Volume 1, No. 3, October 2010
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

A MODEL OF E-MAILING SYSTEM USING POLYNOMIALS OVER NON-CUMMUTATIVE DIVISION SEMIRING

Deo Brat Ojha[*1], Abhishek Shukla[2] and Meenu Sahani[3]

[*1] Department of Mathematics, R.K.G. Institute of Technology, Ghaziabad, U.P. INDIA -201003
Email: ojhabrat@gmail.com[1]
[2](Research Scholar Singhania Univ., Jhunjhunu, Rajsthan)
College of Computer Application,R.K.G. I.T., Ghaziabad ,U.P. INDIA-201003
Email:abhishekknit@gmail.com[2]
[3]Department of Mathematics, Bhagwati Institute of Technology & Science, Ghaziabad, U.P. INDIA-201002
Email: mnu.sahni@rediffmail.com[3]

Abstract: In this paper we show a model of e-mailing system using polynomials over non-commutative Division semiring for internet communication. It is the model of a real-life secure mailing system. In this model, a sender can send a secret message even to a unacquainted person in an anonymous way. The users of this model are assumed to be may or may not be the members of a closed organization.

***Keywords*:** Stegnography, Symmetric key, Semirings , Encryption / Decryption, Mailing System

INTRODUCTION

Human beings have long hoped to have a technique to communicate with a distant partner anonymously but later on distinctive and must be secure. We may be able to realize this hope by using stegnography.
Modern steganography has a relatively short history because people did not pay much attention to this skill until Internet security became a social concern. Most people did not know what stegnography was because they did not have any means to know the meaning. Even today ordinary dictionaries do not contain the word "stegnography." Books on stegnography are still very few [1], [2]. The most important feature of this stegnography is that it has a very large data hiding capacity [3], [4]. It normally embeds 50% or more of a container image file with information without increasing its size. Stegnography can be applied to variety of information systems. Some key is used in these systems when it embeds/extracts secret data. One natural application is a secret mailing system [7] that uses a symmetric key. Another application pays attention to the nature of stegnography whereby the external data (e.g., visible image data) and the internal data (any hidden information) cannot be separated by any means. We will term this nature as an "inseparability" of the two forms of data. For more details [5,6,8,9,10,11,12].
In the present paper we will show our basic model of e-mailing system using polynomials over non-commutative division semiring. The structure of the present paper is as follows. In Section 1.1, we will make a short discussion on the problem of an encrypted mailing system. Section 2.1 describes the scheme of the e-mailing system using polynomials over non-cummutative division semiring.

PROBLEMS OF AN ENCRYPTED MAILING SYSTEM

There are two types of cryptography scheme: Symmetric key schemes and asymmetric key schemes.
In a symmetric system a message sender and receiver use a same encryption/decryption key. In this scheme, however, the sender and the receiver must negotiate on what key they are going to use before they start communication. Such a negotiation must be absolutely secret. They usually use some second channel (e.g., fax or phone). However, the second channels may not be very secure. There is another problem in this situation in that if the sender is not acquainted with the receiver, it is difficult to start the key-negotiation in secret. Furthermore, the more secure the key system is, the more inconvenient the system usage is. An asymmetric system uses a public key and a private key system. The public key is open to the public, and it is used for message encoding when a sender is sending a message to the key owner.

MATERIAL AND METHODS

A Model of e-mailing system using polynomials over non-commutative division semirings

We do not intend to develop a new "message reader-and-sender" or "message composer", but we are developing three system components that make e-mailing system using polynomials over non-commutative division semirings (EPNCDS) A message sender inserts (actually, embeds) a secret message in an envelope using steganography and sends it as an e-mail attachment. The receiver receives the attached envelope and opens it to receive the message. An "envelope" in this system is actually an image file that is a container, vessel, cover, or dummy data in the terminology of steganography. This system can solve all the problems mentioned above.
The following items are the conditions we have set forth in designing the system.
1.The name of the message sender may or may not be anonymous, as depends upon their wish.
2.The message is hidden in the envelope and only the designated receiver can open it.

