Global Journal of Mathematical Sciences: Theory and Practical
ISSN 0974-3200 Volume 10, Number 1 (2018), pp. 37-42

http://www.irphouse.com

Elgamal Encryption Using Regular Semiring

V. Thiruveni

Saiva Bhanu Kshatriya College Aruppukottai -626101, Tamilnadu, India.

Abstract

In this paper we present a procedure to share secret key in a publickey cryptosystem using action of a semiring over a semimodule.

Keywords: Public key, Private key, Semiring, Semimodule and Semiring action

AMS Classification: 11 T71, 14G50, 94A 60

1. INTRODUCTION

The fundamental objective of cryptography is to enable two people, usually referred as Alice and Bob, to communicate over an insecure channel in such a way that an opponent cannot understand what is being said. There are two keys involved - Public key and Private key. Compemporary publlic key cryptography relies mainly on two different computational problems, the factorization of integers and the discrete logarithm in groups. Rosenthal and his team suggested a first protocol for a key exchange using semigroup action, as a generalization of the exponentiation in groups. In their paper, M.Sundar, P.Victor and M.Chandramouleeswaran [4] presented a generalization of Diffie-Hellmann key exchange protocol. They constructed semiring action on a finite left-semimodule over a semiring.

In this paper, I give Elgamol Encryption scheme based on that generalization of Diffie-Hellmann key exchange protocol.

2. PRELIMINARIES

In this section we recall some basic definitions of cryptography and semirings that are needed for our work.

Definition 2.1. *Let A denotes a finite set called alphabet of definition and M denotes the set called the message space which consists of strings of symbols from alphabet of*

definition. An element of M is called a plain text message.

Let C denotes a set called ciphertext space. It consisits of strings of symbols from the alphabet of definition which may differ from the alphabet of definition of M. An element of C is called a ciphertext.

Let K denotes the key space and whose elements are called keys.

A key specifies the transformation of plaintext into ciphertext, and vice versa. We can classify the key into two types- one is a publickey and the other is a private key. Public key is made available to everyone through publicly accessible directory and the private key must remain confidential to its respective owner.

Definition 2.2. *A one-to-one function f from a set M to a set C is called one-way if it is easy to compute* $f(m)$ *for all* $m \in M$*,but for a randomly selected* $c \in C$*,finding an* $m \in M$ *such that* $c = f(m)$*is computationally infeasible. In otherwords, we can easily compute f,but it is computationally infeasible to compute* f^{-1}.

Definition 2.3. *An Encryption function* e_k *is a mapping from M to C and a Decryption function* d_k *is a mapping from C to M such that* $d_k(e_k(x)) = x$*, for every* $x \in M$*. Let E denote the set of all encryption functions from M to C and D, the set of all decryption function from C to M.*

Definition 2.4. *A cryptosystem is defined as a five-tuple* (M,C,K,E,D) *where M,C,K,E,D are mentioned above.*

There are two types of cryptosystems based on the manner in which encryptiondecryption is carried out in the system.

(i) Symmetric key cryptosystem

(ii) Asymmetric or Publickey cryptosystem

The former one is the encryption process where same keys are used for encryption and decryption. But in the Publickey cryptosystem different keys are used for encryption and decryption

Definition 2.5. *A semiring is a non-empty set S together with two binary operations + and · such that*

(1) $(S,+)$ *is a commutative monoid with identity element* 0.

(2) $(S, \bullet)$ *is a semigroup.*

(3) *Multiplication distributes over addition from either sides.*

(4) $0r = 0 = r0, \forall r \in S$.

Definition 2.6. *A zero of a semiring S is an element* $^0 0^0$ *such that* $a+0 = 0+a = a$ *and* $a.0 = 0.a = 0$*, for all* $a \in S$*.A one of the semiring S is an element* $^0 1^0$ *such that* $a.1 = 1.a = a$*, for all* $a \in S$*.*

Definition 2.7. *A left-ideal I of S is a non-empty subset of S satisfying the following conditions:*

(1) *If* $a,b \in I$*,then* $a + b \in I$*,*

(2) *If* $a \in I, r \in S$ *then* $ra \in S$*,* (3) $1 \in / I$*.*

Definition 2.8. *Let S be a semiring. A left S -semimodule is a commutative monoid* $(M,+)$ *with additive identity* 0_M *for which we have a function* $S \times M \rightarrow M$*, denoted by* (r,m) $7\rightarrow$ *rm and called the scalar multiplication, which satisfies the following conditions :*

(1) $(rr')m = r(r'm)$;

(2) $r(m + m') = rm + rm'$;

(3) $(r + r')m = rm + r'm$;

(4) $r0_M = 0_M = 0_R m$.

