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

Secure E-Alliance Model for E-Communication

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

Meenu Sahni
Department of Mathematics
B.I.T.S.U.P.T.U.,
Ghaziabad, (U.P.), India
mnu.sahni @rediffmail.com

Abhishek Shukla
Department of M.C.A.
R.K.G.Institute of Technology
Ghaziabad,(U.P.),India
abhishekknit@gmail.com

Abstract: In this paper, the attempt has been made to explain secure E-alliance model for E-communication with the help of polynomials on division semi ring based public key cryptosystem. Here, we presented a model to remove error with the help of error correction function.

Keywords: Cryptography; Error Correcting Codes; Fuzzy logic; division semi ring; error correction function.

I. INTRODUCTION

In cryptography, 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 [1]. 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.

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 "New directions in Cryptography" [2] Diffie and Hellman invited public key Cryptography. On Quantum computer, IFP, DLP, as well as DLP over ECDLP, turned out to be efficiently solved by algorithms due to Shor [3] , Kitaev [4] and Proos–Zalka [5].Although practical quantum computers are as least 10 years away, their potential weakness will soon create distrust in current cryptographic methods [6].As addressed in [6], 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[7]. In, [8], Cao et.al. Proposed a new DH-like key exchange protocol and ElGamal–like cryptosystems using the polynomials over noncommutative rings .

II. PRELIMINARIES

A. 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 canassign 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) [8].

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 ci and cj 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 [11].

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 [10].

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 $0 \leq nearness(c, c') \leq 1$ [9].

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.

III. CUSTOMIZATION OF SEAMEC

Customization of an SEAMEC for a member $(M_{SEAMEC\ I})$ takes place in the following way. $(M_{SEAMEC\ I})$ first decides a key $(Key_{SEAMEC\ I})$ when he installs the SEAMEC onto his computer. Then he types in his name $(Name_{SEAMEC\ I})$ and e-mail address $(\text{Email adr}_{SEAMEC\ I})$. $(Key_{SEAMEC\ I})$ is secretly hidden (according to a steganographic procedure in his envelope $(E_{SEAMEC\ I})$ This $(Key_{SEAMEC\ I})$ is eventually transferred to a message sender's $(MI_{SEAMEC\ II})$ in an invisible way. $(Name_{SEAMEC\ I})$ and $(Name\ adr_{SEAMEC\ I})$ are printed out on the envelope surface when $(M_{SEAMEC\ I})$ produces $(E_{SEAMEC\ I})$ by using $(EP_{SEAMEC\ I})$. $(Key_{SEAMEC\ I})$ is also set to $(EO_{SEAMEC\ I})$ at the time of installation. $(Name_{SEAMEC\ I})$ and $(\text{Email adr}_{SEAMEC\ I})$ are also inserted (actually, embedded) automatically by $(MI_{SEAMEC\ I})$ any time $(M_{SEAMEC\ I})$ inserts his message $(Mess._{SEAMEC\ I})$ in another member's envelope $(E_{SEAMEC\ I})$. The embedded $(Name_{SEAMEC\ I})$ and $(\text{Email adr}_{SEAMEC\ I})$ are extracted by a message receiver $(M_{SEAMEC\ II})$ by $(EO_{SEAMEC\ II})$.

A. Our Proposed SEAMEC Scheme

Our SEAMEC involves, D={ First(Sender),Second (Receiver)},Message Space $M \subset \{0,1\}^4$

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 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 private key, computes $y = f(p)^m q f(p)^n$ and publishes 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 $g(m) = f(p)^m K(m) u f(p)^n$ and by introducing error e , make $E = h(p)^m g(m) h(p)^n$.

Commit phase: at time t_1

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

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

First sends c to second, which second will receive, where t is the transmission function.

Open Phase: At time t_2

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

Suppose second gets $t(g(m)) = h(p)^m K(m) f(p)^n$ and $t(E) = f(p)^m K(m) h(p)^n$. Then second computes

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

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

Second apply the error correction function F to c'

Then Second 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 $t(c) = F(c')$. Second will apply inverse function then get original message.

IV. COMPONENTS OF THE SECURE E-ALLIANCE

SEAMEC is a steganography application .It makes use of the inseparability of the external and internal data. The E-alliance can be implemented differently according to different programmers or different specifications.

SEAMEC consists of the three following components.

