ISSN: 0975-766X
CODEN: IJPTFI
Available Online through
www.ijptonline.com
Research Article

NEW PUBLIC KEY CRYPTOGRAPHY BASED ON QUOTIENT NEAR RING OF N-MODULO

Ezhilmaran D[1], Muthukumaran*[1]
[1]School of Advanced Sciences, VIT University, Vellore-632014, Tamilnadu India.
Email: ezhilmarn.d@vit.ac.in & muthu.v2404@gmail.com*

Received on 17-03-2015 *Accepted on 08-04-2015*

Abstract

In A generalization of the original Diffie-Hellman key exchange in $(Z/_PZ)^*$ found a new depth when Miller and Koblitz suggested that such a protocol could be used with the group over an elliptic curve. Maze, Monico and Rosenthal extend such a generalization to the setting of a Semi-group action on a finite set, more precisely, linear actions of abelian semi-rings on semi-modules. In this paper, we extend such a generalization to the linear actions of quotient near-ring of modulo. We show how the action of quotient near-ring of N-module gives rise to generalized Diffie-Hellman and ElGamal Protocol. This leads naturally to a cryptographic protocol whose difficulty is based on the hardness of a particular control problem, namely the problem of steering the state of some dynamical system from an initial vector to some final location.

Keywords: Public key cryptography, Diffie-Hellman protocol, One-way trapdoor functions, semigroup actions, quotient near-ring.

1. Introduction

The Diffe-Hellman key exchange and ElGamal one-way trapdoor function are basic ingredients of public key cryptography. Both these protocols are based on hardness of the discrete logarithm problem in a finite in a finite semi-ring. The discrete logarithm problem, commonly abbreviated DLP, is a recurrent tool in public-key cryptography. The problem takes place in any group G, but we shall always assume the group is finite and commutative.

Protocol 1.1 [The Discrete Logarithm Problem] Let G be a finite commutative group. Given two group elements a and b such that that $b \in \langle a \rangle$, find $0 \le a \le ord(a)$ such that $a^n = b$ we denote such an n by $\log_a b$.

For cryptographic purpose, we will always assume that the group G is presented in such a way that multiplication is computationally easy. The difficulty of the DLP strongly depends on the type of group that is used: It goes from easy to non-feasible. For instance the DLP in the additive group of any finite field F_q is trivial since division can be performed in polynomial time. However, the DLP in the multiplicative group F_q^* is a difficult problem as well as the DLP in the group $E(F_q)$ of an elliptic curve defined over a finite field. In fact the latter is much more difficult than the former and intuition tells us that the less structure the group has, the more difficult that DLP will be. Protocols where the discrete logarithm problem plays a significant role are the Diffie-Hellman key agreement [3], the ElGamal public key cryptosystem [4], the digital signature algorithm (DSA) and ElGamal signature scheme [1].This is one of the reasons why we have developed the ideas of this paper. The Diffie-Hellman protocol [4] allows Alice and Bob, to exchange key over some insecure channel. In order to achieve this goal Alice and bob agree on a group G and a common base $a \in g$. Alice chooses a random positive integer a and chooses a random positive integer b Alice transmits to Bob g^a and Bob transmits to Alice g^b. Their common secret key is $k = g^{ab}$.

The El Gamal public key cryptosystem [4] works in the following way: Alice chooses positive integer n and $h, g \in G$, where $h = g^n$. The private key of Alice consists of (g, h, n), the public key consists of $(\mathrm{g,h})$ Bob chooses a random positive integer *r* and with this he applies the encryption function $V : V \to G \times G$ (sending m to $(\mathrm{c_1, c_2}) = (\mathrm{g}^r, \mathrm{m}, \mathrm{h}^r)$. Alice, who knows $n = \log_g h$ readily, computes m from the cipher text $(\mathrm{c_1, c_2}) : \mathrm{m} = \mathrm{c_2}(\mathrm{c_1}^n)^{-1}$. for the protocol to work it is required that multiplication and inversion inside the group G can be efficiently done and it should be computationally infeasible to compute a discrete logarithm with base $g \in G$.

