ISSN No. 0976-5697

Volume 8, No. 3, March – April 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Public Key Cryptographic Technique Based On Suzuki 2-Group

Akshaykumar Meshram
Department of Applied Mathematics
YeshwantraoChavan College of Engineering,
Nagpur, (M.S.), India

Chandrashekhar Meshram
Department of Mathematics and ComputerScience
R.D. University,
Jabalpur (M.P.), India

N.W. Khobragade
Department of Mathematics
RTM Nagpur University, Nagpur, (M.S.), India

Abstract:Public key cryptography is one of the most important fields in computer security. . It is a method of transferring private information 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 new public key cryptographic technique based on Suzuki 2- group. We demonstrated the security of proposed public key cryptographic technique in the chosen plaintext attack in the random oracle model.

Keywords:Public key cryptography, ring polynomial, Suzuki 2-group, chosen plaintext attack, random oracle.

INTRODUCTION

The conception of public key cryptography (PKC) was introduced by Diffie and Hellman [1] in 1976, many PKC schemes have been proposed and broken. 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, integer factorization problem (IFP) and discrete logarithm problem (DLP), as well as DLP over elliptic curves (ECDLP), 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]. As addressed in [6], in order to develop cryptography as well as not to put all eggs in one basket, there have been many attempts to develop alternative PKC based on different kinds of problems [6]:

In 1984, Wagner et al. [7] proposed a method to design public-key cryptosystems based on the undecidable word problem for groups and semi-groups. In 2005, Birget et al. [8] pointed out that Wagner's idea is actually not based on word problem, but on another, generally easier, premise problem. Afterwards, Birget et al. finally proposed a new public-key cryptosystem which is based on finitely presented groups with hard word problem.

In 1999, Anshel et al. [9] proposed a compact algebraic key establishment protocol. The foundation of their method lies in the difficulty of solving equations over algebraic structure (non-commutative groups). Subsequently, Ko et al. [10] firstly proposed new PKC by using braid groups in 2000. The security foundation is that the conjugator search problem (CSP) is intractable when the system parameters, such as braid index and the canonical length of the working braids, are selected properly.

In 2001, Paeng et al. [11] published a new PKC built on finite non-abelian groups. Their method is based on the DLP in the inner automorphism group defined via the conjugate action. Their system was later improved to the so-called MOR systems [12]. Meanwhile, Magliveras et al. [13] developed new approaches to design PKC using one-way functions and trapdoors in finite groups. Two public key cryptosystems based on the difficulty of computing certain factorizations in finite groups, have been introduced: MST1 and MST2. Subsequently, in 2002, Vasco et al. [14] demonstrated that, after a suitable generalization, the factorization concepts used in MST1 and MST2 allow a uniform description of several cryptographic primitives.

In 2002, certain homomorphic cryptosystems were constructed for the first time for non-abelian groups due to Grigoriev and Ponomarenko [15]. Shortly afterwards, Grigoriev and Ponomarenko [16] extended their method to arbitrary nonidentify finite groups based on the difficulty of the membership problem for groups of integer matrices. Enlightened by the idea in the arithmetic key exchange [9], in 2004, Eick and Kahrobaei [17] proposed a new cryptosystem based on polycyclic groups.

In 2005, Shpilrain and Ushakov [18] suggested that R. Thompson's group may be is a good platform for constructing PKC. In their contribution, the key assumption is the intractability of the decomposition problem, which is more general than the conjugator search problem, defined over R. Thompson's group, also an infinite non-abelian group given by finite presentation.

Generic algebraic systems, especially non-commutative ones, attract more and more attentions among the above cryptosystems. It is find difficulty of solving CSP over certain non-abelian groups using non-

commutative algebraic systems. Although there are algorithms for solving some variants of CSP in certain groups, such as braid groups [19,20,21,22,23], with respect to the system parameters, none of them can solve CSP itself defined over general non -abelian group in polynomial time. However, non-commutative is a double-edged sword: on the one hand, it makes CSP meaningful; on the other hand, it brings some inconvenience for designing PKC schemes. How to utilize non-commutative and overcome its inconvenience is the key problem for developing PKC over non-commutative algebraic systems.

Recentaly, Meshram [24, 25, 26, 27, 28] presented new variant of public key cryptographic technique based on discrete logarithm problem and integer factorization problem and its generalization. Also developed some ideas for identity-based cryptography in [29, 30, 31, 32, 33, 34, 35].

