ISSN No. 0976-5697

Volume 1, No. 4, Nov-Dec 2010

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Fuzzy Commitment Scheme On Polynomials Over Division Semi Ring

Deo Brat Ojha*
Department of Mathematics
R.K.G.Institute of Technology
Ghaziabad,U.P.,INDIA
ojhdb@yahoo.co.in

Nitin Pandey
Department of Information Technology
Amity Institute of Information Technology
Noida,U.P.,INDIA
npandeyg@gmail.com

Abstract: In this paper, the attempt has been made to explain a fuzzy commitment scheme on an algebraic coding theory based public key cryptosystem which relay on the difficulty of decoding. Here, we presented a fuzzy commitment scheme over division semi ring which enhance the efficiency of fuzzy commitment scheme.

Keywords: Cryptography; Error Correcting Codes; Fuzzy logic; division semi ring; fuzzy Commitment scheme.

I. INTRODUCTION

In cryptography, a commitment scheme or a bit commitment scheme is a method that allows a user to commit a value while keeping it hidden and preserving the user's ability to reveal the committed value later. A useful way to visualize a commitment scheme is to think of the sender as putting the value in a locked box and giving the box to the receiver. The value in the box is hidden from the receiver, who cannot open the lock (without the help of the sender), but since the receiver has the box, the value inside cannot be changed. Commitment schemes are important to a variety of cryptographic protocols, especially zero-knowledge proofs and secure computation. Bit-commitment from any one-way function: One can create a bit-commitment scheme from any one-way function. The scheme relies on the fact that every one-way function can be modified to possess a computationally hard-core predicate. Let w be a one-way function, with j a hard-core predicate. Then to commit to a bit e, Alice picks a random input t and sends the triple (j,w(t), $e \oplus j(t)$) to Bob, where $\oplus$ denotes XOR, i.e. addition modulo 2. To decommit Alice simply sends t to Bob. This scheme is concealing because for Bob to recover e he must recover j(t). Since j is a computationally hard-core predicate, recovering j(t) from w(t) with probability greater than one-half is as hard as inverting w The scheme bindingness depends greatly on whether or not w is injective. For more knowledge readers may see [15,16]. The idea behind public-key cryptosystem is based on the fact that the decoding problem of an arbitrary linear code is an NP-hard problem [1].The other previous schemes employs probabilistic encryption [2, 3] in preventing the elimination of any information leaked through public-key cryptography as well as our scheme also.

Moreover in the conventional commitment schemes, opening key are required to enable the sender to prove the commitment. However there could be many instances where the transmission involves noise or minor errors arising purely because of the factors over which neither sender nor the receiver have any control , which creates uncertainties. Fuzzy commitment scheme was first introduced by Juels and Martin [4]. The new property "fuzziness" in the open phase to allow, acceptance of the commitment using corrupted opening key that is close to the original one inappropriate metric or distance.

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 e-Business, e-Commerce, and e-Government. 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" [5] 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.

Another good case is that the ElGamal signature scheme [6] is based on the difficulty of solving the discrete logarithm problem (DLP) defined over a finite field Zp (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 [7].On Quantum computer, IFP, DLP, as well as DLP over ECDLP, turned out to be efficiently solved by algorithms due to Shor [8] , Kitaev [9] and Proos–Zalka [10].Although practical quantum computers are as least 10 years away, their potential weakness will soon create distrust in current cryptographic methods [11].As addressed in [11], 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 [12], where a proposition to use non-commutative groups and semi groups in session key

agreement protocol is presented. Some realization of key agreement protocol using [12] methodology with application of the semi group action level could be found in [13]. Some concrete construction of commutative sub semi group is proposed there. But there is an essential gap existing between the Conjugacy Decision Problem (CDP) and conjugator Search Problem (CSP) in noncommutative group . In, [14], Cao et.al. Proposed a new DH-like key exchange protocol and ElGamal–like cryptosystems using the polynomials over noncommutative rings .

