A Novel Public Key Crypto system Based on Semi-modules over Quotient Semi-rings

Reza Ebrahimi Atani[1], Shahabaddin Ebrahimi Atani [2], Sattar Mirzakuchaki[3]

[1, 3] Electrical Engineering, Department,
Iran University of Science & Technology, Tehran, Iran
[1]rebrahimi@iust.ac.ir , [3] m_kuchaki@iust.ac.ir

[2] Faculty of Science, Department of Mathematics,
Guilan University, Rasht, Iran
ebrahimi@guilan.ac.ir

Abstract: In A generalization of the original Diffie-Hellman key exchange in $(\mathbb{Z}/p\mathbb{Z})^*$ found a new depth when Miller and Koblitz suggested that such a protocol could be used with the group over an elliptic curve. Maze, Monico and Rosenthal extend such a generalization to the setting of a Semi-group action on a finite set, more precisely, linear actions of abelian semi-rings on semi-modules. In this paper, we extend such a generalization to the linear actions of quotient semi-rings on semi-modules. In fact, we show how the action of quotient semi-rings on a semi-module gives rise to a generalized Diffie-Hellman and ElGamal protocol. This leads naturally to a cryptographic protocol whose difficulty is based on the hardness of a particular control problem, namely the problem of steering the state of some dynamical system from an initial vector to some final location.

Keywords: Public key cryptography, Diffie-Helman protocol, One-way trapdoor functions, Semi group actions, Quotient semi-rings

Introduction

The Diffie-Hellman key exchange and the ElGamal one-way trapdoor function are the basic ingredients of public key cryptography. Both these protocols are based on the hardness of the discrete logarithm problem in a finite semi-ring. The discrete logarithm problem, commonly abbreviated DLP, is a recurrent tool in public-key cryptography. The problem takes place in any group G, but we shall always assume the group is finite and commutative.

Protocol 1.1 [The Discrete Logarithm Problem - DLP] Let G be a finite commutative group. Given two group elements a (the base) and b such that that $b \in < a >$, find $0 \le n \le ord(a)$ such that $a^n = b$. We denote such an n by $\log_a b$.

For cryptographic purpose, we will always assume that the group G is presented in such a way that multiplication is computationally easy. Note that this requirement makes exponentiation feasible as well using well-known methods of type square-and multiply (see [1] or [3]).

The difficulty of the DLP strongly depends on the type of group that is used: It goes from easy to non-feasible. For instance the DLP in the additive group of any finite field F_q is trivial since division can be performed in polynomial time. However, the DLP in the multiplicative group F_q^* is a difficult problem as well as the DLP in the group $E(F_q)$ of an elliptic curve defined over a finite field. In fact the latter is much more difficult than the former and intuition tells us that the less structure the group has, the more difficult that DLP will be. Protocols where the discrete logarithm problem plays a significant role are the Diffie-Hellman key agreement [4], the Elgamal public key

cryptosystem [5], the digital signature algorithm (DSA) and ElGamal's signature scheme [1]. This is one of the reasons why we have developed the ideas of this paper. In the sequel we outline two of these protocols and we refer the interested reader to [1] for further details.

Let $\{E_e: e \in K\}$ be a set of encryption transformations, and let $\{D_d: d \in K\}$ be the set of corresponding decryption transformations, where K is the key space. Consider any pair of associated encryption/decryption transformations (E_e, D_d) and suppose that each pair has the property that knowing E_e it is computationally infeasible, given a random cipher-text $c \in C$, to find the message $m \in M$ such that $E_e(m) = c$. This property implies that given e it is infeasible to determine the corresponding decryption key d. (Of course e and d are simply means to describe the encryption and decryption functions, respectively.) E_e is being viewed here as a trapdoor one-way function with d being the trapdoor information necessary to compute the inverse function and hence allow decryption. This is unlike symmetric-key ciphers where e and d are essentially the same. Under these assumptions, consider the two-party communication between Alice and Bob illustrated in Figure 1. Bob selects the key pair (e, d). Bob sends the encryption key e (called the *public key*) to Alice over any channel but keeps the decryption key d (called the *private key*) secure and secret. Alice may subsequently send a message to Bob by applying the encryption transformation determined by Bob's public key to get $c = E_e(m)$. Bob decrypts the cipher-text c by applying the inverse transformation D_d uniquely determined by d [1].

