International J. of Math. Sci. & Engg. Appls. (IJMSEA)
ISSN 0973-9424, Vol. 11 No. I (April, 2017), pp. 195-204

# PUBLICKEY CRYPTOGRAPHY - KEY SHARING WITH SEMIRING ACTION

**M. SUNDAR[1], P. VICTOR[2] AND M. CHANDRAMOULEESWARAN[3]**
[1] Sree Sowdambika College of Engineering, Aruppukottai, India.
[2] Mohamed Sathak Engineering College, Killakarai, India.
[3] Saiva Bhanu Kshatriya College, Aruppukottai, India.

**Abstract**

In this paper we present a generalised procedure for Diffie-Hellman key exchange problem to share secret key in a publickey cryptosystem using action of a semiring over a semimodule.

---

Key Words and Phrases : Public key, Private key, Semiring, Semimodule and Semiring action

2000 AMS Subject Classification : 11T71,14G50,94A60,16Y60.

# 1 Introduction

The brilliant and important cryptographic system is the RSA system which has the strange but extremely useful asymmetric property: There are two keys involved - Publickey and Private key. Each recipient of messages could have both the keys. The recipient announces his publickey to everyone but keeps the private key secret. Anyone can encode messages for a particular recipient using the publickey. However only someone with the knowledge of the private key can decode them.

Asymmetric cryptographic system used the notion of a (one way)trapdoor functions - functions whose outputs can be computed in a reasonable amount of time but whose inverses are inordinately difficult and time consuming to compute. Cryptographic systems based on trapdoor functions are now used in real world communications by governments, businesses and individuals, notably for secured transactions over internet.

The first step in a cryptosystem is to label all possible plaintext message units and all possible cyphertext message units by means of mathematical objects from which enciphering transformation and deciphering transformation can easily be constructed. There are several techniques available in the literature to construct these structural informations. In practice one can have an equipment for enciphering and deciphering which is constructed to implement only one type of crptosystem. Over a peroid of time the information about the type of system they are using be leakout. To increase the security, they need to change frequently the choice of parameters used with the system. The parameter is called a key(secret key).

The origin of using the discrete logarithmic problem in cryptographic schemes goes back to the seminal paper of Diffie and Helllman [1]. The discrete logarithm problem is the basic incredient of many cryptographic protocols. Given a finite group $G$ and elements $g, h \in G$,find a positive integer $n \in \mathbb{N}$ such that $g^n = h$. The above problem has a solution if and only if $h \in < g >$,the cyclic group generated by $g$.If $h \in < g >$ then there is a unique integer $n$ satisfying $1 \leq n \leq ord(g)$such that $g^n = h$. We call this unique integer the discrete logarithm of $h$ with base $g$ and we denote it by $log_g\ h$. Diffie

and Hellman proposed the DLP as a good source for a (one way)trapdoor function. In Diffie and Hellman method, using the DLP, two users agree on a secret cryptographic key using only an insecure channel of communication. Before the discovery of publickey systems the two parties wishing to communicate will meet beforehand to agree upon a secter key. This severly limits the spontaneity of secure communication and may require a courier. The Diffie-Hellman key selection protocol eliminates this problem. It is desccribed as follows: The key construction between two parties A and B proceeds as follows. Let M be a large integer (say $> 10^{40}$).

1. A chooses a random integer $x$ with $0 < x < M$,computes $g^x$ and sends the result to B, keeping $x$ secret.

2. B chooses a random integer $y$ with $0 < y < M$,computes $g^y$ and sends the result to A, keeping $y$ secret.

3. Both A and B construct the key from $g^{xy}$, which A computes from $(g^y)^x$ and B computes from $(g^x)^y$.

If this scheme is to be secure then the problem of computing $g^{xy}$ from knowledge of $g, g^x$and $g^y$should be interactable. We shall refer this problem as the Diffie-Hellman problem. It is clear that solving the underlying discrete logarithm problem is sufficient for breaking the Diffie-Hellman protocol. For this reason researchers have been searching for groups where the discrete logarithm problem is considered a computationally difficult problem. In the literature many groups have been proposed as candidates for studying the discrete logarithm problem.The discrete logarithm problem over a group can be seen as a special instance of an action by a semigroup. The interesting thing is that every semigroup action by an abelian group gives rise to a Diffie-Hellman key exchange. The generalisation of the original Diffie-Hellman key exchange in $(\mathbb{Z}/p\mathbb{Z})^*$found a new depth when Koblitz [4] suggested that such a protocol could be used with the group over an elliptic curve.

