ADV MATH SCI JOURNAL

Advances in Mathematics: Scientific Journal **9** (2020), no.3, 1271–1279
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.3.71 Spec. Issue on ICNTMMA

SEMIRING ACTIONS FOR MULTIPLE KEY SHARING IN PUBLIC KEY CRYPTOGRAPHY

S. NIVETHA[1] AND M. CHANDRAMOULEESWARAN

ABSTRACT. In this paper we discuss the semiring action problem for a public key symmetric cipher model where the action of the semiring, not necessarily commutative, on a multiplicative left (right or two sided) ideal of the semiring.

1. INTRODUCTION

In the present scenerio, the security of data transmission plays a vital role. It is susceptible to attack by hackers. In [1] Diffie Hellman developed a protocol to share the public key which is a generalization of DLP. To improve the security using a public key encryption, in [6] the authors extended the semigroup action problem into a semiring action problem by using the action of semiring on a semi module. Recently, in our paper [5], we have used the action of a semiring over a multiplicative sub semi group where the semiring under consideration is an exponential semiring. In this paper, we consider the action of a semiring, not necessarily an exponential semiring or a commutative semiring, on a multiplicative left or right ideal of the semiring to share the common key. We develop a procedure to encrypt a plain text that consists of several instructions that has to be sent. Each instruction is considered as a block B_i. We use keys k_i for encrypting each block B_i or we can use the same key k to encrypt all the

[1] *corresponding author*

2010 *Mathematics Subject Classification.* 16Y60, 12K10, 11T71, 14G50, 94A60.

Key words and phrases. Semirings, Semiring Action, Multiplicative Left Ideal, Encryption, Decryption.

blocks. The cipher text c_i need not be sent linearly. Each cipher text c_i can be represented as an ordered pair $(k_i, B_i).(i.e.)$ $c_i(k_i, B_i)$ where k_i is the common key corresponding to the block $B_i,$ that represent some instruction. We develop this algorithm in the third section and illustrate it with an example. The second section contains the preliminary concepts required.

2. PRELIMINARIES

In this section, we recall some fundamendal concepts that are required for sequal. Cryptography provides us secret communication between two parties sharing some information. Two parties share some secret information called a $key.$ Using this key they communicate secretly with each other. A party sending a message uses the key to $encrypt$ the message before it is sent, and the receiver uses the same key to $decrypt$ and recover the message upon receipt. The message itself is called the $plaintext$ and the scrambled information that is actually transmitted from the sender to the receiver is called the $ciphertext.$ The process of encrypting the plaintext to ciphertext is called $encryption$ and the process of decrypting the ciphertext to plaintext is called $decryption.$ A function which is easy to compute but hard to invert is known as a $trapdoor function.$

Definition 2.1. *[2] A semiring is a nonempty set S on which operations of addition and multiplication have been defined such that ,$(S, +, 0)$ is a monoid, $(S, \cdot)$ is a semigroup, Multiplication distributes over addition from either side, $0s = 0 = s0$ for all $s \in S$. A semiring $(S, +, \cdot)$ is said to have a unit element if there exists an element $1 \neq 0$ belonging to S such that $1 \cdot s = s \cdot 1 = s$ for all $s \in S$.*

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

Definition 2.2. *A semiring $(S, +, \cdot)$ is said to be additively commutative if $(S, +)$ is a commutative monoid; is said to be multiplicatively commutative if $(S, \cdot)$ is a* *commutative semigroup. A semiring $(S, +, \cdot)$ is said to be a commutative semiring if it is both additively and multiplicatively commutative.*

Definition 2.3. *[2] Consider a semiring $(S, +, \cdot)$. A non empty subset A of S is said to be a sub semiring if $(A, +, \cdot)$ is itself a semiring under the induced operations.*

Definition 2.4. *Consider a semiring $(S, +, \cdot)$. $\phi \neq A \subseteq S$ is called an ideal (two sided) such that, $1 \notin A$, $x + a, a + x \in A$, $xa, ax \in A$ for all $x \in S$ and $a \in A$.*

