Semiring Actions for Public Key Cryptography

S. Nivetha[1,3] , V. Thiruveni[2] and M. Chandramouleeswaran[3]

[1,3]Sri Ramanas College of Arts and Science for Women,
Aruppukottai – 626134, Tamilnadu, INDIA.
email:[1]nivethasoundar9127@gmail.com, [3]moulee59@gmail.com
[2]Saiva Bhanu Kshatriya College,
Aruppukottai – 626101, Tamilnadu, INDIA.
email:[2]thiriveni2009@gmail.com

(Received on: January 13, 2019)

ABSTRACT

In this paper we give a protocol for public key sharing and encryption and decryption of plaintext using semiring action problem which is a generalization of discrete logarithmic problem.

AMS Classification: 16Y60, 11T71, 14G50, 94A60.

Keywords: Semirings, Public key, Encryption, Decryption.

1. INTRODUCTION S

Data that can be read and understood without any special measures is called plaintext or cleartext. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called ciphertext. You use encryption to ensure that the information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting ciphertext to its original plaintext is called decryption. Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone, except the intended recipient.

In public-key encryption systems each entity A has a public key e and a corresponding private key d. In secure systems, the task of computing d given e is computationally infeasible. The public key defines an encryption transformation E_e, while the private key defines the associated decryption transformation D_d. Any entity B wishing to send a message m to A obtains an authentic copy of $A's$ public key e, uses the encryption transformation to obtain the ciphertext $c = E_e(m)$, and transmits c to A. To decrypt c, A applies the decryption transformation to obtain the original message $m = D_d(c)$.

The public key need not be kept secret, and in fact, may be widely available; only its authenticity is required to guarantee that A is indeed the only party who knows the corresponding private key. A primary advantage of such systems is that providing authentic public keys is generally easier than distributing secret keys securely, as required in symmetric key systems.

Public-key encryption schemes are typically substantially slower than symmetric-key encryption algorithms. For this reason, public-key encryption is most commonly used in practice for the transport of keys subsequently used for bulk data encryption by symmetric algorithms and other applications including data integrity and authentication, and for encrypting small data items such as credit card numbers and PINs. Public-key decryption may also provide authentication - guarantees in entity authentication and authenticated key establishment protocols.

The primary objective of an adversary who wishes to attack a public-key encryption scheme is to systematically recover plaintext from ciphertext intended for some other entity A. If this is achieved, the encryption scheme is informally said to have been broken. A more ambitious objective is key recovery to recover $A's$ private key. If this is achieved, the encryption scheme is informally said to have been completely broken since the adversary then has the ability to decrypt all ciphertext sent to A.

Semirings generalize the notion of non-commutative rings in the sense that negative elements do not have to exist. Finite semirings and matrices over them can be applied in public key cryptography to construct interesting commutative semigroup actions $G \times X \to X$ given by $(g, x) \to gx$ .This means that they are efficiently computable through the orbit maps $G \to G \times X \subseteq X$ defined by $g \to gx$, which are hard to invert in general. They provide a frame work for natural generalizations of discrete logarithmic based cryptosystems. In this case the semigroup action is taken to be the exponentiation, $(\mathrm{Z_n}, \cdot) \times H \to H$ given by $(\mathrm{a}, x) \to a^x$ in the cyclic group $(H, \cdot)$ of order n.

In paper[5] the authors generalize the DLP as a semiring action problem by defining an action by a semiring on a semimodule over a semiring.

In this paper we further generalize the DLP as a semiring action problem when we use the action of a semiring on a multiplicative monoid. The semiring under consideration is taken as an exponential semiring which resembles the logarithmic process. We introduce the notion of exponential semiring that replaces the logarithmic function used in DLP. We have provided protocols for public key sharing that is Diffie Hellman key exchange and the protocol for encrypting and decrypting the plain text which are hard to attack.

2. PRELIMINARIES

In this section we recall basic definitions that are required for our work.

Definition 2.1.[1] **Group Action** Let $(G,\cdot)$ be a group and X a set. Then a group action of G on X is a map from ¤ $: G\times X \to X$ with ¤$(a,x) = a\cdot x$, such that for all $a,b\in G, x\in X$,
(i) $e\cdot x = x$
(ii) $a\cdot(b\cdot x) = (a\cdot b)\cdot x.$

Next we define the stabilizer of an element $x\in X$ with an action from a group G on X.

Definition 2.2.[1] Let G be group acting on a set X and let $x\in X$. Then the set $G_x = \{g\in G / g\cdot x = x\}$, which is a subgroup of G is called the stabilizer subgroup of x in G.

Definition 2.3.[1] Let G be a group acting on a set X, and let $x\in X$. Then the set $Gx = \{g\cdot x / g\in G\}$, is called the orbit of x in G.