The idea of using semigroup actions for the purpose of buiding one-way trapdoor function is not a new one and it appeared in one way or the other in several

papers[5],[6],[7]. In this paper, we present a generalisation of the Diffie-Hellman key exchange protocol. Crucial for this generalisation is the semigroup actions on finite sets. Our main aim will be the semigroup actions built from multiplicative structure on semirings, acting on finite semimodules over semirings. In particular, we construct semiring action on a finite left-semimodule over a semiring. The setup is general enough that it includes the Diffie-Hellman protocol over a general finite left semimodule.

## 2 Preliminaries

In this section we recall some basic definitions from cryptosystem and semirings that are needed for our work. [2] Let $A$ denote a finite set called alphabet of definition and $M$ denote 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 $C$ denote 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.

[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 $f^{-1}$. [2] A key is a piece of information or a parameter that determines the functional output of a cryptographic algorithm. A key specifies the transformation of plaintext into ciphertext, and vice versa. Let $K$ denote the key space which consists of a set of keys. 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. [2] 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 functions from $C$ to $M$.

[2] 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 encryption-decryption 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

[3] A semiring is a non-empty set $S$ together with two binary operations $+$ and $\cdot$ such that

1. $(S, +)$ is a commutative monoid with identity element 0.
2. $(S, \cdot)$ is a moniod with 1.
3. Multiplication distributes over addition from either sides.
4. $0r = 0 = r0, \forall r \in S$.

[3] A left-ideal $I$ of $S$ is a non-empty subset of $S$ satisfying the following conditions:

1. $1 \notin I$.
2. If $a, b \in I$,then $a + b \in I$,
3. If $a \in I, r \in S$ then $ra \in S$,

Analogously we can define right-ideal of a semiring. [3] 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 $S \times M \to M$, denoted by $(r, m) \mapsto rm$ 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 $S$. **(Group Action)**[5] Let $A = (S, \cdot)$ 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. $(ab)x = a(bx), \ \forall \ a, b \in A, x \in M$

**(Semiroup Action Problem)**[5] Given a semigroup $G$ acting on a set $S$and elements $x \in S$and $y \in Gx$,find $g \in G$such that $gx = y$.

## 3 Key Sharing with semiring Actions

In this section we describe a procedure to share the secret key in a publickey cryptosystem using semiring action on a semimodule. We start with the following definitions. Let $S$ be a semiring and $M$ be a semimodule over $S$.The mapping $S \times M \to M$is said to be an action of $S$ on $M$if the following conditions are satisfied:

1. $s_1(s_2m) = (s_1s_2)m$;
2. $(s_1 + s_2)m = s_1m + s_2m$;
3. $s_1(m + n) = s_1m + s_1n$, for all $s_1, s_2 \in S$ and $m, n \in M$.

A semigroup M is said to be bicyclic if for any $x \in M$,there exists two elements $a, b$ such that $x = a^m b^n$ for some $m, n \in \mathbb{N}$. We consider two commutative semirings $S_1$ and $S_2$ and $M_1$ is a $S_1-$left semimodule and $M_2$ is a $S_2-$left semimodule.
Then $A = S_1 \times S_2$ is a commutative semiring and $M = M_1 \times M_2$ is a left semimodule of A. Define $\phi : A \times M \to M$ by

$$\phi[(f, g), (m_1, m_2)] \mapsto (fm_1, gm_2), \forall f \in S_1, g \in S_2, m_1 \in M_1, m_2 \in M_2.$$

Then $\phi$ is a semiring action on $M$. Now define

$$\phi_{S_1} : A \times M \to M \ by \ \phi_{S_1}[(f, g), (m_1, m_2)] \mapsto (fm_1, m_2)$$

$$\phi_{S_2} : A \times M \to M \text{ by } \phi_{S_2}[(f,g),(m_1,m_2)] \mapsto (m_1, gm_2.)$$

**Protocol:**

Let $A = S_1 \times S_2$ be a commutative semiring, $M = M_1 \times M_2$ be a left semimodule of A, and $\phi_{S_1}, \phi_{S_2}$ are semiring actions on $M$. Then the key exchange in $(A, M, \phi_{S_1}, \phi_{S_2})$ is the following protocol.