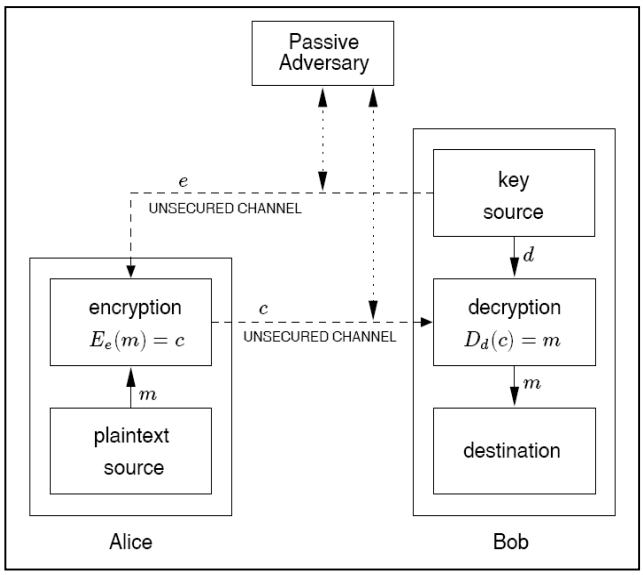

Fig.1 Encryption using public-key techniques [1].

The Diffie-Hellman protocol [4] allows Alice and Bob, to exchange key over some insecure channel. In order to achieve this goal Alice and bob agree on a group G and a common base $g \in G$. Alice chooses a random positive integer a and Bob chooses a random positive integer b. Alice transmits to Bob g^a and Bob transmits to Alice g^b. Their common secret key is $k = g^{a\,b}$.

The ElGamal public key cryptosystem [5] works in the following way: Alice chooses positive integer n and $h, g \in G$, where $h = g^n$. The private key of Alice consists of (g, h, n), the public key consists of (g, h). Bob chooses a random positive integer r and with this he applies the encryption function $v: G \longrightarrow G \times G$ (sending m to $(c_1, c_2) = (g^r, m\,h^r)$). Alice, who knows $n = \log_g h$ readily, computes m from the cipher text $(c_1, c_2): m = c_2\,(c_1^{\,n})^{-1}$. In order for the protocol to work it is required that multiplication and inversion inside the group G can be efficiently done and it should be computationally infeasible to compute a discrete logarithm with base $g \in G$.

In [6], Maze, Monico and Rosenthal have shown how the discrete logarithm problem over a group can be seen as a special instance of an action by a Semi-group. In fact, they have shown every Semi group action by an abelian Semi-group gives rise the Diffie-Hellman key exchange. With an additional assumption it is also possible to extend the ElGamal protocol. Let us explain them in detail. Assume that s is a finite set and let G be a Semi-group. Consider an action of G on s: $G \times S \longrightarrow S$ (sending (g, s) to $g.s$). By the definition of a group action we require that $(g\,h)\,s = g\,(h\,s)$ for all $g, h \in G$ and $s \in S$. We also assume throughout that arithmetic in G and computation of the G-action can be done in polynomial time. If the Semi-group G is commutative then every G-action gives rise to a generalized Diffie-Hellman Key Exchange [6]:

Protocol 1.2 (Extended Diffie-Hellman Key Exchange) Let s be a finite set, G a commutative Semi-group and an action of G on S as defined above. The Extended Diffie-Hellman Key Exchange is the following protocol [6]:

1) Alice and Bob agree on an element $s \in S$.

2) Alice chooses $a \in G$ and computes as. Alice's secret key is a, her public key is as.

3) Bob chooses $b \in G$ and computes bs. Bob's secret key is b, his public key is bs.

4) Their common secret key is then $a\,(b\,s) = (a\,b)\,s = (b\,a)\,s = b\,(a\,s)$.

Protocol 1.3 (Extended ElGamal Public Key System) Let s be a group with respect to some operation $\mathbf{0}$, G an abelian Semi-group and an action of G on s as defined above. The Extended ElGamal Public Key System is the following protocol [6]:

1) Alice's public key is $(s, a\,s)$.