Definition 2.4.[2] **(DLP)** Let g be a primitive root for F_p and let h be a nonzero element of F_p. The discrete logarithm problem is the problem of finding an exponent x such that $g^x \equiv h(\bmod p).$ This number x is called the discrete logarithm of h to the base g and is denoted by $\log_g(h).$

Definition 2.5. [4] **(Semigroup Action Problem)** Given a semigroup G acting on a set S and elements $x\in S$ and $y\in Gx$, find $g\in G$ such that $gx = y.$

Definition 2.6. [3] A semiring is a nonempty set R on which operations of addition and multiplication has been defined such that the following conditions are satisfied:
(1) $(R,+)$ is a commutative monoid with identity element 0.
(2) $(R,\cdot)$ is a monoid with identity element $1_R.$
(3) Multiplication distributes over addition from either side.
(4) $0r = 0 = r0$ for all $r\in R.$
(5) $1\neq 0$.

Example 2.7. Let $n>1$ be an integer and let $0\le i\le n-1.$ Set $B(n,i) = \{0,1,2,\cdots,n-1\}.$ Define an operation $\oplus$ on $B(n,i)$ as, if $a,b\in B(n,i)$ then $a\oplus b = \begin{cases} a+b & if\ a+b\le n-1 \\ c & otherwise \end{cases}$ where c is a unique element of $B(n,i)$ satisfying, $c\equiv a+b \bmod (n-i), i\le c\le n-1.$ Define an operation $\otimes$ on $B(n,i)$ as, if $a,b\in B(n,i)$ then $a\otimes b = \begin{cases} ab & if\ ab\le n-1 \\ c & otherwise \end{cases}$ where c is a unique element of $B(n,i)$ satisfying, $c\equiv ab \bmod (n-i), i\le c\le n-1.$

Definition 2.8.[5] **(Semiring Action Problem):** Given a semiring $A = S_1 \times S_2$ acting on a left semimodule $M = M_1 \times M_2$ and elements $n = (n_1, n_2 \in M)$ and $r = (r_1, r_2) \in ¤_{S_1}(A_n)$ or $¤_{S_2}(A_n)$, find $q = (q_1, q_2 \in A)$ such that $¤_{S_1}(q_n) = r$ or $¤_{S_2}(q_n) = r$

3. SEMIRING ACTIONS FOR PUBLICKEY CRYPTOGRAPHY

In this section, we introduce the notion of exponential semiring and apply the same for public key sharing. We present protocols for key sharing and encryption of message.

Definition 3.1. Exponential Semiring Let $(S, +, \cdot)$ be a semiring. Let B be the multiplicative semigroup of $(S \setminus \{0\}, \cdot)$. Define a binary operation $E : B \times S \to B$ by $E(b, s) = b^s$ for all $b \in B$ and $s \in S$ satisfying the following conditions:

(1) $b^{s_1} \cdot d^{s_1} = (bd)^{s_1}$

(2) $b^{s_1 \cdot s_2} = (b^{s_1})^{s_2}$

(3) $b^{s_1 + s_2} = b^{s_1} . b^{s_1}$

(4) $b^1 = b$

Then (S, B) is called an exponential semiring.

Example 3.2.

(1) Consider a semiring $S = B(5,0)$ with operation + and $\cdot$ defined by the following caley tables.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

.	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	4	1

Let $B = \{1,2,3,4\}$ be the multiplicative semigroup $(S \setminus \{0\}, \cdot)$. Define the action of S over B by the mapping $E : B \times S \to B$ given by $E(a, s) = a^s$ where $a \in B$ and $s \in S$. Then (S, B) forms an exponential semiring.

(2) Consider the semiring $S = (R^+ \cup \{0\}, +, \cdot)$. $R^+ = \{r \in S / r > 0\}$ be the multiplicative semigroup of S. Then (S, R^+) forms an exponential semiring under usual addition and multiplication.

Similarly (S, Q^+), (S, Z^+) are exponential semirings.

In the semiring action problem, dealt in[4] the authors have used the action of semiring on a semi module to exchange the keys. Here, we generalize the Diffie Hellman procedure using exponential semiring on a multiplicative monoid to share the key. Further, we use the action of a semiring on the additive monoid to encrypt the given plain text. The encrypted text will be shared by Alice to Bob. Bob will decrypt the message using the additive inverse of the common key to decrypt the message. The common key belongs to a sub semiring which possess both additive and multiplicative inverse.