Organization: In this article, we would like to propose a new approach based on Suzuki 2-group for designing public key cryptographic technique. The key idea of our proposal is that we can define polynomials and take them as the fundamental work structure for a given Suzuki 2-group. By doing so, it is much easy to implement the efficient public key cryptographic technique secure under choose plaintext attack in random oracle model.

The structure of the article: This paper is organized as follows. In Section 2, background and material are introduced; In Section 3, we demonstrated some extension of over Suzuki 2-group; In Section 4, we proposed new public key cryptographic technique. In Section 5, we demonstrated supporting example for proposed new public key cryptographic technique. Discussed security of proposed technique in Section 6. Finally, concluding remarks are made in Section 7.

BACKGROUND AND MATERIAL

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

Integral Coefficient Ring Polynomials

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

At first, the notion of scale multiplication over $\Re$ is now close by. For $l \in Z_{>0}$ and $r \in \Re$,

$$(l)r \triangleq \underbrace{r + \cdots \ldots \ldots \ldots + r}_{l \ times}(1) \qquad (1)$$

when $l \in Z_{>0}$, we can define

$$(l)r \triangleq (-l)(-r) = \underbrace{(-r) + \cdots + (-r)}_{-l \ times} \qquad (2)$$

For $l = 0$, it is natural to define $(l)r = 0$.

Property1. $(s)r^n.(t)r^m = (st)r^{n+m} = (t)r^m.(s)r^n, \forall s,t,n,m \in Z$ and $\forall r \in \Re$

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

Remark. Note that in general, $(s)r \cdot (t)j \neq (t)j \cdot (s)r$ when $r \neq j$, since multiplication in $\Re$ is non-commutative.

Now, let us continue to define positive integral coefficient ring polynomials. Assume that

$h(y) = s_0 + s_1 y + \cdots + s_m y_m \in Z_{>0}[y]$ is a given positive integral coefficient polynomial. We can allocate this polynomial by utilizing a component r in $\Re$ and finally get $h(r) = \sum_{a=0}^{m}(s_a)r^a = (s_0)1 + (s_1)r + \cdots + (s_m)r^m$, (3)

which is a component in $\Re$, obviously. Advance, in the event that we view r as a variable in $\Re$, then $h(r)$ can be looked as a polynomial about variable r. The arrangement of this types of polynomials, taking over all $h(y) \in Z_{>0}[y]$, can be looked the expansion of $Z_{>0}$ with r, indicated by $Z_{>0}[r]$. For comfort, we call it the arrangement of 1-ary positive integral coefficient R-polynomials.

Assume that $h(r) = \sum_{a=0}^{m}(s_a)r^a \in Z_{>0}[r]$, $f(r) = \sum_{b=0}^{n}(t_b)r^b \in Z_{>0}[r]$ and $m \geq n$, then $(\sum_{a=0}^{m}(s_a)r^a) + (\sum_{b=0}^{n}(t_b)r^b) = (\sum_{a=0}^{n}(s_a + t^a)r^a + \sum_{a=n+1}^{m}(s^a)r^a$ (4)

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

$$\left(\sum_{a=0}^{m}(s_a)r^a\right).\left(\sum_{b=0}^{n}(t_b)r^b\right) = \left(\sum_{a=0}^{n+1}(p_a)r^a\right)$$

where $p_a = \sum_{b=0}^{a} s_a t_{a-b} = \sum_{b+c=a} s_a t_k$ and then, we can finish up instantly the following hypothesis as per Property 1.

Theorem2.1. $h(r) \cdot f(r) = f(r) \cdot h(r), \forall h(r), f(r) \in Z_{>0}[r]$. Remark 3. If r and s are two different variable, then $h(r) \cdot f(s) \neq f(s).h(r)$ in general.

Suzuki 2-group

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

The set $Z(G) = \{z \in G : zg = gz \ \forall g \in G\}$ is called the center of G. It is outstanding that $Z(G)$ is a normal subgroup of request at any rate q for any q-group G. The subgroup G' generated by every one of the components of the form $x^{-1}y^{-1}xy$ with $x, y \in G$ is called the commutator subgroup of G. The so-called Frattini subgroup of G, indicated by $\varphi(G) = < g^2/g \in G >$. At last, a component of order 2 in a gathering is called an involution.