2) Bob chooses a random element $b \in G$ and encrypts a message m using the encryption function

$$(m, b) \longrightarrow (b\,s, (b\,(a\,s)) \,\mathbf{0}\, m) = (c_1, c_2)$$

3) Alice can decrypt the message using

$$m = (b\,(a\,s))^{-1} \,\mathbf{0}\, c_2 = (a\,c_1)^{-1} \,\mathbf{0}\, c_2 .$$

In [6] Maze, Monico and Rosenthal show how to build Semi-group actions from actions by semi-rings on semi-modules. In this paper we show how to build Semi-group actions from actions by quotient semi-rings on semi-modules.

1. Quotient semi-rings acting on semi-modules

A set R together with two associative binary operations called addition and multiplication (denoted by $+$ and, $.$ respectively) will be called a semi-ring provided 1) addition is a commutative operation and that the multiplication is distributive with respect to the addition both from the left and from the right; 2) there exists $0 \in R$ such that $r + 0 = r$ and $r.0 = 0.r = 0$ for all $r \in R$. A subset I of a semi-ring R will be called an ideal if $a, b \in I$ and $r \in R$ implies $a + b \in I$ and $r\,a, a\,r \in I$. A subtractive ideal (= k-ideal) K is an ideal such that if $x, x + y \in I$ then $y \in K \cdot$ A (left) semi-module M over a semi-ring R is a commutative additive Semi-group which has a zero element, together a mapping from

$$R \times M \longrightarrow M$$

Sending (r, m) to $r\,m$ such that $(r + s)\,m = r\,m + s\,m$, $r\,(m + p) = r\,m + r\,p$, $r\,(s\,m) = (r\,s)\,m$

And $0m = r\,0_M = 0_M$ For all $m, p \in M$ and $r, s \in R$.

An ideal I of a semi-ring R is called a partitioning ideal ($=Q$-ideal) if there exists a non-empty subset Q of R such that

(1) $R = \mathbf{U}\{q + I : q \in Q\}$;

(2) If $q_1, q_2 \in Q$ then $(q_1 + I)\ \mathbf{I}\ (q_2 + I) \neq f$ if and only if $q_1 = q_2$

Let I be a Q-ideal of a semi-ring R and let $R/I = \{q + I : q \in Q\}$. Then R/I forms a semi-ring under the binary operations $\oplus$ and $\otimes$ defined as follows: $(q_1 + I) \oplus (q_2 + I) = q_3\ I$ where $q_3 \in Q$ is the unique element such that $q_1 + q_2 + I \subseteq q_3 + I$ and $(q_1 + I) \otimes (q_2 + I) = q_4 + I$ where $q_4 \in Q$ is the unique element such that $q_1\, q_2 + I \subseteq q_4 + I$. This semi-ring R/I is called the quotient semi-ring of R by I. By definition of Q-ideal, there exists a unique $q_0 \in Q$ such that $0 + I \subseteq q_0 + I$. Then $q_0 + I$ is a zero element of R/I [8, 10]. It is well-known that if R is a semi-ring, then $\mathrm{Mat}(R)$, the set of $n \times n$ matrices with entries in R is a semi-ring.

Let M be a finite semi-module over a semi-ring R, and let I be a Q-ideal of R. Now let $r \in R$ and suppose that $q_1 + I, q_2 + I \in R/I$ are such that $q_1 + I = q_2 + I$ in R/I. Then $q_1 = q_2$, we must have $q_1\, m = q_2\, m$ for every $m \in M$. Hence we can unambiguously define a mapping $R/I \times M$ into M (sending $(q + I, m)$ to $q\, m$) and it is routine to check that this turns the commutative Semi-group M into an R/I- semi-module.

Convention. The remaining of this paper we will assume unless otherwise stated, if I is an Q-ideal of R, and then Q is closed under addition and multiplication of R.

