Secured Directed Digital Signature over Non-Commutative Division Semirings and Allocation of Experimental Registration Number

Dr. G.S.G.N.Anjaneyulu [1] ***Dr.D.U.M.Reddy*** [2]

Corresponding Author
[1]Associate Professor, Division of Applied Algebra, SAS, VIT University, Vellore, India .Pin-632014.

[2]Associate Professor(Rtd), Dept. of Mathematics, S.V.U.C.E, Tirupati, India . Pin-517502

ABSTRACT:

Directed digital signatures are probably the most important and widely used cryptographic primitive enabled by public key technology, and they are building blocks of many modern distributed computer applications. But many existing signatures schemes lie in the intractability of problems closely related to the number theory than group theory. In this paper, we present a new directed digital signature scheme based on general non-commutative division semiring. For this, we construct the polynomials as the elements of additive structure of the semiring and take them as the underlying work structure. Then the signature scheme is developed on the multiplicative structure of the division semiring. And also

We present one important application 'Registration Process' in different situations in common practice. For this, we use a directed digital signature, to design a scheme such that the scheme provides a registration number to a person or an organization. The registration number can't be forged and misused and is the strength of the algorithm.

The security of the proposed directed signature scheme and registration number is based on the intractability of the Polynomial Symmetrical Decomposition Problem over the given non-commutative division semirings.

Keywords: Directed Digital Signature, Polynomial Decomposition problem, Non-commutative Division Semiring, Registration number.

1. INTRODUCTION

1.1 Background of Public Key Infrastructure and proposals based on Commutative Rings

There is no doubt that the Internet is affecting every aspect of our lives; the most significant changes are occurring in private and public sector organizations that are transforming their conventional operating models to Internet based service models, known as eBusiness, eCommerce, and eGovernment. Public Key Infrastructure (PKI) is probably one of the most important items in the arsenal of security measures that can be brought to bear against the aforementioned growing risks and threats. The design of reliable Public Key Infrastructure presents a compendium challenging problems that have fascinated researchers in computer science, electrical engineering and mathematics alike for the past few decades and are sure to continue to do so.

In their seminal paper "New directions in Cryptography" [1] Diffie and Hellman invented public key Cryptography and, in particular, digital signature schemes. Today most successful signature schemes are based on the difficulty of certain problems in particular large finite commutative rings. For example, the difficulty of solving Integer Factorization Problem (IFP) defined over Z_n (where n is the product of primes) forms the ground of the basic RSA signature scheme [2], variants of RSA and elliptic curve version of RSA like KMOV [3]. Another good case is ElGamal signature scheme[4] that is based on the difficulty of solving the discrete logarithm problem (DLP) defined over a finite field Z_p (where P is a large prime), of course a commutative ring.

The theoretical foundations for the above signature schemes lie in the intractability of problems closely related to the number theory than group theory [5]. On Quantum computer, IFP, DLP, as well as DLP over ECDLP, are turned out to be efficiently solved by algorithms due to Shor [6] , Kitaev [7] and proos–Zalka [8]. Although practical quantum computers are as least 10 years away, their potential weakness will soon create distrust in current cryptographic methods [9].

As addressed in [9], in order to enrich Cryptography, there have been many attempts to develop alternative PKC based on different kinds of problems. Historically, some attempts were made for a Cryptographic Primitives construction using more complex algebraic systems instead of traditional finite cyclic groups or finite fields during the last decade. The originator in this trend was [10], where a proposition to use non-commutative groups and semigroups in session key agreement protocol is presented. Some realization of key agreement protocol using [10] methodology with application of the semigroup action level could be found in [11]. Some concrete construction of commutative sub-semigroup was proposed there.

According to our knowledge, the first signature scheme designed in an infinite non commutative groups appeared in [12]. This invention is based on an essential gap existing between the Conjugacy Decision Problem (CDP) and Conjugator Search Problem (CSP) in non-commutative group [13]. In, [14], Cao et.al. Proposed a new DH-like key exchange protocol and ElGamal–like cryptosystems using polynomials over non-commutative rings.

Digital signature is one of the most important techniques in modern information security system for its functionality of providing data integrity and authentication. A normal digital signature [2,4,15] has the property that any one having a copy of the signature and can check it's validity using the corresponding public information. This "self authentication" property is necessarily required for some applications of digital signature such as official documents issued by some authorities. However it is not suitable for some other applications, where a signed message is personally or commercially sensitive to the signature receiver. For example as in bill of tax, bill of health etc. Therefore, to prevent the potential misuse of signatures, it is preferable to place some restrictions on this property.

To achieve this purpose, Lim and Lee [16], first proposed the concept of directed digital signature at AUSCRYPTO'92. In directed signature scheme, when a signer sends a signed message 'm' to a designated verifier(receiver), then, only the designated verifier can directly verify the signature on message 'm', while the the others know nothing on the origin and validity of the message 'm' without help of the signer or designated verifier. On the other hand, if necessary both the signer and the designated verifier can prove to any third party that the signature is a valid signature on the message 'm' issued by the signer to the designated verifier. This property enables a dispute resolution in case that the signer tries to deny her signature or the designated verifier tries to deny the directedness of the signature.

In [16], Lim and Lee presented such a directed signature, in which the construction is based on the GQ signature [17] scheme. D.Chaum [18] introduced the concept of designated confirmer signatures. Later T.Okamato [19] presented a more practical construction of designated signatures. Recently, Manoj kumar and Sunder lal [20] proposed two other types of directed signature schemes based on Schnorr signature. This work is the motivation for the present article.

In the first type of scheme, any third party can check the signature validity with the help of signature receiver or the signer as well. Both the signer and signature receiver have full control over the signature verification process. In other words, they are independent to prove the validity of the signature to any third party, whenever necessary. Where as in the second type of scheme, they presented two different applications of directed signature.

(i). Directed delegated signature scheme, this scheme combines the idea of proxy signatures with directed signatures.

(ii). Allocation of registration number, this scheme provides a registration number to an applicant, in which the registration number can't be forged and misused.

However to our best knowledge, none of them has provided the provable security proof. On the other hand, there still does not exit any directed signature scheme based on RSA assumption presently, though the ordinary RSA digital signature scheme is very popular. In 2006, Rongxing Lu and Zhenfu Cao [21] presented a new directed signature scheme based on RSA assumption, but it is fit for signing personally or commercially sensitive message and may be useful to the internet community and web based system community. Particularly, it uses the techniques from provable security to analyze its security.

1.2. Our contributions

In this paper, we would like to propose new method for directed digital signature scheme based on general non-commutative division semirings. The key idea of our proposal is that for given non-commutative division semiring, we generate polynomials on additive structure and take them as the underlying work structure. By doing so, we implement a new directed digital signature scheme on multiplicative structure of the division semiring.

And also, we present one important application in different situations in common practice. For this, we use a directed digital signature, to design a scheme such that the scheme provides a registration number to a person or an organization, when he or organization wants to apply for the same to a government office in different situations. This scheme proposes a registration scheme, in which the registration number can't be forged and misused. The advantage of this system is that we can take all types of registration numbers under a unique providing authority. In this system, there is no chance of getting unique registration number for any pair of applicants, even if there are more applicants in number.

The security of the proposed directed signature scheme and registration number are based on the intractability of the Polynomial Symmetrical Decomposition Problem over the given non-commutative division semiring. But the construction of polynomials on additive structure and operating them on multiplicative structure, are strength of the directed digital signature and registration number.

