Review Article

Neha Goel*, Indivar Gupta and B. K. Dass

Survey on SAP and its application in public-key cryptography

https://doi.org/10.1515/jmc-2016-0004
Received January 11, 2016; accepted June 20, 2019

Abstract: The concept of the semigroup action problem (SAP) was first introduced by Monico in 2002. Monico explained in his paper that the discrete logarithm problem (DLP) can be generalized to SAP. After defining the action problem in a semigroup, the concept was extended using different mathematical structures. In this paper, we discuss the concept of SAP and present a detailed survey of the work which has been done using it in public-key cryptography.

Keywords: Semigroup action problem, Diffie–Hellman key exchange, ElGamal cryptosystem

MSC 2010: 94A60

1 Introduction

Before 1976, secret key cryptography was used to achieve the security for communication over an open communication channel. In 1976, Diffie and Hellman [4] gave a completely different and new direction to cryptography by introducing the concept of public key cryptography. Since then it became a noticeable area of research, and a lot of research made public key cryptography more advanced. The security of public key cryptography relies on the intractability of some computationally hard problems, like integer factorization [15], discrete logarithm problems (DLP) [4, 6] and many others. DLP forms the basis for many cryptographic protocols.

In 2002, Monico generalized the concept of DLP and proposed a semigroup action problem (SAP) [13]. He defined the Diffie–Hellman key exchange protocol and ElGamal cryptosystem using this new computational problem SAP. After defining a semigroup action on an abelian group, the same concept was transferred to the action of a semiring on a semimodule in [10–12] and to the action of a quotient semiring on a semimodule in [1, 5]. In [5, 10, 11], the ElGamal cryptosystem was defined whose security depends on the hardness of finding a control sequence which steers the initial vector to the final vector. The idea of two-sided matrix action over a semiring was proposed in [9], which seems to be intractable if a simple semiring is used and the size of the matrices used to define the action are chosen appropriately. The use of simple semiring avoids the chances of Pohlig–Hellman type reduction attack [14]. In [7, 23], the idea of getting simple semiring was classified, and in [23], a classification of proper finite simple semirings with zero was given, which was further investigated in [7] to explain computational aspects of finite simple semiring.

Stolbunov presented the reductionist security argument for public-key cryptographic schemes based on group action in [21]. Some signature schemes were also proposed in [16–18], whose underlying hard problem comes from monoid and semiring action problems.

***Corresponding author: Neha Goel,** Department of Mathematics, University of Delhi, Delhi 110 007, India, e-mail: nehagoel_7@yahoo.com
Indivar Gupta, SAG, Metcalfe House, DRDO, Delhi 110 054, India, e-mail: indivar_gupta@yahoo.com
B. K. Dass, Department of Mathematics, University of Delhi, Delhi 110 007, India, e-mail: dassbk@rediffmail.com

The paper is organized in the following manner. In Section 2, mathematical preliminaries are given. In Section 3, the semigroup action in public-key cryptography is explained. In Section 4, the security of the SAP and cryptosystems based on it is discussed with a heuristic approach and with the help of a formal security model. In Section 5, the work based on action of algebraic structure is explained. In Section 6, the future scope of SAP is discussed. Finally, in Section 7, we conclude the paper.

2 Mathematical preliminaries

In this section some basic definitions are given which are required for the understanding of paper.

Definition 2.1 (Group action). Let $(G, \cdot)$ be a group and let S be a non-empty set. Then G is said to act on S if there exist a function $\phi\colon G \times S \to S$, with $\phi(a, x) = ax$, such that $a(bx) = (ab)x$ and $ex = x$ (e is the identity element of G) for all $a, b \in G$, $x \in S$. This mapping ϕ is called the group action of G on S.

Definition 2.2 (Semigroup action). Let S be a finite set. Then the (left) action of the semigroup $(G, \cdot)$ on S is defined as $\phi\colon G \times S \to S$, with $\phi(g, s) = gs$, such that $(gh)s = g(hs)$ for all $g, h \in G$. This action is semigroup action on the set S. (A right action is similarly defined.)