Definition 2.5. *[2] Consider a semiring $(S, +, \cdot)$. Let $a \in S$. The multiplicative order (additive order) of a is the least positive integer n such that $a^n = 1$ ($na = 0$). It is denoted by $o(a) = n$.*
Consider a semiring $(S, +, \cdot)$. Let $a \in S$. An element $0 \neq b \in S$ is said to be an additive inverse of a if $a + b = 0 = b + a$.
Consider a semiring $(S, +, \cdot)$. Let $0 \neq a \in S$. An element $b \in S$ is said to be a multiplicative inverse of a if $ab = 1 = ba$.

Definition 2.6. *[6] (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 $r = (r_1, r_2) \in \phi_{S_1}(A_n)$ or $\phi_{S_2}(A_n)$, find $q = (q_1, q_2) \in A$ such that $\phi_{S_1}(q_n) = r$ or $\phi_{S_2}(q_n) = r$*

3. Semiring Actions for Publickey Cryptography

In this section we discuss the Diffie Hellman protocol by using the action of a semiring over a multiplicative left ideal of the semiring. We start with the following:

Definition 3.1. *Consider a semiring $(S, +, \cdot)$. $\phi \neq A \subseteq S$ is said to be additively left (right) ideal of S if $s + a \in A$ ($a + s \in A$) for all $s \in S$ and $a \in A$. A is said to be multiplicatively left (right) ideal of S if $sa \in A$ ($as \in A$) for all $s \in S$ and $a \in A$ and $1 \notin A$. A is said to be left (right) ideal if it is both additively left (right) and multiplicatively left (right) ideal of S.*

Alice and Bob accept the language they wish to communicate. Let A be the set of alphabets of that language including the blank space and $|A| = n$. Moreover they accept the semiring S and $B(n, i), 0 \leq i \leq n - 1$.

Protocol for key sharing:
Let S be a semiring. Let $\phi : S \to B(n,i)$ be a set mapping used to share key. Let B be a multiplicative left (right or two sided) ideal of S. Choose an element $Y \in B$, as a public key. Define $E : S \times B \to B$ where $E = \phi \times \phi|_B : B(n,i) \times B(n,i) \to B(n,i)$ by $E(a,x) = (\phi \times \phi|_B)(a,x) = \phi(a)\phi|_B(x)$. Alice chooses her private key as $X_A \in S$. She calculates $E(X_A, Y) = \phi(X_A)\phi|_B(Y)$. Then she sends $E(X_A, Y)$ to Bob. Bob chooses his private key as $X_B \in S$. He computes $E(X_B, Y) = \phi(X_B)\phi|_B(Y)$.Then he sends $E(X_B, Y)$ to Alice. Now $k = E(X_B, Y)\phi(X_A) = E(X_A, Y)\phi(X_B)$ will be the common key if k is invertible in $B(n,i)$.

Protocol for Encoding and Encryption:
Let $S(A)$ be the set of all possible strings from the set of alphabets A. $S^*(A) \subseteq S(A)$ where $S^*(A)$ be the set of all strings that convey meaningful message. Let $subS^*(A) =$ set of all subsets of $S^*(A)$.
For any $L_1, L_2 \in subS^*(A)$, define

- $L_1 + L_2 = L_1 \cup L_2$;
- $L_1 \times L_2 = \{w_1 w_2 / w_1 \in L_1, w_2 \in L_2\}$.

Then $(sub(S^*(A)), +, \times)$ becomes a semiring with empty set as the zero element 0 and $\{\Box\}$ as the multiplicative identity.