1.3 Outline of the paper:

The rest of the paper is organized as follows. In Section 2, we present the necessary Cryptographic assumptions over non-commutative groups. In

Section 3, first we define semiring, division semiring and integral co-efficient division semiring polynomials and then we present necessary cryptographic assumptions over non-commutative division semirings . In Section 4, we propose new directed digital signature scheme based on underlying structure and assumptions. In section 5, we study the confirmation theorem and security concepts of the proposed signature scheme. We study the application of directed digital signature scheme i.e allocation of registration number in section 6. In section 7, we verify the algorithm by concrete example. Finally, concluding remarks are made in Sec-8.

2. CRYPTOGRAPHIC ASSUMPTIONS ON NON-COMMUTATIVE GROUPS:

2.1 Two Well-known Cryptographic Assumptions

As Z.Cao discussed in [14], In a non-commutative group G, two elements x, y are conjugate, written $x \sim y$, if $y = z^{-1} x z$ for some $z \in G$. Here z or z^{-1} is called a conjugator. Over a non commutative group G, we can define the following two cryptographic problems which are related to conjugacy.

***Conjugator Search Problem* (CSP):**
Given $(x,y) \in G \times G$, find $z \in G$ such that $y = z^{-1} x z$

Decomposition Problem (DP): Given $(x,y) \in G \times G$ and $S \subseteq G$, find $z_1, z_2 \in S$ such that $y = z_1 x z_2$

At present, we believe that for general non-commutative group G, both of the above problems CSP and DP are intractable. More precisely, CSP(DP) assumption states that there does not exist probabilistic polynomial time algorithm which can solve CSP(DP respectively) with non-negligible accuracy with respect to the problem scale.

Note: May be, in theoretical, these problems are not solvable for arbitrary instance. But in practice of the cryptographic applications, we usually start from some solvable instances to construct desired schemes.

2.2 Symmetrical Decomposition problem over Non-Commutative Groups

Enlightened by the above problems, Z. Cao [14] defined the following Cryptographic problems over a non-commutative group G.

***Symmetrical Decomposition Problem* (SDP):**
Given $(x,y) \in G \times G$ and $m, n \in I$, find $z \in G$ such that $y = z^m x z^n$, where I is set of integers.

***Generalized symmetrical Decomposition Problems* (GSDP):** Given $(x,y) \in G \times G$, $S \subseteq G$ and $m, n \in I$, find $z \in S$ such that $y = z^m x z^n$.

Hardness of z: Clearly, GSDP can be looked as a type of constrained SDP. In general, if the size of S is large enough and its membership information does not help one to extract z from $z^m x z^n$, then we can say that GSDP is at least as hard as SDP.So that GSD assumption says that GSDP is intractable i.e there is no probabilistic polynomial time algorithm which can solve GSDP with non-negligible accuracy with respect to the problem scale.

3. BUILDING BLOCKS FOR PROPOSED DIRECTED DIGITAL SIGNATURE SCHEME AND REGISTRATION NUMBE

3.1 Semiring

A Semiring R is a non-empty set, on which the operations of addition & multiplication have been defined such that the following conditions are satisfied.

(i). (R, +) is a commutative monoid with identity element "0"

(ii). (R, •) is a monoid with identity element 1.

(iii).Multiplication distributes over addition from either side

(iv). $0 \bullet r = r \bullet 0$ for all r in R

3.2 Division semiring

An element r of a semiring R, is a "unit" if and only if there exists an element r^1 of R satisfying $r \bullet r^1 = 1 = r^1 \bullet r$

The element r^1 is called the inverse of r in R. If such an inverse r^1 exists for a unit r, it must be unique. We will normally denote the inverse of r by r^{-1}. It is straightforward to see that , if r and r^1 units of R, then $r \bullet (r^1)^{-1} = (r^1)^{-1} \bullet r^{-1}$ and In particular $(r^{-1})^{-1} = r$.

We will denote the set of all units of R, by U(R). This set is non-empty, since it contains "1" and is not all of R, since it does not contain '0'.we have just noted that U(R) is a submonoid of (R, •), which is infact a group. If $U(R) = R/\{0\}$, Then R, is a *division semiring.*

3.3 Integral co-efficient Polynomials on Division Semiring

Let (R, +, •) be a non-commutative division semiring. Let us consider positive integral co-efficient polynomials with semiring assignment as follows.

At first, the notion of scale multiplication over R is already on hand. For $k \in Z_{>0}$ & $r \in R$ Then (k) r =r + r + r +… + r + r (k times), For k = 0, it is natural to define (k) r = 0

Property 1. $(a)r^m \bullet (b)r^n = (ab) \bullet r^{m+n} = (b)r^n \bullet (a)r^m$,

$\forall$ a,b ,m,n $\in Z$, $\forall$ $r \in R$

Remark: Note that in general

$(a)r \bullet (b)s \neq (b)s \bullet (a)r$ when $r \neq s$, since the multiplication in R is non-commutative.

Now, Let us proceed to define positive integral coefficient semiring polynomials. Suppose that

$$f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n \in Z_{>0}[x]$$

is given positive integral coefficient polynomial. We can assign this polynomial by using an element r in R & finally , we obtain

$$f(r) = a_0 + a_1 r + a_2 r^2 + ... + a_n r^n \in R$$

Similarly

$$h(r) = b_0 + b_1 r + b_2 r^2 + ... + b_m r^m \in R$$

for some $n \geq m$. Then we have the following

Theorem1: f(r).h(r) = h(r).f(r) for f(r), h(r) € R

Remark: If r & s are two different variables in R, then $f(r) \bullet h(s) \neq h(s) \bullet f(r)$ in general.

3.4 Further cryptographic assumptions on Non- Commutative Division Semirings

Let (R, +, •) be a non-commutative division semiring. For any $a \in R$, we define the set $P_a \subseteq R$ by

$$P_a \stackrel{\Delta}{=} \{ f(a) / f(x) \in Z_{>0}[x] \}$$

Then, let us consider the new version of GSD over (R,•.) with respect to its subset P_a, and name it as polynomial symmetrical decomposition (PSD) problem.

Polynomial Symmetrical Decomposition (PSD) problem over Non- Commutative Division Semiring

R: Given $(a, x, y) \in R^3$ and $m, n \in Z$, find $z \in P_a$ such that $y = z^m x z^n$

4. PROPOSED DIRECTED SIGNATURE SCHEME

Directed Signature Scheme from Non-Commutative Division Semiring:

Digital Signature on semirings could be found in [22]. This is, Directed digital signature scheme and contains the following main steps.

Initial setup:

Suppose that a Signer "A" wants to generate a signature on a message 'M'. So that the receiver B only can verify the signature & that B can prove the validity of signature to any third party "C", whenever necessary.

Let (R, +, •) be a non-commutative division semiring & Let p, q € R, m € Z^+, H are the public parameters of the system. Let H:R →*M* be a collision free hash function, which maps R to the message space *M*.

Key Generation:

(a). The Signer "A" chooses a polynomial at random , f (x) € $Z_{>0}$[x] such that f (p) ≠ 0, f (p) € R, then "A" takes f(p) as his private key and computes $y = f(p)^{-m} q f(p)^m$ as his public key[14].