Definition 2.3 (Semiring). A non-empty set R equipped with two binary operations $(\cdot)$ and $(+)$, termed as multiplication and addition, respectively, is called a semiring if it has following three properties:
(a) $(R, +)$ is an abelian semigroup,
(b) $(R, \cdot)$ is a semigroup,
(c) $\cdot$ is distributive over $+$.

Definition 2.4 (Congruence simple semiring (or c-simple semiring)). A semiring R that does not possess any congruence relation (except the trivial relations id_R and $R \times R$) is said to be congruence simple semiring or c-simple semiring. A congruence relation is an equivalence relation $\sim$ on R that satisfies the following properties:

$$r_1 \sim r_2 \Rightarrow \begin{cases} r + r_1 \sim r + r_2, \\ r_1 + r \sim r_2 + r, \\ rr_1 \sim rr_2, \\ r_1 r \sim r_2 r \end{cases}$$

for every $r, r_1, r_2 \in R$.

Definition 2.5 (Semimodule). Let R be a semiring. A (left) semimodule is a commutative monoid $(M, +)$ with the neutral element $0 \in M$ such that for all $a, b \in M$ and $r, s \in R$, the following conditions are satisfied:
(a) $r0 = 0$, $0a = 0$,
(b) $r(a + b) = ra + rb$,
(c) $(r + s)a = ra + sa$,
(d) $(rs)a = r(sa)$.
If the elements of R act on right we call it a (right) semimodule.

Definition 2.6 (Partitioning ideal). An ideal I of a semiring R is called a partitioning ideal (or Q-ideal) if there exists a non-empty subset Q of R such that
(q) $R = \bigcup\{q + I : q \in Q\}$,
(q) if $q_1, q_2 \in Q$, then $(q_1 + I) \cap (q_2 + I) \neq \varnothing$ if and only if $q_1 = q_2$.

Definition 2.7 (Quotient semiring). Let I be a Q-ideal of a semiring R and let $R/I = \{q + I : q \in Q\}$. Then R/I forms a semiring under the binary operation $\oplus$ defined as $(q_1 + I) \oplus (q_2 + I) = q_3 + I$, where $q_3 \in Q$ is the unique element such that $q_1 + q_2 + I \subseteq q_3 + I$, and $(q_1 + I) \oplus (q_2 + I) = q_4 + I$, where $q_4 \in Q$ is the unique element such that $q_1 q_2 + I \subseteq q_4 + I$. This semiring R/I is called the quotient semiring of R by I.

Definition 2.8 (Discrete logarithm problem). Given a prime p, a generator α of Z_p^* and an element $\beta \in Z_p^*$, find an integer x, $0 \leq x \leq p-2$ such that $\alpha^x \equiv \beta \pmod{p}$.

Definition 2.9 (Diffie–Hellman problem). Given a prime p, a generator α of Z_p^*, and elements $\alpha^a \bmod p$, $\beta^b \bmod p$, find $\alpha^{ab} \bmod p$.

3 Semigroup action in public key cryptography

In 2002, Monico presented the semigroup action problem by considering DLP as a special instance of an action by a semigroup. He defined the key-exchange protocol and the extended ElGamal cryptosystem whose security relies on the intractability of SAP.

Definition 3.1 (Semigroup action problem (SAP)). Let G be a semigroup acting on a set S. Then, for given $x \in S$ and $y \in Gx$, find $g \in G$ such that $g * x = y$ where, $*$ is the operation between the elements of G and S.[1]

Definition 3.2 (Semigroup action problem on two sides matrix action). Let R be a semiring (not necessarily commutative) with 0 and 1. If $M \in G = \mathrm{Mat}_{m\times m}(R)$, then $C[M]$ (where C is the center of R) is the multiplicatively commutative sub-semiring generated by M. Let $M_1, M_2 \in G$. Then the following action is linear as explained in [9] and [11]:

$$(C[M_1] \times C[M_2]) \times G \to G$$

$((p(M_1), q(M_2)), A) \mapsto p(M_1) \cdot A \cdot q(M_2)$, where $A \in G$, $p(M_1) \in C[M_1]$ and $p(M_2) \in C[M_2]$. The semigroup action problem defined on this action is defined as follows: For given $M_1, M_2, S \in G$ and $T \in C[M_1]SC[M_2]$, find $U_1 \in C[M_1]$ and $U_2 \in C[M_2]$ so that $T = U_1SU_2$.