In [6], Maze, Monico and Rosenthal have shown how the discrete logarithm problem over a group can be seen as a special instance of an action by a Semi-group. In fact, they have shown every Semi group action by an abelian Semi-group gives rise the Diffie-Hellman key exchange. With an additional assumption it is also possible to extend the ElGamal protocol. Let us explain them in detail. Assume that s is a finite set and let G be a Semi-group. Consider an action of G on S: $G \times S \to S$ (sending (g, s) to $g.s$). By the definition of a group action we require that $(gh)s = g(hs)$ for all $g, h \in G$ and $s \in S$. We also assume throughout that arithmetic in G and computation of the G -action can be done

in polynomial time. If the Semi-group G is commutative then every G -action gives rise to a generalized Diffie-Hellman Key Exchange [6].

Protocol 1.2 [Extended Diffie-Hellman Key Exchange] Let s be a finite set G a commutative semi-group and an action of G on S as defined. The Extended Diffie-Hellman Key Exchange is the following protocol [6]:

1) Alice and Bob agree on an element $s \in S$.
2) Alice chooses $a \in G$ and computes as . Alice's secret key is a , her public key is as.
3) Bob chooses $b \in G$ and computes bs . Bob's secret key is b , his public key is bs.
4) Their common secret key is then $\mathrm{a}(\mathrm{b}\,s) = (\mathrm{ab})\mathrm{s} = (\mathrm{ba})\mathrm{s} = b(\mathrm{a}\,s)$.

Protocol 1.3 [Extended ElGamal Public Key System] Let s be a group with respect to some Operation $\circ$, G an abelian Semi-group and an action of G on s as defined above. The Extended ElGamal Public Key System is the following protocol [6]:

1. Alice's public key is $(\mathrm{s}, \mathrm{as})$.
2. Bob chooses a random element $b \in G$ and encrypts a message m using the encryption function

$$(m, \mathrm{b}) \to (\mathrm{bs}, (\mathrm{b(as)} \circ \mathrm{m}) = (\mathrm{c}_1, \mathrm{c}_2)$$

3. Alice can decrypt the message using

$$m = (\mathrm{b(as)})^{-1} \circ c_2 = (\mathrm{ac}_1)^{-1} \circ c_2 .$$

In [6] Maze, Monico and Rosenthal show how to build Semi-group actions from actions by semirings on semi-modules. In this paper we show how to build Semi-group actions from actions by quotient near ring of N-modulo.

2. Quotient near-ring acting on N-modules

Definition 2.1

A near-ring N is a system with two binary compositions addition and multiplication such that

i. The element of N forms N^+ under addition.
ii. The element forms a semigroup under multiplication.
iii. $a(\mathrm{b}+\mathrm{c}) = \mathrm{ab}+\mathrm{ac},$ For all $a, b, c \in N$.
iv. $0.a = 0,$ Where 0 is the additive identity of N^+ and a is an element of N in particular, if N contains a multiplicative semigroups whose element generate N^+ satisfy the conditions.

v. $(a+b)s = as+bs$ for $a,b \in N$ and $s \in S$ then N is called distributive generated near-ring.

Let + and $\circ$ on N/I as have following conditions $(a+I)+(b+I) = (a+b)+I$ and $(a+I)\circ(b+I) = ab+I$ .Then it follows that $(N/I,+,\circ)$ is a near ring. In this near ring, $0+I$ is the additive identity and $-a+I$ is the additive inverses of $a+I$ .This near ring N/I is called the Quotient near ring on N-modulo I

Definition 2.2

An ideal I in near-ring N will be called a Q-ideal if there exists a subset Q of N satisfying the following conditions:

i. $\{n+I\}_{n\in Q}$ is partition of N.

ii. If $n_1, n_2 \in Q$ such that $n_1 \neq n_2$ then $(n_1+I)\cap(n_2+I) = \varphi$ it is clear that ever near ring ideal I in a near ring N is a Q-ideal.

Theorem 2.3

Let I be a Q-ideal in the near ring N if $x \in N$, then there exists a unique $n \in Q$ such that $x+I \subset n+I$.