(b). Another person "B" chooses a polynomial at random g(x) € $Z_{>0}$[x] such that g (p) ≠ 0,g (p) € R, then "B" takes g (p) as his private key and computes $z = g(p)^{-m} q g(p)^m$ as her public key.

Signature Generation:

(a). Again "A" chooses , another polynomial at random h (x) € $Z_{>0}$[x], such that h (p) ≠ 0, h (p) € R and then computes

$w_B = h(p)^{-m} q h(p)^m$ $z_B = h(p)^{-m} z h(p)^m$

(b). Using one way hash function 'H' and a message M, "A" also computes

$r_A = H(z_B, w_B, M)$, $s_A = f(p)^{-m} r_A f(p)^m$

(c) A sends { s_A, w_B, r_A, M } to B as his signature on the message M.

Signature Verification by B:

(a). B collects the signature of A i.e

{ s_A, w_B, r_A, M } and make this public

(b). B also computes $\mu = s_A^{-m} w_B s_A^m$

$\lambda = s_A^{-m} g(p)^m$ and $z_B = \lambda^{-1} \mu \lambda$ and B checks the validity of signature by computing $r_A = H(z_B, w_B, M)$ locally, and then comparing it to the r_A, received from signer.

Proof of validity by B to any third party C:

(a). B sends { s_A, w_B, r_A, M , m, λ } to C

(b). C checks $r_A = H(z_B, w_B, M)$ by computing r_A locally, and then comparing it to the r_A, received from signer.

If this does not hold, C stops the process, otherwise goes to the next steps.

(c). B in a zero knowledge fashion proves to C that S = T as follows.

(i). C chooses a polynomial at random, Φ(x) € $Z_{>0}$[x], such that Φ(p) ≠ 0, Φ(p) € R and Computes the challenge

$Q = \Phi(p)^m [s_A^m \lambda z] \Phi(p)^{-m}$ and C sends Q to B.

(ii). B chooses a polynomial at random, ψ(x) € $Z_{>0}$[x] such that ψ (p) ≠ 0, ψ(p)€R and Computes the response

$T = \psi(p)^{-m} [Q.g(p)^{-m}] \psi(p)^m$ and B sends T to C

(iii). C sends Φ(p) to B.

(iv). B verifies that $Q = \Phi(p)^m [s_A^m \lambda z] \Phi(p)^{-m}$

(v). B sends ψ(p) to C

(vi). C verifies that

$$S = \psi(p)^{-m} [\Phi(p)^m q \Phi(p)^{-m}] \psi(p)^m$$

If it holds (S=T), then C accepts {s_A, w_B, r_A, M} is an authenticated signature .

5. CONFIRMATION THEOREM AND SECURITY

5.1 CONFIRMATION THEOREMS

5.1(a)Theorem: Let (p, q, y, z) € R^4

Completeness: Given a signature {s_A ,w_B , r_A, M} if the person 'A' follows signature verification algorithm, then the person 'B' always accepts { s_A, w_B, r_A, M} is an authenticated signature.

Proof: we recall that $z = g(p)^{-m} q g(p)^m$ is the public key of the person B.

$w_B = h(p)^{-m} q h(p)^m$ $\mu = s_A^{-m} w_B s_A^m$

$\lambda = s_A^{-m} g(p)^m$ $\lambda^{-1} = g(p)^{-m} s_A^m$

are other parameters of the signature algorithm. Then

$\lambda^{-1} \mu \lambda = g(p)^{-m} s_A{}^m . s_A{}^{-m} w_B s_A{}^m . s_A{}^{-m} g(p)^m$
$= g(p)^{-m} w_B g(p)^m$
$= g(p)^{-m} h(p)^{-m} q h(p)^m g(p)^m$

Since $g(p). h(p) = h(p). g(p)$ then $g(p)^{-1}.h(p)^{-1} = h(p)^{-1}.g(p)^{-1}$, by theorem 1 of 3.3

And also note that $g(p)^m.h(p)^m = h(p)^m.g(p)^m$ then $g(p)^{-m}.h(p)^{-m} = h(p)^{-m}.g(p)^{-m}$ and hence

$\lambda^{-1}\mu\lambda = h(p)^{-m}[g(p)^{-m} q g(p)^m]h(p)^m$
$= h(p)^{-m} z h(p)^m = z_B$ [$\because z_B = h(p)^{-m} z h(p)^m$]

Then B computes $H(z_B, w_B, M)$ and is always equal to r_A, when A follows this algorithm. So that B accepts the signature $\{ s_A, w_B, r_A, M \}$ is an authenticated signature, which is generated by A to B. Hence the proof is complete.

5.1(b)Theorem: (zero-knowledge case)

Let $(p, q, y, z) \in R^4$

Completeness: Given a signature $\{s_A, w_B, r_A, M\}$ if the person 'A' follows signature verification algorithm , then the person 'B' always accepts $\{ s_A, w_B, r_A, M\}$ is an authenticated signature.

Proof: From the zero-knowledge case, we have

$T = \psi(p)^{-m}[Q.g(p)^{-m}] \psi(p)^m$, $\lambda = s_A{}^{-m} g(p)^m$
and $z = g(p)^{-m} q g(p)^m$, where
$Q = \Phi(p)^m[s_A{}^m \lambda z] \Phi(p)^{-m}$
$= \Phi(p)^m[s_A{}^m s_A{}^{-m} g(p)^m g(p)^{-m} q g(p)^m]\Phi(p)^{-m}$
$= \Phi(p)^m[q g(p)^m] \Phi(p)^{-m}$

So that, we can have

$Q .g(p)^{-m} = \Phi(p)^m[q g(p)^m] \Phi(p)^{-m}. g(p)^{-m}$
$= \Phi(p)^m[q g(p)^m] g(p)^{-m} \Phi(p)^{-m}$
[$\because \Phi(p)^{-m}. g(p)^{-m} = g(p)^{-m} \Phi(p)^{-m}$]
$= \Phi(p)^m q \Phi(p)^{-m}$

And hence $T = \psi(p)^{-m}[Q. g(p)^{-m}] \psi(p)^m$
$= \psi(p)^{-m}[\Phi(p)^m q \Phi(p)^{-m}] \psi(p)^m = S$

Which means that T = S. So that, C accepts the signature $\{s_A, w_B, r_A, M \}$ is an authenticated signature, which is generated by A to B.

Hence the proof is complete.

5.1(c)Theorem: Our proposed signature scheme is a really directed signature scheme

Proof: To verify the signature $\{s_A, w_B, r_A, M\}$, we need the following parameters

$$\lambda = s_A^{-m} g(p)^m \quad and \quad \mu = s_A^{-m} w_B s_A^m, \; z_B = \lambda^{-1}\mu\lambda$$

i.e this verification process needs the private key g(p) of the designated verifier B. Therefore, only designated verifier B, can verify the authenticity of this signature scheme.

As far as third party C is concerned, computing $\psi(p)$ from T, is equivalent to solve the polynomial symmetrical decomposition problem. However , when C holds $\psi(p)$ with the help of designated verifier B, he can easily verify the signature. Hence our proposed signature scheme is actually a directed signature scheme.

5.1(d)Theorem : Our proposed signature scheme is based on zero-knowledgeness verification for third parties.

Proof: The protocol is zero knowledge, namely on input of a message and its valid signature, any third (possibly cheating) verifier V^* interacting with the prover B, does not learn any information from the validity of the signature.

