Volume 2, No. 3, March 2011

Journal of Global Research in Computer Science

ISSN-2229-371X

RESEARCH PAPER

Available Online at www.jgrcs.info

A Model of Key Agreement Protocol using Polynomials over Non-Cummutative Division Semirings

Abhishek Dwivedi[1*], D.B.Ojha[2], Ajay Sharma[3], Awakash Mishra[4]

[1*]Research Scholar Singhania University, Jhunjhunu, Rajsthan
& Department of M.C.A, Raj Kumar Goel Engineering College, Ghaziabad, U.P., India.
dwivediabhi@gmail.com[1]
[2]Department of Mathematics, R. K. G. Institute of Technology, Ghaziabad, U.P., India.
ojhdb@yahoo.co.in[2]
[3] Research Scholar Singhania University, Jhunjhunu, Rajsthan
&Department of Information Technology, R.K.G.Institute of Technology ,Ghaziabad,U.P.,INDIA
ajaypulast@rediffmail.com[3]
[4]Research Scholar Singhania University, Jhunjhunu, Rajsthan
& Department of M.C.A, Raj Kumar Goel Engineering College, Ghaziabad, U.P., India.
awakashmishra@gmail.com[4]

***Abstract*:** The basic aim of key exchange is that two people who can only communicate via an insecure channel want to find a common secret key without any attack. In this paper we show a model of key-agreement protocol using polynomials over non-commutative division semiring for network security. It is proved that the proposed protocol meets several security attributes under the assumption that the polynomials over the non- commutative division semiring.

Keywords: Symmetric key, Semirings, Polynomial rings, Key agreement, and Security.

INTRODUCTION

The Key exchange problems are of central interest in security world. The basic aim is that two people who can only communicate via an insecure channel want to find a common secret key without any attack.

In this paper, we elaborated the process for well secured and assured for sanctity of correctness about the sender's and receiver's identity, as key agreement protocol under the polynomial over the non- commutative division semiring (KPNCD).

In recent years have emerged as suitable settings for cryptographic protocols [4, 5, 6, and 7]. 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 [3]. Some concrete construction of commutative sub-semigroup is proposed there.

Here we use polynomial to suggest a new key agreement scheme. If sender and receiver both are in separate physically, they must trust a transmission medium to prevent the disclosure of the secret key being communicated. Anyone who intercepts the key in transit can later read, modify, and forge all messages encrypted using that key. The generation of such keys is called key agreement; and all cryptosystems must deal with key agreement issues. Because all keys in a symmetric cryptosystem must remain secret, secret-key cryptography often has difficulty providing secure key agreement, especially in open systems with a large number of users.

The concept of key agreement was introduced in 1976 by W. Diffie and M. Hellman [11]. In their seminal scheme each person gets a pair of keys, one called the public key and the other called the private key. Each person's public key is published while the private key is kept secret. The need for the sender and receiver to share secret information is thus eliminated; all communications involve only public keys, and no private key is ever transmitted or shared.

This paper is organized as follows: We present a brief introduction of public key infrastructure and proposals based on commutative rings in section 2. In section 3, we define the proposed key agreement protocol mention its desirable attributes. In section 4, the security consideration is mentioned. Finally ends with conclusion.

PRELIMINARY INFRASTRUCTURE BASED ON NON-COMMUTATIVE RINGS

There is no doubt that the internetworked communication 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.

Proposed Key-Agreement Protocol

a) 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 $f(x) = a_0 + a_1x + \ldots\ldots + a_nx^n \in Z_{>0}[x]$ is given positive integral coefficient polynomial. We can assign this polynomial by using an element r in R and finally obtain $f(r) = \Sigma_{i=0}^{n}(a_i)r^i = (a_0) + (a_1)r \ldots\ldots + (a_n)r^n$, 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.

b) 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 $r^1 + r = 0 \Longrightarrow r^1 = r = 0$

c) 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 and 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 $(R,\bullet)$, 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 $r^1 + r = 0 \Longrightarrow r^1 = r = 0$.

