Secured Digital Signature Scheme using Polynomials over Non-Commutative Division Semirings

G.S.G.N.Anjaneyulu** * Dr. P. Vasudeva Reddy** ***** Prof. Dr.U.M.Reddy**

* Head & Associate Professor, Dept. of Mathematics, Narayana Engg college, Nellore, A.P, India .Pin 524003.
** Asso. Professor, Dept. of Mathematics, A.U.College of Engg, Andhra University, Visakhapatnam A.P, India .Pin 530 003.
*** Associate Professor, Dept of Mathematics, S.V.U. College of Engg.,S.V.University, Tirupati,A.P. India. Pin 517502.

Abstract:
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, like, electronic contract signing, certified email, and secure web browsing etc. But many existing signatures schemes lie in the intractability of problems closely related to the number theory than group theory. In this paper, we propose a new signature scheme based on general non-commutative division semiring. The key idea of our scheme is that for a given non-commutative division semiring, we can build polynomials on additive structure and take them as the underlying work structure. By doing so, we can implement a new signature scheme on multiplicative structure of the semiring. The security of the proposed signature scheme is based on the intractability of the Polynomial Symmetrical Decomposition Problem over the given non-commutative division semiring.

Keywords:
Public Key Cryptography, Digital Signature, Polynomial rings, Symmetrical decomposition problem and Non-commutative division semiring

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 invited public key Cryptography and, in particular, digital signature schemes. The trapdoor one-way functions play the key role in idea of PKC and digital signature schemes. Today most successful signature schemes 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 that the ElGamal signature scheme[4] 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, 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 is proposed there.

According to our knowledge, the first signature scheme designed in an infinite non commutative groups was

Manuscript received August 5, 2008
Manuscript revised August 20, 2008

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 the polynomials over non-commutative rings.

1.2 Our contributions

In this paper, we would like to propose new method for 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 digital signature scheme on multiplicative structure of the semiring. The security of the signature basically depends on polynomial symmetrical decomposition problem. But the collection of polynomials on additive structure and are operated on multiplicative structure, are strength of the security of the digital signature.

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 polynomial over an arbitrary non-commutative ring and present necessary assumptions over non-commutative division semirings . In Section 4, we propose new 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. In section 6, we verify the algorithm by concrete example. Finally, concluding remarks are made in Sec-7.

2. Cryptographic Assumptions On Non-Commutative Groups:

2.1 Two Well-known Cryptographic Assumptions

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.

2.2 Symmetrical Decomposition and Computational Diffie–Hellman Assumptions over Non-commutative Groups

Enlightened by the above problems, we would like to define the following Cryptographic problems over a non-commutative group G.

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

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

Computational Diffie–Hellman (CDH) problem over Non-Commutative Group G:

Compute $x^{z_1 z_2}$ (or) $x^{z_2 z_1}$ for given x, x^{z_1} *and* x^{z_2}, where $x \in G$, $z_1, z_2 \in S$, for $S \subseteq G$.

At present, we have no clue to solve this kind of CDH problem without extracting z_1 *or* z_2 from x and x^{z_1} (or x^{z_2}). Then, the CDH assumption over G says that CDH problem over G is intractable.

3. Building Blocks For Proposed Digital SIGNATURE SCHEME

3.1 Integral Co-efficient Ring Polynomials:

Suppose that R is a ring with (R, +, 0) and (R, •, 1) as its additive abelian group and multiple non-abelian semigroup, respectively. Let us proceed to define positive integral co-efficient ring Polynomials. Suppose that $f(x) = a_0+a_1x+\ldots + a_n x^n \in Z_{>0}[x]$ is given positive integral coefficient polynomial. We can assign this polynomial by using an element r in R and finally obtain

$$f(r) = \sum_{i=0}^{n} (a_i) r^i = (a_0) + (a_1) r + \ldots + (a_n) r^n$$

which is an element in R. (Details see section 3.4)

Further, if we regard *r* as a variable in R, then *f(r)* can be looked as polynomial about *r*. The set of all this kind of polynomials, taking over all *f(x)* ∈ $Z_{>0}[x]$, can be looked the extension of $Z_{>0}$ with *r*, denoted by $Z_{>0}[r]$. We call it the set of 1- ary positive integral coefficient R – Polynomials.

