ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 10(12), DOI: 10.17485/ijst/2017/v10i12/111588, March 2017* ISSN (Online) : 0974-5645

An IND-CCA2 Secure Public Key Cryptographic Protocol using Suzuki 2-Group

Akshaykumar Meshram[1,3*], Chandrashekhar Meshram[2,3] and N. W. Khobragade[3]

[1]Department of Applied Mathematics, Yeshwantrao Chavan College of Engineering, Wanadongari, Nagpur - 441110, Maharashtra, India; akshaykjmeshram@gmail.com
[2]Department of Mathematics and Computer Science, Rani Durgavati Vishwavidyalaya, Saraswati Vihar, Pachpedi, Jabalpur – 482001, Madhya Pradesh, India; cs_meshram@rediffmail.com
[3]Department of Mathematics, Rashtrasant Tukadoji Maharaj Nagpur University, Amravati Road, Ram Nagar, Nagpur – 440033, Maharashtra, India; khobragadenw@gmail.com

Abstract

Objectives: The public key cryptographic protocol is one of the most important fields in computer security. These new public key cryptographic protocols provide high security as compare to past results in the same field. **Methods/Statistical Analysis:** Public key cryptographic is a protocol 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. **Findings:** In this study, we propose the new IND-CCA2 secure public key cryptographic protocol using the concept of integral coefficient ring polynomial based on Suzuki 2-group. We demonstrated the security of proposed public key cryptographic protocol in the adaptively chosen cipher text secure (IND-CCA2) in the random oracle model. **Application/Improvements:** We discussed the new strategy with change over an IND-CPA public key cryptographic protocol into an IND-CCA2 cryptographic protocol.

Keywords: IND-CCA2, Public Key Cryptography, Ring Polynomial, Random Oracle, Suzuki 2-Group

1. Introduction

The conception of Public Key Cryptography (PKC) first brought in public domain and introduced[1]. Since then various public key cryptographic protocols have been developed but could not take desired results. It is a one-way functions show the significant roles in the conception of public key cryptographic protocols. On the apparent difficulty of specific predicaments specifically huge finite commutative rings, these days most prosperous public key cryptographic protocols are established.

To outline public key cryptographic protocol using the undesirable word issue for groups and semi-groups is proposed[2]. The thought is really not in view of word issue, but rather on another, comparatively easier, introduce issue. For a new public key cryptographic protocol which depends on finitely gave assembles hard word problem[3].

One of successful key establishment protocol came up with a compact algebraic structure[4]. The establishment of their strategy included in the difficulty of explaining conditions over arithmetical structure. Subsequently the first proposed new public key cryptographic protocol is used by braid groups[5]. The security foundation is that when the framework parameters, for example, braid index and the canonical length of the working braids, are chosen legitimately, the Conjugator Search Problem (CSP) is unmanageable. A new public key cryptographic protocol built on finite non-abelian groups was published[6]. Their strategy depends on the discrete logarithm problem in which the inner automorphism group is defined by means of the conjugate action. Later, their system was developed and improves to the so-called MOR systems[7]. In the interim, utilizing one-way functions and trapdoors in finite groups developed new approaches to design public key cryptographic protocol[8].

Homomorphic public key cryptographic protocol was developed for the first time for non-abelian groups[9]. Afterwards, the extended and expanded their process

* *Author for correspondence*

to discretionary nonidentity finite groups in view of the difficulty of the participation issue for groups of integer matrices[10]. Edified thought the number-crunching key exchange[4], proposed a new public key cryptographic protocol using polycyclic groups[11].

Generic algebraic systems are especially a non-commutative one which is creating its significances, making its marks and attracting many among the above public key cryptographic protocols. There are some difficulties of resolving CSP over certain non-abelian groups using non-commutative algebraic systems. In spite of the fact that there are algorithms for understanding a few variations of CSP in specific groups, such as braid groups with respect to the system parameters[12–16], none of them can resolve CSP itself defined over general non-abelian group in polynomial time. However, non-commutative acts favorably and unfavorably from one perspective, it makes CSP significant; then again, it brings some bother for planning public key cryptographic protocols. Rectifying the problem, making it favorable is the key concern for developing public key cryptographic protocol over non-commutative algebraic systems.

1.1 Organization

In this article, we establish new ideas for scheming adaptively chosen cipher-text secure (IND-CCA2) secure public key cryptographic protocol using the concept of dihedral group. The main idea of our purpose is to define the technique in 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 IND-CCA2 secure public key cryptographic protocol in the random oracle model.

1.2 The Structure of the Article

This paper is sorted out as takes after. In Section 2, preliminaries are presented; In Section 3, we demonstrated some extension over dihedral group; In Section 4, we proposed new IND-CCA2 secure public key cryptographic protocol using dihedral group. In Section 5, we demonstrated supporting example for proposed new public key cryptographic protocol. The security of proposed public key cryptographic protocol is discussed in Section 6. Finally, concluding remarks are made in Section 7.

2. Preliminaries

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

2.1 Integral Coefficient Ring Polynomials (ICRP)

Assume $(®, *, 1)$ is algebraic structure for ring ® with multiplicative operation $*$ of non-commutative semi group and $(®, +, 0)$ is algebraic structure with additive operation $+$ of commutative group. Now we consider Integral Coefficient Polynomials (ICP) with ring assignment as follows:

For $ȝ \in ℤ_{>0}$ and $\theta \in ®$,

$$(ȝ)\theta \triangleq \underbrace{\theta + \cdots \ldots \ldots + \theta}_{l \ times} \quad (1)$$

When $ȝ \in ℤ_{>0}$, we can define

$$(ȝ)\theta \triangleq (-ȝ)(-\theta) = \underbrace{(-\theta) + \cdots + (-\theta)}_{-ȝ \ times} \quad (2)$$

For $ȝ = 0$, it is normal to define $(ȝ)\theta = 0$.