Encoding and Encryption:
Consider a plaintext p. Let A_p be the set of alphabets in the plaintext p, so that $A_p \in sub(S^*(A))$ is a semiring. Define $\psi : A_p \to B(n,i)$ where $0 \leq i \leq n-1$ by $\psi(x) = j$ where j is the alphabetical order of x in A. By this way Alice encodes each character of the plaintext p and gets the encoded message m. Each encoded character of m is encrypted as $j \times (k)^{o(k)-1}$ where $o(k)$ is the order of k in $B(n,i)$. In this way each character of m is encrypted to obtain the ciphertext c. Now Alice sends c to Bob.

Decryption and Decoding:
Bob receives the ciphertext c and he decrypts each character of c by $c_i \times k$ where c_i is a character of c. After decrypt all the characters in the ciphertext c, Bob gets the encoded message m. Using the function $\psi^{-1} : B(n,i) \to A_p$ Bob decodes the message m and obtain the plaintext p.

Hardness of the problem:
Assume that we are implementing a symmetric cipher model with a common

key k. Suppose now that an eavesdropper Eve wishes to find the common key k. Eventhough Eve knows the finite semiring S, the public key $Y, E(X_A, Y)$ and $E(X_B, Y)$, there is no obvious way for her to find k without knowing the private keys: either X_A or X_B. Moreover the determination of k depends on the trapdoor function ϕ. Number of such functions is given by $|B(n,i)|^{|S|}$. Among these functions it is harder to determine the function ϕ such that $\phi(B)$ is a sub semiring of $B(n,i)$ for any multiplicative ideal B of S. Thus the problem of finding k in this symmetric model is very hard. Thus Alice and Bob can probably share the common key in a smart way so that Eve will not be able to find k. Then both Alice and Bob are free to use k as the common key for their favorite cipher and communicate securely with each other.

Illustration:
We illustrate the above protocol for Key sharing as well as Encryption and Decryption by an example.
Let us choose the English language for communication. Let A be the set of all upper case English alphabets including blank space. Hence $|A| = n = 27$ then we need to consider the semiring $B(n,i)$ where $0 \leq i \leq 26$. Now choose $i = 2$, so that the semiring $B(n,i) = B(27,2)$.

Key sharing:
Let $S = (\{0, a, b, c\}, +, \cdot)$ be a semiring where addition and multiplication operators are defined as

+	0	a	b	c
0	0	a	b	c
a	a	a	b	c
b	b	b	b	b
c	c	c	b	c

·	0	a	b	c
0	0	0	0	0
a	0	0	a	0
b	0	a	b	c
c	0	0	c	c

Define $\phi : S \to B(27,2)$ by, $\phi(0) = 00$; $\phi(a) = 04$; $\phi(b) = 01$; $\phi(c) = 23$; Let $B = \{0, a, c\}$ be the multiplicative left ideal of S. Let $Y = c \in B$ be the public key and $\phi(Y) = 23$. Define $E : S \times B \to B$ where $E = \phi \times \phi|_B : B(n,i) \times B(n,i) \to B(n,i)$ by $E(a,x) = (\phi \times \phi|_B)(a,x) = \phi(a)\phi|_B(x)$. Alice chooses her private key as $X_A = a \in S$ and $\phi(X_A) = \phi(a) = 04$. She computes $E(X_A, Y) = \phi(X_A)\phi|_B(Y) = 04 \cdot 23 = 17$. She sends 17 to Bob. Bob chooses his private key as $X_B = b \in S$ and $\phi(X_B) = \phi(b) = 01$. He computes $E(X_B, Y) =$

$\phi(X_B)\phi|_B(Y) = 01 \cdot 23 = 23$.He sends 23 to Alice. Now the common key k is $E(X_B, Y)\phi(X_A) = 23 \cdot 04 = 17 = 17 \cdot 01 = E(X_A, Y)\phi(X_B)$. Hence $k = 17$ which is invertible in $B(27, 2)$.