Formally, a Suzuki 2-group [36] 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 examined and characterized by G. Higman [37].

Specifically, in any Suzuki 2-group $\mathcal{G}$ we have $\mathcal{Z}(\mathcal{G}) = \varphi(\mathcal{G}) = \mathcal{G}' = \Omega_1(\mathcal{G})$, where $\Omega_1(\mathcal{G}) =< g^2 = 1/g \in \mathcal{G} >$ and $|\mathcal{Z}(\mathcal{G})| = q = 2^m, m > 1$. It is appeared in [37] that the order of g is either p^2 *or* p^3. In this manner all the involution of $\mathcal{G}$ are in the center of $\mathcal{G}$, there $\mathcal{Z}(\mathcal{G})$ and the factor group $\mathcal{G}/\varphi(\mathcal{G})$ are rudimentary abelian. Subsequently, all components not in $\mathcal{Z}(\mathcal{G})$ have order 4, i.e., $\mathcal{G}$ is of exponent 4. It is realized that $\mathcal{G}$ has an automorphi ξ of order $p - 1$ consistently permuting the involution of $\mathcal{G}$.

2.3. Symmetrical Decomposition Problem (SDP): For given $(x, y) \in \mathcal{G} \times \mathcal{G}$ and $m, n \in Z$, find $z \in \mathcal{G}$ such that $y = z^m x z^n$.

2.4. Polynomial Diffie-Hellman (PDH) Problem over Suzuki 2-geoup: Suppose that $(\mathcal{G},\cdot)$ is a Suzuki 2-geoup. For any arbitrarily selected component $a \in \mathcal{G}$, we define a set $P_a \subseteq \mathcal{G}$ by

$$P_a \triangleq \{f(a) : f(x) \in Z_{>0}[x]\}.$$

Then, let we consider the new versions of computational Diffie-Hellman problem over $(\mathcal{G},\cdot)$ with respect to its subset P_a, 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 $x \in \mathcal{G}$, $z_1, z_2 \in P_a$.

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

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 $(\mathcal{G},\cdot, 1_{\mathcal{G}})$. Suppose that there is a ring $(\Re, +,\cdot, 1_{\Re})$ and a monomorphism $\tau : (\mathcal{G},\cdot, 1_{\mathcal{G}}) \to (\Re, +,\cdot, 1_{\Re})$. Then, the inverse map $\tau^{-1} : \tau(\mathcal{G}) \to \mathcal{G}$ is also a well-defined monomorphism and for $s, t \in \mathcal{G}$, if $\tau(s) + \tau(t) \in \tau(\mathcal{G})$, we can assign a new element $u \in \mathcal{G}$ as

$$u \triangleq \tau^{-1}(\tau(s) + \tau(t)), \qquad (5)$$

and call u as the quasi-sum of s and t, denoted by $u = s \oplus t$. Similarly, for $l \in R$ and $s \in \mathcal{G}$, if $l \cdot \tau(a) \in \tau(\mathcal{G})$, then we can assign a new element $v \in \mathcal{G}$ as

$$v \triangleq \tau^{-1}(l.\tau(s)), \qquad (6)$$

and call v as the l *quasi-multiple* of s, denoted by $v = l \otimes s$.

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

$$\tau(l \otimes s \oplus t) = \tau((l \otimes s) \oplus t)$$

$$\overset{v \leftarrow (l \otimes s)}{=} \tau(v \oplus t)$$

$$= \tau(\tau^{-1}(\tau(v) + \tau(t)))$$

$$= \tau(\tau^{-1}(\tau(\tau^{-1}(l.\tau(s))) + \tau(t)))$$

$$= \tau(\tau^{-1}(l.\tau(s) + \tau(t)))$$

$$= l.\tau(s) + \tau(t).$$

for$s, t \in \mathcal{G}$ and $l \cdot \tau(s) + \tau(t) \in \tau(\mathcal{G})$.