Property1.

$(\alpha)\theta^i.(\beta)\theta^j = (\alpha\beta)\theta^{i+j} = (\beta)\theta^j \cdot (\alpha)\theta^i, \forall \alpha, \beta, i, j \in ℤ$

$\forall\ \theta \in ®$

2.1.1 Proof

As indicated by the definition of the distributive of multiplication, scale multiplication concerning commutative of addition and addition, this statement is finished up instantly.

Remark. In non-commutative ring ®, we get

Presently, let us continue to define positive ICRP

$(\alpha)\theta.(\beta)k \neq (\beta)k.(\alpha)\theta$ for $\theta \neq k$.

$$\hbar(u) = \alpha_0 + \alpha_1 u + \ldots + \alpha_j u_j \in ℤ_{>0}[u]$$

We can allocate this polynomial by utilizing a component in ® and finally get

$$\hbar(\theta) = \sum_{s=0}^{j}(\alpha_s)\theta^s = (\alpha_0)1 + (\alpha_1)\theta + \cdots + (\alpha_j)\theta^j, (3)$$

This is a component in ®, obviously. Advance, in the event that we view as a component in ®, then

$\hbar$ (θ) can be observed as a polynomial about factor. The arrangement of these types of polynomials, assuming over all $\hbar(u) \in 2_{>0}[\theta]$ can be observed the expansion of $2_{>0}$ with, indicated by $2_{>0}[\theta]$. For comfort, we call it the arrangement of 1-ary positive ICRP.

Assume that

$$\hbar(\theta) = \sum_{s=0}^{j}(\alpha_s)\theta^s \in 2_{>0}[\theta],\ \hbar(\theta) = \sum_{t=0}^{i}(\beta_t)r^t \in 2_{>0}[\theta],\ j \geq i,$$

then

$$\left(\sum_{s=0}^{j}(\alpha_s)\theta^s\right) + \left(\sum_{t=0}^{i}(\beta_t)\theta^t\right) = \left(\sum_{s=0}^{i}(\alpha_s+\beta_s)\theta^s\right) + \left(\sum_{s=i+1}^{j}(\alpha_s)\theta^s\right) \quad (4),$$

Also, as per Property 1 and additionally the distributive, we have

$$\left(\sum_{s=0}^{j}(\alpha_s)\theta^s\right)\cdot\left(\sum_{t=0}^{i}(\beta_t)\theta^t\right) = \left(\sum_{s=0}^{i+1}(\tau_s)\theta^s\right)$$

Where and then,

$$\tau_s = \sum_{t=0}^{s}\alpha_s\beta_{s-t} = \sum_{t+c=s}\alpha_s\beta_k$$

we can finish up instantly the following hypothesis as per Property 1.

Theorem 2.1

$\hbar$ (θ). $\hbar$ (θ)= $\hbar$ (θ)• $\hbar$ (θ),∀ $\hbar$ (θ), $\hbar$ (θ) ∈ $2_{>0}$ [θ].

Remark 3.If θ and α are two distinct components, then

2.2 Suzuki 2-Group

In the first place, we review some essential actualities about q -groups, where q means a prime number. A limited gathering $\mathcal{G}_S$ of request a force of q is called a q -group, i.e.$|\mathcal{G}_S| = q^n$ for a specific positive number n . The smallest common multiple of the order of the component of $\mathcal{G}_S$ is known as the exponent of$\mathcal{G}_S$. An abelian q -group $\mathcal{G}_S$ of exponent q is said to be rudimentary abelian.

The set$\mathcal{Z}(\mathcal{G}_S) = \{z \in \mathcal{G}_S : gz = zg, \forall g \in \mathcal{G}_S\}$ is known as the center of $\mathcal{G}_S$. It is outstanding that $\mathcal{Z}(\mathcal{G}_S)$ is a normal subgroup of request at any rate q for any q -group $\mathcal{G}_S$. The subgroup $\mathcal{G}_S'$ created by every one of the components of the arrangement$m^{-1}n^{-1}m$ with $m, n \in \mathcal{G}_S$ is known as the commentator subgroup of $\mathcal{G}_S$. The alleged Frattini subgroup of $\mathcal{G}_S$, indicated by $\varphi(\mathcal{G}_S) = <\frac{g^2}{g} \in \mathcal{G}_S>$. At last, a component of order 2 in a gathering is called an involution.

Formally, a Suzuki 2-group[17] is well characterized as a non-abelian 2-group with more than one involution having a cyclic group of automorphisms which permutes its involutions transitively. This class of 2-group was analyzed and described by[17].

Specifically, in any Suzuki 2-group $\mathcal{G}_S$ we have $\mathcal{Z}(\mathcal{G}_S) = \varphi(\mathcal{G}_S) = \mathcal{G}_S' = \Omega_1(\mathcal{G}_S)$, where

$$\Omega_1(\mathcal{G}_S) = <g^2 = \frac{1}{g} \in \mathcal{G}_S> \text{ and}$$

$|\mathcal{Z}(\mathcal{G}_S)| = q = 2^\eta, \eta > 1$. It is appeared in[17] that the order of g is either p^2 or p^3. In this manner all the involution of $\mathcal{G}_S$ are in the center of $\mathcal{G}_S$, there $\mathcal{Z}(\mathcal{G}_S)$ and the factor group $\mathcal{G}_S/\varphi(\mathcal{G}_S)$ are rudimentary abelian. Subsequently, all components not in $\mathcal{Z}(\mathcal{G}_S)$ have order 4. It is realized that $\mathcal{G}_S$ has an automorphism ξ of order $p-1$ consistently permuting the involution of $\mathcal{G}_S$.

2.3 Symmetrical Decomposition Problem (SDP)

For given $(a, b) \in \mathcal{G}_S \times \mathcal{G}_S$ and $j, i \in 2$, find $z \in \mathcal{G}_S$ such that $b = z^j a z^i$.