Protocol for key sharing:

- Let S be an exponential semiring.
- Let B be a sub semigroup of $(S \setminus \{0\}, \cdot)$.
- Choose an element $x \in B$. This x is a public key.
- Consider the function $E : B \times S \to B$ defined by, $E(a, x) = x^a$ where $a \in S$ and $x \in B$.
- Now Alice chooses her private key $a \in S$. She computes x^a . She sends x^a to Bob.
- Bob chooses his private key, $b \in S$. He computes x^b . He sends x^b to Alice.
- Alice computes $(x^b)^a$ and Bob computes $(x^a)^b$.
- If $(x^b)^a = (x^a)^b$, then it is said that they have exchanged their private keys and their common key is $k = (x^b)^a = (x^a)^b$ which will be used to encrypt a given plaintext.

Define a mapping $\text{¤} : S \to B(n,i), 0 \le i \le n-1$ such that $\text{¤}(k)$ has additive inverse, $k \in S$.

Protocol for Encryption:

Let A be the set of alphabets of any language. Consider the plain text p . Let A_p is set of alphabets in p .

- Define $E : A_p \to B(n,i)$ such that $E(x) = j$ where j represents the order of x in A . Thus we have obtained the encoded message m.
- The encoded character j is encrypted as $j + \text{¤}(k)$ where k is the common key. In this way each alphabet of p is encrypted to obtain the ciphertext c .
- Alice sends c to Bob.
- Bob decrypts each character of c by adding the additive inverse of $\text{¤}(k)$ to obtain the characters in the encoded message m .
- Bob decodes the message by applying the function $D : R(A_p) \to A_p$ to obtain the corresponding alphabet of the plain text p .

In the above protocol for encryption we have used the additive action of the semiring $B(n,i)$ on the alphabet set A_p .

4. ILLUSTRATION

In this section we illustrate the protocol by an example. We consider the set A of upper case English alphabets and blank space.

Key Sharing:

- Let $S = B(27,0)$ be a semiring.
- Let $;\mathrm{B} = \{01, 02, 04, 05, 07, 08, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26\}$. B is a multiplicative sub semigroup of S .
- Let $x = 20 \in B.$
- Alice Chooses her private key as, $a = 21 \in S$. She calculate $x^a = 20^{21} = 08.$ She sends 08 to Bob.
- Bob chooses his private key as, $b = 15 \in S$ He calculate $x^b = 20^{15} = 17.$ He sends 17 to Alice.
- Common key $k = (x^b)^a = (x^b)^b.k = 17^{21} = 08^{15} = 26 \in B.$

Protocol for encryption:

Let A be set of upper case English alphabets.
Let the plain text be **HELLO**.
$A_p = \{H, E, L, O\}.$

- Define $E : A_p \to B(n,i)$ by $E(x) = j$ where j represents the order of x in A . $E(H) = 08; E(E) = 05; E(L) = 12; E(O) = 15.$ The encoded message is 0805121215.
- The encoded character j is encrypted as $j + ¤(k)$. Here encrypted characters are,
  08 + 26 = 07
  05 + 26 = 04
  12 + 26 = 11
  12 + 26 = 11
  15 + 26 = 14

Hence the cipher text c is 0704111114.

- Alice sends c to Bob.
- Bob decrypts each character of c by adding additive inverse of $¤(k)$. Decrypted characters are,
  07 + 01 = 08
  04 + 01 = 05
  11 + 01 = 12
  11 + 01 = 12
  14 + 01 = 15

Decrypted message is 0805121215.

- Bob decodes the message by using the function $D : R(A_p) \to A_p$ as follows: *D(08) = H; D(05) = E; D(12) = L; D(12) = L; D(15) = O:*
  Hence the Plain text is **HELLO**.

Attack: For the key $k \in B$ we find the orbit of *k* in *S*. If the size of the orbit is small it is very difficult to hack the message.

In the above example the value of *n* depends on the number of alphabets in the language chosen and *i* vary from 0 to $n-1$. Both Alice and Bob alone will know the language chosen and the corresponding *i*. Thus it becomes very hard for the Eve's dropper to hack the message.

5. CONCLUSION

In this paper we have studied the Diffie Hellman procedure for public key sharing using semiring action on a monoid or on a sub semiring. In future we apply the semiring action to discuss other protocols and to improve the efficiency of secured message transmission.

REFERENCES

1. David S. Dummit and Richard M. Foote: Abstract Algebra, Third Edition, John Wiley and Sons, Inc., (2004).
2. Di e W. and Hellman M. New directions in cryptography, IEEE Transactions, *Inform. Theory* 22, 472-492 (1976).
3. Jonathan S. Golan The Semirings and their Applications, Kluwer Academic Publishers-London.
4. Maze G., Monico C. and Rosenthal J: Public key Cryptography Based on Semigroup Actions, *Advances in Mathematics of Communications*, Vol.1, No.4, 489-507 (2007).
5. Sundar M., Victor P. and Chandramouleeswaran M.: Public key Cryptography-Key sharing with Semiring Action, *IJMSEA*, Vol.11, No.1, 195-204 (April, 2017).