Further, for $h(y) = z_0 + z_1 y + \cdots + z_n y^n \in Z[y]$and $s \in \mathcal{G}$, if $h(\tau(s)) = z_0 \cdot 1_R + z_1 \cdot \tau(s) + \cdots + z_n \cdot \tau(s)^n \in \tau(\mathcal{G})$, then we can assign a new element $w \in \mathcal{G}$ as

$$w \triangleq \tau^{-1}(h(\tau(s))) = \tau^{-1}(z_0 \cdot 1_R + z_1 \cdot \tau(s) + \cdots + z_n \cdot \tau(s)^n), \qquad (7)$$

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

Clearly, for arbitrary $s, t \in \mathcal{G}, l \in R$ *and* $h(y) \in Z[y], s \oplus t, l \otimes s$ and $h(s)$ are not always well-defined. But, we can prove that the following theorem holds.

Theorem 3.1. For some $s \in \mathcal{G}$ and some $h(y), f(y) \in Z[y]$, if $h(s)$ and $f(s)$ are well-defined, then

(i). $\tau(h(s)) = h(\tau(s))$;

(ii) $h(s).f(s) = f(s).h(s)$.

Proof. A**fi** rst, (i) is apparent according to the definition of quasi-polynomial. Next, we have,

$$h(s).f(s) = \tau\left(\tau^{-1}(h(s))\right).\tau\left(\tau^{-1}(f(s))\right)$$
$$(\because \tau(\tau^{-1}(g)) = g, g \in \mathcal{G}.)$$
$$= \tau(\tau^{-1}(h(s)).\tau^{-1}(f(s)))$$
$$= \tau\left(\tau^{-1}(h(s).f(s))\right)$$
$$(\because \tau^{-1} \text{ is monomorphism})$$
$$= \tau\left(\tau^{-1}(f(s)h(s))\right)$$
$$(\because \text{Theorem } 2.1)$$
$$= \tau(\tau^{-1}(f(s)) \cdot \tau^{-1}(h(s)))$$
$$= \tau\left(\tau^{-1}(f(s))\right).\tau(\tau^{-1}(h(s)))$$
$$= f(s).h(s).$$

PROPOSE PKC TECHNIQUE

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

4.1Setup:

1. We assume that SDP on $\mathcal{G}$ for a given suzuki 2-group $(\mathcal{G},*)$.
2. Select two random integers $n, m \in \mathbb{Z}$.
3. Select two component q and $p$from $\mathcal{G}$.
4. Let $\mathcal{H}$ be the cryptographic hash function define as $\mathcal{H} : \mathcal{G} \to \mathcal{M}$.

The public parameters of the technique is given by the tuple $\{\mathcal{G}, q, p, n, m, \mathcal{M}, \mathcal{H}\}$.

4.2 Key generation:

1. Each entity selects an arbitrary polynomial $h(y) \in Z[y]$ such that $h(\tau(q)) \in \tau(\mathcal{G})$and then takes $h(q)$ as his/her private key.
2. Computes $x = h(q)^n . p . h(q)^m$ and publishes his/her public key (q, p, x) .

4.3 Encryption: For a given message $M \in \mathcal{M}$ and receiver's key (q, p, x) , the sender adopt the below procedure

1. Picks an arbitrary polynomial $f(y) \in Z[y]$such that $f(\tau(q)) \in \tau(\mathcal{G})$ and then takes $f(q)$as salt.
2. Estimates

$$a = f(q)^n . p . f(q)^m, \quad b = \mathcal{H}(f(q)^n . p . f(q)^m) \oplus M,$$

Lastly yields the ciphertext

$$\mathcal{C} = (a, b) \in \mathcal{G} \times \mathcal{M}.$$

4.4 Decryption: Upon receiving a ciphertext $\mathcal{C}$, the receiver, by using his private key $h(q)$, estimates the plaintext M as following

$$M = \mathcal{H}(h(q)^n . a . h(q)^m) \oplus b$$

EXAMPLE

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

Consider the class of Suzuki 2-group having orderp^2. Utilizing Higman's documentation, a Suzuki 2-group order p^2 will be indicated by $A(m, \theta)$. Let $p = 2^m$with $3 \leq m \epsilon \mathbb{N}$ to such an extent that the field F_p has nontrivial automorphism θ of odd order. This infers m is not a force of 2. At that point the gathering $A(m, \theta)$do exist.