1. Alice and Bob publicly agree on an element $m = (m_1, m_2) \in M$
2. Alice chooses $(s_1, s_2) \in A$ and computes $\phi_{S_1}[(s_1, s_2)(m_1, m_2)]$. Alice's private key is $(s_1, s_2)$, her public key is $\phi_{S_1}[(s_1, s_2)(m_1, m_2)]$.
3. Bob chooses $(t_1, t_2) \in A$ and computes $\phi_{S_2}[(t_1, t_2)(m_1, m_2)]$. Bob's private key is $(t_1, t_2)$, his public key is $\phi_{S_2}[(t_1, t_2)(m_1, m_2)]$.
4. Their common secret key is then

$$\phi_{S_1}[(s_1, s_2)\phi_{S_2}(t_1, t_2)(m_1, m_2)] = \phi_{S_1}[(s_1, s_2)(m_1, t_2 m_2)] = (s_1 m_1, t_2 m_2)$$

$$\phi_{S_2}[(t_1, t_2)\phi_{S_1}(s_1, s_2)(m_1, m_2)] = \phi_{S_2}[(t_1, t_2)(s_1 m_1, m_2)] = (s_1 m_1, t_2 m_2)$$

This protocol is illustrated by the following example: Let $S_1 = B(5,3) = (\{0,1,2,3,4\}, \oplus, \odot)$ be a 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 $M_1 = \{e_1, x, y\}$ be an $S_1-$semimodule under addition and scalar multiplication defined by the following cayley table:

| $+$ | $e_1$ | $x$ | $y$ |
|---|---|---|---|
| $e_1$ | $e_1$ | $x$ | $y$ |
| $x$ | $x$ | $x$ | $e_1$ |
| $y$ | $y$ | $e_1$ | $y$ |

| $*$ | $e_1$ | $x$ | $y$ |
|---|---|---|---|
| 0 | $e_1$ | $e_1$ | $e_1$ |
| 1 | $e_1$ | $x$ | $e_1$ |
| 2 | $e_1$ | $x$ | $e_1$ |
| 3 | $e_1$ | $x$ | $e_1$ |
| 4 | $e_1$ | $x$ | $e_1$ |

Let $S_2 = B(4,2) = (\{0,1,2,3\}, \oplus, \odot)$ be a semiring with the following Cayley tables.

| $\oplus$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 2 |
| 2 | 2 | 3 | 2 | 3 |
| 3 | 3 | 2 | 3 | 2 |

| $\odot$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 2 | 2 |
| 3 | 0 | 3 | 2 | 3 |

Let $M_2 = \{e_2, a, b, c\}$be an $S_2-$semimodule under addition and scalar multiplication defined by the following cayley table:

| $+$ | $e_2$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e_2$ | $e_2$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $a$ | $b$ | $b$ |
| $b$ | $b$ | $b$ | $b$ | $a$ |
| $c$ | $c$ | $b$ | $a$ | $c$ |

| $*$ | $e_2$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| 0 | $e_2$ | $e_2$ | $e_2$ | $e_2$ |
| 1 | $e_2$ | $e_2$ | $e_2$ | $e_2$ |
| 2 | $e_2$ | $b$ | $b$ | $e_2$ |
| 3 | $e_2$ | $b$ | $b$ | $e_2$ |

Let $A = S_1 \times S_2$ be the semiring with the operations $\oplus$ and $\odot$ defined componentwise. Let $M = M_1 \times M_2$ be the semimodule over $A$. Let $(x, b) \in M$ be the public key.

Alice chooses $(2,3) \in A$ as her private key and calculates

$$\phi_{S_1}[(2,3),(x,b)] = (2x,b) = (x,b)$$

and sends it to Bob. Bob chooses $(3,1) \in A$ as his private key and calculates

$$\phi_{S_2}[(3,1),(x,b)] = (x,1b) = (x,e_2)$$

and sends it to Alice. Now Alice calculates

$\phi_{S_1}((2,3),(x,e_2)) = (2x,e_2) = (x,e_2)$Bob calculate

$\phi_{S_2}((3,1),(x,b)) = (x,1.b) = (x,e_2)$Since 3 and 3 are equal Allice and Bob have exchanged the secret key.

Let $S_1$ and $S_2$ and $A = S_1 \times S_2$ be the semirings as in the previous example. Let $M_1 = \{0,3,4\}$ be a left ideal of $S_1$and let $M_2 = \{0,2,3\}$ be a left ideal of $S_2$. Then $M = M_1 \times M_2$ is a left semi-module over $A$.

Let $(3,2) \in M$ be the public key. Alice chooses $(1,3) \in A$ as her private key and calculates $\phi_{S_1}[(1,3),(3,2)] = (1.3,2) = (3,2)$ and sends it to Bob. Bob chooses

$(1,0) \in A$ as his private key and calculates $\phi_{S_2}[(1,0),(3,2)] = (3,0.2) = (3,0)$ and sends it to Alice.

Now Alice calculates

$\phi_{S_1}((1,3),(3,0)) = (1.3,0) = (3,0)$Bob calculates

$\phi_{S_2}((1,0),(3,2)) = (3,0.2) = (3,0)$Since 3 and 3 are equal both Allice and Bob have exchanged the secret key.