Definition 3.3 (Computational Diffie–Hellman group action problem (CDHAP)). Let G be an abelian semigroup acting on the set S and let $x, y, z \in S$, where, $y = ax$, $z = bx$ and a, b are chosen randomly from G. Then, for this tuple (x, ax, bx), find cx, where $c = ab$.

Definition 3.4 (Decisional Diffie–Hellman group action problem (DDHAP)). Let G be an abelian semigroup acting on the set S. Then for given triplet (ax, bx, cx), decide whether $c = ab$ or not, where a, b and c are randomly chosen from G and x is a fixed element of S.

Definition 3.5 (DDHAP assumption). Let $\mathcal{A}$ be the polynomial time DDHAP distinguisher and $Pr_{\mathcal{A}}^{\mathrm{DDHAP}}$ is the probability of returning the correct solution for DDHAP. Then the advantage of polynomial time DDHAP distinguisher $\mathcal{A}$ is given by

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{DDHAP}} = \left|\mathrm{Pr}_{\mathcal{A}}^{\mathrm{DDHAP}} - \frac{1}{2}\right|.$$

Now, according to DDHAP assumption [21], the advantage $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{DDHAP}}$ is negligible function of k for any polynomial-time distinguisher $\mathcal{A}$, where $k(= \log \sharp(Gx))$ is the security parameter.

3.1 Applications of SAP to public-key cryptography

After the proposal of SAP, cryptographic protocols have been designed using SAP as trapdoor in different algebraic structures.

[1] For convenience we represent this operation as simple multiplication throughout the paper.

3.1.1 Key exchange protocols based on SAP using different algebraic structures

The key-agreement protocol whose security relies on the intractability of SAP and proposed by Monico in [13] is defined as follows.

Key exchange protocol using action of semigroup over finite set.

(i) *Domain parameters*: Let (S, G, φ, s) be the domain parameters used to define the key exchange protocol. Here, the abelian semigroup G is acting over a finite set S under the mapping φ and $s \in S$.

(ii) *Key exchange algorithm*: Alice secretly chooses $a \in G$, computes as and sends it to Bob. Similarly, Bob chooses $b \in G$, computes bs and sends it to Alice. The common secret key is then

$$a(bs) = (ab)s = (ba)s = b(as).$$

An interesting example is presented in [13] using the action of the semigroup $\mathrm{Mat}_m(\mathbb{Z})$ over a $\mathbb{Z}$-module $H = S^m = S \times S \times \cdots \times S$, where $(S, \cdot)$ is a finite abelian semigroup and for which the SAP may be considered hard. The cryptosystem defined over this action is discussed as follows.

Key exchange protocol using matrix action.

(i) *Domain parameters*: Let $(S, \mathrm{Mat}_m(\mathbb{Z}_k), X, \mathbb{Z}_k[X], \varphi, s)$ be the domain parameters used to define the key exchange protocol. Here S is a finite abelian group of order k, $\mathrm{Mat}_m(\mathbb{Z}_k)$ is the semigroup of $m \times m$ matrices over $\mathbb{Z}_k$, $X \in \mathrm{Mat}_m(\mathbb{Z}_k)$, $\mathbb{Z}_k[X]$ is abelian sub-semigroup of $\mathrm{Mat}_m(\mathbb{Z}_k)$, φ is the mapping defining the restricted action of $\mathbb{Z}_k[X] = \{\varphi(X) | \varphi(x) \in \mathbb{Z}_k[x]\}$ over S^m and $s = (s_1, \dots, s_m)$.