Honestly, in case we describe $\mathcal{G} = \{\mathcal{G}(i, j)/i, j \in F_p\}$, where $\mathcal{G}(i, j) = \begin{bmatrix} 1 & 0 & 0 \\ i & 1 & 0 \\ j & i^\theta & 1 \end{bmatrix}$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 $N = q \cdot p$ 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

$$A = \begin{pmatrix} i & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in M_3(GL(3, p)) \subset M_3(F_p) \subset M_3(Z_N)$$

Form

$$A^2 = \begin{pmatrix} i^2 mod\ N & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in M_3(GL(3, p)) \subset M_3(F_p) \subset M_3(Z_N).$$

without knowing the figuring of N.

Next, let $N = 2.5$ for example. Suppose that the system parameters are

$$n = 2, m = 3, q = \begin{pmatrix} 1 & 0 & 0 \\ 6 & 1 & 0 \\ 8 & 6 & 1 \end{pmatrix}, p = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 6 & 8 & 1 \end{pmatrix}.$$

5.1 Encryption and Decryption

Suppose that the polynomial $f(y) = 5y^3 + 3y^2 + y + 2$picked by sender

Then, Sender's private key is

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

Then, the corresponding public key would be

$$x \triangleq h(q)^2 p\, h(q)^3 = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 4 & 2 & 1 \end{pmatrix}^2 \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 6 & 8 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 4 & 2 & 1 \end{pmatrix}^3 = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 2 & 8 & 1 \end{pmatrix}$$

Let us pick a message M randomly, say $= \begin{pmatrix} 2 & 4 & 3 \\ 1 & 5 & 8 \\ 3 & 2 & 1 \end{pmatrix}$. Suppose the salt polynomial we picked randomly is coincide to $f(y)$. Then, the salt matrix from $f(y) = 2y^5 + y + 3$ and computes

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

Now, let us compute the ciphertext $\mathcal{C} = (a, b)$ as follows:

$$a = f(q)^2 . p . f(q)^3 = \begin{pmatrix} 6 & 0 & 0 \\ 6 & 6 & 0 \\ 8 & 6 & 6 \end{pmatrix}^2 \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 6 & 8 & 1 \end{pmatrix} \begin{pmatrix} 6 & 0 & 0 \\ 6 & 6 & 0 \\ 8 & 6 & 6 \end{pmatrix}^3 = \begin{pmatrix} 6 & 0 & 0 \\ 2 & 6 & 0 \\ 4 & 8 & 6 \end{pmatrix},$$ and

$$b = \mathcal{H}(f(q)^2 . qk . f(q)^3) \oplus M$$

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

$$= \mathcal{H}\left(\begin{pmatrix} 6 & 0 & 0 \\ 2 & 6 & 0 \\ 4 & 8 & 6 \end{pmatrix}\right) \oplus \begin{pmatrix} 2 & 4 & 3 \\ 1 & 5 & 8 \\ 3 & 2 & 1 \end{pmatrix}$$

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

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

$$= \begin{pmatrix} 6 & 5 & 2 \\ 5 & 1 & 9 \\ 5 & 4 & 5 \end{pmatrix}$$

Now, let us check the decryption process:

$$M' = \mathcal{H}(\hbar(q)^2 . a . \hbar(q)^3) \oplus \mathcal{b}$$

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

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

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

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

$$= \begin{pmatrix} 2 & 4 & 3 \\ 1 & 5 & 8 \\ 3 & 2 & 1 \end{pmatrix}$$

$$= M.$$

SECURITY INVESTIGATION AND DISCUSSION

Theorem 6.1: Let$\mathcal{H}$ be a random oracle and plaintext of proposed technique consistently dispersed in the $\mathcal{M}$, then the proposed technique is "all-or-nothing" secure against chosen plaintext attack under the polynomial Diffie-Hellman problem assumption over the Suzuki 2-group $(\mathcal{G},*)$

Proof. From one viewpoint, if polynomial Diffie-Hellman problem is tractable, for any given ciphertext pair (c, d) and the comparing public key $(q,\ p,\ x)$), it is easily calculate $l = p(log_p a)(log_p x)$ from the triple (p, a, x) and then extract the plaintext $M = \mathcal{b} \oplus \mathcal{H}(l)$.