In this directed signature scheme, the designated verifier B, chooses at random, a polynomial $\psi(x) \in Z_{>0}[x]$ such that $\psi(p) (\neq 0) \in (R, +, \bullet)$ a non-commutative division semiring and compute the response $T \in (R, +, \bullet)$. So we can treat C as having a random element of (R, +, •). Any random choice of $\psi(p) (\neq 0) \in (R, +, \bullet)$ by B in practice makes the response T to appear as a random element.

During this transactions, the third party C could not learn any thing about the directed signature scheme. Hence the protocol is zero-knowledgeable.

5.2 Security Analysis:

Assume that the active eavesdropper Eve can obtain, remove, forge and retransmit any message that Alice sends to Bob.

As security analysis given by E.Sakalauskas [24], we discuss security of signature scheme for four main attacks: Total break, Data forgering on valid signature, Signature repudiation on valid data and existential forgering.

5.2(a). Total Break (Retrieving the secret keys):

This is as difficult as solving Polynomial symmetrical decomposition problem on non-commutative division semiring. No one get the secret key f(p), since $f(x) \in Z_{>0}[x]$ is a randomly and secretly generated polynomial. On the other hand, by using the public keys A and B are $y = f(p)^{-m} q f(p)^m$, $z = g(p)^{-m} q g(p)^m$, no one get the secret keys f(p) and g(p), as we believe that polynomial symmetrical decomposition problem is intractable on non-commutative division semiring.

5.2(b). Data forgering :

Assume that a forger replaces the original message 'M' with a forgered one 'M_f'. then he sends M_f to the designated signer B and taking the signature $\{s_A, w_B, r_A, M_f\}$ and verifies that $r_A = H(z_B, w_B, M_f)$, but verification fails since $r_A = H(z_B, w_B, M) \neq H(z_B, w_B, M_f)$.

Another attempt is try to find M_f, for valid r_A. But this is impossible in two ways, because we assume that hash function (H) is cryptographically secure in one side, and he is not able to find z_B as it is CSP based, so it is intractable in other side. So the invalid data, can't be signed with a valid signature.

5.2(c) Signature Repudiation:

Assume original signer "A" intends to refuse recognition of his signature on some valid data. Then

valid signature $\{s_A, w_B, r_A, M\}$ can be forgered by an attacker Eve and she can replace message M with forgered signature $\{s_A^*, w_B^*, r_A^*, M^*\}$ instead. Then the designated verifier B computes

$$\mu^* = \left(s^*\right)^{-m} . w_B^* . \left(s^*\right)^m$$

$$\lambda^* = (s^*)^{-m} . g(p)^m, \quad z_B^* = \left(\lambda^*\right)^{-1} \mu^* \lambda^*$$

And then checks the validity of the signature by using the inequality $r_A = H(z_B, w_B, M) \neq H(z_B^*, w_B^*, M^*)$ and detects the forgery. Note that there is a negligible probability to hold this equality, because this equation needs elements satisfying commutative property on non-commutative division semiring and parameters based on PSD problem. So Eve is not able to find those elements on (R, +, •). Hence, this signature scheme ensures the non-repudiation property.

5.2(d) Existential Forgery

A forger may try to impersonate the designated signer B, by choosing a random polynomial $h_1(x) \in Z_{>0}[x]$ such that $h_1(p) \in (R, +, \bullet)$ and an element $q_1 \in (R, +, \bullet)$ then calculates

$w_B = h_1(p)^{-m} q\, h_1(p)^m$ $\quad z_B = h_1(p)^{-m} z\, h_1(p)^m$

$r_A = H(z_B, w_B, M)$ for some message M

but without knowing the secret key f(p), it is highly difficult to generate a valid $s_A = f(p)^{-m} r_A f(p)^m$ and hence to satisfy verification equation $r_A = H(z_B, w_B, M)$, where $z_B = \lambda^{-1} \mu \lambda$ for

$\lambda = s_A^{-m} g(p)^m$ *and* $\mu = s_A^{-m} w_B s_A^m$ so that signature is secure under existential forgery.

Supporting Actions of Security:

5.2(d). If the designated signer B, is dishonest, then he can cheat the original signer A and get her/his signature $\{s_A, w_B, r_A, M\}$ on any message 'M' of her/his own choice.

The solution of this problem is the existence of a trusted third party. The original signer 'A' may stress that all messages between two parties A and B, during the key generation algorithm to be authenticated. The third party keeps the records of original signer's orders and checks any case of designated signer disobeying original signer's order.

5.2(e)Can one forge a signature$\{s_A, w_B, r_A, M\}$ using the equation $\mu = s_A^{-m} w_B s_A^m$

Computing the element $s_A \in (S, +, \bullet)$, a non-commutative division semiring, from the above equation is equivalent to solving symmetrical decomposition problem. We believe that PSD is intractable on the designed underlying work structure.

Even then, if any forger selects s^* in some way, and sends the fake signature $\{s^*, w_B, r_A, M\}$ to B, receiver B computes

$$\mu^* = \left(s^*\right)^{-m} . w_B . \left(s^*\right)^m$$

$$\lambda^* = (s^*)^{-m} . g(p)^m, \quad z_B^* = \left(\lambda^*\right)^{-1} \mu^* \lambda^*$$

Then concludes that

$$r_A = H(z_B, w_B, M) \neq H(z_B^*, W_B, M)$$

and detects the forgery.

6. ALLOCATION OF REGISTRATION NUMBER

6.1 INTRODUCTION AND MOTIVATION

In 2004, Sunder Lal and Manoj Kumar [20], presented a registration scheme, which is based on directed digital signature scheme on discrete logarithms. This directed signature follows Schnorr signature, according to its structures [23].

Registrations of various kinds are a common practice in our society, like that of vehicle, shop, and factory etc. in daily life, there are so many situations, when it is necessary, beneficial and expedient to have registration number for vehicles etc. This section proposes a registration scheme, in which the registration number cannot be forged and misused. Under this scheme, the validity of an allocated registration number can be verified at any time by any authority. The allocating authority and verifying authority may be different. For practical implementation of this idea, we use directed digital signature scheme.

We all are familiar with the present status of our registration system. A hand written signature is used for the allocation of registration number by any authority. Every signature is followed by lot of formalities and records of verification. Even though and unfortunately, the present system is not much secure and liable.

6.2 PROPOSED REGISTRATION NUMBER

This procedure for allocation of a registration number contains the following main five steps.

Initial setup:

We assume a government center , providing the registration number for the public. An officer "YAMU" heads this center .Y possesses a secret and public key pair. Again consider a public person "CHAYA" with a secret and public key pair. C wants her registration number. The officer "Y" generates a registration number with a message m **,** so that "C" can directly collect her registration number. She can use her registration number publicly. She is able to prove its validity to any

authorized party "R", whenever necessary. No one other than "C" can use this registration number , because only she can prove its validity. Allocation of registration number and verifying process are as follows.

Let (S, +, •) be a non-commutative division semiring. & p, q € S are the public parameters of the system. H:S→*M* be a cryptographic hash function, which maps S to the message space *M.* To implement this idea, we use the directed signature scheme which is presented in the section 4 , for m=1.

Key Generation:

The officer "Y" chooses a polynomial at random , $f(x) \in Z_{>0}[x]$ such that $f(p) \neq 0$, $f(p) \in S$, then Y takes f (p) as his private key and computes $y = f(p)^{-1} q f(p)$ as his public key.