Let $\mathrm{Mat}(R/I)$ be the set of $n \times n$ all matrices with entries in R/I. The semi-ring structure on R/I induces a semi-ring structure on $\mathrm{Mat}(R/I)$. Moreover the semi-module structure on M lifts to a semi-module structure on M^n via the matrix multiplication:

$$\mathrm{Mat}(R/I) \times M^n \longrightarrow M^n$$

Sending (A, x) to Ax where x is a $n \times 1$ matrix with entries $m_{11}, ..., m_{n1}$ and $A = (q_{ij} + I)_{n \times n}$ with $q_{ij} \in Q$ for every i, j. One readily verifies that

$$\mathrm{Mat}(R/I) \times M^n \longrightarrow M^n$$

is an action by a semi-group, indeed one readily computes that $A\,(B\,x) = (A\,B)\,x$. Let us explain this equality in more detail. For simplicity, assume that $n = 2$ and let $A = (a_{ij} + I)_{2\times 2}$, $B = (b_{ij} + I)_{2\times 2}$ and $x = (m_{i1})_{2\times 1}$. Let $A\,(B\,x) = (c_{ij})_{2\times 1}$. Then we must have

$$a_{11}\, b_{11}\, m_{11} + a_{11}\, b_{12}\, m_{21} + a_{12}\, b_{21}\, m_{11} + a_{12}\, b_{22}\, m_{21} = c_{11} \qquad (1)$$

$$a_{21}\, b_{11}\, m_{11} + a_{21}\, b_{12}\, m_{21} + a_{22}\, b_{21}\, m_{11} + a_{22}\, b_{22}\, m_{21} = c_{21} \qquad (2)$$

Let $A\,B = (e_{i\,j} + I)_{2\times 2}$. Then we must have

$$(a_{11} + I) \otimes (b_{11} + I) \oplus (a_{12} + I) \otimes (b_{21} + l) = = e_{11} + l \qquad (3)$$

$$(a_{11} + I) \otimes (b_{12} + I) \oplus (a_{12} + I) \otimes (b_{22} + l) = = e_{12} + l \qquad (4)$$

$$(a_{21}+I)\otimes(b_{11}+I)\oplus(a_{22}+I)\otimes(b_{21}+l)= \\ =e_{21}+l \qquad (5)$$

$$(a_{21}+I)\otimes(b_{12}+I)\oplus(a_{22}+I)\otimes(b_{22}+l)= \\ =e_{22}+l \qquad (6)$$

It then follows from (3) that there are unique elements $d_{11},\ d_{12}$ of Q such that

$$(d_{11}+I)\oplus(d_{12}+I)=e_{11}+l \qquad (7)$$

Where $a_{11}\,b_{11}+I\subseteq d_{11}+I$, $a_{12}\,b_{21}+I\subseteq d_{12}+I$ and $d_{11}+d_{12}+I\subseteq e_{11}+I$; hence

$$a_{11}\,b_{11}+a_{12}\,b_{21}=d_{11}+d_{12}=e_{11} \qquad (8)$$

Since I is a Q-ideal of R. Similarly, the relations (4), (5) and (6) give:

$$a_{11}\,b_{12}+a_{12}\,b_{22}=e_{12}, a_{21}\,b_{11}+a_{22}\,b_{21}= \\ e_{21}, a_{21}\,b_{12}+a_{22}\,b_{22}=e_{22} \qquad (9)$$

Let $(A\,B)\,x=(e_{ij}+I)_{2\times2}(m_{i1})_{2\times1}=(f_{i1})_{2\times1}$. Then we must have:

$$e_{11}\,m_{11}+e_{12}\,m_{21}=f_{11}, e_{21}\,m_{11} \\ +e_{22}\,m_{21}=f_{21} \qquad (10)$$

Now the relation (1), (2), (8), (9) and (10) gives

$$f_{11}=a_{11}\,b_{11}\,m_{11}+a_{11}\,b_{12}\,m_{21}+a_{12}\,b_{21}m_{11} \\ +a_{12}\,b_{22}\,m_{21}=c_{11} \qquad (11)$$

$$f_{21}=a_{21}\,b_{11}\,m_{11}+a_{21}\,b_{12}\,m_{21}+a_{22}\,b_{21}\,m_{11} \\ +a_{22}\,b_{22}\,m_{21}=c_{21} \qquad (12)$$

Thus $(A\,B)\,x=A(B\,x)$.