1. First to agree with step 3.
2. Envelope Producer (EP)
3. Message Inserter (MI)
4. Envelope Opener (EO)

In this scheme we have two communicating parties first and second. We denote first's SEAMEC as $SEAMEC_{first}$ So, it is described as $SEAMEC_{first} = EP_{first}.MI_{first}.EO_{first}.EP_{first}$ is a component that produces MI_{first}'s envelope E_{first}. E_{first} is the envelope (actually, an image file) which is used by all, when they send a secret message to $SEAMEC_{first}$. EO_{first} is produced from an original image . $SEAMEC_{first}$ can select it according to his preference. E_{first} has both the name and e-mail address of $SEAMEC_{first}$ on the envelope surface (actually, the name and address are "printed" on image E_{first}). It will be placed at downloadable site, so that anyone can get it freely and use it any time or someone may ask $SEAMEC_{first}$ to send it directly to him/her. MI_{first} is the component to insert (i.e., embedded according to the steganographic scheme) $SEAMEC_{first}$'s message into another member's (e.g., $SEAMEC_{second}$'s envelope (E_{second}) when $SEAMEC_{first}$ is sending a secret message ($MESSAGE_{first}$) to $SEAMEC_{second}$. One important function of MI_{first} is that it detects a key (KEY_{second}) that has been hidden in the envelope (E_{second}), and uses it when inserting a message ($MESSAGE_{first}$) in $MESSAGE_{first}$. is a component that opens (extracts) E_{first}'s "message inserted" envelop E_{first} ($MESSAGE_{second}$) which $SEAMEC_{first}$ received from someone as an e-mail attachment. The sender ($SEAMEC_{second}$') of the secret message ($MESSAGE_{second}$) is not known until $SEAMEC_{first}$ opens the envelope by using .

V. HOW IT WORKS

When some member $(M_{SEAMEC\ II})$ wants to send a secret message $(MESS_{SEAMEC\ II})$ to another member $(M_{SEAMECC\ I})$, whether they are acquainted or not, $(M_{SEAMEC\ II})$ gets (e.g., downloads) the $(M_{SEAMEC\ I})$'s envelope $(E_{SEAMEC\ I})$, and uses it to insert his message $(Mess._{MECC\ II})$ by using $(MI_{MECC\ II})$. When $(M_{SEAMEC\ II})$ tries to insert a message, $(M_{SEAMEC\ I})$'s key $(Key_{SEAMEC\ I})$ is transferred to $(MI_{SEAMEC\ II})$ automatically in an invisible manner, and is actually used. $(M_{SEAMEC\ I})$ can send $(E_{SEAMEC\ I}(M_{SEAMEC\ II}))$ directly, or ask someone else to send, it to $(M_{SEAMEC\ I})$ as an e-mail attachment. $(M_{SEAMEC\ II})$ can be anonymous because no sender's information is seen on $(E_{SEAMEC\ I}(M_{SEAMEC\ II}))$. $(Mess._{SEAMEC\ I})$ is hidden, and only $(M_{SEAMEC\ I})$ can see it by opening the envelope. It is not a problem for $(M_{SEAMEC\ II})$ and $(M_{SEAMEC\ I})$ to be acquainted or not because $(M_{SEAMEC\ II})$ can get anyone's envelope from an open site.

Due to the stymieing channel, there is a chance for the occurrence of error. Let $(M_{SEAMEC\ I})$ get message $(t(c)_{SEAMEC\ II})$ instead of $(c_{SEAMEC\ II})$, where t denote the transmission error. Now, $(M_{SEAMEC\ I})$ apply error correction function on $(t(c)_{SEAMEC\ II})$ and gets $(t(c)_{SEAMEC\ II})'$.

$(M_{SEAMEC\ I})$ check that $dist\{(t(c)_{SEAMEC\ II}), t(c)_{SEAMEC\ II})'\} > 0$, $(M_{SEAMEC\ I})$ will realize that there is an error occur during the transmission. $(M_{SEAMEC\ I})$ apply the error correction function f to $(c_{SEAMEC\ II})' : f((c_{SEAMEC\ II})'$.

Then $(M_{SEAMEC\ I})$ will compute nearness

$$(t(c_{MECC\ II}), f((c_{MECC\ II})')) = \frac{dist\{t(c_{MECC\ II}), f((c_{MECC\ II})')\}}{n}.$$

.

$$FUZZ((c_{SEAMEC\ II})') = \begin{cases} 0 & if\ nearness(c_{SEAMEC\ II}), (c_{SEAMEC\ II})') = z \le z_0 < 1 \\ z & otherwise \end{cases}$$

When some member ($SEAMEC_{second}$) wants to send a secret message ($MESSAGE_{second}$) to another member ($SEAMEC_{first}$). and $SEAMEC_{second}$ complete step 4 , then $SEAMEC_{second}$ gets (e.g., downloads) the $SEAMEC_{first}$'s envelope ( ), and uses it to insert his message ($MESSAGE_{second}$) by using . When $SEAMEC_{second}$ tries to insert a message, $SEAMEC_{first}$'s key is transferred to automatically in an invisible manner, and is actually used. $SEAMEC_{first}$ can send $E_{first}MESSAGE_{second}$ directly, or ask someone else to send, it to $SEAMEC_{first}$ as an e-mail attachment. $SEAMEC_{second}$ can be anonymous because no sender's information is seen on $E_{first}MESSAGE_{second}$, $MESSAGE_{second}$ is hidden, and only $MECC_{first}$ can see it by opening the envelope. It is not a problem for $SEAMEC_{second}$ and $SEAMEC_{first}$ to be acquainted or not but step 4 is required for authenticity.

VI. CONCLUSION

In this paper, we would like to propose new model secure e-alliance for e-communication 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 our process 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.

VII. REFERENCES

[1] 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.

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

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

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

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

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

[7] 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.

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

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

[10] 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.

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