If the semiring S consists of an unity 1 *in S then the semimodule M over S satisfies* $1 \cdot m = m \; \forall \; m \in M$*.*

Analogously we can define right semimodules over S.

Definition 2.9. *Let* $(S, \circ_S)$ *and* $(T, \circ_T)$ *are semigroups. Amorphism of semigroup is a map* $\varphi : (S, \circ_s) \rightarrow (TR, \circ_t)$ *such that*

$$\phi(s \circ_S s') = \phi(s) \circ_T \phi(t), \forall s, s' \in S.$$

If S,T has 1_S *and* 1_T *then* φ *is such that* $\varphi(1_S) = 1_T$*.*

Definition 2.10. *A congruence relation on a semiring S is a relation* $\sim$ *such that* $a \sim b$ *implies that* $ac \sim bc$*,* $cd \sim cb$*,* $a + c \sim b + c$*, and* $c + a \sim c + b$ *for all possible choice of a,b and c.*

Definition 2.11. *A semiring S is congruence-free or simple, if the only congruence relations are* $S \times S$ *and* $\{(a,a) \mid a \in S\}$*.*

Definition 2.12. (Group Action) *Let $A = (S,\bullet)$ be a semigroup and A a semimodule over S . Then a left semigroup action of A on M is a map from $A \times M \to M$ such that*

(1) $ex = x$

(2) $(ab)x = a(bx)$, $\forall\ a,b \in A, x \in M$

Definition 2.13. *An element 'a' of a semiring S is called multiplicatively regular if there exists an element 'b' of S satisfying aba = a.Such an element b is called a generalised inverse of a.*

A semiring S is multiplicatively regular if each element of S is multiplicatively regular.

Definition 2.14. *An element 'a' of a left S semimodule M is called additively regular if there exists an element 'b' of M satisfying a+b+a = a. Such an element b is called a generalised inverse of a.*

A left S semimodule M is additively regular if each element of M is additively regular.

3. ELGAMAL PUBLICKEY CRYPTOSYSTEM

(1) Alice chooses a multiplicatively regular semiring S and $s \in S$.She also choose an integer a and computes $\alpha = s^a$. She publish her publickey (s,α).

(2) Bob wishes to send Alice a message $m \in S$.He first obtains her publickey (s,α).

(3) Bob chooses a random integer b and computes $\beta = s^b$ and $\mu = m\alpha^b$. He sends the pair (β,μ) to Alice.

(4) Alice recovers m by computing $\mu\beta^{-a} = \mu s^{-ab} = m(s^a)^b s^{-ab} = m$.

Let us illustarte this protocol as in the following example.

Example 3.1. Let $S = \{a,b,c,d,e,f\}$ be a multiplicatively regular semiring with the following Cayley tables.

$+$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	c	d	e	f	a
c	c	d	e	f	a	b
d	d	e	f	a	b	c
e	e	f	a	b	c	d
f	f	a	b	c	d	e

$\bullet$	a	b	c	d	e	f
a	b	d	f	a	c	e
b	d	a	e	b	f	c
c	f	e	d	c	b	a
d	a	b	c	d	e	f
e	c	f	b	e	a	d
f	e	c	a	f	d	b

Then $(S,+,\bullet)$ is a multiplicatively regular semiring. a and b are generalized inverses of each other. Similarly e and f are generalized inverses of each other. c and d are generalized self inverses.

Alice choose $s = b \in S$ and a random integer $a = 5$ and computes $\alpha = s^a = b^5 = a$.

Alice publishes her public key $(s,\alpha) = (b,a)$

Now Bob wishes to send Alice a message $m = f \in S$.