(ii) *Key exchange algorithm*: Alice secretly chooses $A \in \mathbb{Z}_k[X]$, computes As and sends it to Bob. Similarly, Bob chooses $B \in \mathbb{Z}_k[X]$, computes Bs and sends it to Alice. The common secret key is then

$$A(Bs) = (AB)s = (BA)s = B(As).$$

In [11] Maze, Monico and Rosenthal extended the action of a semigroup over a semiring by defining the action of a simple ring over a simple module. The security of this system depends on the problem of steering the state of some dynamical system from an initial vector to some final position [11]. However, this system breaks down in the case where the rings and modules used for the system are more general as explained in [10]. Therefore, for security purposes, simple semirings are preferred. The system is defined as follows.

Key exchange protocol using action of semiring over semimodule.

(i) *Domain parameters*: Let $(R, M, G, \mathcal{M}^m, A, C[A], s)$ be the domain parameters, where R is a semiring (finite or infinite), M is a finite semimodule over R, G is the set of all $m \times m$ matrices over R, $\mathcal{M} = M \times M \times \cdots \times M$, A is an element of G and $C[A] = \{p(A) : p(t) \in C[t]\}$, where C is the center of R and $C[t]$ is the polynomial ring in the indeterminate in t.

(ii) *Key exchange algorithm*: Alice chooses a matrix $X \in C[A]$ and sends to Bob the vector $Xs(\in \mathcal{M}^m)$. Bob chooses a matrix $Y \in C[A]$ and sends to Alice the vector Ys. The common key is then the vector XYs.

In [5], Ebrahimi Atani et al. extend the semigroup action to the actions of quotient semirings on semimodule. The security of this system also depends on the problem of steering the state of some dynamical system from an initial vector to some final position. However, this system breaks down in some cases, for example, when $\frac{R}{I} = M = F$, a finite field, i.e., if the quotient semiring is a field, then the system can be easily solved using [11, Theorem 3.1].

Key exchange protocol using action of quotient semirings over semimodule.

(i) *Domain parameters*: Let $(R, I, M, G, \mathcal{M}^m, A, R^*, x)$ be the domain parameters, where R is the semiring, I is a Q-ideal of R such that $qq' = q'q$ for all $q, q' \in Q$, M is the semimodule over the quotient ring $\frac{R}{I}$, G is the set of all $m \times m$ matrices with entries in $\frac{R}{I}$, $\mathcal{M}^m = M \times M \times \cdots \times M$, A is an element of G and $R^*[A] = \{p^*(A) : p^*(t) \in R^*[t]\}$, where $R^* = \frac{R}{I} = \{q + I : q \in Q\} = \{q^* : q \in Q\}$, $R^*[t]$ is the polynomial semiring in the indeterminate t and $x \in \mathcal{M}^m$.

(ii) *Key exchange algorithm*: Alice chooses $p^*(t) \in R^*[t]$, computes $p^*(A)x$ and sends the result to Bob. Similarly, Bob chooses $q^*(t) \in R^*[t]$, computes $q^*(A)x$ and sends the result to Alice. The common key is then $k = p^*(A)q^*(A)x$.

In [5], a more generalized form is also defined using the action of matrix quotient semirings over semimodule. The key exchange protocol using the semigroup action problem as two-sided matrix action [11] is defined as follows.

Key exchange protocol using two-sided matrix action.

(i) *Domain parameters*: Let (R, C, G, M_1, M_2, S) be the domain parameters which are defined in Definition 3.2.

(ii) *Key exchange algorithm*: Alice chooses polynomials $p_a, q_a \in C[t]$, computes $A = p_a(M_1) \cdot S \cdot q_a(M_2)$ and sends the result to Bob. Bob chooses polynomials $p_b, q_b \in C[t]$, computes $B = p_b(M_1) \cdot S \cdot q_b(M_2)$ and sends the result to Alice. The common key is then

$$p_a(M_1)Bq_a(M_2) = p_a(M_1)p_b(M_1)Sq_b(M_2)q_a(M_2) = p_b(M_1)Aq_b(M_2).$$

3.1.2 ElGamal cryptosystem based on SAP

The ElGamal cryptosystem based on SAP [13] is defined as follows.

ElGamal cryptosystem using action of semigroup over finite group.

