \varphi_1)(log_u \varphi_2)} = \chi \oplus$ ħ$(u^{z_1 z_2}) = \chi \oplus$ ħ(φ).

Guess: Ƒ yields its figure $\alpha' \in \{0, 1\}$. Presently, $\mathcal{A}$ selects an unpredictable tuple (d_j, t_j) from the ħ^{list} and yields d_j as the response for the given event of polynomial Diffie-Hellman problem.

It is definitely not hard to see that Ƒ's view in $\mathcal{A}$'s proliferation is the same as in a genuine assault, as it were, the amusement is extraordinary. So Ƒ's advantage in this simulation will be ϵ. We let ħbe the event that φ is addressed to ħ oracle amid $\mathcal{A}$'s simulation.

See that ħ(φ) is autonomous of Ƒ's view, so if Ƒ never inquiries φ to the ħ oracle in the above mention simulation, then the decryption of Ć is likewise free of its view. In this way, in the simulation we have $Pr[\alpha = \alpha' | \neg$ħ$] = \frac{1}{2}$. By the def nition of Ƒ, we realize that in the genuine attack (furthermore in the simulation) $|Pr[\alpha = \alpha'] - 1/2| \geq \epsilon$. We have the accompanying limits on $Pr[\alpha = \alpha']$:

$$Pr[\alpha = \alpha'] = Pr[\alpha = \alpha' | \neg ħ] Pr[\neg ħ] + Pr[\alpha = \alpha' | ħ] Pr[ħ]$$
$$\leq \Pr[\alpha = \alpha' | \neg ħ] \Pr[\neg ħ] + \Pr[ħ]$$
$$= \frac{1}{2} Pr[\neg ħ] + Pr[ħ] = \frac{1}{2} + \frac{1}{2} Pr[ħ],$$
$$Pr[\alpha = \alpha'] \geq Pr[\alpha = \alpha' | \neg ħ] Pr[\neg ħ]$$
$$= \frac{1}{2} Pr[\neg ħ]$$
$$= \tfrac{1}{2} (1 - Pr[ħ])$$
$$= \frac{1}{2} - \frac{1}{2} Pr[ħ]).$$

Hence we have $| Pr[\alpha = \alpha'] - 1/2 | \leq 1/2 \; Pr[ħ]$. By $\left| Pr[\alpha = \alpha'] - \frac{1}{2} \right| \geq \epsilon$ we know that $Pr[ħ] \geq 2\epsilon$. Besides, by the def nition of the occasion ħ, werealize that y shows up in some tuple on the ħ^{list} with probability at least 2ϵ. It takes after that $\mathcal{A}$ yields the right response to the above case of polynomial Diffie-Hellman problem with probability no less than $\frac{2\epsilon}{q_ħ}$ as required.

7. Conclusions

In this article, we purposed the new mechanism for designing the PKC technique using the conception of general non-commutative algebraic system such as dihedral group. The main idea behind our proposal lies that we take polynomials over the given non-commutative algebraic system as the fundamental work structure for developing PKC plans. Thusly, we can efficiently acquire some commutative sub-structures for the given non-commutative mathematical frameworks. The proposed new PKC technique is secure under indistinguishability chosen plaintext attack (IND-CPA) in the random oracle model.

References

[1] W. Diffie and M.E. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory 22 (1976), 644-654.

[2] S.S. Magliveras, D.R. Stinson and T. van Trungn, "New approaches to designing public key cryptosystems using one-way functions and trapdoors in f nite groups", J. Cryptography 15 (2002), pp. 285-297.

[3] P. Shor, "Polynomail-time algorithms for prime factorization and discrete logarithms on a quantum computer", SIAM J. Comput. 5 (1997), pp. 1484-1509.

[4] A. Kitaev, "Quantum measurements and the Abelian Stabilizer Problem", Preprint arXir: cs.CR/quant-ph/9511026, 1995.

[5] J. Proos and C. Zalka,Shor's, "Discrete logarithm quantum algorithm for elliptic curves", Quantum Information and Computation 3 (2003), pp. 317-344.

[6] E. Lee, "Braig groups in cryptography", IEICE Trans. Fundamentals, E87-A, no. 5, (2004), pp. 986-992.