Another person "CHAYA" who wants registration number, chooses a polynomial at random $g(x) \in Z_{>0}[x]$ such that $g(p) \neq 0$, $g(p) \in S$, then "C" takes g (p) as his private key and computes $z = g(p)^{-1} q g(p)$ as her public key.

∴ The private and public key pairs of Y and C are (f(p), y) and (g(p), z).

Allocation of Registration number by Y to C: *(Signature Generation)*

(a). Again Y chooses , another polynomial at random $h(x) \in Z_{>0}[x]$, such that $h(p) \neq 0$, $h(p) \in S$ and computes

$$w_y = h(p)^{-1} q\, h(p), \qquad z_c = h(p)^{-1} z\, h(p)$$

(b). Using one way hash function H and a message m, Y also computes

$$r_y = H(z_c, w_y, m) \qquad s_y = f(p)^{-1} r_y f(p)$$

(c) The officer Y sends $\{s_y, w_y, r_y, m\}$ to C, as her registration number

Collecting & Verification of Registration number by C:

(a). C collects $\{s_y, w_y, r_y, m\}$ & make this public as her registration number

(b). C computes

$$\mu = S_y^{-1} w_y S_y \qquad \lambda = s_y^{-1} g(p) \qquad z_C = \lambda^{-1} \mu \lambda$$

and then checks the validity of her registration number by computing $r_y = H(z_c, w_y, m)$

Verification of Registration number by authority R:

(a). C sends $\{s_y, w_y, r_y, m, \lambda\}$ to R

(b). R checks $r_y = H(z_c, w_y, m)$

If this does not hold, R stops the process, otherwise goes to the next steps.

(c). C in a zero knowledge fashion proves to R that V = T as follows.

(i). R chooses a polynomial at random, $\Phi(x) \in Z_{>0}[x]$, such that $\Phi(p) \neq 0$, $\Phi(p) \in S$, next computes the challenge $Q = \Phi(p)[S_y \lambda z]\Phi(p)^{-1}$ and then R sends Q to C.

(ii). C chooses a polynomial at random, $\psi(x) \in Z_{>0}[x]$ such that $\psi(p) \neq 0$, $\psi(p) \in S$, next Computes the response $T = \psi(p)^{-1}[Q.g(p)^{-1}]\ \psi(p)$ and then C sends T to R

(iii) R sends Φ(p) to C.

(iv). C verifies that $Q = \Phi(p)[S_y \lambda z]\ \Phi(p)^{-1}$

(v). C sends ψ(p) to R

(vi). R verifies that $V = \psi(p)^{-1}[\Phi(p) q \Phi(p)^{-1}]\ \psi(p)$

If it holds (V=T) then R accepts $\{s_y, w_y, r_y m\}$ is an authenticated registration number.

6.3 CONFIRMATION THEOREMS AND SECURITY OF REGISTRATION NUMBER

Confirmation theorems, security and soundness of allocation registration number follows security concepts of directed digital signature, which is described in section 5, but for m =1, because allocation of registration number is an application of directed digital signature scheme on non-commutative division semiring. Thus the allocation of registration number in the electronic world has the following characteristics.

(i). Only the user can use his/her registration number, due to the property of directed Signature scheme.

(ii). The problems of forgery can be easily identified and solved easily, as discussed in section 5.2

(iii). By using this system, we can minimize the possible misuse of the present system

(iv). The obvious advantage of our scheme over present system is that resulting registration number has no meaning to any third person.

(v). Since the relation between the signature and the signer secret key is not known to any one, but the designated receiver. Hence the security level is much higher than any scheme based on discrete logarithms.

7. CONCRETE MODEL ON MATRIX DIVISION SEMIRINGS

We illustrate the allocation of registration number by using matrix division semiring, which is clearly non-commutative.

Initial setup:

Suppose, we choose S is a 2x2 Matrix division semiring, under the usual operations of Addition & Multiplication. Trivially it is non-commutative. So we define $M_2(Z_P) =$

$$\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in Z_p, \text{for prime } p, ad - bc \neq 0 \right\} \text{ and } S$$

$= M_2(Z_P) \cup \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$; where p is large secure prime. Then (S, +, •) is clearly non-commutative division semiring and is the fundamental work infrastructure. For convenience, Choose p=23, and evaluated all calculations in the group of multiplication modulo 23.

Let $H:SXSXS \rightarrow M=M_2(Z_p)$ be a cryptographic hash function, which maps SXSXS to the message space M & is defined as

$$H\left\{\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}, \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix}, \begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix}\right\} = \begin{bmatrix} 2^{\sum a_i \bmod p} & 2^{\sum b_i \bmod p} \\ 2^{\sum c_i \bmod p} & 2^{\sum c_i^2 \bmod p} \end{bmatrix} \bmod p$$

Key Generation:

An officer 'Y' chooses at randomly , two elements $p=\begin{bmatrix} 2 & 5 \\ 7 & 4 \end{bmatrix}$, $q=\begin{bmatrix} 1 & 9 \\ 3 & 2 \end{bmatrix} \in (S, +, \bullet)$

Also chooses a polynomial randomly $f(x) = 3x^3 + 4x^2 + 5x + 6$,such that

$$f(p) = 3\begin{bmatrix} 2 & 5 \\ 7 & 4 \end{bmatrix}^3 + 4\begin{bmatrix} 2 & 5 \\ 7 & 4 \end{bmatrix}^2 + 5\begin{bmatrix} 2 & 5 \\ 7 & 4 \end{bmatrix} + 6I$$

$$= \begin{bmatrix} 1036 & 1090 \\ 1526 & 1472 \end{bmatrix} \bmod 23 = \begin{bmatrix} 1 & 9 \\ 8 & 0 \end{bmatrix}$$

as his private key & Also computes

$$y = f(p)^{-1} q f(p) = \begin{bmatrix} 1 & 9 \\ 8 & 0 \end{bmatrix}^{-1} \begin{bmatrix} 1 & 9 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 1 & 9 \\ 8 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 57 & 12 \\ 357 & 222 \end{bmatrix} \bmod 23 = \begin{bmatrix} 11 & 12 \\ 12 & 15 \end{bmatrix}$$

as his public key. Similarly, the person CHAYA, chooses a polynomial at random $g(x) = x^4 + 5x^3 + 2x + 1$ such that $g(p) \neq 0$, $g(p) \in S$ and

$$g(p) = \begin{bmatrix} 2 & 5 \\ 7 & 4 \end{bmatrix}^4 + 5\begin{bmatrix} 2 & 5 \\ 7 & 4 \end{bmatrix}^3 + 2\begin{bmatrix} 2 & 5 \\ 7 & 4 \end{bmatrix} + I$$

$= \begin{bmatrix} 40 & 30 \\ 42 & 29 \end{bmatrix} \bmod 23 = \begin{bmatrix} 17 & 07 \\ 19 & 06 \end{bmatrix}$ as her private key. & also computes $z = g(p)^{-1} q g(p)$

$$= \begin{bmatrix} 17 & 07 \\ 19 & 06 \end{bmatrix}^{-1} \begin{bmatrix} 1 & 9 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 17 & 07 \\ 19 & 06 \end{bmatrix} \bmod 23$$

$$= \begin{bmatrix} 716 & 262 \\ 703 & 253 \end{bmatrix} \bmod 23 = \begin{bmatrix} 03 & 09 \\ 13 & 00 \end{bmatrix}$$

as her public key.