3.Sender can send a secret message even to an unaccustomed person.
4.It is easy to use for both sender and receiver.

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.

BUILDING BLOCKS FOR PROPOSED SCHEME

INTEGRAL CO-EFFICIENT RING POLYNOMIALS:

Suppose that R is a ring with $(R,+,0)$ and $(R,\bullet,1)$ 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.

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). $(R,\bullet)$ 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

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

DIVISION SEMIRING

An element r of a semiring R, is a "unit" if and only if there exists an element r^1 r1 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.
2. A Semiring R is Zerosumfree semiring if and only
If $r^1+r=0\Rightarrow r^1=r=0$

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 • (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 & finally , we obtain
$f(x)=a_0+a_1r+.a_2r^2+....+a_nr^n\in R$

Simiilarly
$f(x)=b_0+b_1x+b_2x^2+....+b_mx^m\in R$
for some $n\geq m$. Then we have the following

Theorem: $f(r).h(r)=h(r).f(r)$ 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.

RESULTS AND DISCUSSION

PROPOSED SCHEME

Our 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 noncommutative group (S, ●). Choose two small integers *m n* □Z.
Let $H : S \to M = M_2(z_p)$ 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:
EPNCDS_{first} wants to sign and send a message M to EPNCDS_{second} for verification. First EPNCDS_{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 her private key, computes $y = f(p)^m q f(p)^n$ and publishes her public key $(p, q, y) \in S^n$.

EPNCDS_{first} performs the following simultaneously.

1. EPNCDS_{first} selects randomly another polynomial $h(x) \in Z_{>0}[x]$ such that $h(p) \in S$ Then , EPNCDS_{first} defines salt as

We denote by

$f(p)^m, f(p)^n$: EPNCDS_{first} 's long term private key pair;

$f(p)^m q f(p)^n = X_a$: EPNCDS_{first} 's long term public key ;

$g(p)^m, g(p)^n$: EPNCDS_{second} 's long term private keypair;

$g(p)^m q g(p)^n = X_b$: EPNCDS_{second} 's long term public key.

Following the above mentioned notations, we describe the EPNCDS below. The protocol works in the following steps.

EPNCDS_{first} EPNCDS_{second}

$h(p)^m q h(p)^n = Y_a$ ⟶ $K_b = g(p)^m f(p)^m q f(p)^n g(p)^n$

$Y_b = g(p)^m f(p)^m q f(p)^n$
$g(p)^n w(p)^m q w(p)^n$
$g(p)^m f(p)^m q f(p)^n g(p)^n$

⟵

1. EPNCDS_{first} choose $f(p)^m, f(p)^n$,computes $h(p)^m q h(p)^n = Y_a$. If Y_a = I (Identity braid), EPNCDS_{first} terminates the protocol and restarts $h(p)^m$ and $h(p)^n$, EPNCDS_{first} then sends $h(h(p)^m q h(p)^n)$ to EPNCDS_{first} sends it to EPNCDS_{second}.

2. Upon receiving $h(p)^m q h(p)^n$, EPNCDS_{second} randomly chooses $w(p)^m, w(p)^n$, computes $K_b = g(p)^m f(p)^m q f(p)^n g(p)^n$,and
$Y_b = g(p)^m f(p)^m q f(p)^n g(p)^n w(p)^m q w(p)^n g(p)^m$
$f(p)^m q f(p)^n g(p)^n$.

3.If $f(p)^m g(p)^m q g(p)^n f(p)^n$ or
$g(p)^m f(p)^m q f(p)^n g(p)^n w(p)^m q w(p)^n g(p)^m$
$f(p)^m q f(p)^n g(p)^n = I$
EPNCDS_{first} terminates the protocol and restarts with new $w(p)^m$ and $w(p)^n$. otherwise EPNCDS_{second} sends it to EPNCDS_{first}.