Proof : Let $x \in N$ .since $\{n+I\}_{n\in Q}$ is a partition of N there exists $n \in Q$ such that $x \in n+I$ and $y \in x+I$ there exists $i_1 \in I$ such that $y = x+i_1$ .since $x \in n+I$,there exists $i_2 \in I$ such that $x = n+i_2$ .clearly $y = x+i_1$ $= (n+i_2)+i_1 = n+(i_1+i_2) \in n+I$. Then $z \in x+i_1$ there exist $i_1 \in I$ since $x \in n+I$ there exists $i_2 \in I$ such that $z = (x_1+x_2)x_3+i_1$, $z = (n_1+n_2)n_3+i_1+i_2$, $z = (n_1n_3+i_1+i_2)+(n_2n_3+i_1+i_2)$, $z = (n_1n_3+I)+(n_2n_3+I)$.

Thus $x+I \subset n+I$.

Definition 2.4

Let I be a Q-ideal in the nearing N and let $N/I = \{n+I : n \in Q\}$ .Then N/I forms a near-ring under the binary operations $\oplus_Q$ and $\otimes_Q$ defined as follows:

i. $(n_1+I)\oplus_Q(n_2+I) = n_3+I$ where n_3 is the unique element in Q such that $n_1+n_2+I \subset n_3+I$.

ii. $(n_1+I)\otimes_Q(n_2+I) = n_4+I$ where n_4 is the unique element in Q such that $n_1n_2+I \subset n_4+I$.

This near-ring N/I is called the quotient nearing of N by I. Then $n_0 \in Q$ such that $0+I \subseteq n_0+I$ .Then q_0+I is a zero element of N/I .It is well-known that if N is a near-ring, then Mat (R) , the set $n\times n$ matrices with entries in N is a near-ring.

Let M be a finite near-ring of N module, and let I be a Q-ideal of N. Now let $n \in N$ and suppose that $n_1 + I, n_2 + I \in N/I$ are such that $n_1 + I = n_2 + I$ in N/I. Then $n_1 = n_2$ we must have $n_1 m = n_2 m$ for every $m \in M$ .We defined a mapping $N/I \times M$ into M and it is routine to check that this turns the commutative semi-group M in to an N/I-N modulo.

Convention

The remaining of this paper we will assume unless otherwise stated, If I is an Q-ideal of N, and then Q is closed under addition and multiplication of N.

Let Mat(N/I) be the set of $n \times n$ all matrices with entries in N/I .The near-ring structure on N/I induces a nearing structure on Mat(N/I).Moreover the N-module structure on M lifts to a N-module structure on M^n via the matrix multiplication:

$$Mat(\mathrm{N/\ I}) \times \mathrm{M}^n \to M^n$$

Sending (U, y) to Uy where y 's $n \times 1$ matrix with entries $m_{11}, ..., m_{22}$ and $U = (\mathrm{q}_{ij} + \mathrm{I})_{n \times n}$ with $q_{ij} \in Q$ for every i, j .One readily verifies that

$$Mat(\mathrm{N/\ I}) \times \mathrm{M}^n \to M^n$$

Is an action by semi-group, indeed one readily computes $\mathrm{U(Vy)} = \mathrm{(UV)\,y}$ .Let us explain this equality in more detail. For simplicity, assume $n = 3$ and let $U = (\mathrm{u}_{ij} + \mathrm{I})_{3\times3}$ $V = (\mathrm{v}_{ij} + \mathrm{I})_{3\times3}$ and $y = (\mathrm{m}_{i1})_{3\times1}$. Let $\mathrm{U(Vy)} = (\mathrm{c}_{ij})_{3\times1}$ .Then we must have

$$\left.\begin{array}{l} u_{11}v_{11}m_{11} + u_{11}v_{12}m_{21} + u_{11}v_{13}m_{31} + u_{12}v_{21}m_{11} + u_{12}v_{22}m_{21} + u_{12}v_{23}m_{31} + u_{13}v_{31}m_{11} + \\ u_{13}v_{32}m_{21} + u_{13}v_{33}m_{31} = c_{11} \end{array}\right\} \quad (1)$$