where $f(p)^{-1} = \frac{1}{-72}\begin{bmatrix} 0 & -9 \\ -8 & 1 \end{bmatrix} = \frac{1}{20}\begin{bmatrix} 0 & 14 \\ 15 & 1 \end{bmatrix}$

$$= 15\begin{bmatrix} 0 & 14 \\ 15 & 1 \end{bmatrix} \bmod 23 = \begin{bmatrix} 0 & 3 \\ 18 & 15 \end{bmatrix}$$

and $g(p)^{-1} = \frac{1}{-31}\begin{bmatrix} 6 & -7 \\ -19 & 17 \end{bmatrix} = \frac{1}{15}\begin{bmatrix} 6 & 16 \\ 4 & 17 \end{bmatrix}$

$$= 20\begin{bmatrix} 6 & 16 \\ 4 & 17 \end{bmatrix} \bmod 23 = \begin{bmatrix} 5 & 21 \\ 11 & 18 \end{bmatrix}$$

Allocation of Registration Number by Y to C :

YAMU, also chooses another polynomial $h(x) = x^5 + 5x + 1$, such that $h(p) \neq 0$, $h(p) \in S$.

$$h(p) = \begin{bmatrix} 2 & 5 \\ 7 & 4 \end{bmatrix}^5 + 5\begin{bmatrix} 2 & 5 \\ 7 & 4 \end{bmatrix} + I$$

$$= \begin{bmatrix} 24473 & 24730 \\ 34622 & 34365 \end{bmatrix} \bmod 23 = \begin{bmatrix} 01 & 05 \\ 07 & 03 \end{bmatrix}$$

and then computes $w_y = h(p)^{-1} q h(p)$

$$= \begin{bmatrix} 01 & 05 \\ 07 & 03 \end{bmatrix}^{-1} \begin{bmatrix} 1 & 9 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 01 & 05 \\ 07 & 03 \end{bmatrix} \bmod 23$$

$$= \begin{bmatrix} 627 & 576 \\ 283 & 204 \end{bmatrix} \bmod 23 = \begin{bmatrix} 06 & 01 \\ 07 & 20 \end{bmatrix}$$ &

$z_C = h(p)^{-1}.z\, h(p)$

$$= \begin{bmatrix} 01 & 05 \\ 07 & 03 \end{bmatrix}^{-1} \begin{bmatrix} 03 & 09 \\ 13 & 0 \end{bmatrix} \begin{bmatrix} 01 & 05 \\ 07 & 03 \end{bmatrix} \bmod 23$$

$$= \begin{bmatrix} 573 & 684 \\ 285 & 304 \end{bmatrix} \bmod 23 = \begin{bmatrix} 21 & 17 \\ 09 & 05 \end{bmatrix}$$

Where $h(p)^{-1} = \frac{1}{-32}\begin{bmatrix} 3 & -5 \\ -7 & 1 \end{bmatrix} = \frac{1}{14}\begin{bmatrix} 3 & 18 \\ 16 & 1 \end{bmatrix}$

$$= 5\begin{bmatrix} 3 & 18 \\ 16 & 1 \end{bmatrix} \bmod 23 = \begin{bmatrix} 15 & 21 \\ 11 & 05 \end{bmatrix}$$

Let $m = \begin{bmatrix} 8 & 13 \\ 19 & 22 \end{bmatrix}$ be the message & hence computes

$$r_y = H(z_c, w_y, m) = \begin{bmatrix} 2^{52} & 2^{34} \\ 2^{62} & 2^{1078} \end{bmatrix} \bmod 23$$

$$= \begin{bmatrix} 2^{06} & 2^{11} \\ 2^{16} & 2^{20} \end{bmatrix} \bmod 23 = \begin{bmatrix} 18 & 01 \\ 09 & 06 \end{bmatrix}$$

and then computes the other parameters of the algorithm are

$$s_y = f(p)^{-1} r_y f(p) = \begin{bmatrix} 1 & 9 \\ 8 & 0 \end{bmatrix}^{-1} \begin{bmatrix} 18 & 01 \\ 09 & 06 \end{bmatrix} \begin{bmatrix} 1 & 9 \\ 8 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 148 & 36 \\ 150 & 198 \end{bmatrix} \bmod 23 = \begin{bmatrix} 10 & 13 \\ 12 & 14 \end{bmatrix}$$

Then y sends $\{s_y, w_y, r_y, m\}$ i.e

$$\left\{ \begin{bmatrix} 10 & 13 \\ 12 & 14 \end{bmatrix}, \begin{bmatrix} 06 & 01 \\ 07 & 20 \end{bmatrix}, \begin{bmatrix} 18 & 01 \\ 09 & 06 \end{bmatrix}, \begin{bmatrix} 08 & 13 \\ 19 & 22 \end{bmatrix} \right\}$$

as her registration number.

Collecting & Verification of Registration Number by C:

(a). C collects

$$\left\{\begin{bmatrix} 10 & 13 \\ 12 & 14 \end{bmatrix}, \begin{bmatrix} 06 & 01 \\ 07 & 20 \end{bmatrix}, \begin{bmatrix} 18 & 01 \\ 09 & 06 \end{bmatrix}, \begin{bmatrix} 08 & 13 \\ 19 & 22 \end{bmatrix}\right\}$$ &

make this public as her registration number.

(b). C computes $\mu = s_y^{-1} w_y s_y$

$$= \begin{bmatrix} 10 & 13 \\ 12 & 14 \end{bmatrix}^{-1} \begin{bmatrix} 06 & 01 \\ 07 & 20 \end{bmatrix} \begin{bmatrix} 10 & 13 \\ 12 & 14 \end{bmatrix} \bmod 23$$

$$= \begin{bmatrix} 232 & 300 \\ 234 & 277 \end{bmatrix} \bmod 23 = \begin{bmatrix} 02 & 01 \\ 04 & 01 \end{bmatrix}$$

$$\lambda = s_y^{-1} g(p) = \begin{bmatrix} 10 & 13 \\ 12 & 14 \end{bmatrix}^{-1} \begin{bmatrix} 17 & 07 \\ 19 & 06 \end{bmatrix} \bmod 23$$

$$= \begin{bmatrix} 186 & 62 \\ 458 & 174 \end{bmatrix} \bmod 23 = \begin{bmatrix} 02 & 16 \\ 21 & 13 \end{bmatrix} \text{ and}$$

$$z_C = \lambda^{-1} \mu\lambda = \begin{bmatrix} 02 & 16 \\ 21 & 13 \end{bmatrix}^{-1} \begin{bmatrix} 02 & 01 \\ 04 & 01 \end{bmatrix} \begin{bmatrix} 02 & 16 \\ 21 & 13 \end{bmatrix} \bmod 23$$

$$= \begin{bmatrix} 389 & 477 \\ 170 & 120 \end{bmatrix} \bmod 23 = \begin{bmatrix} 21 & 17 \\ 09 & 05 \end{bmatrix}; \text{ where}$$

$$s_y^{-1} = \begin{bmatrix} 10 & 13 \\ 12 & 14 \end{bmatrix}^{-1} = \begin{bmatrix} 140 & 100 \\ 110 & 100 \end{bmatrix} \bmod 23 = \begin{bmatrix} 2 & 8 \\ 18 & 8 \end{bmatrix}$$

$$\lambda^{-1} = \begin{bmatrix} 02 & 16 \\ 21 & 13 \end{bmatrix}^{-1} = \begin{bmatrix} 26 & 14 \\ 04 & 04 \end{bmatrix} \bmod 23 = \begin{bmatrix} 3 & 14 \\ 4 & 4 \end{bmatrix}$$

and Checks the Validity of her registration number by computing $r_y = H(z_c, w_y, m)$

$$= \begin{bmatrix} 2^{52 \bmod 23} & 2^{34 \bmod 23} \\ 2^{62 \bmod 23} & 2^{1078 \bmod 23} \end{bmatrix} \bmod 23$$

$$= \begin{bmatrix} 2^{06} & 2^{11} \\ 2^{16} & 2^{20} \end{bmatrix} \bmod 23 = \begin{bmatrix} 18 & 01 \\ 09 & 06 \end{bmatrix}$$