2.4 Polynomial Diffie-Hellman (PDH) Problem over Suzuki 2-Group

Suppose that $(\mathcal{G}_S, \cdot)$ is a Suzuki 2-geoup. For any arbitrarily selected component $s \in \mathcal{G}_S$, we define a set $\tau_s \subseteq \mathcal{G}_S$ by

$\tau_s \triangleq \{f(s): f(u) \in 2_{>0}) [u]\}$

At that point, let we consider the new forms of computational Diffie-Hellman problem over $(\mathcal{G}_S, \cdot)$ with respect to its subset τ_s, it is known as polynomial Diffie-Hellman (PDH) problem and define as: For given x, x^{z_1} and x^{z_2}, we compute $x^{z_1 z_2}$ (or $x^{z_2 z_1}$), where $x \in \mathcal{G}_S$, z_1, $z_2 \in \tau_s$.

Accordingly, the cryptographic based on PDH supposition says that PDH, problem over $(\mathcal{G}_S, \cdot)$ is intractable, i.e., there doesn't exist PPT process which can resolve PDH, problem over $(\mathcal{G}_S, \cdot)$ with non-negligible precision w. r. t. problem scale.

3. Extension of Over Suzuki 2-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 Suzuki 2-group.

Now, given a Suzuki 2-group $(\mathcal{G}_S, \cdot, 1_{\mathcal{G}_S})$. Assume that there is a ring $(\mathbb{R}, +, \cdot, 1_{\mathbb{R}})$ and a monomorphism $\mathfrak{w} : (\mathcal{G}_S, \cdot, 1_{\mathcal{G}_S}) \to (\mathbb{R}, +, \cdot, 1_{\mathbb{R}})$. Then, the inverse map $\mathfrak{w}^{-1} : \mathfrak{w}(\mathcal{G}_S) \to \mathcal{G}_S$ is also a well-defined monomorphism and for $\alpha, \beta \in \mathcal{G}_S$, **if** $\mathfrak{w}(\alpha) + \mathfrak{w}(\beta) \in \mathfrak{w}(\mathcal{G}_S)$, we can allot another component $u \in \mathcal{G}_S$ as

$$\delta \triangleq \mathfrak{w}^{-1}(\mathfrak{w}(\alpha) + \mathfrak{w}(\beta)), \quad (5)$$

and call $\delta = \alpha \oplus \beta$ as the quasi_sum of α and β. Correspondingly, for $k \in \mathbb{R}$ and $\alpha \in \mathcal{G}_S$, $\alpha \in \mathcal{G}_S$, if $k \cdot \mathfrak{w}(a) \in \mathfrak{w}(\mathcal{G}_S)$, then we can allot another component $a \in \mathcal{G}_S$ as

$$a \triangleq \mathfrak{w}^{-1}(k \cdot \mathfrak{w}(\alpha)), \quad (6)$$

and call $a = k \otimes \alpha$ as the k *quasi_multiple* of α.

At that point, we can see that the monomorphism $\mathfrak{w}$ is linear in sense of that the accompanying equalities hold

$$\mathfrak{w}(k \otimes \alpha \oplus \beta) = \mathfrak{w}((k \otimes \alpha) \oplus \beta)$$
$$a \leftarrow (k \otimes \alpha) = \mathfrak{w}(v \oplus \beta)$$
$$= \mathfrak{w}(\mathfrak{w}^{-1}(\mathfrak{w}(v) + \mathfrak{w}(\beta)))$$
$$= \mathfrak{w}\left(\mathfrak{w}^{-1}\left(\mathfrak{w}(\mathfrak{w}^{-1}(k \cdot \mathfrak{w}(\alpha))) + \mathfrak{w}(\beta)\right)\right)$$
$$= \mathfrak{w}(\mathfrak{w}^{-1}(k \cdot \mathfrak{w}(\alpha) + \mathfrak{w}(\beta)))$$
$$= k \cdot \mathfrak{w}(\alpha) + \mathfrak{w}(\beta).$$

for $\alpha, \beta \in \mathcal{G}_S$ and $k \cdot \mathfrak{w}(\alpha) + \mathfrak{w}(\beta) \in \mathfrak{w}(\mathcal{G}_S)$. Further, for $h(u) = z_0 + z_1 u + \cdots + z_i u^i \in \mathbb{Z}[u]$ and $\alpha \in \mathcal{G}_S$, if $h(\mathfrak{w}(\alpha)) = z_0 \cdot 1_{\mathbb{R}} + z_1 \cdot \mathfrak{w}(\alpha) + \cdots + z_n \cdot \mathfrak{w}(\alpha)^n \in \mathfrak{w}(\mathcal{G}_S)$, then for new member $w \in \mathcal{G}_S$ as

$$w \triangleq \mathfrak{w}^{-1}\left(h(\mathfrak{w}(\alpha))\right) = \mathfrak{w}^{-1}(z_0 \cdot 1_{\mathbb{R}} + z_1 \cdot \tau(\alpha) + \cdots + z_n \cdot \mathfrak{w}(\alpha)^n), \quad (7)$$

and call $w = h(\alpha)$ as the *quasi_polynomial* of h on $\mathcal{S}$.

Clearly, for arbitrary $\alpha, \beta \in \mathcal{G}_S, k \in \mathbb{R}$ *and* $h(u) \in \mathbb{Z}[u], \alpha \oplus \beta, k \otimes \alpha$ and $h(\alpha)$ are not always well-defined. But, we can prove that the following theorem holds.

3.1 Theorem

For some $\alpha \in \mathcal{G}_S$ and some $h(u), f(u) \in \mathbb{Z}[u]$, if $h(\alpha)$ and $f(\alpha)$ are well-defined, then

(i). $\mathfrak{w}\left(h(\alpha)\right) = h\left(\mathfrak{w}(\alpha)\right)$;

(ii) $h(\alpha).f(\alpha) = f(\alpha).h(\alpha)$.