Remark Assume that I is an Q-ideal of R such that $a\,b=b\,a$ for all $a,b\in Q$ and let $q_I, q'+I\in R/I$. Then there are unique elements $c,c'\in Q$ with $q\,q'+I\subseteq c+I$ and $q'\,q+I\subseteq c'+I$, so $(q+I)\otimes(q'+I)=(q'+I)\otimes(q+I)$ since $q\,q'=q'\,q$; hence R/I is a commutative ring.

Assume that I is an Q-ideal of R such that $q\,q'=q'\,q$ for all $q,q'\in Q$ and set $\overline{R}=R/I=\{q+I:q\in Q\}=\{\bar{q}:q\in Q\}$. Let $\overline{R}[t]$ be the polynomial semi-ring in the in determinant t, and let $A\in Mat(\overline{R})$ be a fixed matrix. If

$$\bar{p}(t)=\bar{q}_0+\bar{q}_1\,t+\ldots+\bar{q}_k\,t^k\in\overline{R}[t]$$

then we define in the usual way $\bar{p}(A)=\bar{q}_0\,I_n+\overline{q_1}\,A+\ldots+\overline{q_k}\,A^k$, where $\overline{q_0}\,I_n$ is the $n\times n$ diagonal matrix with entry $\overline{q_0}$ in each diagonal element. Consider the Semi-group

$$\overline{G}=\overline{R}[A]=\{\bar{p}(A):\bar{p}(t)\in\overline{R}[t]\}$$

it is easy to see that $\overline{G}$ has the structure of an abelian Semi-group.

Protocol 2.1 then simply requires that Alice and Bob agree on an Q-ideal I of a semi-ring R, an element $x \in M_n$ and a matrix $A \in Mat(\overline{R})$. Alice chooses secretly $\overline{P}(t) \in \overline{R}[t]$ and computes $\overline{p}(A)x$ and sends the result to Bob. Bob chooses secretly $\overline{q}(t) \in \overline{R}[t]$ and computes $\overline{q}(A)x$ and sends the result to Alice. As a common secret key serves $k = \overline{p}(A)\overline{q}(A)x$ since $\overline{p}(A)$ and $\overline{q}(A)$ commute.

System Theoretic Interpretation: It is possible to give the key exchange a systems theoretic interpretation. For this note that in order to choose $p(A) \in \overline{R}[A]$ Alice has to choose $\overline{q}_0 = \overline{q}_0 + I$, ..., $\overline{q}_k = \overline{q}_k + I \in \overline{R} = R/I$ and with this she can compute

$$\overline{p}(A)x = (\overline{q}_0 + \overline{q}_1 A + ... + \overline{q}_k A^k)x =$$
$$\overline{q}_0 x + \overline{q}_1 A x + ... + \overline{q}_k A^k x$$

Consider now the linear time invariant system: $y_{t+1} = A y_t + \overline{u}_t x$ Where $x, y_t \in M^n$ and $\overline{u}_t \in \overline{R}$. Suppose further that $y_0 = 0_M$. If Alice chooses the input sequence $\overline{u}_0 = \overline{q}_k, \overline{u}_1 = \overline{q}_{k-1}$, ..., $\overline{u}_k = \overline{q}_0$ then $\overline{y}_{k+1}$, the state vector at time $k+1$ is exactly $\overline{p}(A)x$ the public vector to be computed by Alice. Once Alice receives from Bob his public key $\overline{f}(A)x$, then she defines $b = \overline{f}(A)x$ and by choosing her input sequences $\overline{u}_0 ... \overline{u}_k$ in the system $y_{t+1} = A y_t + \overline{u}_t b$. Then she will be able to compute the common secret key $\overline{p}(A)\overline{f}(A)x$.

Adversary who wants to find an element $\overline{g}(t) \in \overline{R}[t]$ such that $\overline{g}(A)x = \overline{p}(A)x$ faces the task of finding a control sequence $\overline{u}_0, ..., \overline{u}_k$ which steers the initial state y_0 in to the state $\overline{p}(A)x$. This problem is in general very hard, but it contains some of the hardest known discrete logarithm problem as a special case. For example, when $R/I = M = F$, a finite field then the problem is however simply solved by [6, Theorem 3.1].