$$\left.\begin{array}{l} u_{21}v_{11}m_{11} + u_{21}v_{12}m_{21} + u_{21}v_{13}m_{31} + u_{22}v_{21}m_{11} + u_{22}v_{22}m_{21} + u_{22}v_{23}m_{31} + u_{23}v_{31}m_{11} + \\ u_{23}v_{32}m_{21} + u_{23}v_{33}m_{31} = c_{21} \end{array}\right\} \quad (2)$$

$$\left.\begin{array}{l} u_{31}v_{11}m_{11} + u_{32}v_{12}m_{21} + u_{31}v_{13}m_{31} + u_{32}v_{21}m_{11} + u_{32}v_{22}m_{21} + u_{32}v_{23}m_{31} + u_{33}v_{31}m_{11} + \\ u_{33}v_{32}m_{21} + u_{33}v_{33}m_{32} = c_{31} \end{array}\right\} \quad (3)$$

Let $UV = (e_{ij} + I)_{3\times3}$ .Then we have

$$(u_{11}+I)\otimes_Q(v_{11}+I)\oplus_Q(u_{12}+I)\otimes_Q(v_{21}+I)\oplus_Q(u_{13}+I)\otimes_Q(v_{31}+I)=e_{11}+I \quad (4)$$

$$(u_{11}+I)\otimes_Q(v_{12}+I)\oplus_Q(u_{12}+I)\otimes_Q(v_{22}+I)\oplus_Q(u_{13}+I)\otimes_Q(v_{32}+I)=e_{12}+I \quad (5)$$

$$(u_{11}+I)\otimes_Q(v_{13}+I)\oplus_Q(u_{12}+I)\otimes_Q(v_{23}+I)\oplus_Q(u_{13}+I)\otimes_Q(v_{33}+I)=e_{13}+I \quad (6)$$

$$(u_{21}+I)\otimes_Q(v_{11}+I)\oplus_Q(u_{22}+I)\otimes_Q(v_{21}+I)\oplus_Q(u_{23}+I)\otimes_Q(v_{31}+I)=e_{21}+I \quad (7)$$

$$(u_{21}+I)\otimes_Q(v_{12}+I)\oplus_Q(u_{22}+I)\otimes_Q(v_{22}+I)\oplus_Q(u_{23}+I)\otimes_Q(v_{32}+I)=e_{22}+I \quad (8)$$

$$(u_{21}+I)\otimes_Q(v_{13}+I)\oplus_Q(u_{22}+I)\otimes_Q(v_{23}+I)\oplus_Q(u_{23}+I)\otimes_Q(v_{33}+I)=e_{23}+I \quad (9)$$

$$(u_{31}+I)\otimes_Q(v_{11}+I)\oplus_Q(u_{32}+I)\otimes_Q(v_{21}+I)\oplus_Q(u_{33}+I)\otimes_Q(v_{31}+I)=e_{31}+I \quad (10)$$

$$(u_{31}+I)\otimes_Q(v_{12}+I)\oplus_Q(u_{32}+I)\otimes_Q(v_{22}+I)\oplus_Q(u_{33}+I)\otimes_Q(v_{32}+I)=e_{32}+I \quad (11)$$

$$(u_{31}+I)\otimes_Q(v_{13}+I)\oplus_Q(u_{32}+I)\otimes_Q(v_{23}+I)\oplus_Q(u_{33}+I)\otimes_Q(v_{33}+I)=e_{33}+I \quad (12)$$

By following [4] n_{11}, n_{12}, n_{13} of Q such that

$$(n_{11}+I)\oplus_Q(n_{12}+I)\oplus_Q(n_{13}+I)=e_{11}+I \quad (13)$$

Where $u_{11}v_{11}+I\subseteq n_{11}+I, \mathrm{u}_{12}v_{22}+I\subseteq n_{12}+I, \mathrm{u}_{13}v_{31}+I\subseteq n_{13}+I$ and $n_{11}+n_{12}+n_{13}+I\subseteq e_{11}+I$ then we have