[7] I. Anshel, M. Anshel, and D. Goldfeld, "An algebraic method for public-key cryptography", Math. Research Letters 6 (1999) 287-291.
[8] K.H. Ko, S.J. Lee, J.H. Cheon and J.W. Han., "New Public-Key Cryptosystem Using Braid Groups", In M.Bellare (Ed.): CRYPTO 2000, LNCS 1880, pp. 166-183, Springer-Verlag, 2000.
[9] S.-H. Paeng, K.-C. Ha, J.-H. Kim, S. Chee and C. Park, New public key cryptosystem using f nite Non Abelian Groups. In J. Kilian (Ed.): CRYPTO 2001, LNCS, 2139, (2001) pp. 470-485.
[10] S.-H. Paeng, D. Kwon, K.-C. Ha, and J. H. Kim, "Improved public key cryptosystem using f nite non abelian groups", Cryptology ePrint Archive: Report 2001/066, (2001).
[11] S.S. Magliveras, D.R. Stinson, and T. van Trung, "New Approaches to Designing Public Key Cryptosystems Using One-Way Functions and Trapdoors in Finite Groups", Technical Report CORR 2000-49, Centre for Applied Crypto- graphic Research, University of Waterloo. http://www.cacr.math.uwaterloo.ca/ techreports/2000/corr2000-49.ps
[12] D. Grigoriev and I. Ponomarenko, "On non-abelianhomomorphic public-key cryptosystems", Preprint arXiv: cs.CR/0207079, 2002.
[13] D. Grigoriev and I. Ponomarenko, "Homomorphic public-key cryptosystems over groups and rings", Preprint arXiv: cs.CR/0309010, 2003.
[14] I. Anshel, M. Anshel, and D. Goldfeld, "An algebraic method for public-key cryptography", Math. Research Letters 6 (1999) 287-291.
[15] B. Eick and D. Kahrobaei, "Polycyclic groups: a new platform for cryptography", Preprint arXiv: math.GR/0411077, 2004.
[16] V. Shpilrain and A. Ushakov, "Thmposon's group and public key cryptography", Preprint arXir: math.GR/0505487, 2005.
[17] C. Meshram, "The Beta Cryptosystem", Bulletin of Electrical Engineering and Informatics, 4 (2), (2015), pp. 155-159.
[18] C. Meshram and S. A. Meshram, "PKC Scheme Based on DDLP", International Journal of Information & Network Security, 2 (2), (2013), pp. 154-159.
[19] C. Meshram and S.A. Meshram, "A Public Key Cryptosystem based on IFP and DLP", International Journal of Advanced Research in Computer Science, 2 (5), (2011), pp. 616-619.
[20] C. Meshram, "A Cryptosystem based on Double Generalized Discrete Logarithm Problem", International Journal of Contemporary Mathematical Sciences, 6(6), (2011), pp. 285 – 297.
[21] C. Meshram and S.S. Agrawal, "Enhancing the security of A Public key cryptosystem based on DLP $\gamma \equiv \alpha\alpha\beta b \pmod p$", International Journal of Research and Reviews in Computer Science 1 (4),(2010), pp.67-70,.
[22] C. Meshram and S. A. Meshram, "An identity based cryptographic model for discrete logarithm and integer factoring based cryptosystem", Information Processing Letters, 113 (10), (2013), pp. 375-380.
[23] C. Meshram, "An Efficient ID-based Cryptographic Encryption based on Discrete Logarithm Problem and Integer Factorization Problem", Information Processing Letters, 115 (2), (2015), pp. 351-358.
[24] C. Meshram and Mohammad S. Obaidat, "An ID-based Quadratic-Exponentiation Randomized Cryptographic Scheme", IEEE International Conference on Computer, Information and Telecommunication Systems,(2015), pp.1-5.
[25] C. Meshram, "An efficient ID-based Beta Cryptosystem", International Journal of Security and Its Applications, 9(2), (2015), pp. 189-202.
[26] C. Meshram, P. L. Powar, M. S. Obaidat and Cheng-Chi Lee, "An IBE Technique using Partial Discrete Logarithm" ,Procedia Computer Science, 93, (2016), pp. 735-741.
[27] C. Meshram, S. A. Meshram and Mingwu Zhang, "An ID-based cryptographic mechanisms based on GDLP and IFP", Information Processing Letters, 112 (19), (2012), pp.753-758.
[28] C. Meshram and P. L. Powar, "An Efficient Identity-based QER Cryptographic Scheme", Complex & Intelligent Systems, 2 (4), (2016), pp. 285-291.