II. PRELIMINARIES

2.1 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 $f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n, f(x) \in Z_{>0}[x]$ is given positive integral coefficient polynomial. We can assign this polynomial by using an element r in R and finally obtain

$f(r) = \sum_{i=1}^{n} (a_i) r^i = a_0 + a_1 r + a_2 r^2 + ... + a_n r^n, f(r) \in Z_{>0}[r], r \in R$,which is an element in R.

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.

2.2 Polynomials on Division semiring

Let $(R,+,.)$ be a non-commutative division semi ring. Let us consider positive integral co-efficient polynomials with semi ring 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 $k(r) = r + r + ... + r$ (k times).

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

Property 1.

$(a)r^m.(b)r^n = (ab)r^{m+n} = (b)r^n.(a)r^m$ For all $a, b, m, n \in Z$ and for all $r \in R$.

Remark: Note that in general

$(a)r.(b)s \neq (b)s.(a)r$, when r ≠ s, since the multiplication in R is non-commutative. Now, Let us proceed to define positive integral coefficient semi ring polynomials. Suppose that

$f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n, f(x) \in Z_{>0}[x]$ is given positive integral coefficient polynomial. We can assign this polynomial by using an element r in R & finally , we obtain

$f(r) = \sum_{i=1}^{n} (a_i) r^i \in R$ .Similarly, $h(r) = \sum_{i=1}^{n} (a_i) r^i \in R$,for some n ≥ m. Then we have the following

Theorem2.3*:* $f(r).h(r) = h(r).f(r)$ for $f(r).h(r) \in R$

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

We combine well-known techniques from the areas of error-correcting codes and cryptography to achieve a improve type of cryptographic primitive. Fuzzy commitment scheme is both concealing and binding: it is infeasible for an attacker to learn the committed value, and also for the committer to decommit a value in more than one way. In a conventional scheme, a commitment must be opened using a unique witness, which acts, essentially, as a decryption key. , it accepts a witness that is close to the original encrypting witness in a suitable metric, but not necessarily identical. This characteristic of fuzzy commitment scheme makes it useful for various applications. Also in which the probability that data will be associate with random noise during communication is very high. Because the scheme is tolerant of error, it is capable of protecting data just as conventional cryptographic techniques.

A metric space is a set C with a detection function $dist : C \times C \to R_+ = [0, \infty)$, which obeys the usual properties (symmetric, triangle inequalities, zero distance between equal points) [13], [14].

Definition 2.4 : Let $c \in \{0,1\}^n$ be a code set which consists of a set code words ci of length n. The distance metric between any two code words c_i and c_j in C is defined by $dist(c_i, c_j) = \sum_{r=1}^{n} \left| c_{ir} - c_{jr} \right| \forall c_i, c_j \in C$

This is known as Hamming distance [17].

Definition 2.5: An error correction function f for a code C is defined as

$f(c_i) = \{ \frac{c_j}{dist(c_i, c_j)} = \min C - \{c_i\} \}$ Here, $c_i = f(c_i)$ is called the nearest neighbour of c_i [18].

Definition 2.6: The measurement of nearness between two code words c and c' is defined by $nearness(c, c') = dist(c, c')/n$, it is obvious that $0 \leq nearness(c, c') \leq 1$ [15].

Definition 2.7: The fuzzy membership function for a code word c' to be equal to a given c is defined as [17] –

FUZZ (c')=0 if $nearness(c, c') = z \leq z_0 < 1$

= z otherwise.

The rest of the paper is organized as follows. In Section 2, we present the necessary Cryptographic assumptions over non-commutative groups. We define polynomial over an arbitrary noncumulative ring and present necessary assumptions over non-commutative division semi rings. In Section 3, we proposed commitment scheme based on underlying structure and assumptions. Finally, concluding remarks are made in section4.