3.1.1 Proof

(i) $\mathfrak{w}\left(h(\alpha)\right) = h\left(\mathfrak{w}(\alpha)\right)$ is straight forward from the definition of quasi_polynomial.

(ii)

$h(\alpha).f(\alpha) = \mathfrak{w}(\mathfrak{w}^{-1}(h(\alpha))).\mathfrak{w}(\mathfrak{w}^{-1}(f(\alpha)))$ $(\because \mathfrak{w}(\mathfrak{w}^{-1}(g)) = g, g \in \mathcal{G}_S.)$
$= \mathfrak{w}(\mathfrak{w}^{-1}(h(\alpha)).\mathfrak{w}^{-1}(f(\alpha)))$ $(\because \mathfrak{w}$ is monomorphism $)$

$$= \mathfrak{w}\left(\mathfrak{w}^{-1}\left(f(\alpha)\right) \cdot \mathfrak{w}^{-1}\left(h(\alpha)\right)\right)$$

$$= f(\alpha).h(\alpha).$$

4. An IND-CCA2 Secure Public Key Cryptographic Protocol

In[18] introduced a method to translate an IND-CPA encryption protocol into an IND-CCA2 scheme[18]. By using concept of Fujisaki and Okamoto[18], we convert IND-CPA public key cryptographic technique based on Suzuki 2-group in IND-CCA2 public key cryptographic technique based on Suzuki 2-group.

The technique described as follows:

4.1 Setup

- We assume that SDP on $\mathcal{G}_S$ for a given Suzuki 2-group $(\mathcal{G}_S, *)$.
- Select two random integers $i, j \in \mathbb{Z}$.
- Select two component c and d from $\mathcal{G}_S$.
- Let $\mathfrak{h}_1$ and $\mathfrak{h}_2$ are two hash functions define (cryptographic) as $\mathfrak{h}_1 : \{0,1\}^{\mu+\nu_0} \to \mathbb{Z}[u]$ $\mathfrak{h}_1 : \{0,1\}^{\mathbb{B}+\mathbb{B}_0} \to \mathbb{Z}[u]$ and $\mathfrak{h}_2 : \mathcal{G}_S \to \{0,1\}^{\mu+\nu_0}$.

The public parameters of the technique is given by the tuple $\{\mathcal{G}_S, c, d, i, j, \mathcal{M}, \mathfrak{h}_1, \mathfrak{h}_2\}$.

4.2 Key Generation

- Each entity selects an arbitrary polynomial $h(u) \in \mathbb{Z}[u]$ such that $h(\mathfrak{w}(c)) \in \mathfrak{w}(\mathcal{G}_S)$ and then takes $h(c)$ as his/her private key.
- Calculates $ck = h(c)^i * d * h(c)^j$ and publishes his/her public key (c, d, ck).

4.3 Encryption

For given a M $\in \mathcal{M}$ and Receiver's key (c, d, ch), the sender

- Selects a random component $w \in \{0,1\}^{k_0}$.
- Selects extracts polynomial $f(u) = \mathfrak{h}_1(M \| w) \in \mathbb{Z}[u]$ such that $f(c) \neq 0$.
- Calculates $s = f(c)^i * d * f(c)^j, t = (M \| w) \oplus \mathfrak{h}_2(f(c)^i * ch * f(c)^j)$

Finally outputs the cipher-text
C=(s,t) $\in \mathcal{G}_S \times \{0,1\}^{v+v_0}$.

4.4 Decryption

Upon getting a $\mathcal{C}$, the receiver utilizing his/her private key $h(c)$, calculates

$$M' = b \oplus \mathfrak{h}_2\left(h(c)^i * d * h(c)^j\right)$$

Finally, extracts $f(y) = \mathfrak{h}_1(M') \in \mathbb{Z}[u]$ and checks whether $s = f(c)^i * d * f(c)^j$ holds. Assuming this is the case, yields the starting k bits of M'; generally, yields empty string, which implies that the given cipher-text is invalid.

5. Concrete Examples

In this segment, we illustrate example for supporting our proposed new public key cryptographic technique based on Suzuki 2-group.

Let us the class of Suzuki 2-group with order p^2. Utilizing Higman's documentation, a Suzuki 2-group of order p^2 will be indicated by $\delta(\eta, \theta)$. Assume $p = 2^\eta$ where $\eta \geq 3$ belongs natural number such as an extent that the field F_p has nontrivial automorphism θ of non-even order. This infers η is not a force of 2. At that point the gatherings $\delta(\eta, \theta)$ do exist.

Honestly, in case we describe $\mathcal{G}_S = \left\{\frac{\mathcal{G}_S(i,j)}{i}, j \in F_p\right\}$, where $\mathcal{G}_S(i,j) = \begin{bmatrix} 1 & 0 & 0 \\ i & 1 & 0 \\ j & i^\theta & 1 \end{bmatrix}$ is a 3×3 -matrix over F_p.

Give us a chance to delineate our technique by utilizing a Suzuki 2-group: $M_3(F_p)$, where $\mathcal{N} = q \cdot p$ while q and p are two extensive secure primes. We have strong motivation to trust that symmetrical decomposition problem over $M_3(GL(3,p)) \subset M_3(F_p)$ is immovable, since it is infeasible to extract.

$$\gamma = \begin{pmatrix} i & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in M_3\left(GL(3,p)\right) \subset M_3\left(F_p\right) \subset M_3(\mathbb{Z}_\mathcal{N})$$

Form

$$\gamma^2 = \begin{pmatrix} i^2 mod\ \mathcal{N} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in M_3\left(GL(3,p)\right) \subset M_3\left(F_p\right) \subset M_3\left(\mathbb{Z}_\mathcal{N}\right).$$

without knowing the figuring of $\mathcal{N}$.