2. Matrix quotient semi-rings acting on semi-modules

Assume that R is a semi-ring and let $Mat(R)$ be the set of $n \times n$ matrices with entries in R. Our starting point in this section is the following theorem:

Theorem 3.1 Let I be a Q-ideal of a semi-ring R. Then $Mat_n(I)$ is a $Mat(Q)$-ideal of $Mat(R)$. In particular:

$$Mat(R)/Mat(I) = \{C + Mat(I) : C \in Mat(Q)\}$$

is a semi-ring.

Proof: It is easy to see that $Mat(I)$ is an ideal of $Mat(R)$.

Since the inclusion:

$$\mathbf{U}\{q + Mat(I) : q \in Mat(Q)\} \subseteq Mat(R)$$

is trivial, we will prove the reverse inclusion. Suppose that $A = (a_{ij})_{n \times n} \in Mat(R)$. Then there are elements $q_{ij} \in Q$ and $c_{ij} \in I$ such that $a_{ij} = q_{ij} + c_{ij}$ for all i, j since I is a Q-ideal of R. Set $B = (q_{ij})_{n \times n}$ and $C = (c_{ij})_{n \times n}$. Then $A = B + C \in Mat(Q) + Mat(I)$, and so we have equality. Suppose that $(E + Mat(I))\ \mathbf{I}\ (F + Mat(I)) \neq f$ where $E = (e_{i,j})_{n \times n}$, $F = (f_{i,j})_{n \times n} \in Mat_{n \times n}(Q)$. We show that $E = F$. There exist $H = (h_{ij})_{n \times n}$, $K = (k_{i \times j})_{n \times n} \in Mat_{n \times n}(I)$ such that $E + H = F + K$, so for all $i, j, (e_{ij} + I)\ \mathbf{I}\ (f_{ij} + I) \neq f$; Hence $E = F$ since I is a Q-ideal, as needed.

Let M be a finite semi-module over a semi-ring R. The semi-module structure on M lifts to a semi-module structure on M^n via the matrix multiplication:

$$Mat(R) \times M^n \to M^n$$

Sending (A, x) to Ax [6].

If I is an Q-ideal of R, then Theorem 3.1 gives $Mat(R)/Mat(I)$ is a semi-ring. Moreover, if I is closed under addition and multiplication of R, then it is easy to see that $Mat(I)$ is closed under addition and multiplication of $Mat(R)$. Now the matrix multiplication:

$$Mat(R)/Mat(I) \times M^n \rightarrow M^n$$

sending $(A + Mat(I), x)$ to $A\,x$ is a semi-module structure on M^n where $A \in Mat(Q)$. One readily verifies that

$$Mat(R)/Mat(I) \times M^n \rightarrow M^n$$

is an action by a semi-group, indeed one readily computes that $A\,(B\,x) = (A\,B)\,x$. Let us explain this equality in more detail. Let $A = (a_{i\,j})_{n\times n} + Mat(I)$,

$$B = (b_{ij})_{n\times n} + Mat(I)$$

And $x = (m_{i1})_{n\times 1}$ where $a_{Ij}, b_{ij} \in Q$. Then we must have

$$(A\,(B\,x) = (a_{ij})_{n\times n}\,(b_{ij})_{n\times n}\,(m_{i1})_{n\times 1} \qquad (13)$$

Let $A\,B = (e_{i\,j})_{n\times n} + Mat(I)$. Then we must have $(a_{ij})_{n\times n}\,(b_{ij})_{n\times n} + Mat(I) \subseteq (e_{ij})_{n\times n} + Mat(I)$, so we get $(a_{ij})_{n\times n}\,(b_{ij})_{n\times n} = (e_{ij})_{n\times n}$ since $Mat(I)$ is a $Mat(Q)$- Ideal of $Mat(R)$. It follows that

$$(A\,B)\,x = (a_{ij})_{n\times n}\,(b_{ij})_{n\times n}\,(m_{i1})_{n\times 1} \qquad (14)$$

Now the assertion follows from (13) and (14).

