Noname manuscript No.
(will be inserted by the editor)

New Digital Signature Scheme using Multiple Private Keys over Non-Commutative Division Semirings

Dr.G.S.G.N.Anjaneyulu · **A.Vijayabarathi** ·

Received: date / Accepted: date

Abstract In this paper, we propose a new signature scheme connecting two private keys and two public keys based on general non-commutative division semiring. The key idea of our technique engrosses three core steps. In the first step, we assemble polynomials on additive structure of non-commutative division semiring and take them as underlying work infrastructure. In the second step, we generate first set of private and public key pair using polynomial symmetrical decomposition problem. In the third step, we generate second set of private and public key pair using discrete logarithm. We use factorization theorem to generate the private key in discrete logarithm problem. By doing so, we can execute a new signature scheme on multiplicative structure of the semiring using multiple private keys. The security of the proposed signature scheme is based on the intractability of the Polynomial Symmetrical Decomposition Problem and discrete logarithm problem over the given non-commutative division semiring. Hence , this signature scheme is so much strong in security point of view.

Keywords Digital Signature · Factorization theorem · Discrete logarithm problem · Symmetrical decomposition problem · Non-commutative division semiring.

Mathematics Subject Classification (2000) 16 Y 60 · 14 G 50

Dr.G.S.G.N.Anjaneyulu
Associate professor,Applied Algebra Division, School of Advanced Sciences, VIT University, Vellore-14, Tamilnadu, India.
Tel.: +91-9047288639
E-mail: anjaneyulu.gsgn@vit.ac.in

A.Vijayabarathi
Research Scholar,Applied Algebra Division, School of Advanced Sciences, VIT University, Vellore-14, Tamilnadu, India.
E-mail: vijayabarathia2010@vit.ac.in

1 Introduction

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.

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 "*NewdirectionsinCryptography*" [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]. 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 noncommutative groups was 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 **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.

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 x G, find z $\in$ G such that y = z^{-1} x z
-Decomposition Problem (DP): Given (x,y)$\in$G x 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 generalnon-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 x 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 x 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}(orx^{z2}).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) = $a_0 + a_1x + + a_nx_n \in Z_{>0}[x]$ is given positive integral coefficient polynomial. We can assign this polynomial by using an element r in R and finally obtain

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

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)$\in Z_{>0}[x]$, 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 and 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

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 • r^1 = 1 = r^1•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• $(r^1)^{-1}$ =$(r^1)^{-1}$•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*.

3.4 **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$\in Z_{>0}$ and 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 • (b)r^n = (ab)•r^{m+n} =(b)r^n•(a)r^m , $\forall$ a,b,m,n $\in$Z,$\forall$r$\in$ 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 $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n \in Z_{>0}[x]$ is given positive integral coefficient polynomial. We can assign this polynomial by using an element r in R and finally , we obtain $f(r) = a_0 + a_1r + a_2r^2 + ... + a_nr^n \in R$ Similarly $h(r) = b_0 + b_1r + b_2r^2 + ... + b_mr^m \in R$ 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 and 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⊆R by $P_a \overset{\Delta}{=} \{ f(a)/f(x) \in Z_{>0}[x]\}$ 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∈ P_a such that y = $z^m xz^n$
-Polynomial Diffie - Hellman (PDH) problem over Non-commutative division semiring R: Compute$x^{z_1z_2}(or\, x^{z_2z_1})$ for a given x,x^{z_1} and x^{z_2}, where x ∈ R and z_1, z_2 ∈ 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 and is the underlying work fundamental infrastructure in which PSD and conjugacy problem are intractable on the non-commutative group (S,•). Choose two small integers m, n∈Z. Let H: S → S be a cryptographic hash function which maps S to the message space S. Choose m, n≠0∈Z , Then the public parameters of the system would be the tuple $< S, m, n, S, H >$
Remark: In this case, we must choose message space is also S.
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 polynomial f(x)∈ $Z_{>0}[x]$ randomly such that f(p)(≠0)∈ S and then she takes f(p) as her private key, computes g = $f(p)^m q f(p)^n$ and publishes this as her public key. Let k be the product of two