Next, let $\mathcal{N} = 2.5 = 10$ for instance. Assume that the framework parameters are

$i = 2, j = 3,$

$$c = \begin{pmatrix} 1 & 0 & 0 \\ 6 & 1 & 0 \\ 8 & 6 & 1 \end{pmatrix}, d = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 6 & 8 & 1 \end{pmatrix} \& h(v) = 5v^3 + 3v^2 + v + 2$$

Hence private key will be

$$h(c) = 5\begin{pmatrix} 1 & 0 & 0 \\ 6 & 1 & 0 \\ 8 & 6 & 1 \end{pmatrix}^3 + 3\begin{pmatrix} 1 & 0 & 0 \\ 6 & 1 & 0 \\ 8 & 6 & 1 \end{pmatrix}^2 + \begin{pmatrix} 1 & 0 & 0 \\ 6 & 1 & 0 \\ 8 & 6 & 1 \end{pmatrix} + 2I = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 4 & 2 & 1 \end{pmatrix}$$

Then, the corresponding public key would be

$$ch \triangleq h(c)^2 d h(c)^3 = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 4 & 2 & 1 \end{pmatrix}^2 \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 6 & 8 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 4 & 2 & 1 \end{pmatrix}^3 = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 2 & 8 & 1 \end{pmatrix}$$

Give us a chance to pick a message M arbitrarily, say $M = \begin{pmatrix} 2 & 4 & 9 \\ 5 & 3 & 1 \\ 8 & 2 & 0 \end{pmatrix}$.Suppose the compound number we picked arbitrarily is $w = 15$. At that point, we separate a polynomial as takes after:

$$f(u) = (2^{15}\ mod\ \mathcal{N}) + (2^2\ mod\ \mathcal{N})u + (2^4\ \mathbf{mod}\ \mathcal{N})u^2 + (2^9\ \mathbf{mod}\ \mathcal{N})u^3$$

$$+ (2^5\ mod\ \mathcal{N})u^4 + (2^3\ mod\ \mathcal{N})u^5 + (2^1\ \mathbf{mod}\ \mathcal{N})u^6 + (2^8\ \mathbf{mod}\ \mathcal{N})u^7$$

$$+ (2^2\ \mathbf{mod}\ \mathcal{N})u^8$$

$$= 8 + 4u + 6u^2 + 2u^3 + 2u^4 + 8u^5 + 2u^6 + 6u^7 + 4u^8.$$

Which gives?

$$f(c) = 8I + 4\begin{pmatrix} 1 & 0 & 0 \\ 6 & 1 & 0 \\ 8 & 6 & 1 \end{pmatrix} + 6\begin{pmatrix} 1 & 0 & 0 \\ 6 & 1 & 0 \\ 8 & 6 & 1 \end{pmatrix}^2 + 2\begin{pmatrix} 1 & 0 & 0 \\ 6 & 1 & 0 \\ 8 & 6 & 1 \end{pmatrix}^3$$

$$+ 2\begin{pmatrix} 1 & 0 & 0 \\ 6 & 1 & 0 \\ 8 & 6 & 1 \end{pmatrix}^4 + 8\begin{pmatrix} 1 & 0 & 0 \\ 6 & 1 & 0 \\ 8 & 6 & 1 \end{pmatrix}^5 + 2\begin{pmatrix} 1 & 0 & 0 \\ 6 & 1 & 0 \\ 8 & 6 & 1 \end{pmatrix}^6$$

$$+ 6\begin{pmatrix} 1 & 0 & 0 \\ 6 & 1 & 0 \\ 8 & 6 & 1 \end{pmatrix}^7 + 4\begin{pmatrix} 1 & 0 & 0 \\ 6 & 1 & 0 \\ 8 & 6 & 1 \end{pmatrix}^8$$

$$= \begin{pmatrix} 8 & 0 & 0 \\ 4 & 8 & 0 \\ 2 & 4 & 8 \end{pmatrix} \neq 0.$$

(Take note of that if $f(u)$ does not satisfy the condition of $f(c) \neq 0$,we ought to at first amend $f(u)$to $f(u) = f(u) + \Delta$, Where

$$\Delta = \min\left\{\varsigma \in \mathbb{Z}_{\geq 0} : f(c) + \varsigma * \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \neq 0\right\}$$

Luckily, in this illustration. The above extracted $f(u)$ meets the necessity of $f(c) \neq 0, i.e. \Delta = 0.$) At that point, then cipher-text combine is

$$s = f(c)^2 * d * f(c)^5 = \begin{pmatrix} 8 & 0 & 0 \\ 4 & 8 & 0 \\ 2 & 4 & 8 \end{pmatrix}^2 \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 6 & 8 & 1 \end{pmatrix} \begin{pmatrix} 8 & 0 & 0 \\ 4 & 8 & 0 \\ 2 & 4 & 8 \end{pmatrix}^3 = \begin{pmatrix} 8 & 0 & 0 \\ 6 & 8 & 0 \\ 0 & 4 & 8 \end{pmatrix},$$

and

$$t = (M \parallel w) \oplus \mathfrak{h}_2(f(c)^2 * ck * f(c)^3)$$

$$= \begin{pmatrix} 2 & 4 & 9 \\ 5 & 3 & 1 \\ 8 & 2 & 15 \end{pmatrix} \oplus \mathfrak{h}_2\left(\begin{pmatrix} 8 & 0 & 0 \\ 4 & 8 & 0 \\ 2 & 4 & 8 \end{pmatrix}^2 \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 2 & 8 & 1 \end{pmatrix} \begin{pmatrix} 8 & 0 & 0 \\ 4 & 8 & 0 \\ 2 & 4 & 8 \end{pmatrix}^3\right)$$

$$= \begin{pmatrix} 2 & 4 & 9 \\ 5 & 3 & 1 \\ 8 & 2 & 15 \end{pmatrix} \mathfrak{U} \mathfrak{h}_2\left(\begin{pmatrix} 8 & 0 & 0 \\ 6 & 8 & 0 \\ 8 & 4 & 8 \end{pmatrix}\right)$$