3.2 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 • r = r • 0 for all r in R

Note:

1. A Semiring without zero divisors is called Entire semiring.
2. A Semiring R is Zerosumfree semiring if and only if $r^1 + r = 0 \Rightarrow r^1 = r = 0$

3.3 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 & r^1 units of R, then $r \bullet (r^1)^{-1} = (r^1)^{-1} \bullet r^{-1}$ & 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" & 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.*

Note:

1. A commutative division semiring is called a semifield.

3.4 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∈R

Then (k) r =r + r + r +… + r + r (k times)

For k = 0, it is natural to define (k) r = 0

Property 1.

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

∀ a,b,m,n ∈ Z , ∀ r∈R

Remark: Note that in general

(a)r • (b)s ≠ (b)s • (a)r when r ≠ s, since the multiplication in R is non-commutative.

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

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

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

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

Similarly

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

for some n ≥ 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) •h(s) ≠ h(s) •f(r) in general.

3.5 Further cryptographic assumptions on Non- commutative division semirings

Let (R, +, •) be a non-commutative division semiring. For any a ∈ 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 versions of GSD and CDH problems over (R,●.) with respect to its subset P_a, and name them as polynomial symmetrical decomposition (PSD) problem and polynomial Diffie – Hellman (PDH) problem – respectively:

- Polynomial Symmetrical Decomposition(PSD) problem over Non- commutative division semiring R:

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

$$y = z^m x z^n$$

-Polynomial Diffie – Hellman (PDH) problem over Non-commutative division semirring R:

Compute $x^{z_1 z_2}$ $(or\, x^{z_2 z_1})$ for a given x, x^{z_1} and x^{z_2}, where $x \in R$ and $z_1, z_2 \in P_a$.
Accordingly, the PSD (PDH) Cryptographic assumption says that PSD (PDH) problem over
(R, •) is intractable, i.e. there does not exist probabilistic polynomial time algorithm which can solve PSD (PDH) problem over (R, •) .

4. Proposed Signature Scheme

Signature Scheme from Non-commutative Division semirings: This Digital Signature scheme contains the following main steps.

Initial setup:

suppose that (S, +, •) is the non commutative division semiring & is the underlying work fundamental infrastructure in which PSD is intractable on the non-commutative group (S, •). Choose two small integers *m, n* ∈Z.

Let H: S → *M* be a cryptographic hash function which maps S to the message space *M.* Then, the public parameters of the system would be the tuple < S, *m, n*, *M*, H >

Key Generation:

Alice wants to sign and send a message M to Bob for verification. First Alice selects two random elements p, q ∈ S and a random polynomial $f(x) \in Z_{>0}[x]$ such that $f(p)(\neq 0) \in S$ and then takes *f(p)* as her private key, computes $y=f(p)^m\, q\, f(p)^n$ and publishes her public key
$(p, q, y) \in S^3$.

Signature Generation :

Alice performs the following simultaneously.

1. Alice selects randomly another polynomial
   $h(x) \in Z_{>0}[x]$ such that $h(p) \in S$

Then ,She defines salt as

$$u = h(p)^m q\, h(p)^n \quad \text{and}$$

computes $r = f(p)^m\{H(M)u\}f(p)^n$,

$$s = h(p)^m\, r\, h(p)^n$$

$$\alpha = h(p)^m\, r\, f(p)^n$$

$$\beta = f(p)^m\, H(M)\, h(p)^n$$

$$v_1= h(p)^m H(M) h(p)^n$$

Then (u, s, α, β, v_1) is the signature of Alice on message M & sends it to the Bob for verification and then for acceptance.

Verification:

On receiving the signature (u, s, α, β , v_1)
Bob will do the following. For this, he computes $v_2 = \alpha\, y^{-1}\, \beta$
Bob accepts Alice's signature iff

$$u^{-1}v_1 = s^{-1}v_2$$

Otherwise, he rejects the signature.
Remark: If H(M) do not contain multiplicative inverse, then verification takes form $su^{-1}v_1 = v_2$