Then again, assume that ∃ foe $\mathfrak{F}$, with access to the random oracle $\mathcal{H}$, against the purpose public key cryptographic technique, that is, given any public key $(q, p, x = \hbar(q)^n . p . \hbar(q)^m)$ and ciphertext $(a, \mathcal{b})$, for $\mathfrak{F}$ yields $M \leftarrow \mathfrak{F}^{\mathcal{H}}(q, p, x, a, \mathcal{b})$ with a non-negligible advantage such that M satisfies

$$M = \mathcal{b} \oplus \mathcal{H}\left(x^{log_p a}\right) = \mathcal{b} \oplus \mathcal{H}\left(p^{log_p x\, log_p a}\right),$$

$i.e. M = \mathcal{b} \oplus \mathcal{H}(\mathfrak{f}^n x \mathfrak{f}^m)$ and $a = \mathfrak{f}^n p \mathfrak{f}^m$, $\forall\, \mathfrak{f} \in Pq$.

Then, for a random polynomial Diffie-Hellman problem instance (s, y, y^{z_1}, y^{z_2}). We set (s, y, y^{z_1}) public key and ciphertext pair for $\mathcal{b} \in M$ as (s, y, y^{z_1}) and $(y^{z_2}, \mathcal{b})$ respectively. Then, with the advantage ϵ, foe $\mathfrak{F}$ yields

$$M \leftarrow \mathfrak{F}^{\mathcal{H}}(s, y, y^{z_1}, y^{z_2}, \mathcal{b})$$

with$M$ filling $M = \mathcal{b} \oplus \mathcal{H}(y^{z_1 z_2}), i.e. M = \mathcal{b} \oplus \mathcal{H}({z_2}^n {z_1}^n y {z_1}^m {z_2}^m) \forall z_2 \in P_s$.

Recall that $z_1 \in P_s$, thus $z_2 z_1 = z_1 z_2$ according to above Theorem 2.1. Then,

$$M = \mathcal{b} \oplus \mathcal{H}({z_2}^n {z_1}^n y {z_1}^m {z_2}^m) = \mathcal{b} \oplus \mathcal{H}(y^{z_2 z_1}) = \mathcal{b} \oplus \mathcal{H}(y^{z_1 z_2}).$$

Clearly, if the foe $\mathfrak{F}$'s benefit is non-insignificant, then $\mathfrak{F}$ must make corresponding $\mathcal{H}$-query on $y^{z_2 z_1}$; Otherwise, since $\mathcal{H}$ is displayed as a cryptographic hash function, $\mathfrak{F}$'s benefit should be negligible no matter what he can calculate before making such an inquiry.

By the random oracle assumption on $\mathcal{H}$, we can keep up a $\mathcal{H}_\ell$-list which contains twofields component $(d_i, \mathfrak{f}_i)$ and is initialized with empty. At whatever point the foe $\mathfrak{F}$ makes a $\mathcal{H}$ -inquiry with information d , we inspect whether there exists the combine pair $(d, \mathfrak{f})$ in $\mathcal{H}_\ell$-list. If so, back $\mathfrak{f}$ as the answer to $\mathfrak{F}$; Otherwise, arbitrarily select $\in M$, include the pair $(d, \mathfrak{f})$ into $\mathcal{H}_\ell$-list and reply $\mathfrak{f}$ as the response to $\mathfrak{F}$. Clearly, the simulation on $\mathcal{H}$ is perfect. At long last, when $\mathfrak{F}$yields M, we can retrieval the correct information $d_i = y^{z_1 z_2}$ by scrutiny the equivalence $M = \mathcal{b} \oplus \mathfrak{f}_i$. In this way, we can tackle polynomial Diffie-Hellman problem with the non-negligible probability. This negates the holding of the polynomial Diffie-Hellman problem supposition.

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. The main idea behind our proposition lies that we take polynomials over the given non-commutative algebraic system as the fundamental work structure for developing cryptographic plans. Thusly, we can efficiently acquire some commutative sub-structures for the given non-commutative mathematical frameworks. The proposed new public key cryptographic technique is secure under choose plaintext attack.

ACKNOWLEDGEMENTS

The author would like to thank anonymous reviewers for their helpful advice.

REFRENCES

[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 infinite 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, vol. E87-A, no. 5, (2004), pp. 986-992.

[7] N.R. Wagner, M.R. Magyarik, "A public-key cryptosystem based on the word problem", In G.R. Blakley and D.Chaum (Eds): CRYPTO'84, LNCS 196, Springer- Verlag, 1985, pp. 19-36.

[8] J. Birget,, S.S. Magliveras and M. Sramka, "On public-key cryptosystems based on combinatorial group theory", Cryptology ePrint Archive: Report 2005/070, 2005.