large secure primes a, b. Its security is based on the difficulty of factoring k, such that $1 < e < \Phi(k) = (a-1).(b-1)$ and gcd(e, $\Phi(k)$) =1. Since (a-1)(b-1) is even then 'e' is always odd.
So we can compute second private key 'd' with $1 < e < \Phi(k)$=(a-1)(b-1) and de $\equiv 1(mod\Phi(k))$. Then we calculate second public key by discrete logarithm y = g^d . So that the private and public key pairs are (f(p), d) and (g, y, e).
Signature Generation : Alice performs the following simultaneously by taking a message M from message space. 1. Alice selects randomly another polynomial h(x)$\in$ $Z_{>0}[x]$ such that h(p)$\in$ S Then ,She defines h(p) as salt and
computes u = $h(p)^{-m}$q $h(p)^{-n}$ and
r = $f(p)^m$.H(M+ du).$f(p)^n$,
α= f(p)h(p),
s = $f(p)^{-n}\{(H(M+du))^{-1}.q\}$.$f(p)^n$,
v = α^m.u.α^n Then (v, r, s) is the signature of Alice on the message M and sends it to the bob for acceptance and it needs verification.
Verification: On receiving the signature (v, r, s) from Alice Bob will do the following. For this, he computes z = r.s and w = y^e.
Bob accepts Alice's signature iff $g^{-1}v = wz^{-1}$ Otherwise, he rejects the signature.

5 CONFIRMATION THEOREM

5.1 **Completeness**

Let (p, q, g, y, e) be the public parameters for p, q, g, y$\in$ S. Given a signature (v, r, s), if Alice follows signature verification algorithm, then Bob always accepts (v, r, s) as a valid signature.
Proof : In verification , the parameters are v, r, s, z and w.
$g^{-1}v = w\, z^{-1} \rightarrow v.z = g.w$
now LHS = v.z = v.r.s = $\{\alpha^m.u.\alpha^n\}$.r.s on simplification ,
we obtain vz = $\{f(p)^m q f(p)^n\}$.$\{f(p)^m q f(p)^n\}$
= $\{f(p)^m q f(p)^n\}.\{f(p)^m q f(p)^n\}^{ed}$
= g. $(g^d)^e$ = gw, which is RHS. as the reason de$\equiv$ 1(mod Φ(k))

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 $(u_f, s_f, \alpha_f, \beta_f, v_{1f})$ instead. The verification procedure as follows

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

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

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 $\in$ S, such that f(p) ($\neq$ 0)$\in$ (S,+,$\bullet$). A cheating prover P^* has no way to identify the polynomial f(x)$\in Z_{>0}[x]$ such that f(p)($\neq$0)$\in$(S, +, $\bullet$), 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 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, 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, 120-126,(1978).
3. K. Komaya, V. Maurer, T. Okamoto and S.Vanstone, New PKC based on elliptic curves over the ring Zn, 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, 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, 285-297,(2002).
6. P. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,*SIAM J. Computing* Vol.5, 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, 317-344,(2003).
9. E. Lee, Braid groups in cryptography,*IEICE Trans. Fundamentals*, vol.E87-A, no.5, 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.*,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*, 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) 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 thirteen 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'.

A.Vijayabarathi received B.Sc degree in Mathematics, from Seethalakshmi Ramaswamy college, Tiruchirapalli in 1998, M.Sc in Mathematics from Seethalakshmi Ramaswamy college,Tiruchirapalli in 2000, M.phil in mathematics from St. Joseph's college, Tiruchirapalli in 2001.She worked as a lecturer of Mathematics in Seethalakshmi Ramaswamy college, Tiruchirapalli. She has nearly Seven years of teaching experience in graduate and post graduate. She attended one international conference in Discrete Mathematics.She is currently pursuing Ph.D in Graph labellings and Applications at VIT University in Vellore, Tamilnadu, India.