5. Confirmation Theorem

Let $(p, q, y) \in S^3$

5.1 Completeness

Given a Signature (u, s, α ,β, v_1) if Alice follows signature verification algorithm, then Bob always accepts (u, s, α ,β, v_1) as a valid signature.
Proof : Let s be the main part of the valid signature and computes

$$
\begin{aligned}
u^{-1}.v_1 &= h(p)^{--n}.q^{-1}.\, h(p)^{--m}.\, h(p)^m.H(M).h(p)^n \\
&= h(p)^{--n}.q^{-1}.H(M).h(p)^n \\
&= h(p)^{--n}.r^{-1}.\, h(p)^{--m}.\, h(p)^m.r.q^{-1}\, H(M).h(p)^n \\
&=[h(p)^m.r.h(p)^n]^{-1}[h(p)^m.r.f(p)^n][f(p)^{-n}q^{-1}H(M).h(p)^n] \\
&= s^{-1}\alpha.[f(p)^{-n}q^{-1}\, f(p)^{-m}\,]\,[f(p)^m\, H(M).h(p)^n] \\
&= s^{-1}\, \alpha.[f(p)^m\, q\, f(p)^n\,]^{-1}\, \beta \\
&= s^{-1}\, [\alpha.y^{-1}\, \beta] = s^{-1}.v_2
\end{aligned}
$$

Therefore $u^{-1}.v_1 = s^{-1}.v_2$
Hence the protocol is complete.

5.2 Security Analysis:

Assume that the active eavesdropper " Eve" can obtain , remove , forge and retransmit any message, Alice sends to Bob. Any forgered data d, we denote it by d_f . We study the security of the signature scheme for three main attacks. Data forgering on valid signature and signature repudiation on valid data, existential forgering.

(a) Data forgering:

Suppose Eve replaces the original message M, with forgered one M_f. Then Bob receives the signature (u, s, α ,β, v_1) . Using forgered data M_f or $H(M_f)$, verifying the equation

$$u^{-1}.v_1 = s^{-1}.v_2$$

is impossible, because M_f or $H(M_f)$ is completely involved in the signature generation, but not in the verification algorithm.
Hence $u^{-1}.v_1 = s^{-1}.v_2$ is true only for the original message. Data forgery without extracting signature is not possible.

Another attempt is to try to find M_f , for valid H(M). But this is impossible, because we assumed that hash function H is cryptographically secure. So the invalid data can't be signed with a valid signature.

(b) Signature Repudiation:

Assume Alice intends to refuse recognition of his signature on some valid data. Then it follows that valid signature (u, s, α ,β, v_1) can be forged by Eve and she can sign the message M , with the forgered signature (u_f, s_f, α_f, β_f, v_{1f}) instead. The verification procedure as follows

$V_2 = \alpha_f . y^{-1}\beta_f$

$=[h(p)^m.r\ f(p)^n]_f[f(p)^{-n}.q^{-1}.f(p)^{-m}][f(p)^m\ H(M).h(p)^n]_f$

Since $[f(p)^n]_f . [f(p)^n] \neq I$, $[f(p)^{-m}].[f(p)^m]_f \neq I$, where I is the identity element in the multiplicative structure of the division semiring. Consequently $[u^{-1}.v_1]_f \neq [s^{-1}.v_2]_f$. So this signature scheme ensures that the non-repudiation property.

(c) Existential Forgery:

Suppose Eve is trying to sign a forgered message M_f. Then she must forge the private key by replacing with some $[f(p)]_f$. Immediately, she faces a difficult with the public key, as we believe that PSD is intractable on non-commutative division semiring. Also note that all the structures in this signature scheme are constructed on non-commutative division semiring and based on PSD. Exact identification these structures are almost intractable as long as PSD is so hard on this underlying work structure. Consequently construction new valid signatures, without proper knowledge of private key are impossible. So Eve is not able to calculate forgered signatures.

5.3 Soundness

The key idea is that choosing a polynomial f(x) randomly, with semiring assignment and for any p € S, such that f(p) (≠ 0) € (S,+,●). A cheating prover P^* has no way to identify the polynomial f(x) € $Z_{>0}[x]$ such that f(p) (≠0) € (S, +, ●), even if he has infinite computational power. Let n be the number of elements of S, P^* best strategy is to guess the value of p, and there are n choices for p. Hence , even with infinite computing power, the cheating prover P^* with a negligible probability to trace the exact private key f(p) € S, so as to provide a valid response for an invalid signature. Hence this signature scheme is sound.