Encoding and Encryption

Let the plaintext p be **WELCOME**. Define $\psi : A_p \to B(27, 2)$ where $A_p = \{W, E, L, C, O, M\}$ by $\psi(W) = 23$, $\psi(E) = 05$, $\psi(L) = 12$, $\psi(C) = 03$, $\psi(O) = 15$, $\psi(M) = 13$. Hence the encoded message $m = 23051203151305$. Each character of m is encrypted as $j \times (k)^{o(k)-1}$ where $o(k)$ is the order common key in $B(n, i)$. Here $o(17)$ in $B(27, 2)$ is 20. Hence $(17)^{19} = 03$. Thus Alice sends the ciphertext $c = 19151109201415$ to Bob. Bob decrypts each character of c by $c_i \times k.$ and gets the decrypted message as $m = 23051203151305.$ Bob decodes each character of m by using the function $\psi^{-1} : B(n, i) \to A_p$ and gets the plaintext as **WELCOME.** The key used for locking depends on order of the key on $B(n, i)$ and when the order of the key is very large we lock the plaintext by $o(k) - 1$ times. Finding such a key depends on the trapdoor function ϕ this makes the problem very harder.

4. Publickey cryptography using multiple keys

In [4] the authors have discussed the authenticated key distribution using number theory - Pell's Equation. In this section we introduce a public key symmetric cipher model using multiple keys to ensure the security of communication as well as to find the error that occur in the transmission. Thus the protocol described in section three can be generalized.

Alice and Bob accept the language they wish to communicate. Let A be the set of alphabets of that language including the blank space and $|A| = n.$ Moreover they accept the semiring S_1, S_2 and $B(n, i), 0 \leq i \leq n - 1.$

Key Sharing

Let S_1 and S_2 be two semirings. Let $\phi_1 : S_1 \to B(n, i)$ and $\phi_2 : S_2 \to B(n, i)$ be a mapping where $0 \leq i \leq n - 1$, used to share keys. Let B_1 and B_2 be multiplicative left (right or two sided) ideals of S_1 and S_2 respectively. choose an element $Y = (Y_1, Y_2) \in B_1 \times B_2$. This Y is a public key. Define $E : (S_1 \times B_1) \times (S_2 \times B_2) \to B_1 \times B_2$ where $E = (\phi_1 \times \phi_1|_{B_1}) \times (\phi_2 \times \phi_2|_{B_2})$ by $E((a_1, x_1), (a_2, x_2)) = (\phi_1(a_1) \cdot \phi_1|_{B_1}(x_1), \phi_2(a_2) \cdot \phi_2|_{B_2}(x_2))$ where $(a_1, x_1) \in S_1 \times B_1$ and $(a_2, x_2) \in S_2 \times B_2$. Alice chooses her private key as $X_A = (X_{A_1}, X_{A_2}) \in S_1 \times S_2$. She

calculates $E((X_{A_1}, Y_1), (X_{A_2}, Y_2)) = (\phi_1(X_{A_1}) \cdot \phi_1|_{B_1}(Y_1), \phi_2(X_{A_2}) \cdot \phi_2|_{B_2}(Y_2))$. Then she sends $E((X_{A_1}, Y_1), (X_{A_2}, Y_2))$ to Bob. Bob chooses his private key as $X_B = (X_{B_1}, X_{B_2}) \in S_1 \times S_2$. He calculates $E((X_{B_1}, Y_1), (X_{B_2}, Y_2)) = (\phi_1(X_{B_1}) \cdot \phi_1|_{B_1}(Y_1), \phi_2(X_{B_2}) \cdot \phi_2|_{B_2}(Y_2))$. Then she sends $E((X_{B_1}, Y_1), (X_{B_2}, Y_2))$ to Alice. Now $k = (k_1, k_2) = E((X_{B_1}, Y_1), (X_{B_2}, Y_2)) \cdot (\phi_1 \times \phi_2)(X_{A_1}, X_{A_2}) =$
$E((X_{A_1}, Y_1), (X_{A_2}, Y_2)) \cdot (\phi_1 \times \phi_2)(X_{B_1}, X_{B_2})$