(i) *Domain parameters*: Let (S, G, φ, s) be the domain parameters used to define the cryptosystem. Here, the abelian semigroup G is acting over a finite group S under the mapping φ and $s \in S$.

(ii) *Key-generation:* This algorithm, using domain parameters, generates the key pair (sk, pk), where $sk = b$ is the secret key and $pk = bs$ is the public key of Bob.

(iii) *Encryption*: Alice wants to send the message $m \in S$. Using Bob's public key $pk = bs$ and her private key $a \in G$, Alice calculates the ciphertext $c = (as, (abs) \circ m) = (c_1, c_2)$ and sends it to Bob.

(iv) *Decryption*: On receiving c, Bob decipher m as $(bc_1)^{-1} \circ c_2 = m$.

Example 3.6. Monico presented an example in [13] on SAP using the following parameters: Let $E\colon y^2 = x^3 + x + 47$ be an elliptic curve over F_{71} with group of rational points $E(71) \cong Z_5 \oplus Z_{15}$ having the identity element $\mathcal{O}$. Let $P_1 = (1;7)$, $P_2 = (51;11)$ and $P_3 = (49;58)$ be three points which do not lie in a common cyclic subgroup:

$$\begin{aligned}
\langle P_1\rangle &= \{(1;7), (43;52); (43;19); (1;64); (\mathcal{O})\},\\
\langle P_2\rangle &= \{(51;11), (70;20), (70,51); (51;60); (\mathcal{O})\},\\
\langle P_3\rangle &= \{(49;58), (60;57), (60;14), (49;13), (\mathcal{O})\}.
\end{aligned}$$

Let G be the subgroup generated by these three points, i.e., $G = \langle P_1, P_2, P_3\rangle$ and $\mathrm{Mat}_3(\mathbb{Z}_5)$ is a group of 3×3 matrices over $\mathbb{Z}_5$. Now, using these parameters, the key exchange protocol is defined as follows:

(i) *Domain parameters*: Let $(\mathcal{G}, H, \varphi, A, x)$ be the domain parameters used to define the cryptosystem. Here, φ is the mapping used to define the action of H over $\mathcal{G}$, where $\mathcal{G} = G \times G \times G$, $H = \mathbb{Z}_5[A]$, for

$$A = \begin{pmatrix} 3 & 1 & 1\\ 2 & 2 & 4\\ 1 & 2 & 3 \end{pmatrix} \in \mathrm{Mat}_3(\mathbb{Z}_5) \quad \text{and} \quad x = \begin{pmatrix} (1,7)\\ (51,11)\\ (49,58) \end{pmatrix} \in \mathcal{G}.$$

(ii) *Key exchange algorithm*: Using the domain parameters Alice and Bob follow the following algorithm to exchange the common secret key:

(a) Alice chooses

$$M_a = \begin{pmatrix} 3 & 4 & 1\\ 3 & 0 & 2\\ 1 & 1 & 2 \end{pmatrix} \in H$$

and computes $\alpha = M_a x$. Alice's private key is M_a and her public key is α.

(b) Bob chooses

$$M_b = \begin{pmatrix} 3 & 2 & 4 \\ 4 & 2 & 4 \\ 4 & 2 & 2 \end{pmatrix} \in H$$

and computes $\beta = M_b x$. Bob's private key is M_b and his public key is β.

(c) Their common secret key is then

$$M_a \beta = M_b \alpha.$$

4 Security of SAP and cryptographic protocols based on SAP

The security of SAP and cryptographic protocols based on SAP is explained in this section.

4.1 Security of SAP and cryptographic protocols against brute force attack

To break SAP using Brute force attack, the attacker will try all possible $g_i \in G$, $0 \leq i \leq |G|$ to get an appropriate g_i which satisfies $g_i s = gs$, where G is an abelian semigroup acting over a finite set S and $s \in S$. Therefore, the size of the abelian semigroup G should be chosen in such a way that it is computationally hard for the attacker to find g_i (see [10, 11]).

When G is a cyclic group instead of an abelian semigroup, then the total number of operations required to break SAP using square root attack are $O\sqrt{|G|}$. If G is not a cyclic group, then the overall complexity of applying Pollard's rho attack is $O(\sqrt{|O_s|})$, where O_s is the orbit of $s \in S$.