Bob chooses a random integer $b = 7$and computes $\beta = s^b = b^7 = b$and$\mu = m\alpha^b = fa^7 = fa = e$ and sends the pair$(\beta,\mu) = (b,e)$to Alice.

Now Alice computes$\mu\beta^{-a} = e(b^{-1})^5 = ea^5 = eb = f$. Thus Alice receives the message $m = f$.

Remark 3.2. ElGamal encryption is closely related to the Diffie-Hellman key agreement protocol. Suppose (g^a,a) is the key pair generated by party A. Then if a party B sends a secret message to A, it sends g^b, retaining b secretly. Both the parties can compute the Diffie-Hellmann key g^{ab}, which is used to disquise the message m. The difference is that A's key a is here a long term secret key in contrast to the short term secret kys in the Diffie-Hellmann protocol.

Remark 3.3. In this encryption $E(m) = \{g^b, m, h^b\}$, the operation $m \cdot h^b$ can be replaced by any related group operation, say XOR.

4. EXTENDED ELGAMAL CRYPTOSYSTEM

Let $(s,+,\bullet)$ be a commutative semiring and $(M,\circ)$ be a multiplicatively regular Ssemimodule. Consider the semiring action on a semimodule. The Extended ElGamal cryptosystem is the following protocol:

(1) Alice chooses $a \in S, x \in M$ and computes $\alpha = ax$. She publishes her publickey (x,α).

(2) Bob wishes to send Alice a message $m \in M$.He first obtains her publickey (x,α).

(3) Bob choose a random integer $b \in S$ and computes $\beta = bx$ and $\gamma = (b\alpha) \circ m$ and sends the pair (β,γ) to Alice.

(4) Alice recovers m by computing $(\alpha\beta)^{-1} \circ \gamma = (abx)^{-1} \circ (bax \circ m) = (abx)^{-1} \circ (abx \circ m) = m$

Example 4.1. Let $S = B(5,3) = (\{0,1,2,3,4\}, \oplus, \odot)$ be a commutative semiring with the following Cayley tables.

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	3
2	2	3	4	3	4
3	3	4	3	4	3
4	4	3	4	3	4

$\odot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	4	4
3	0	3	4	3	4
4	0	4	4	4	4

Let $M = \{0,1,2\}$ be an additively regular left S-semimodule with the following operations:

$+$	0	1	2
0	0	1	2
1	1	0	2
2	2	2	0

$\circ$	0	1	2
0	0	0	0
1	0	1	2
2	0	1	1
3	0	1	2
4	0	1	2

(1) Alice chooses $a = 3 \in S$ and$x = 1 \in M$ and computes $\alpha = ax = 3 \cdot 1 = 1$. She publishes her publickey $(x,\alpha) = (1,1)$

(2) Bob wishes to send Alice a message$m = 2 \in M$.He first obtain Alice's publickey (1,1).

(3) Bob chooses$b = 4 \in S$ and copmputes$\beta = bx = 4 \cdot 1 = 1and\gamma = (\alpha + \beta) + m = (1 + 1) + 2 = 2$ and sends the keypair$(\beta,\gamma) = (1,2)$ to Alice.

(4) Alice recovers m by computing $-(\alpha+\beta)+\gamma = -(1+1)+2 = -0+2 = 2$.

5. CONCLUSION

The ElGamal cryptosystem is based on the discrete logarithm problem. It is nondeterministic since the ciphertext depends on both plaintext x and on the random number a chosen by Alice. So there will be many ciphertexts encrypted on the same plaintext. The cryptosystem described above is more secure whenever the size of the semiring and the choice of a is as large as possible.

REFERENCES

[1] Douglas R. Stinson: Cryptography Theory and Practice, CRC Press.

[2] Jonathan S. Golan: The Semirings and their Applications, Kluwer Academic PublishersLondan.

[3] Monico, C: Semirings and Semigroup Actions in publickey cryptography, Ph.D Thesis, University of Notre Dame, May 2002.

[4] Sundar M. Victor P, Chandramouleeswaran M: Public Key Cryptography – Key Sharing wtih Semiring Actioin, International J. of MAth. Sci. and Engg. Appls.,Vol.11, No.1, (April 2017), pp. 195-204.