6. Example: Proposed Digital Signaturte

SCHEME ON MATRIX DIVISION SEMIRING:

Initial setup:

In this case, we choose S = $M_2(Z_P)$ as defined below, is a matrix division semiring, under the usual operations of addition & multiplication. Trivially it is non-commutative.

Let H : S→ ***M*** = $M_2(Z_P)$ be a cryptographic hash function, which maps **S** to the message space ***M*** & is defined by

$$m_{ij} \to 2^{m_{ij}} \mod p \quad \text{for } m_{ij} \in Z_p$$

We choose P = 23, m = 3, n = 5. & (S , +, ●)

$$S = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in Z_p \ \& \ ad - bc \neq 0\right\} \cup \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$ is clearly non-commutative division semiring.

For simplifying computation & verification , we evaluate the calculations over the multiplication modulo 23.

Key Generation

Alice chooses two random elements

$$p = \begin{bmatrix} 2 & 5 \\ 7 & 4 \end{bmatrix}, \quad q = \begin{bmatrix} 1 & 9 \\ 3 & 2 \end{bmatrix} \in S \ \&$$

a polynomial randomly

$f(x) = 3x^3 + 4x^2 + 5x + 6$ € $Z_{>0}[x]$

such that f(p) (≠ 0) € S.

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

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

as her private key. & Computes

$y = f(p)^m q f(p)^n = f(p)^3 q f(p)^5$

$$= \begin{bmatrix} 1 & 9 \\ 8 & 0 \end{bmatrix}^3 \begin{bmatrix} 1 & 9 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 1 & 9 \\ 8 & 0 \end{bmatrix}^5 \mod 23 = \begin{bmatrix} 4 & 6 \\ 6 & 6 \end{bmatrix}$$

Publishes her public key (p, q, y) € S^3.

Signature Generation

For a given message $M = \begin{bmatrix} 22 & 19 \\ 14 & 08 \end{bmatrix}$ & then

Alice computes

$$H(M) = \begin{bmatrix} 2^{22} & 2^{19} \\ 2^{14} & 2^{08} \end{bmatrix} \mod 23 = \begin{bmatrix} 1 & 3 \\ 8 & 3 \end{bmatrix}$$

Alice also chooses another polynomial randomly $h(x) = x^5 + 5x + 1$ € $Z_{>0}[x]$ and Computes

$$h(p) = \left\{\begin{bmatrix} 2 & 5 \\ 7 & 4 \end{bmatrix}^5 + 5\begin{bmatrix} 2 & 5 \\ 7 & 4 \end{bmatrix} + I\right\}\{\mathrm{mod}\,23\} = \begin{bmatrix} 1 & 5 \\ 7 & 3 \end{bmatrix}$$

$u = h(p)^m q h(p)^n = h(p)^3 q h(p)^5$

$$= \begin{bmatrix} 1 & 5 \\ 7 & 3 \end{bmatrix}^3 \begin{bmatrix} 1 & 9 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 1 & 5 \\ 7 & 3 \end{bmatrix}^5 \mod 23 = \begin{bmatrix} 2 & 16 \\ 10 & 21 \end{bmatrix}$$

$r = f(p)^m \{H(M)u\} f(p)^n = f(p)^3 \{H(M)u\} f(p)^5$

$$= \begin{bmatrix} 1 & 9 \\ 8 & 0 \end{bmatrix}^3 \left\{\begin{bmatrix} 1 & 3 \\ 8 & 3 \end{bmatrix} \begin{bmatrix} 2 & 16 \\ 10 & 21 \end{bmatrix}\right\} \begin{bmatrix} 1 & 9 \\ 8 & 0 \end{bmatrix}^5 \mod 23$$

$$= \begin{bmatrix} 13 & 09 \\ 10 & 13 \end{bmatrix}$$

$s = h(p)^m\ r\ h(p)^n = h(p)^3\ r\ h(p)^5$

$$= \begin{bmatrix} 1 & 5 \\ 7 & 3 \end{bmatrix}^3 \begin{bmatrix} 13 & 9 \\ 10 & 13 \end{bmatrix} \begin{bmatrix} 1 & 5 \\ 7 & 3 \end{bmatrix}^5 \bmod 23 = \begin{bmatrix} 21 & 13 \\ 19 & 07 \end{bmatrix}$$