If this is true, then She receives her registration number as authenticated.

Verification of Registration number of C by authority R:

(a). C sends $\{s_y, w_y, r_y, m, \lambda\}$ to R

$$\left\{ \begin{bmatrix} 10 & 13 \\ 12 & 14 \end{bmatrix}, \begin{bmatrix} 06 & 01 \\ 07 & 20 \end{bmatrix}, \begin{bmatrix} 18 & 01 \\ 09 & 06 \end{bmatrix}, \begin{bmatrix} 08 & 13 \\ 19 & 22 \end{bmatrix}, \begin{bmatrix} 02 & 16 \\ 21 & 13 \end{bmatrix} \right\}.$$

(b). R checks $r_y = H(z_c, w_y, m) = \begin{bmatrix} 18 & 01 \\ 09 & 06 \end{bmatrix}$

If this not hold, R stops the process, otherwise goes to the next steps.

(c). C in a zero knowledge fashion proves to R that V = T as follows.

(i). R chooses a polynomial at random, $\Phi(x) = x^3 + 9x + 1$ such that $\Phi(p) \neq 0$ and $\Phi(p) \in S$, computes

$$\Phi(p) = \begin{bmatrix} 2 & 5 \\ 7 & 4 \end{bmatrix}^3 + 9 \begin{bmatrix} 2 & 5 \\ 7 & 4 \end{bmatrix} + I$$

$$= \begin{bmatrix} 307 & 360 \\ 504 & 451 \end{bmatrix} \bmod 23 = \begin{bmatrix} 08 & 15 \\ 21 & 14 \end{bmatrix}$$

& computes the challenge $Q = \Phi(p)[s_y \lambda z] \Phi(p)^{-1}$

$$= \begin{bmatrix} 08 & 15 \\ 21 & 14 \end{bmatrix} \begin{bmatrix} 04 & 15 \\ 20 & 10 \end{bmatrix} \begin{bmatrix} 08 & 15 \\ 21 & 14 \end{bmatrix}^{-1}$$

$$= \begin{bmatrix} 354 & 54 \\ 501 & 74 \end{bmatrix} \bmod 23 = \begin{bmatrix} 09 & 08 \\ 18 & 05 \end{bmatrix};$$

and R sends Q to C.

Where $\Phi(p)^{-1} = \begin{bmatrix} 08 & 15 \\ 21 & 14 \end{bmatrix}^{-1} = \begin{bmatrix} 84 & 48 \\ 12 & 48 \end{bmatrix} \bmod 23$

$$= \begin{bmatrix} 15 & 02 \\ 12 & 02 \end{bmatrix} \text{ and}$$

$$s_y \lambda z = \begin{bmatrix} 10 & 13 \\ 12 & 14 \end{bmatrix} \begin{bmatrix} 02 & 16 \\ 21 & 13 \end{bmatrix} \begin{bmatrix} 03 & 09 \\ 13 & 00 \end{bmatrix} \bmod 23$$

$$= \begin{bmatrix} 142 & 153 \\ 135 & 171 \end{bmatrix} \bmod 23 = \begin{bmatrix} 04 & 15 \\ 20 & 10 \end{bmatrix}$$

(ii). C chooses a polynomial at random, $\psi(x) = x^4 + 3x^2 + 5$ such that $\psi(p) \neq 0$, $\psi(p) \in S$, computes

$$\psi(p) = \begin{bmatrix} 2 & 5 \\ 7 & 4 \end{bmatrix}^4 + 3 \begin{bmatrix} 2 & 5 \\ 7 & 4 \end{bmatrix}^2 + 5I$$

$$= \begin{bmatrix} 28 & 30 \\ 19 & 40 \end{bmatrix} \bmod 23 = \begin{bmatrix} 05 & 07 \\ 19 & 17 \end{bmatrix}$$

and calculates the response

$$T = \psi(p)^{-1}[Q.g(p)^{-1}] \psi(p)$$

$$= \begin{bmatrix} 05 & 07 \\ 19 & 17 \end{bmatrix}^{-1} \begin{bmatrix} 18 & 11 \\ 07 & 08 \end{bmatrix} \begin{bmatrix} 05 & 07 \\ 19 & 17 \end{bmatrix} \bmod 23$$

$$= \begin{bmatrix} 390 & 402 \\ 96 & 96 \end{bmatrix} \bmod 23 = \begin{bmatrix} 22 & 11 \\ 04 & 04 \end{bmatrix}$$

and C sends T to R. where

$$\psi(p)^{-1} = \begin{bmatrix} 05 & 07 \\ 19 & 17 \end{bmatrix}^{-1} = \begin{bmatrix} 187 & 176 \\ 44 & 55 \end{bmatrix} \bmod 23$$

$$= \begin{bmatrix} 3 & 15 \\ 21 & 09 \end{bmatrix}$$

and $Q.g(p)^{-1} = \begin{bmatrix} 9 & 8 \\ 18 & 5 \end{bmatrix} \begin{bmatrix} 5 & 21 \\ 11 & 18 \end{bmatrix} \bmod 23$

$$= \begin{bmatrix} 18 & 11 \\ 7 & 8 \end{bmatrix}$$

(iii). R sends $\Phi(p) = \begin{bmatrix} 08 & 15 \\ 21 & 14 \end{bmatrix}$ to C

(iv). C verifies that $Q = \Phi(p)[s_y \lambda z] \Phi(p)^{-1}$

$$= \begin{bmatrix} 08 & 15 \\ 21 & 14 \end{bmatrix} \begin{bmatrix} 04 & 15 \\ 20 & 10 \end{bmatrix} \begin{bmatrix} 08 & 15 \\ 21 & 14 \end{bmatrix}^{-1} \bmod 23$$

$$= \begin{bmatrix} 354 & 54 \\ 501 & 74 \end{bmatrix} \bmod 23 = \begin{bmatrix} 09 & 08 \\ 18 & 05 \end{bmatrix}$$

(v). C sends $\psi(p) = \begin{bmatrix} 05 & 07 \\ 19 & 17 \end{bmatrix}$ to R

(vi). R verifies that $V=\psi(p)^{-1}[\Phi(p)\, q\, \Phi(p)^{-1}]\psi(p)$

$$= \begin{bmatrix} 05 & 07 \\ 19 & 17 \end{bmatrix}^{-1} \begin{bmatrix} 18 & 11 \\ 07 & 08 \end{bmatrix} \begin{bmatrix} 05 & 07 \\ 19 & 17 \end{bmatrix} \bmod 23$$

$$= \begin{bmatrix} 390 & 402 \\ 96 & 96 \end{bmatrix} \bmod 23 = \begin{bmatrix} 22 & 11 \\ 04 & 04 \end{bmatrix}$$

Where $\Phi(p)\, q\, \Phi(p)^{-1}$

$$= \begin{bmatrix} 08 & 15 \\ 21 & 14 \end{bmatrix} \begin{bmatrix} 1 & 9 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 08 & 15 \\ 21 & 14 \end{bmatrix}^{-1} \bmod 23$$

$$= \begin{bmatrix} 225 & 34 \\ 375 & 54 \end{bmatrix} \bmod 23 = \begin{bmatrix} 18 & 11 \\ 07 & 08 \end{bmatrix}$$

R concludes that V=T, He accepts the Registration number of C as authenticated.