[9] I. Anshel, M. Anshel, and D. Goldfeld, "An algebraic method for public-key cryptography", Math. Research Letters 6 (1999) 287-291.

[10] K.H. Ko, S.J. Lee, J.H. Cheon and J.W. Han et al., "New Public-Key Cryptosystem Using Braid Groups", In M.Bellare (Ed.): CRYPTO 2000, LNCS 1880, pp. 166-183, Springer-Verlag, 2000.

[11] S.-H. Paeng, K.-C. Ha, J.-H. Kim, S. Chee and C. Park, "New public key cryptosystem using finite Non Abelian Groups". In J. Kilian (Ed.): CRYPTO 2001, LNCS 2139, pp. 470-485, Springer-Verlag, 2001.

[12] S.-H. Paeng, D. Kwon, K.-C. Ha, and J. H. Kim, "Improved public key cryptosystem using finite non abelian groups", Cryptology ePrint Archive: Report 2001/066, 2001.

[13] S.S. Magliveras, D.R. Stinson, and T. van Trung, "New Approaches to Design- ing 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

[14] M. Vasco, C. Martinez and R. Steinwandtd, "Towards a uniform description of several group based cryptographic primitives", Cryptology ePrint Archive: Report 2002/048, 2002.

[15] D. Grigoriev and I. Ponomarenko, "On non-abelian homomorphic public-key cryp- tosystems", Preprint arXiv: cs.CR/0207079, 2002.

[16] D. Grigoriev and I. Ponomarenko, "Homomorphic public-key cryptosystems over groups and rings", Preprint arXiv: cs.CR/0309010, 2003.

[17] B. Eick and D. Kahrobaei, "Polycyclic groups: a new platform for cryptography", Preprint arXiv: math.GR/0411077, 2004.

[18] V. Shpilrain and A. Ushakov, "Thmposon's group and public key cryptography", Preprint arXir: math.GR/0505487, 2005.

[19] J. Birman, K.H. Ko, and S.J. Lee, "A new approach to the word and conjugacy problems in the braid groups, Adv. Math. 139 (1998), 322-353.

[20] J. Birman, K.H. Ko, and S.J. Lee, "The infimum, supremum, and geodesic length of a braid conjugacy class", Adv. Math. 164 (2001), 41-56.

[21] E.A. El-Rifai, H.R. Morton, "Algorithms for positive braids", Quart. J. Math. Oxford Ser. (2) 45 (1994), pp. 479-497.

[22] V. Gebhardt, "A new approach to the conjugacy problem in Garside groups", Preprint arxiv: math.GT/0306199, 2003.

[23] J. Gonzales-Meneses, "Improving an algorithm to solve the Multiple Simultaneous Conjugacy Problems in braid groups", Preprint arxiv: math.GT/0212150, 2002.

[24] C. Meshram, "The Beta Cryptosystem", Bulletin of Electrical Engineering and Informatics, 4 (2), (2015), pp. 155-159.

[25] C. Meshram and S. A. Meshram, "PKC Scheme Based on DDLP", International Journal of Information & Network Security, 2 (2), April (2013), pp. 154-159.

[26] 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.

[27] C. Meshram, "A Cryptosystem based on Double Generalized Discrete Logarithm Problem", International Journal of Contemporary Mathematical Sciences, 6(6), (2011), pp. 285 – 297.

[28] C. Meshram and S.S. Agrawal, "Enhancing the security of A Public key cryptosystem based on DLP $\gamma \equiv \alpha a \beta b \pmod p$)", International Journal of Research and Reviews in Computer Science 1 (4),(2010), pp.67-70,.

[29] 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.

[30] 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.

[31] 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.

[32] C. Meshram, "An efficient ID-based Beta Cryptosystem", International Journal of Security and Its Applications, 9(2), (2015), pp. 189-202.

[33] 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.

[34] 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.

[35] C. Meshram and P. L. Powar, "An Efficient Identity-based QER Cryptographic Scheme", Complex & Intelligent Systems, 2 (4), (2016), pp. 285-291

[36] W. Lempken, T. van Trung, S.S.Magliveras and W. Wei, "A public key cryptosystem based on non-abelian finite groups", J. Crypto. 22 (2009), 62-74.

[37] G. Higman, "Suzuki 2-groups", III.J.Math.7, (1963), pp. 79-96.