III. OUR PROPOSED SCHEME

Let D={ Alice, Bob},Message Space: Let

$M \subset \{0,1\}^4 \qquad m = \begin{bmatrix} 22 & 19 \\ 14 & 8 \end{bmatrix}$

Initial set up

In this case, we choose $S = M_2(Z_p)$ as defined below, is a matrix division semi ring, under the usual operations of addition & multiplication. Trivially it is noncommutative. S is the message space M and K is defined by $K : m_{ij} \to 2^{m_{ij}} \bmod p, m_{ij} \in Z_p$. We choose P = any prime, m &n are any prime & $(S,+,.)$ is the non commutative division semi ring and is the underlying work fundamental

Infrastructure in which PSD is intractable on the noncommutative group $(S,.)$. Choose two small integers $m,n \in Z$. First Alice selects two random elements $p,q \in S$ 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 $(p,q,y) \in S^3$. Let $h(p) \in S$, $h(x) \in Z_{>0}[x]$ and Alice computes $u = h(p)^m q h(p)^n$,then computes $g(m) = f(p)^m K(m) f(p)^n$ and by introducing error e from, Make $E = h(p)^m g(m) h(p)^n$.

Commit phase: at time t_1

Alice committed to her message m . For the sake of secrecy she adds error and make E at random. Then her commitment

$$c = commita\lg(*, g(m), E) = h(p)^m K(m) h(p)^n$$

Alice sends c to Bob, which Bob will receive, where t the transmission function is.

Open Phase: At time t_2

Alice disclose the procedure K , $g(m)$ and E to Bob to open the commitment.

Suppose Bob gets $t(g(m)) = h(p)^m K(m) f(p)^n$ and $t(E) = f(p)^m K(m) h(p)^n$

Bob computes

$$c' = open\lg(*, t(g(m)), t(E)) = t(g(m)) y^{-1} t(E)$$

Bob checks the $dist(c,c')$, if $dist(c,c') > 0$, he realizes that there is an error occurs during the transmission.

Bob apply the error correction function F to c'

Then Bob will compute nearness $(t(c), F(c')) = \frac{dist(t(c), F(c'))}{n} < Z$ .If fuzzy commitment nearness $(t(c), F(c'))$ if equal to zero. Then $t(c) = F(c')$.

Bob will apply inverse function then $F = m$.

IV. CONCLUSION

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

V. REFERENCES

[1] G. E. R. Berlekemp, R. J. McEliece and H. C. A.van Tilborg, On the inherent intractability of certain coding problems, IEEE Transactions on Information Theory 24 (1978) No.5, 384-386.

[2] M. Blum and S.Goldwasser, An efficient probabilistic public-key encryption scheme which hides all partial information. Advances in cryptology (Santa Barbara, Calif., 1984), 289–299, Lecture Notes in Comput. Sci., 196, Springer. Berlin, 1985.

[3] S.Goldwasser and S. Micali, Probabilistic encryption & how to play mental poker keeping secret all partial information, Annual ACM Symposium on Theory of Computing, Proceedings of the fourteenth annual ACM symposium on Theory of computing, 1982, 365 - 377.

[4] A. Juels and M.Wattenberg, A fuzzy commitment scheme, In Proceedings of the 6th ACM Conference on Computer and Communication Security, November 1999, 28-36.

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

[6] 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.

[7] 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.

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

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

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

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

[12] 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.

[13] 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.

[14] Z. Cao, X. Dong and L. Wang."New Public Key Cryptosystems using polynomials over Noncommutative rings ".Cryptographye-print archive, http:// eprint. iacr. org/ 2007.

[15] V. Guruswami and M. Sudan, Improved decoding of reed-solomon and algebraic geometric codes, In FOCS '98, 28–39. IEEE Computer Society, 1998.

[16] W. W. Peterson, Encoding and error-correction procedures for Bose-Chaudhuri codes, (Russian. English original) [J] Kibern. Sb. 6, 25-54 (1963); translation from IRE Trans. Inform. Theory IT-6, 459-470 (1960).

[17] A.A.Al-saggaf, H.S.Acharya,(2007),"A Fuzzy Commitment Scheme", IEEE International Conference on Advances in Computer Vision and Information Technology, 28-30.

[18] Deo Brat Ojha and Ajay Sharma, A Fuzzy commitment scheme with Mceliece cipher, Surveys in Mathematics and its Applications, Volume 5 (2010), 73 – 82.