**Problem (Semiring Action Problem (SAP)):** 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 $r = (r_1, r_2) \in \phi_{S_1}(An)$ $(or)$ $\phi_{S_2}(An)$, find $q = (q_1, q_2) \in A$ such that $\phi_{S_1}(qn) = r$ (or) $\phi_{S_2}(qn) = r$.

**Generic Attacks of SAP:** If an attacker, Eve, can find an $\alpha = (\alpha_1, \alpha_2) \in A$ such that $(\alpha_1, \alpha_2)(m_1, m_2) = (s_1, s_2)(m_1, m_2)$, then Eve may find the shared secret by computing

$$\begin{aligned}
\phi_{S_1}[(\alpha_1,\alpha_2)\phi_{S_2}[(t_1,t_2)(m_1,m_2)]] &= (\phi_{S_1}[(\alpha_1,\alpha_2)]\phi_{S_2}[(t_1,t_2)])\,(m_1,m_2) \\
&= \phi_{S_2}[(t_1,t_2)]\,(\phi_{S_1}[(\alpha_1,\alpha_2)(m_1,m_2)]) \\
&= \phi_{S_2}[(t_1,t_2)]\,(\phi_{S_1}[(s_1,s_2)(m_1,m_2)]) \\
&= \phi_{S_2}[(t_1,t_2)]\,(s_1m_1,m_2) \\
&= (s_1m_1,t_2m_2)
\end{aligned}$$

Eve computes $\phi_{S_1}(rm)$ for all possible $r = (r_1, r_2) \in A$ intil she finds some $\alpha = (\alpha_1, \alpha_2)$ with $\phi_{S_1}[(\alpha_1, \alpha_2)(m_1, m_2)] = \phi_{S_1}[(s_1, s_2)(m_1, m_2)]$
Then she is able to break the system as explained above. To avoid this attack, Bob and Alice must choose $A$ and $M$ sufficiently large and select a good candidate for $m = (m_1, m_2)$,such that the size of the set

$$A_{Eve} = \{\alpha \in A \mid \phi_{S_1}[(\alpha_1, \alpha_2)(m_1, m_2)] = \phi_{S_1}[(s_1, s_2)(m_1, m_2)]\}$$

is small with respect to the size of $A$.
Define $Stab(m) = \{q \in A \mid qm = m\}$ ,the subsemiring of $A$. One can observe thet $A_{Eve}$is simply a left coset of $Stab(m)$. Now $A_{Eve}$ will be small in size if $A/Stab(m)$ is large or in other words $Stab(m)$ is small in size with respect to the size of $A$. This is true since

every element $\alpha \in Stab(m)$ has the property that $\alpha \in A_{Eve}$, that is $r\ Stab(m) \subset A_{Eve}$. Consider $S_1, S_2$ and $M_1, M_2$ as in the previous example. Let $(3,2) \in M$ be the public key. Alice chooses $(1,3) \in A$ as her private key and calculates $\phi_{S_1}((1,3),(3,2)) = (3,2)$. Now Eve chooses $(3,3) \in A$ and calculates $\phi_{S_1}((3,3),(3,2)) = (3,2)$. Then Eve may find the shared secret by computing $\phi_{S_1}[(3,3)\phi_{S_2}[(4,2)(3,2)]] = (3,4)$ and break the cryptosystem.

Here $A_{Eve} = \{(1,3),(3,3)\}$ and $Stab(3,2) = \{(1,3),(3,3)\}$ . To avoid the attack by Eve, Alice and Bob choose $A$ and $M$ sufficiently large and select $m \in M$ such that the size of $A_{Eve}$ is small with respect to the size of $A$. If one has the ability to compute efficiently the canonical representatives for the right coset $a\ Stab(m)$ this computed value could potentially be used to an attacker's advantage. However, we use the linear action of commutative semirings on semi modules, so that the above task become difficult.

## References

[1] **Diffie W. and Hellman M.:**New directions in cryptography, IEEE Transactions, Inform.theory 22(1976),472-492.

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

[3] **Jonathan S. Golan:** The Semirings and their Applications, Kluwer Academic Publishers-Londan.

[4] **Koblitz N.:** Elliptic curve cryptosystems, Math. Comp., 48 (1987), 203209.

[5] **Maze G., Monico C. and Rosenthal J.:** Public key Cryptography Based On Semigroup Actions, Advances in Mathematics of Communications, Vol.1, No.4 (2007), 489-507.

[6] **Shpilrain V. and Ushakov A.:** Thompsons group and public key cryptography, in Third International Conference, ACNS 2005, 3531, Lecture Notes in Comput. Sci., Springer, Berlin, 2005, 151163.

[7] **Yamamura A.** Public-key cryptosystems using the modular group in Public Key Cryptography, Lecture Notes in Computer Science, 1431, Springer, Berlin, 1998, 203216.