$$u_{11}v_{11}+u_{12}v_{21}+u_{13}v_{31}=n_{11}+n_{12}+n_{13} \quad (14)$$

$$u_{11}v_{11}+u_{12}v_{21}+u_{13}v_{31}=e_{11} \quad (15)$$

I is a Q-ideal of N the Similarly the relation (5), (6), (7), (8), (9), (10), (11), (12)

$$\left.\begin{aligned}
u_{11}v_{12}+u_{12}v_{22}+u_{13}v_{31}&=e_{12}\\
u_{11}v_{13}+u_{12}v_{23}+u_{13}v_{33}&=e_{13}\\
u_{21}v_{11}+u_{22}v_{21}+u_{23}v_{31}&=e_{21}\\
u_{21}v_{12}+u_{22}v_{22}+u_{23}v_{32}&=e_{22}\\
u_{21}v_{13}+u_{22}v_{23}+u_{23}v_{33}&=e_{23}\\
u_{31}v_{11}+u_{32}v_{21}+u_{33}v_{31}&=e_{31}\\
u_{31}v_{12}+u_{32}v_{22}+u_{33}v_{32}&=e_{32}\\
u_{31}v_{12}+u_{32}v_{23}+u_{33}v_{33}&=e_{33}
\end{aligned}\right\} \quad (16)$$

Let $(\mathrm{UV})\,\mathrm{y}=(\mathrm{e}_{ij}+I)_{3\times3}(\mathrm{m}_{i1})_{3\times1}=(\mathrm{g}_{ij})_{3\times1}$ then we have

$$\left.\begin{aligned} e_{11}m_{11} + e_{12}m_{21} + e_{13}m_{13} &= g_{11} \\ e_{21}m_{11} + e_{22}m_{21} + e_{23}m_{13} &= g_{21} \\ e_{31}m_{11} + e_{32}m_{21} + e_{33}m_{13} &= g_{31} \end{aligned}\right\} \quad (17)$$

The relation [1], [2], [3], [15], [16], [17] gives that,

$$\left.\begin{aligned} g_{11} = u_{11}v_{11}m_{11} + u_{11}v_{12}m_{21} + u_{11}v_{13}m_{31} + u_{12}v_{21}m_{11} + u_{12}v_{22}m_{21} + u_{12}v_{23}m_{31} + u_{13}v_{31}m_{11} + \\ u_{13}v_{32}m_{21} + u_{13}v_{33}m_{31} = c_{11} \end{aligned}\right\} \quad (18)$$

$$\left.\begin{aligned} g_{21} = u_{21}v_{11}m_{11} + u_{21}v_{12}m_{21} + u_{21}v_{13}m_{31} + u_{22}v_{21}m_{11} + u_{22}v_{22}m_{21} + u_{22}v_{23}m_{31} + u_{23}v_{31}m_{11} + \\ u_{23}v_{32}m_{21} + u_{23}v_{33}m_{31} = c_{21} \end{aligned}\right\} \quad (19)$$

$$\left.\begin{aligned} g_{31} = u_{31}v_{11}m_{11} + u_{31}v_{12}m_{21} + u_{31}v_{13}m_{31} + u_{32}v_{21}m_{11} + u_{32}v_{22}m_{21} + u_{32}v_{23}m_{31} + u_{33}v_{31}m_{11} + \\ u_{33}v_{32}m_{21} + u_{33}v_{33}m_{31} = c_{31} \end{aligned}\right\} \quad (20)$$

Thus we get $(\mathrm{UV})\,\mathrm{y} = U(\mathrm{Vy})$

Remark

Assume that I is an Q-ideal of N such that $uv = vu$ for all $u, v \in Q$ and let $n_1 + \mathrm{I}, n_2 + I \in N / I$ .Then there are unique elements $r, r' \in Q$ with $n_1 n_2 + I \subseteq r + I$ and $n_2 n_1 + I \subseteq r' + I$ so that $(\mathrm{n}_1 + \mathrm{I}) \otimes_Q (\mathrm{n}_2 + \mathrm{I}) = (\mathrm{n}_2 + \mathrm{I}) \otimes_Q (\mathrm{n}_1 + \mathrm{I})$ since $n_1 n_2 = n_2 n_1$ hence N/I is the a commutative near ring.