d) Polynomials on Division Semiring

Let $(R,+,\bullet)$ 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 $(k)r = r + r + r + \ldots + r + r(k\ times) for\ k = 0$, 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 $(a)r \bullet (b)s \neq (b)s \bullet (a)r$ when $r \neq s$, since the multiplication in R is non-commutative.
Now, Let us proceed to define positive integral coefficient semiring polynomials. Suppose that $f(x) = a_0 + a_1 + a_2x^2 + \ldots + a_nx^n \in Z_{>0}[x]$ is given positive integral coefficient polynomial. We can assign this polynomial by using an element r in R & finally, we obtain $f(x) = a_0 + a_1r + a_2r^2 + \ldots + a_nr^n \in R$

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

Theorem:

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

PROPOSED SCHEME

Our scheme contains the following main steps.

Initial setup:
Suppose that $(S,+,\bullet)$ is the non commutative division semiring & is the underlying work fundamental infrastructure in which PSD is intractable on the noncommutative group $(S,\bullet)$. Choose two small integers $m, n \in Z$.

Key generation:
Sender (A) wants to sign and send a message M to Receiver (B) for verification. First, Sender 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 $(p, q, y) \in S^n$.

Sender performs the following simultaneously.

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

defines salt as:

We denote by

$f(p)$: $A's$ long term private key pair;
$g(p)$: $B's$ long term private key pair;
$f(p)qf(p)^{-1} = Y_a$: $A's$ long term public key;
$g(p)qg(p)^{-1} = Y_b$: $B's$ long term public key;

Following the above mentioned notations, we describe the key-agreement scheme below. The protocol works in the following steps.

Sender (A) Receiver (B)
$h(p)qh(p)^{-1} = X_a$ ⟶ $K_b = g(p)Y_a g(p)^{-1}$

$X_b = K_b w(p) X_a w(p)^{-1} (K_b)^{-1}$

⟵

1. Sender choose $f(p)$, computes $h(p)qh(p)^{-1} = X_a$ If $X_a = I(Identity)$, Sender terminates the protocol and restarts $h(p)$ and $h(p)^{-1}$, Sender then sends it to Receiver.
2. Upon receiving $h(p)qh(p)^{-1} = X_a$, Receiver randomly chooses $w(p), w(p)^{-1}$, computes $K_b = g(p)Y_a g(p)^{-1}$ and $X_b = K_b w(p) X_a w(p)^{-1} (K_b)^{-1}$.
3. If $K_b = g(p)Y_a g(p)^{-1}$ or $X_b = K_b w(p) X_a w(p)^{-1} (K_b)^{-1} = I$, Reciever terminates the protocol and restarts with new $w(p)$ and $w(p)^{-1}$. Otherwise Receiver sends it to Sender.
4.Upon receiving $X_b = K_b w(p) X_a w(p)^{-1} (K_b)^{-1}$, Sender computes $K_b = f(p)Y_b f(p)^{-1} = K_a$, and the shared key $Key_a = h(p)K_a X_b K_a^{-1} h(p)^{-1}$.
5. Receiver also computes the shared key $Key_b = w(p)X_a w(p)^{-1}$.
6. In each step 4 and 5, if $h(p)K_a X_b K_a^{-1} h(p)^{-1}$ or $w(p)X_a w(p)^{-1}$ is I, then the protocol run is terminated with failure.
7. After regular protocol running, Sender and Reciever share the secret $K = Key_a = Key_b$.

SECURITY CONSIDERATION

Here we show that our protocol meets the following desirable attributes under the assumption that the polynomial over the non- commutative division semiring.

Known-Key Security:
If A and B execute the regular protocol run, they clearly share their unique session key K, because
$Key_a = h(p)K_a X_b K_a^{-1} h(p)^{-1}$.
$Key_a = h(p)K_a K_b w(p) X_a w(p)^{-1} (K_b)^{-1} K_a^{-1} h(p)^{-1}$.
$= h(p)K_a K_b w(p) h(p)qh(p)^{-1} w(p)^{-1} (K_b)^{-1} K_a^{-1} h(p)^{-1}$.
$= w(p)h(p)qh(p)^{-1} w(p)^{-1}$.
$= w(p)X_a w(p)^{-1}$.
$= Key_b$

(Perfect) forward secrecy:
During the computation of the session key K for each entity, an adversary who captured their private keys $h(p)$ or $w(p)$ should extract K_a and K_b from the information $X_a and$ X_b to know the previous or next session keys between them. However, this is the polynomial problem. Hence, under the assumption that the polynomial is computationally infeasible, KPNCD meets the forward secrecy requirement.