$$= \begin{pmatrix} 2 & 4 & 9 \\ 5 & 3 & 1 \\ 8 & 2 & 15 \end{pmatrix} \oplus \left(\begin{pmatrix} 2^8 & 2^0 & 2^0 \\ 2^6 & 2^8 & 2^0 \\ 2^8 & 2^4 & 2^8 \end{pmatrix} mod\ \mathcal{N}\right)$$

$$= \begin{pmatrix} 2 & 4 & 9 \\ 5 & 3 & 1 \\ 8 & 2 & 15 \end{pmatrix} \oplus \begin{pmatrix} 6 & 1 & 1 \\ 4 & 6 & 1 \\ 6 & 6 & 6 \end{pmatrix}$$

$$= \begin{pmatrix} 4 & 5 & 8 \\ 1 & 5 & 0 \\ 14 & 4 & 9 \end{pmatrix}$$

Presently, let us check the decryption process:

$$M' = b \oplus \mathfrak{h}_2\left(h(c)^2 * d * h(c)^3\right)$$

$$= \begin{pmatrix} 4 & 5 & 8 \\ 1 & 5 & 0 \\ 14 & 4 & 9 \end{pmatrix} \bigoplus \mathfrak{h}_2\left(\begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 4 & 2 & 1 \end{pmatrix}^2 \begin{pmatrix} 8 & 0 & 0 \\ 6 & 8 & 0 \\ 0 & 4 & 8 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 4 & 2 & 1 \end{pmatrix}^3\right)$$

$$= \begin{pmatrix} 4 & 5 & 8 \\ 1 & 5 & 0 \\ 14 & 4 & 9 \end{pmatrix} \bigoplus \mathfrak{h}_2\left(\begin{pmatrix} 6 & 1 & 1 \\ 4 & 6 & 1 \\ 6 & 6 & 6 \end{pmatrix}\right)$$

$$= \begin{pmatrix} 4 & 5 & 8 \\ 1 & 5 & 0 \\ 14 & 4 & 9 \end{pmatrix} \oplus \left(\begin{pmatrix} 2^6 & 2^0 & 2^0 \\ 2^2 & 2^6 & 2^0 \\ 2^0 & 2^8 & 2^6 \end{pmatrix} mod\ \mathcal{N}\right)$$

$$= \begin{pmatrix} 4 & 5 & 8 \\ 1 & 5 & 0 \\ 14 & 4 & 9 \end{pmatrix} \oplus \begin{pmatrix} 2 & 4 & 9 \\ 5 & 3 & 1 \\ 8 & 2 & 15 \end{pmatrix}$$

$$= \begin{pmatrix} 2 & 4 & 9 \\ 5 & 3 & 1 \\ 8 & 2 & 15 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 15 \end{pmatrix}$$

$$= (M \parallel w).$$

6. Security Analysis and Discussion

In 1999, [18]acquainted a strategy with change over an IND-CPA cryptographic technique into an IND-CCA2 cryptographic technique. For self-containing, we practice their principle thought as takes after:

Assume that $\Lambda \mapsto \{\Omega, \bar{e}_n, \bar{d}_c\}$ is an IND-CPA secure public-key cryptographic technique with key generation procedure $\Omega(1^{\mathfrak{u}})$, encryption procedure $\bar{e}_{n_{c\hbar}}(\mathbf{M}, S)$ and decryption procedure $\bar{d}_{c_{\hbar(c)}}(y)$, where $\hbar(c)$ and $c\hbar$ are a private key and the conforming public key, M a message with $\mathfrak{u}+\mathfrak{u}_0$ bits, ş a random string with ł bits and $\mathcal{C}$ a cipher-text. The transformed public-key cryptographic technique $\Lambda \mapsto \{\Omega, \bar{e}_n, \bar{d}_c\}$ is defined by $\bar{\Omega}(1^{\mathfrak{u}}) \mapsto \Omega(1^{\mathfrak{u}+\mathfrak{u}_0})$,

$$\overline{\bar{e}_{n_{c\hbar}}}(\mathbf{M}, \text{ş}) \mapsto \epsilon_{c\hbar}\left(m \parallel w, \mathfrak{h}(m \parallel w)\right),$$

$$\bar{d}_{c_{\hbar(c)}}(\mathcal{C}) := \begin{cases} \left[\bar{d}_{c_{\hbar(c)}}(\mathcal{C})\right]^{\mathfrak{u}}, \text{if } \mathcal{C} = \epsilon_{c\hbar}(\bar{d}_{c_{\hbar(c)}}(\mathcal{C}), \mathfrak{h}\left(\bar{d}_{c_{\hbar(c)}}(\mathcal{C})\right)) \\ \perp, \text{otherwise} \end{cases}$$

where $\mathfrak{h} : \{0,1\}^{\mathfrak{u}+\mathfrak{u}_0} \to \{0,1\}^{\mathfrak{l}}$ is a random function of, m is a message with $\mathfrak{u}$ bits, w an arbitrary string with $\mathfrak{u}_0$ bits and || denotes concatenation.