Assume that I is a Q-ideal of N such that $n_1 n_2 = n_2 n_1$ for all $n_1 n_2 \in Q$ and set $\overline{N} = N / I = \{\mathrm{n} + \mathrm{I} : \mathrm{n} \in \mathrm{Q}\} = \{\bar{n} : \mathrm{n} \in \mathrm{Q}\}$ .Let $\overline{N}[\mathrm{t}]$ be the polynomial of near-ring in the in determinant t. Let $U \in Mat(\overline{N})$ be a fixed matrix.

$$\overline{p}(\mathrm{t}) = \overline{n_0} + \overline{n_1} t + \ldots\ldots + \overline{n_k} t^k \in \overline{N}[\mathrm{t}]$$

Then we define the usual way $\overline{p}(\mathrm{U}) = \overline{n_0} I_n + \overline{n_1} U + \ldots\ldots + \overline{n_k} U^k$ where $\overline{n_0} I_n$ is the $n \times n$ diagonal matrix with entry $\overline{n_0}$ in each diagonal element. Consider the semi-group.

$$\overline{G} = \overline{N}[\mathrm{U}] = \{\overline{p}(\mathrm{U}) : \overline{p}(\mathrm{t}) \in \overline{N}[\mathrm{t}]\}$$

It is easy to see that $\overline{G}$ has the structure of an abelian semigroup.

Protocol 1.2 the simply requires the Alice and Bob agree on an Q-ideal I of near-ring of N an element $y \in M_n$ and a matrix $U \in Mat(\overline{N})$ .Alice chooses secretly and compute $\overline{p}(\mathrm{t}) \in \overline{N}(\mathrm{t})$ and computes $\overline{p}(\mathrm{U})\,\mathrm{y}$ and sends the result to Bob.

Bob chooses secretly $\bar{q}(\mathrm{t}) \in \overline{N}(\mathrm{t})$ and computes $\bar{q}(\mathrm{U})\,\mathrm{y}$ and sends the result to Alice. As a common secret key serves $k = \bar{p}(\mathrm{U})\bar{q}(\mathrm{U})\,\mathrm{y}$ since $\bar{p}(\mathrm{U})$ and $\bar{q}(\mathrm{U})$ compute.

System Theoretic Interpretation

It is possible to give the key exchange a system theoretic interpretation. For this note that in order to choose $p(\mathrm{U}) \in \overline{N}(\mathrm{U})$ Alice has to choose $\overline{n_0} = \overline{n_0} + I, \ldots\ldots, \overline{n_k} = \overline{n_k} + I \in \overline{N} = N / I$ then we compute

$$\bar{p}(\mathrm{U})\,\mathrm{y} = (\overline{n_0} + \overline{n_1}U + \ldots. + \overline{n_k}U^k)\,\mathrm{y} = \overline{n_0}y + \overline{n_1}Uy + \ldots\ldots + \overline{n_k}U^k y$$

Consider now the linear time invariant system:

$$z_{t+1} = Uz_t + \overline{w_t}y$$

Where $\mathrm{y}, \mathrm{z}_t \in M^n$ and $\overline{w_t} \in \overline{N}.$ suppose that $z_0 = 0_M$ .If Alice choose the input sequence $\overline{w_0} = \overline{n_k}, \overline{w_1} = \overline{n}_{k-1} \ldots\ldots \overline{w_k} = \overline{n}_0$ then $\bar{z}_{k+1}$, the state vector at time $k+1$ is exactly $\bar{p}(\mathrm{U})\,\mathrm{y}$ the public vector to be computed by Alice. Once Alice receives from Bob his public key $\bar{g}(\mathrm{U})\,\mathrm{y}$, then she define $v = \bar{g}(\mathrm{U})\,\mathrm{y}$ and by choosing her input sequence $\bar{w}_0 \ldots\ldots \bar{w}_k$ in the system $z_{t+1} = Uz_t + \overline{w_t}v$ .Then she will be able to compute the common secret key $\bar{p}(U)\bar{g}(U)\,y$.