$\alpha = h(p)^m\, r\, f(p)^n = h(p)^3\, r\, f(p)^5$

$$= \begin{bmatrix} 1 & 5 \\ 7 & 3 \end{bmatrix}^3 \begin{bmatrix} 13 & 9 \\ 10 & 13 \end{bmatrix} \begin{bmatrix} 1 & 9 \\ 8 & 0 \end{bmatrix}^5 \bmod 23 = \begin{bmatrix} 08 & 05 \\ 0 & 07 \end{bmatrix}$$

$\beta = f(p)^m\ H(M)\, h(p)^n = f(p)^3\, H(M)\, h(p)^5$

$$= \begin{bmatrix} 1 & 9 \\ 8 & 0 \end{bmatrix}^3 \begin{bmatrix} 1 & 3 \\ 8 & 3 \end{bmatrix} \begin{bmatrix} 1 & 5 \\ 7 & 3 \end{bmatrix}^5 \bmod 23 = \begin{bmatrix} 0 & 14 \\ 2 & 12 \end{bmatrix}$$

$v_1 = h(p)^m\, H(M) h(p)^n = h(p)^3\, H(M) h(p)^5$

$$= \begin{bmatrix} 1 & 5 \\ 7 & 3 \end{bmatrix}^3 \begin{bmatrix} 1 & 3 \\ 8 & 3 \end{bmatrix} \begin{bmatrix} 1 & 5 \\ 7 & 3 \end{bmatrix}^5 \bmod 23 = \begin{bmatrix} 5 & 15 \\ 13 & 12 \end{bmatrix}$$

Then Alice sends $(u, s, \alpha, \beta, v_1)$ as her signature

Verification:

After receiving the signature of Alice, Bob will do the following. i.e he computes

$v_2 = \alpha\, y^{-1}\, \beta$

$$= \begin{bmatrix} 08 & 05 \\ 0 & 07 \end{bmatrix} \begin{bmatrix} 11 & 12 \\ 12 & 15 \end{bmatrix} \begin{bmatrix} 0 & 14 \\ 2 & 12 \end{bmatrix} \bmod 23 = \begin{bmatrix} 20 & 7 \\ 3 & 21 \end{bmatrix}$$

And Verifies that

$$u^{-1} v_1 = \begin{bmatrix} 16 & 13 \\ 11 & 07 \end{bmatrix} \begin{bmatrix} 5 & 15 \\ 13 & 12 \end{bmatrix} \bmod 23 = \begin{bmatrix} 19 & 05 \\ 08 & 19 \end{bmatrix}$$

$$s^{-1}\, v_2 = \begin{bmatrix} 02 & 16 \\ 11 & 06 \end{bmatrix} \begin{bmatrix} 20 & 7 \\ 3 & 21 \end{bmatrix} \bmod 23 = \begin{bmatrix} 19 & 05 \\ 08 & 19 \end{bmatrix}$$

i.e., $u^{-1} v_1 = s^{-1}\, v_2$

Bob accepts Alice's signature as a Valid signature , otherwise he will reject the same.

7. Conclusions

In this paper, we presented a new signature scheme based on general non-commutative division semiring. The key idea behind our scheme lies that we take polynomials over the given non-commutative algebraic system as the underlying work structure for constructing signature scheme. The security of the proposed scheme is based on the intractability of 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-commutation 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, http://eprint.iacr.org/2007/***

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) from S.V.University, Tirupati., India in 1998, and M.phil in the 'Theory of semirings' from S.V.University, Tirupati in 2004.Currently, he is persuing Ph.D in Digital signatures using semiring structures from S. V. University, Tirupati, India. He has nearly ten years of teaching experience in graduate, post graduate and Engineering
Mathematics. He is currently working as an associate professor, Dept. of Mathematics, Narayana Engineering College, Nellore, Andhra.Pradesh, India. His current research interests include 'Cryptography using algebraic structures'.

Dr. P.Vasudeva Reddy received M. Sc (Mathematics), PhD (Cryptography) from S.V. University, Tirupati, India. He is currently working as an associate professor in the department of mathematics, A.U College of Engineering, Andhra University, and Visakhapatnam, India. His field of interest includes Algebraic Number theory, secret sharing, Multi party computations, and cryptography.

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 and retired as Associate Professor of Mathematics in S.V.University collge 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.