6.1 Theorem 6.1[18]

Assume that $\Lambda \mapsto \Omega(1^{\mathfrak{u}+\mathfrak{u}_0})$ is the first IND-CPA secure cryptographic technique and $\overline{\Lambda}$ is changed over technique. In the event that $\exists$ a $(t, q_H, q_{\bar{d}}, \bar{e}_n)$-adversary $\mathcal{A}$ for $\bar{\Lambda}(1^{\mathfrak{u}})$ in the sense of IND-CCA2 in the ROM, $\exists$ a $(t', q_H, q_{\bar{d}}, \bar{e}_n')$- adversary $\mathcal{A}'$ for $\Lambda(1^{\mathfrak{u}+\mathfrak{u}_0})$ and constant c, where

$$\bar{e}_n' = \left(\bar{e} - \frac{q_H}{2^{\mathfrak{l}(\mathfrak{u}]_0 - 1)}}\right) * \left(1 - \frac{1}{2^{\mathfrak{l}]_0}}\right)^{q_{\bar{d}}} \text{and}$$

$$t' = t + \left(\mathbf{c} * \mathbf{k} + \mathbf{T}_{\bar{e}}(\mathfrak{u})\right) q_H$$

Here, $(t', q_H, q_{\bar{d}}, \bar{e}')$- adversary $\mathcal{A}$, casually, implies that $\mathcal{A}$ stops inside t stages, prevails with probability in any event, makes at most q_H inquiries to H , and most $q_{\bar{d}}$ inquiries to decryption oracle $\bar{d}_{c_{\hbar(c)}}$

. The computational time of the encryption procedure $\bar{e}_{c\hat{k}}(\cdot)$ is $T_{\bar{e}}(k)$ and

$$\mathfrak{l}_0 \mapsto \log_2\left(\min_{m\in\{0,1\}^{\mathfrak{u}+\mathfrak{u}_0}}\left[\#\{\bar{e}_{n_{c\hat{k}}}(M,w)|w\in\{0,1\}^{\mathfrak{l}}\}\right]\right).$$

Proof. See Theorem 3 of [18].

As indicated in[18], we can changeover our fundamental public key cryptographic technique into more secure new public key cryptographic technique, which comes to IND-CCA2 security, with sacrificing of $\mathfrak{u}_0$ bits plaintext.

6.2 Theorem 6.2[19]

Let $\mathfrak{f}$ be a random oracle and $\mathcal{A}$ be an IND-CPA foe that has advantage against the purpose fundamental technique inside $\mathfrak{u}$ iterations. Assume that $\mathcal{A}$ makes a $q_{\mathfrak{f}}$ total of inquiries to $\mathfrak{f}$. Then there is a procedure A that resolves polynomial Diffie-Hellman problem over $\mathfrak{d}_w$ with advantage at least $\bar{e}'$ within $\mathfrak{u}'$ iterations, where

$$\bar{e}_n' = \frac{2\bar{e}_n}{q_{\mathfrak{f}}}, \mathfrak{u}' = O(\Omega).$$

Proof. See the Theorem 6 of[19].

6.3 Theorem 6.3

Assume that $\mathfrak{f}_1$ and $\mathfrak{f}_2$ are two random oracles. Then the presented public key cryptographic technique is an IND-CCA2acceptingpolynomial Diffie-Hellman problem over the Suzuki 2-group $\mathcal{G}_S$ is hard. All that has been assumed is an IND-CCA2 foe $\mathcal{A}$ that has advantage against the presented public key cryptographic technique inside t steps. Assume that adversary $\mathcal{A}$ makes at most q_D decryption inquiries, and at most $q_{\mathfrak{f}_1}$, $q_{\mathfrak{f}_2}$ inquiries to the hash functions $\mathfrak{f}_1$ and $\mathfrak{f}_2$ respectively. Then there is a technique $\mathcal{B}$ which can solve polynomial Diffie-Hellman problem with the probability at least 0 inside t_0 steps, where

$$\bar{e}_n' = \frac{2}{q_{\mathfrak{f}_1}}\left[\frac{\bar{e}_n.2^{-\mathfrak{l}_o}}{(2^{\mathfrak{l}_o}-1)q_D}+\frac{q_{\mathfrak{f}_2}}{2^{\mathfrak{u}_o-1}}\right]$$

$$t' = O(t + (ck + T_{\bar{e}}(\mathfrak{u}))q_{\mathfrak{f}_2})$$

where c is a constant and $T_{\bar{e}}(\mathfrak{u})$ represents the computational time of the encryption process $\bar{e}_{n_{c\hat{k}}}(\cdot)$ in our purposed public key cryptographic technique, and $\mathfrak{l}_0 \mapsto \log_2(\min_{m\in\{0,1\}^{\mathfrak{u}+\mathfrak{u}_0}}[\#\{\bar{e}_{n_{c\hat{k}}}(M,w)|w\in\{0,1\}^{\mathfrak{l}}\}])$

6.4 Proof

We At first, from Theorem 6.1 and Theorem 6.2, it promptly presumes that our presented public key cryptographic technique comes to IND-CCA2 security in the ROM assuming that polynomial Diffie-Hellman problem is hard. Then, consolidating the consequences of both the IND-CPA hypothesis and Fujisaki-Okamoto hypothesis, we get the above limits.

6.5 Remark

It is critical the elaborations on completing a cryptographic hash that maps a binary string to a polynomial, for example, $\mathfrak{h}_1 : \{0,1\}^{\mathfrak{u}+\mathfrak{u}_0} \to 2[u]$. Specifically, the ensuing polynomials should assist imperatives, for instance, the condition $\widetilde{h}(v) \neq 0$ et cetera. We utilize the purported separate and-overcome system to deal with this issue: At first, we extricate a polynomial $f(u) \in f(u)+$ from a binary string in $\{0,1\}^{\mathfrak{u}+\mathfrak{u}_0}$; Then, we receive an interesting deterministic approach to correct $h(v)$ to $\widetilde{h}(v)$ with the end goal that $\widetilde{h}(v)$ satisfies the sought condition C . Toward the day's end, we have to consider the going with issues in sketching out the needed hash.