4.Up on receiving
$g(p)^m f(p)^m q f(p)^n g(p)^n q w(p)^n g(p)^m f(p)^m q f(p)^n g(p)^n$,

EPNCDS_{first} computes $K_b = f(p)^m g(p)^m q g(p)^n f(p)^n = K_a$,
and the shared key
$KEY_a = h(p)^m f(p)^{-m} g(p)^{-m} q g(p)^{-n} f(p)^{-n}$
$g(p)^m f(p)^m q f(p)^n g(p)^n q w(p)^n g(p)^m f(p)^m q f(p)^n$.
$g(p)^n f(p)^{-m} g(p)^{-m} q g(p)^{-n} f(p)^{-n} h(p)^n$

5. EPNCDS_{second} also computes the shared key $KEY_b = w(p)^m h(p)^m q h(p)^n w(p)^n$.

6. In each step 4 and 5, if
$h(p)^m f(p)^{-m} g(p)^{-m} q g(p)^{-n} f(p)^{-n} g(p)^m$
$f(p)^m q f(p)^n g(p)^n q w(p)^n g(p)^m f(p)^m q f(p)^n$
$g(p)^n f(p)^{-m} g(p)^{-m} q g(p)^{-n} f(p)^{-n} h(p)^n$
or $w(p)^m h(p)^m q h(p)^n w(p)^n$ is I, then the protocol run is terminated with failure.

7. After regular protocol running, EPNCDS_{first} and EPNCDS_{second} share the secret $K = KEY_a = KEY_b$.

Customization of an EPNCDS for a member EPNCDS_{first} takes place in the following way. EPNCDS_{first} and EPNCDS_{second} first agree to generate a key

($K = KEY_{first} = KEY_{second}$). Then $EPNCDS_{first}$ types in his name ($NAME_{first}$) and e-mail address ($e-mail_{first}$). Key is secretly hidden (according to a steganographic method or some other method) in $EPNCDS_{first}$ envelope (E_{first}). This *Key* is eventually transferred to a message sender's MI_{second} in an invisible way. $NAME_{first}$ and $e-mail_{first}$ are printed out on the envelope surface when $EPNCDS_{first}$ produces E_{first} by using EP_{first}. *Key* is also set to EO_{first} for the initialization. $NAME_{first}$ and $e-mail_{first}$ are also inserted (actually, embedded) automatically by MI_{first} any time $EPNCDS_{first}$ inserts message ($MESSAGE_{first}$) in envelope (E_{second}). The embedded $NAME_{first}$ and $e-mail_{first}$ are extracted by a message receiver ($EPNCDS_{second}$) by EO_{second}.

COMPONENT OF THE SYSTEM

EPNCDS is a steganography application .It makes use of the inseparability of the external and internal data. The system can be implemented differently according to different programmers or different specifications. Different EPNCDS' are incompatible in operation with others.
An EPNCDS consists of the three following components.
1. Envelope Producer (EP)
2. Message Inserter (MI)
3. Envelope Opener (EO)

In this scheme we have two communicating parties first and second. We denote first's EPNCDS as $EPNCDS_{first}$ So, it is described as $EPNCDS_{first} = EP_{first}, MI_{first}, EO_{first}$. 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 $EPNCDS_{first}$. EO_{first} is produced from an original image EO. $EPNCDS_{first}$ can select it according to his preference. E_{first} has both the name and e-mail address of $EPNCDS_{first}$ 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 $EPNCDS_{first}$ to send it directly to him/her. MI_{first} is the component to insert (i.e., embed according to the steganographic scheme) $EPNCDS_{first}$'s message into another member's (e.g., $EPNCDS_{second}$)'s envelope (E_{second}) when $EPNCDS_{first}$ is sending a secret message ($MESSAGE_{first}$) to $AIMMS_{second}$. 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 E_{second}. EO_{first} is a component that opens (extracts) E_{first}'s "message inserted" envelop E_{first} ($MESSAGE_{second}$) which $EPNCDS_{first}$ received from someone as an e-mail attachment. The sender ($EPNCDS_{second}$) of the secret message ($MESSAGE_{second}$) is not known until $EPNCDS_{first}$ opens the envelope by using EO_{first} .