KEY-COMPROMISE IMPERSONATION: Suppose $A's$ long-term private key, $f(p)$, is disclosed. Now an adversary who knows this value can clearly impersonate A. Is it possible for the adversary impersonates B to A without knowing the $B's$ long-term private key, $g(p)$? For the success of the impersonation, the adversary must know $A's$ ephemeral key $h(p)$ at least. So, also in this case, the adversary should extract $h(p)$ from $A's$ ephemeral public value $X_a = h(p)qh(p)^{-1}$. This also contradicts that polynomial is hard.

Unknown key-share:
Suppose an adversary E now try to make $sender(A)$ believe that the session key is shared with $reciever(B)$, while $reciever(B)$ believes that the session key is shared with E. To launch the unknown key-share attack, the adversary E should set his public key certified even though he does not know his correct private key. For this, E makes it by utility the public values (Y_A) and (Y_B). With some simple calculations, we see that the unknown key-share attack fails.

Key control:
As the same argument in the above, the key-control is clearly impossible for the third party. The only possibility of *key-control* attack may be brought out by the participant of the protocol B. But for the entity B, to make the party, A generate the session key $K(Key_b)$. which is pre -selected value by B, for example B should solve the following $K = w(p)X_a w(p)^{-1}$. But this again falls into the problem of polynomial.

CONCLUSION

Our key agreement protocols have quality for being a useful part of secure e-gaming and e-gambling protocols. In fact, our approach are a guarantee that no player misbehaviors or deviates from the protocols, because they agreed at one point. In this paper, we have presented a key agreement protocol that allows both players to agree at a bitstring based on the polynomials over the non- commutative division semiring.

REFERENCES

[1] A. Menezes, M. Qu, and S. Vanstone, “Key agreement and the need for authentication,” in Proceed-ings of PKS’95, pp. 34-42, 1995.

[2] D.B.Ojha, Abhishek Dwivedi, Ajay Sharma, & Ramveer Singh, *“A Non-Repudiable Biased Bitstring Key Agreement protocol (NBBKAP) Using Conjugacy Problem in Non-abelian Group”*, International Journal of Engineering Science and technology Vol. 2(9), 2010, 4162-4166.

[3] 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.

[4] H.Sibert, P.Dehornoy, & M.Girault, *"Entity authentication schemes using braid word reduction"*, WCC 2003, to appear; http://eprint.iacr.org/2002/187.

[5] I.Anshel, M.Anshel, B.Fisher, and D.Goldfeld, *"New key agreement protocols in braid group cryptography"*, Proc.of CT – RSA 2001, LNCS, 2010, Springer-Verlag, 1-15.

[6] I. Anshel, M. Anshel and D. Goldfeld, *"An algebraic method of public-key cryptography"*, Math. Research Letters, 6, 1999, 287-291.

[7] 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, Advances in Cryptology"*, Proceeding of Crypto - 2000, Lecture Notes in Computer Science 1880, ed. M Bellore, springs Verlag, 2000, 166-183.

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

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

[10] M. Bellare, A. Desai, D. Pointcheval and P. Rogaway, Relations among notions of security for public-key encryption schemes, Advances in Cryptology | CRYPTO '98, Lecture Notes in Computer Science, 1462 (1998), Springer-Verlag, pp. 26-45.

[11] R.Dutta, R. Barua and P. Sarkar,"Pairing Based Cryptography : A Survey Cryptology e-print Archive ", Report 2004/064,2004.

[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] W.Diffie, & M.Hellman, *"New directions in cryptography"*, IEEE Trans. Inform. Theory, 22 (6), 1976, 644-654.

[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/