Encoding and Encryption

Consider a plaintext p. Let A_p be the set of all alphabets in the plaintext p. The plaintext can be encoded twice, represented by blocks B_1 and B_2 respectively. Then the ciphertext c contains two parts c_1 and c_2 that is, $c = (c_1, c_2)$ where $c_1 = (B_1, k_1)$ and $c_2 = (B_2, k_2)$. Each character c_{1_i} of c_1 is encrypted as before (i.e.) $c_{1_i} = j_i \cdot (k_1)^{o(k_1)-1}$. Similarly $c_{2_i} = j_i \cdot (k_2)^{o(k_2)-1}$. By this way Alice sends the ciphertext $c = (c_1, c_2)$. Bob decrypts the ciphertext by $(c_1 \cdot k_1, c_2 \cdot k_2)$ and decodes it get the plaintext as (p_1, p_2).

If $p_1 = p_2$ then they conclude that the correct message has been received.

Illustration 1

Let A be the set of all upper case English alphabets including blank space. Hence $|A| = n = 27$ and $0 \leq i \leq 26$. Let $i = 2$.

Key Sharing:

Let $S_1 = (\{0, a, b, c\}, +, \cdot)$ be a semiring where addition and multiplication operators are defined as

$+$	0	a	b	c
0	0	a	b	c
a	a	a	b	c
b	b	b	b	b
c	c	c	b	c

$\cdot$	0	a	b	c
0	0	0	0	0
a	0	0	a	0
b	0	a	b	c
c	0	0	c	c

Let $S_2 = (\{0, d, e\}, +, \cdot)$ be a semiring where addition and multiplication operators are defined as

$+$	0	d	e
0	0	d	e
d	d	d	e
e	e	e	e

$\cdot$	0	d	e
0	0	0	e
d	0	d	e
e	0	e	e

Define $\phi_1 : S_1 \to B(27, 2)$ and $\phi_2 : S_2 \to B(27, 2)$ by,

$\phi_1(0) = 0; \phi_1(a) = 04; \phi_1(b) = 01; \phi_1(c) = 23$ and $\phi_2(0) = 0; \phi_2(d) = 01; \phi_2(e) =$

19. Let $B_1 = \{0, a, c\}$ be the multiplicative left ideal of S_1 and $B_2 = \{0, e\}$ be the multiplicative left ideal of S_2. Let $Y = (Y_1, Y_2) = (c, e) \in B_1 \times B_2$ be the public key. Define $E : (S_1 \times B_1) \times (S_2 \times B_2) \to B_1 \times B_2$ where $E = (\phi_1 \times \phi_1|_{B_1}) \times (\phi_2 \times \phi_2|_{B_2})$ by $E((a_1, x_1), (a_2, x_2)) = (\phi_1(a_1) \cdot \phi_1|_{B_1}(x_1), \phi_2(a_2) \cdot \phi_2|_{B_2}(x_2))$ where $(a_1, x_1) \in S_1 \times B_1$ and $(a_2, x_2) \in S_2 \times B_2$. Alice chooses her private key as $X_A = (X_{A_1}, X_{A_2}) = (a, d) \in S_1 \times S_2$ and $(\phi_1 \times \phi_2)(a, d) = (04, 01)$. She computes $E((X_{A_1}, Y_1), (X_{A_2}, Y2)) = E((a, c), (d, e)) = (\phi_1(a) \cdot \phi_1|_{B_1}(c), \phi_2(d) \cdot \phi_2|_{B_2}(e)) = (04 \cdot 23, 01 \cdot 19) = (17, 19)$ and sends $(17, 19)$ to Bob. Bob chooses his private key as $X_B = (X_{B_1}, X_{B_2}) = (b, e) \in S_1 \times S_2$ and $(\phi_1 \times \phi_2)(b, e) = (01, 19)$ He computes $E((X_{B_1}, Y_1), (X_{B_2}, Y2)) = E((b, c), (e, e)) = (\phi_1(b) \cdot \phi_1|_{B_1}(c), \phi_2(e) \cdot \phi_2|_{B_2}(e)) = (01 \cdot 23, 19 \cdot 19) = (23, 11)$ and sends $(23, 11)$ to Alice. Now the common key $k = (k_1, k_2)$ is