HOW TO WORKS

When some member ($EPNCDS_{second}$) wants to send a secret message ($MESSAGE_{second}$) to another member ($EPNCDS_{first}$),whether they are acquainted or not, $EPNCDS_{second}$ gets (e.g., downloads) the $EPNCDS_{second}$'s envelope (E_{first}), and uses it to insert his message ($MESSAGE_{second}$) by using MI_{second} . When $EPNCDS_{second}$ tries to insert a message, $EPNCDS_{first}$'s key is transferred to MI_{second} automatically in an invisible manner, and is actually used. $EPNCDS_{first}$ can send E_{first} $MESSAGE_{second}$ directly, or ask someone else to send it to $EPNCDS_{first}$ as an e-mail attachment.

$EPNCDS_{second}$ can be anonymous because no sender's information is seen on E_{first} $MESSAGE_{second}$. $MESSAGE_{second}$ is hidden, and only $EPNCDS_{first}$ can see it by opening the envelope. It is not a problem for $EPNCDS_{second}$ and $EPNCDS_{first}$ to be acquainted or not because $EPNCDS_{second}$ can get anyone's envelope from downloadable site. EPNCDS is a very easy-to-use system because users are not bothered by any key handling.

REFERENCES

[1] Stefan Katzenbeisser and Fabien A.P. Petitcolas (eds) :"Information hiding techniques for steganography and digital watermarking", Artech House, 2000.
[2] Neil F. Johnson, Zoran Duric and Sushil Jajodia :"Information Hiding", Kluwer Academic Publishers, 2001.
[3] M. Niimi, H. Noda and E. Kawaguchi :"An image embedding in image by a complexity based region segmentation method", Proceedings of International Conf.on Image Processing'97, Vol.3, pp.74-77, Santa Barbara, Oct., 1997.
[4] E. Kawaguchi and R. O. Eason :"Principle and applications of BPCS-Steganography", Proceedings of SPIE: Multimeda Systems and Applications, Vol.3528, pp.464-463, 1998.
[5]URLhttp://www.know.comp.kyutech.ac.jp/BPCSe/Dpenv/ DPENVe-pro_ down. html.
[6] E. Kawaguchi,et al: "A concept of digital picture envelope for Internet communication" in Information modeling and knowledge bases X,IOS Press, pp.343-349, 1999.
[7] K. H. Ko, D. H. Choi, M. S. Cho, and J. W. Lee, "New signature scheme using conjugacy problem." (http://eprint.iacr.org/2002/168)

[8] K.H.KO,S.J.Lee, J.H.Cheon, J.W.Han,J. S. Kang, and C Park,"New public- key cryptosystem using braid groups," in Advances in Cryptology (Crypto'00),LNCS1880,pp,166-183,Springer-Verlag,2000.

[9] A. Menezes, M. Qu, and S. Vanstone, "Key agree-ment and the need for authentication," in Proceed-ings of PKS'95, pp. 34-42, 1995.

[10] L. Law, A. Menezes, M. Qu, J. Solinas, and S. Van-stone, An Efficient Protocol for Authenticated Key Agreement, Technical Report CORR98-05, Department of CO, University of Waterloo, 1998.

[11] L. Law, A. Menezes, M. Qu, J. Solinas, and S. Van-stone, "An efficient protocol for authenticated key-agreement," Design, Codes and Cryptography, vol. 28, no. 2, pp. 119-134, 2003.

[12] Eiji Kawaguchi, Hideki Noda, Michiharu Niimi and Richard O. Eason, A Model of Anonymous Covert Mailing System Using Steganographic Scheme, Information modelling and knowledge bases X,IOS Press, pp.81-85,2003.