Adversary who wants to find an element $\bar{h}(\mathrm{t}) \in \overline{N}(\mathrm{t})$ such that $\bar{h}(\mathrm{U})\,\mathrm{y} = \bar{g}(\mathrm{U})\,\mathrm{y}$ faces the task of finding a control sequence $\bar{w}_0 \ldots\ldots \bar{w}_k$ which steers the initial state Z_0 in to the state $\bar{g}(\mathrm{U})\,\mathrm{y}$. This problem very hard ,but it contains some of the hardest known discrete logarithm problem as a special case.

3. Matrix quotient near ring of N-modules

Theorem 3.1

Let I be a Q-ideal of near ring N. Then $Mat(\mathrm{I})$ is a $Mat(\mathrm{Q}) -$ ideal of $Mat(\mathrm{N})$. Then we have $Mat(\mathrm{N}) / \mathrm{Mat(I)} = \{\mathrm{C} + \mathrm{Mat(I)} : \mathrm{C} \in \mathrm{Mat(Q)}\}$ is a near ring.

Proof:

It is easy to see that $Mat(\mathrm{I})$ is an ideal of $Mat(\mathrm{N})$. Since the inclusion $\cup\{n + Mat(I) : n \in Mat(Q)\} \subseteq Mat(N)$ is trivial, We will prove that reverse inclusion .Suppose that $U = (\mathrm{u}_{ij})_{n\times n} \in Mat(\mathrm{N})$ .There are elements $n_{ij} \in Q$ and $c_{ij} \in I$ such that $u_{ij} = n_{ij} + c_{ij}$ for all $i, j \in I$ is a Q-ideal of N. Set $V = (v_{ij})_{n\times n}$ and $C = (\mathrm{c}_{ij})_{n\times n}$ .Then $U = V + C \in Mat(Q) + Mat(I)$,

and so we have equality. Suppose that $(P + Mat(I)) \cap (H + Mat(I)) \neq \varphi$ where $P = (p_{ij})_{n\times n}$, $H = (h_{ij})_{n\times n} \in Mat_{n\times n}(Q)$; we show that $P = H$. There exists $R = (r_{ij})_{n\times n}, S = (s_{ij})_{n\times n} \in Mat_{n\times n}(I)$ such that $P + R = H + S$ for all i, j, $(e_{ij} + I) \cap (\lambda_{ij} + I) \neq \varphi$; hence $P = H$ since I is Q-ideal.

Let M be a finite N-module over a near ring N. The near-module structure on M lifts a near module structure on M^n via the matrix multiplication:

$$Mat(N) \times M^n \to M^n$$

Sending (U, y) to Uy [6].

If I is an Q ideal of N, then Theorem [3.1] Gives $Mat(N) / Mat(I)$ is a near ring. If I is closed under addition and multiplication of N, then it is easy to see that Mat(I) is close under addition and multiplication of $Mat(N)$.Now the matrix multiplication:

$$Mat(N) / Mat(I) \times M^n \to M^n$$

Sending $(U + Mat(I), y)$ to Uy is a near ring module structure on M^n where $U \in Mat(Q)$.One readily verifies that

$$Mat(N) / Mat(I) \times M^n \to M^n$$

is an action by semi-group, indeed one readily computes that $U(Vy) = (UV)y.$ Let us explain this equality is more detail. Let $U = (u_{ij})_{n\times n} + Mat(I)$, $V = (v_{ij})_{n\times n} + Mat(I)$, $y = (m_{i1})_{n\times 1}$ where $u_{ij}, v_{ij} \in Q$ .Then we must have

$$U(Vy) = (u_{ij})_{n\times n}(v_{ij})_{n\times n}(m_{i1})_{n\times 1} \qquad (21)$$

Let $(UV) = (e_{ij})_{n\times n} + Mat(I).$ The we must have $(u_{ij})_{n\times n}(v_{ij})_{n\times n} + Mat(I) \subseteq (e_{ij})_{n\times n} + Mat(I),$ so we get $(u_{ij})_{n\times n}(v_{ij})_{n\times n} = (e_{ij})_{n\times n}$ since $Mat(I)$ is a $Mat(Q) -$ ideal of $Mat(N)$ .If follows that

$$(UV)y = (u_{ij})_{n\times n}(v_{ij})_{n\times n}(m_{i1})_{n\times 1} \qquad (22)$$

From (21) and (22)

$U(Vy) = (UV)y$.