$$E((X_{B_1}, Y_1), (X_{B_2}, Y2)) \cdot \phi_1 \times \phi_2(X_{A_1}, X_{A_2}) = (23, 11) \cdot (04, 01) = (17, 11)$$
$$E((X_{A_1}, Y_1), (X_{A_2}, Y2)) \cdot \phi_1 \times \phi_2(X_{B_1}, X_{B_2}) = (17, 19) \cdot (01, 19) = (17, 11)$$

Encoding and Encryption

Let the plaintext p be **WELCOME**. Alice encodes the plaintext twice and represented it by m_1 and m_2 respectively as $m_1 = m_2 = 23051203151305$.

The encoded blocks will be encrypted by $c_i = m_i \cdot k_i^{o(k_i)-1}, i = 1, 2$. Alice sends $((19151109201415), (18051723150805))$ to Bob. Bob decrypts the ciphertext by $c_i \cdot k_i, i = 1, 2$ and gets $m_1 = 23051203151305$ and $m_2 = 23051203151305$ since $m_1 = m_2$ the original plaintext WELCOME is shared.

Illustration 2

In this example we send a plaintext having multiple instructions by dividing it into blocks, encrypting and decrypting each block with different keys. The main difference is the key sharing where $k = (k_1, k_2, \cdots, k_s)$ where $k_i, i = 1, 2, \cdots, s$ are the common keys corresponding to the blocks $B_i, i = 1, 2, \cdots, s$ respectively. Here s denotes the number of blocks in which the plaintext p is split. For convenience we fix $s = 2$.

Consider the plaintext p be **WELCOME□HOME**.

Let us separate the plaintext p into two blocks B_1, B_2 each block is of length six.B_1 =WELCOM and B_2 =E□HOME. Alice encodes the blocks B_1 and B_2 and gets the encoded message m_1 and m_2 as (230512031513) and (050008151305) respectively. The encoded blocks will be encrypted by $c_i = m_i \cdot k_i^{o(k_i)-1}, i = 1, 2$.

Alice sends c=((191511092014),(050003150805)) to Bob.Bob decrypts the ciphertext by $c_i \cdot k_i, i = 1, 2$ and gets $m = ((230512031513), (050008151305))$ and decodes it obtain the plaintext WELCOME□HOME.

5. Conclusion

In this paper we gave protocols for multiple key sharing as well as encryption and decryption by using actions of semiring on multiplicative left ideal. By using multiple key we can split a message into blocks and each block will be encrypted by a secret key. The secret key will be send as an ordered pair containing key and the corresponding block of the message. In future we apply the semiring action to asymmetric key encryption to improve security.

References

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

[2] J. S. Golan: *The Semirings and their Applications*, Kluwer Academic Publishers-London, 1992.

[3] P. Muralikrishna, S. Srinivasan, N. Chandramowliswaran: *Secure schemes for secret sharing and key distribution using pell's equation*, International Journal of Pure and Applied Mathematics, **85**(5) (2013), 933–937.

[4] S. Nivetha, V. Thiruveni, M. Chandramouleeswaran: *Semiring Actions for Public key Cryptography*, Journal of Computer and Mathematical Sciences, **10**(1) (2019), 238–244.

[5] M. Sundar, P. Victor, M. Chandramouleeswaran: *Public key Cryptography-Key sharing with Semiring Action.*, IJMSEA, **11**(1) (2017), 195–204.

Department of Mathematics
Sri Ramanas College of arts and science for women
Aruppukottai - 626134. Tamilnadu. India
Email address: nivethasoundar9127@gmail.com

Department of Mathematics
Sri Ramanas College of arts and science for women
Aruppukottai - 626134. Tamilnadu. India
Email address: moulee59@gmail.com