8. CONCLUSIONS

In this paper, we presented a new directed digital signature scheme based on general non-commutative division semiring. For this, we construct the polynomials as the elements of additive structure of the semiring and take them as the underlying work structure. Then the signature scheme is developed on the multiplicative structure division semiring. In this case, non-commutative property plays an important role in the signature scheme, as the public key and other structures depend on the conjugacy problem.

We also presented one important application in different situations in common practice. For this, we used a directed digital signature, to design scheme such that the scheme provides a registration number to a person or an organization, when he or organization wants to apply for the same to a government office in different situations.

The advantage of this system is that we can take all types of registration numbers under a unique providing authority. In this system, there is no chance of getting unique registration number for any pair of applicants, even if there are so many applicants in number.

At this instance, the algorithm of registration number designed for theoretical idea only. Next step, how to produce this registration number in sequence of increasing order for practical applications and other difficulties in realization are subjected to further discussion.

The security of the proposed directed signature scheme and registration number are based on the intractability of the Polynomial Symmetrical Decomposition Problem over the given non-commutative division semirings.

REFERENCES:

[1] W.Diffie and M.E. Hellman," New Directions in Cryptography", IEEE Transaction on information theory, Vol.22, pp 644-654, 1976.

[2] R.L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems", communications of the ACM Vol. 27, PP.120-126, 1978.

[3] K. Komaya, V. Maurer, T. Okamoto and S.Vanstone, "New PKC based on elliptic curves over the ring Z_n", LNCS 516, PP.252-266, Springer-verlag 1992.

[4]. T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE transactions on information theory, Vol.31, PP 469-472, 1985.

[5] S.S. Maglivers, D.R. Stinson and T. Van Trungn, "New approaches to designing Public Key Cryptosystems using one-way functions and trapdoors in finite groups", Journal of cryptology, Vol.15, PP. 285-297, 2002.

[6] P. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", SIAM J. Computing Vol.5, PP.31484-1509, 1997

[7] A.Kitaev, "Quantum measurements and the abelian stabilizer problem", preprint arXiv: cs-CR / quant – ph/9511026, 1995.

[8] J. Proos and C. Zalka, "Shorts discrete logarithm quantum algor-ithm for elliptic curves", Quantum Information and Computation, Vol.3, PP. 317-344, 2003.

[9] E. Lee, "Braid groups in cryptography", IEICE Trans. Fundamentals, vol.E87-A, no.5, PP. 986-992, 2004.

[10] V. Sidelnikov, M. Cherepnev, V.Yaschenko, "Systems of open distribution of keys on the basis of non-commutative semi groups". Russian Acad. Sci. Dok L. math., PP. 48 (2), 566-567, 1993.

[11]E. Sakalauskas, T. Burba "Basic semigroup primitive for cryptographic session key exchange protocol (SKEP)". Information Technology and Control. ISSN 1392-124X, No.3 (28), 2003.

[12] K.H. Ko et. al., "New signature scheme using conjugacy problem", Cryptology e print Archive: Report 2002/168, 2002.

[13]K.H. Ko et.al. "New public-key cryptosystem using Braid Groups". Advances in cryptology, proc. CRYPTO 2000. LNCS 1880, PP. 166-183, Springer-verlag, 2000.

[14] Z. Cao, X. Dong and L. Wang. "New Public Key Cryptosystems using polynomials over Non-commutative rings". Cryptography e-print archive, htt://eprint.iacr.org/2007/009

[15] C.P.Schnorr "Efficient identification and signatures for smart cards" Advances in cryptology-

Proceedings of Crypto89,LNCS 435,pages235-251,Springer-Verlag,1990.
[16] C.H.Lim and P.J.Lee"Modified Maurer-yacobi's scheme and its applications" in Auscrypt 92, LNCS 2248, pages 308-323, Springer-Verlag 1992.
[17] L.S.Guillou and J.J.Quisquater " A practical zero knowledge protocol fitted to security microprocessor minimizing both transmission and memory" in Eurocrypt 88 LNCS 403, pages 216-231, Springer-Verlag 1989.
[18] David Chaum " Designated confirmer signatures", Advances in cryptology-
Eurocrypt 94,LNCS 950, pages 86-91, 1995.
[19] T.Okamato " Designated confirmer signatures and public key encryption are equivalent"Advances in cryptology-Crypto 94, LNCS 839, pages 61-74, 1994.
[20] Sunder lal and Manoj Kumar " some pplications of Directed scheme" Crptology, e-Print, arxive.org/org/pdf//cs/0409050, 2004
[21] Rongxing Lu and Z.Cao " A directed signature scheme based on RSA assumption" IJ of network security Vol.2,No.3, pages 182-186, May2006.
[22] G.S.G.N.Anjaneyulu and P.vasudeva reddy U.M.Reddy "Secured Digital signature scheme using polynomials over non-commutative division semirings" International journal of computer science and network security, vol 8, no. 8, page 278-284, 2008.
[23] C.P.Schnorr "Efficient signature generation by smart cards" Journal of cryptology , 4(3), pages 161-174, Springer-Verlag,1991.
[24]. E.Sakalauskas, T.Burba " Digiatal Signature Scheme Based on Action of Infinite Ring" Informacines technologijos IR Valdymas, 2004, Nr(231) pages 60-64. ISSN 1392-124X.

Dr.G.S.G.N.Anjaneyulu received B.Sc degree in computer science with Mathematics, from Andhra university, Vishakhapatnam in 1996, M.Sc in Mathematics(II..rank) in 1998, M.phil in the 'Theory of semirings' in 2004 and in 2008, he received his Ph.D in 'Digital signatures using semiring structures' from S.V.University, Tirupati, India. He has nearly fifteen years of teaching experience in graduate, post graduate and Engineering Mathematics. He is currently working as an Associate professor, Dept. of Mathematics, VIT Universty, vellore, Tamilanadu,India. His current research interest includes 'Cryptography techniques using algebraic structures'.

Dr.U.M.Reddy received B.Sc degree in Mathematics in 1968, M.Sc in Mathematics in 1970 and Ph.D in Mathematics in 1987 from S.V.University, Tirupati, A.P, India. He worked as Associate Professor of Mathematics in S.V.University college of Engineering. He attended two international conferences in Modern algebra and has three publications in international journals. He has nearly fourteen years of teaching experience both in Engineering and P.G. Mathematics.