Assume that $S = Mat\,(R)/Mat\,(I)$ and let $S[t]$ be the polynomial semi-ring in the in determinant t and let $A = (a_{ij})_{n\times n} + Mat(I) \in S$ be a fixed member. Let $C \subseteq S$ be the center of S.If $p(t) = r_0 + r_1\,t + ..., r_k\,t_k\,C[t]$, then we define in the usual way $p(A) = r_0\,I_n + r_1\,A + ..., r_k\,A^k$. Then $C[A] = \{p(A) : p(t) \in C[t]\}$ has the structure of an abelian Semi-group. Alice and Bob agree on an R semi-module M, an element $x \in M^n$ and an element A of S. Alice chooses secretly $p(t) \in C[t]$ and computes $p(A)\,x$ and sends the result to Bob. Bob chooses $q(t) \in C[t]$ and computes $q(A)\,x$ and sends the result to Alice. As a common key serves $k = p(A).q(A).x$. It should be difficult to find $g(t) \in C[t]$ such that $g(A)\,x = p(A)x$.

3. Conclusion

At present, we lack a convincing example of a system based on the previous sections. All of the examples has presented in [6] to be either insecure or already well-known. The insecure examples have arisen by generating random finite semi-ring for base-objects. Of course, there are some strong results in [6] on simple semi-modules over commutative semi-rings, but more work is needed to determine if there exist such objects that will suit our needs. In this paper we showed how the discrete logarithm problem over a finite group can viewed as an instance of an action by a Semi-group. In fact, we show how the action of a quotient semi-ring on a semi-module gives rise to a generalized Diffe-Hellman and ElGamal protocol. It remains to find concrete instances of such actions that have high (believed) security relative to their key size.

References

1. A. J. Meenezes and P. C. van Oorschot, and S. A. Vanstone, "Hand-book of Applied Cryptography", CRC Press Series on Discrete Mathematics and its Applications 1997.

2. V. S. Miller, "Use of elliptic curves in cryptography, In Advances in cryptology" - CRYPTO 85 (Santa Barbara, Calif., 1985), Pages 417-426, Springer, Berlin, 1986.

3. Song Y. Yan, "Number theory for computing", Springer-Verlag, Berlin, 2000.

4. W. Diffie and M. E. Hellmann, "New directions in cryptography", IEEE Trans. Inform. Theory, IT-22 (6) (1976), 644-654.

5. T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithm", IEEE Trans. Inform. Theory, 31 (4) (1985), 469-472.

6. G. Maze, C. Monico and J. Rosenthal, "Public Key Cryptography On Semi-group Actions", arXiv:cs. CR/0501017v2 28 Jan 2005.

7. P. J. Allen, "A fundamental theorem of homeomorphisms for semi-rings", Proc. Amer. Math. Soc., 21 (1969), 412-416.

8. Shahabaddin Ebrahimi Atani, "The ideal theory in quotients of commutative semi-rings", Glasnik Matematicki, to appear (2007).

9. Shahabaddin Ebrahimi Atani and Reza Ebrahimi Atani, "Prime sub-semi-modules of semi-modules", submitted.

10. V. Gupta and J. N. Chaudhari, "Some remarks on Right π-regular semi-rings", Sarajevo J. of Math., 14 (2006), 3-9.

11. N. Koblitz, "Elliptic curve cryptosystem", Math. Comp., 48(177) (1986), 203-209.

12. C. Monico. "Semi-rings and Semi-group Actions in Public Key Cryptography", PhD thesis, University of Notre Dame, May 2002.

13. G. Maze. "Algebraic Methods for Constructing One-Way Trapdoor Functions", PhD thesis, University of Notre Dame, May 2003.

14. A. Yamamura. "Public-key cryptosystems using the modular group. In Public Key Cryptography", volume 1431 of Lecture Notes in Computer Science, pages 203–216. Springer, Berlin, 1998.

15. U.M. Maurer. Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms. In Advances in cryptology—CRYPTO ’94 (Santa Barbara, CA, 1994), pages 271–281. Springer, Berlin, 1994.

16. C. Monico. "On finite congruence-simple semi-rings", Journal of Algebra, 271(2):846–854, 2004.

17. I. E. Shparlinski. "Computational and algorithmic problems in finite fields", volume 88 of Mathematics and its Applications (Soviet Series). Kluwer Academic Publishers Group, Dordrecht, 1992.