6.6 Extracting

In exercise, we need to pick huge coefficients polynomials with low degrees. Allow us to acknowledge that the most vital degree is d_H and the largest coefficient is c_M, then $d_H \cdot c_M$ ought to be sufficiently extensive resist brute force attack. Thusly, there is a trivial solution to implement $\mathfrak{f}_1$:Assume that we starting at now have a cryptographic hash function $\mathfrak{h}': \{0,1\}^{\mathfrak{u}+\mathfrak{u}_0} \to 2^{d_H+1}_{c_M}$. At that point, for any given image of $\mathfrak{f}_1$, i.e., a vector $(\alpha_0, \alpha_1, \cdots \alpha_{d_H}) \in 2^{d_H+1}_{c_M}$, we can outline to an objective polynomial $h(v)$ by a characteristic way:

$$h(v) = \alpha_0 + \alpha_1 v + \cdots + \alpha_{d_H} v^{d_H}$$

6.7 Rectifying

Assume we embrace an added substance rectifying strategy. At that point, for coming about polynomial $f(u)$, it can be rectified to $f(u) = f(u)+ \Delta$ while

$$\Delta = \min\{\varsigma \in 2_{\geq 0} : f(c) + \varsigma.1_{\mathfrak{G}} \in 2_{>0}[x] \cap C\},$$

where $2_{>0}[x] \cap C$ is the arrangement of polynomials in $2_{>0}[u]$ fulfilling the given condition C.

6.8 Collision-Resisting

The above correcting procedure is not to abuse the property of collision resistance. In fact, the collision resistance of f_1 is established in the one-wayness of f'.

7. Conclusions

In this study, we demonstrated new approach for designing the public key cryptographic technique using the concept of general non-commutative algebraic system such as Suzuki 2-group. Also we discussed the new strategy with change over an IND-CPA cryptographic technique into an IND-CCA2 cryptographic technique. By using this new strategy we change our past IND-CPA public key cryptographic technique in to more secure IND-CCA2 public key cryptographic technique. The principle thought in our suggestion lies that we consider polynomials on given non-commutative arithmetical framework as the major work structure for creating cryptographic arrangements. Consequently, we can get some commutative sub-structures for the given non-commutative scientific systems.

8. References

1. Diffie W, Hellma ME. New directions in cryptography. Institute of Electrical and Electronics Engineers (IEEE) Transactions on Information Theory.1976 Nov; 22(6):644–54. Crossref
2. Wagner NR, Magyarik MR. A public-key cryptosystem based on the word problem. In Blakley GR, Chaum D editors. Workshop on the Theory and Application of Cryptographic Techniques (CRYPTO), Advances in Cryptology, Lecture Notes in Computer Science (LNCS), Springer- Verlag.1985; 196:19–36. Crossref
3. Birget J, Magliveras SS, Sramka M. On public-key cryptosystems based on combinatorial group theory [Internet]. 2005 [cited 2005 Jan]. Available from: Crossref.
4. Anshel I, Anshel M, Goldfeld D. An algebraic method for public-key cryptography. Mathematical Research Letters.1999; 6(3):287–91. Crossref
5. Ko KH, Lee SJ, Cheon JH, Han JW et al. Public-key cryptosystem using braid groups. In Bellare M editor. Annual International Cryptology Conference, Advances in Cryptology — CRYPTO, Lecture Notes in Computer Science (LNCS), Springer-Verlag. 2000 Aug 11; 1880:166–83. Crossref.
6. Paeng S–H, Ha K–C, Kim J–H, Chee S, Park C. New public key cryptosystem using finite non Abelian groups. In Kilian J editor. Annual International Cryptology Conference, Advances in Cryptology — CRYPTO, Lecture Notes in Computer Science (LNCS), Springer-Verlag. 2001 Aug 2; 2139:470–85.
7. Paeng S.H, D. Kwon, K.-C. Ha, J. H. New Kim. Improved public key cryptosystem using finite non abelian groups,Cryptology ePrint. 2001. Archive: Report 2001/066.
8. Magliveras SS, Stinson DR, Trung TV. New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups. Journal of Cryptology. 2002 Sep; 15(4):285–97.
9. Grigoriev D, Ponomarenko I. On non-abelian homomorphic public-key crypto systems [Internet]. 2002 [updated 2002 Nov 14; cited 2002 Jul 23]. Available from: Crossref
10. Grigoriev D, Ponomarenko I. Homomorphic public-key cryptosystems over groups and rings [Internet]. 2003 [cited 2003 Sep 8]. Available from: Crossref.
11. Eick B, Kahrobaei D. Polycyclic groups: a new platform for cryptography [Internet]. 2004 [cited 2004 Nov 3]. Available from: Crossref.
12. Birman J, Ko KH, Lee SJ. A new approach to the word and conjugacy problems in the braid groups. Advances in Mathematics, ScienceDirect.1998 Nov 10; 139(2):322–53. Crossref
13. Birman J, Ko KH, Lee SJ. The infimum, supremum, and geodesic length of a braid conjugacy class. Advances in Mathematics, ScienceDirect. 2001 Dec 1; 164(1):41–56. Crossref
14. El-Rifai EA, Morton HR. Algorithms for positive braids. The Quarterly Journal of Mathematics, Oxford Academic.1994 Dec 1; 45(4):479–97. Crossref
15. Gebhardt V. A new approach to the conjugacy problem in Garside groups [Internet]. 2003 [updated 2003 Oct 21; cited 2003 Jun 12]. Available from: Crossref.
16. Gonzales-Meneses J. Improving an algorithm to solve the multiple simultaneous conjugacy problems in braid groups [Internet]. 2002 [cited 2002 Dec 10]. Available from: Crossref.
17. Higman G. Suzuki 2-groups. Illinois Journal of Mathematics.1963; 7:79–96.
18. Fujisaki E, Okamoto T. How to enhance the security of public key encryption at minimum cost. In Imai H, Zheng Y editors. International Workshop on Public Key Cryptography, Public Key Cryptography (PKC), Lecture Notes in Computer Science (LNCS), Springer-Verlag.1999 Oct 29; 1560:53–68.
19. Meshram A, Meshram C, Khobragade N. An IND-CPA Secure PKC Technique Based On Dihedral Group. Indian Journal of Computer Science and Engineering, 2017 Apr..