Assume that $S = Mat(N) / Mat(I)$ and let $S(t)$ the polynomial near-ring in the determinant t and let $U = (u_{ij})_{n\times n} + Mat(I) \in S$ be a fixed number .Let $C \subseteq S$ be the center of S. If $p(\mathrm{t}) = \mathrm{a}_0 + a_1 t + ... + \mathrm{a}_k t^k \in C[\mathrm{t}],$ then we

define in the usual way $p(U) = a_0U_0 + a_1U + ... + a_kU^k$ .Then $C[U] = \{p(U) : p(t) \in C[t]\}$ as the structure of an abelian semi-group. Alice and Bob agree on an N semi-module M, an element $y \in M^n$ and an element U of S . Alice chooses secretly $p(t) \in C[t]$ and computes $p(U)y$ and sends the result to Bob. Bob choose $q(t) \in C[t]$ and compute $q(U)y$ and the result to Alice. As a common key serves $k = p(U)q(V)y$. To difficult to find $h(t) \in C[t]$ such that $h(U)y = p(U)y.$

4. Conclusion

At present, we lack a convincing example of a system based on the previous section. All of the examples has presented in [6] to be either insecure or already well-known. The insecure example have arisen by generating random finite semiring for base-of objects. In this Paper we showed how the discrete logarithm problem over a finite group can viewed as an instance of an action by a semigroup. In fact, we show the action of a quotient near ring of N-module gives rise to a generalization Diffe-Hellman and ElGamal protocol. Using near ring action to avoid the insecureness and they have high security relative to their key size.

5. Reference

1. Meenezes A.J., van Oorschot P.C., and Vanstone S. A. “Hand-book of Applied Cryptography”. CRC Press Series on Discrete Mathematics and its Applications, 1997.
2. Miller V. S., “Use of elliptic curves in cryptography”. Advances in cryptology – CRYPTO, Vol.85, PP.417-426, 1986.
3. Diffie W., Hellmann M.E. “New directions in cryptography”. IEEE Transaction Information Theory, Vol. 22, No. 6, PP. 644-654, 1976.
4. ElGamal T. “A public key cryptosystem and a signature scheme based on discrete Logarithm”. IEEE Transaction Information Theory, Vol.31 No.4, PP. 469-472 ,1985
5. Monico C. “Semi-rings and Semi-group Actions in Public Key Cryptography”. PhD thesis, University of Notre Dame , May 2002.
6. Maze G., Monico C., Rosenthal J. “Public Key Cryptography On Semi-group Actions”. 28 Jan 2005.
7. Maurer U.M. “Towards the equivalence of breaking the Diffie-Hellman protocol and Computing discrete logarithms”. In Advances in cryptology—CRYPTO, Vol.94, PP.271–281, 1994.

8. Deskins W.E. "A radical for near-rings". Proceedings of the American Mathematical Society Vol.5, No.5, PP.825-827, 1954.
9. Maze G., Monico C., Rosenthal J. "A public key cryptosystem based on actions by Semigroups". In Proceedings of the 2002 IEEE International Symposium on Information Theory, PP. 484, Lausanne, Switzerland. 2002.
10. Bhavanari Satyanarayana, Kuncham Syam Prasad-Near Rings, Fuzzy Ideals, and Graph. Theory-Chapman and Hall CRC (2013).
11. Climent., Joan-Josep., Pedro R. Navarro., Leandro Tortosa. "Key exchange protocols over noncommutative rings". The case of." *International Journal of Computer Mathematics* 89, Vol.14, PP. 1753-1763, 2012.
12. LIU N., TANG S., Xiaoyu LI., Lingling XU. "Cryptanalysis of a Key Agreement Protocol over the Ring of Multivariate Polynomials". *Journal of Computational Information Systems* 10, Vol.13, PP. 5431-5436, 2014.

Corresponding Author:
Muthukumaran*[1]
Email: *muthu.v2404@gmail.com*