If the semigroup G has a large subgroup G_1, it may be partitioned in the form $G = G_\circ \cup G_1$, where $G_1 = \{g \in G : g^{-1} \text{ exists}\}$ and $G_\circ = G \setminus G_1$. Now, the attacker will try to find the solution of the equation $y = gs$ in $G_\circ$ using an exhaustive search algorithm. If no solution is found in $G_\circ$, the attacker will restrict the SAP to G_1 and apply Pollard's square root attack. The overall complexity of applying this attack is $|G_\circ| + O(\sqrt{|G_1 s|})$ (see [10]), where $G_1 s = \{gs | g \in G_1\}$.

In case when G is not a group and not a set theoretic union of a small number of cyclic sub-semigroups, then the attacks applicable to DLP are not applicable to SAP. It is suggested in [11] that when G is a group where no attack is applicable except the square root attack, then 160 bit orbit size is sufficient for achieving practical security. Also in the case where no attack is not possible, 80 bit orbit size is sufficient for achieving practical security.

Now, we analyze the security of the two-sided matrix multiplication action discussed in Definition 3.2 and Section 3.1.1. For the security of the two-sided matrix multiplication action, the c-simple semirings of the type $R_m = \mathrm{Mat}_m(\{0, 1\}, \max, \min)$ had been used in [9], where $\mathrm{Mat}_m(\{0, 1\}, \max, \min)$ is a max-min algebra. The use of these types of semirings makes the two-sided matrix multiplication action secure against Pohlig–Hellman attack and square-root attacks.

If R_1 (for $m = 1$) is used as semiring, then the brute force complexity of the two-sided matrix multiplication action defined in Section 3.1.1 will be $O(|R_1[M_1]| \cdot |R_1[M_2]|)$. According to the consequence of [9, Assumption 5.19], the complexity of the two-sided matrix multiplication action can be reduced to $O((ord(M_1) ord(M_2))^d)$ for some $d \in \mathbb{N}$. This bound can also be given in terms of the size of the matrix Z, where $Z = p(M_1) S q(M_2)$ and p, q, S are defined in Definition 3.2 and Section 3.1.1. If the input size of Z is m^2 ($= N$ say) bits, then the expected running time of the algorithm in terms of the key size will be $O(\exp(\sqrt{2}d + o(1)) N^{1/4} \sqrt{\ln(N)})$. But this bound is not good comparative to the bound of the best known algorithm used to solve DLP, which is $O(\exp(1.92 + o(1)) N_{\mathbb{F}_p}^{1/3} (\ln(N_{\mathbb{F}_p})^{2/3}))$. However, by applying some restrictions on the parameters, a competitive bound can be achieved. For this, M_1, M_2 and S are considered to be permutation matrices and it is assumed that the polynomials p, q have l monomials. Then the matrix Z can be encoded with $N_\alpha = ml \log_2(m)$ bits and according to [9, Proposition 5.21], the expected running time complexity of the algorithm will be $O(\exp(\mu + o(1)) \sqrt{N_\alpha})$, where $\mu = \frac{\sqrt{2}d}{\sqrt{\ln(2)}l}$. This bound is assumed to be competitive to the bound of the best known algorithm used to solve DLP.

One particular example of two-sided matrix multiplication action is given in [11], in which the size of the matrices M_1, M_2 is taken greater than 420, and a particular semiring is used, which gives the maximum possible size of Z. With these choice of parameters, Alice has more than 2^{420} choices to select the polynomial p for which $p(M_1)$ can be computed with at most 420 matrix multiplications and additions. However, Alice may restrict the choice of p to reduce the number of multiplications and additions. If the degrees of p, q are restricted in the range of 50, then the complexity of brute force attack will depend on the size of the set $\mathcal{A} = \{p(M_1)Sq(M_2) : \deg p \leq 50, \deg q \leq 5\}$. The upper bound for the size of this set is 2^{100} and the least value is 2^{25}. The cryptanalysis of this example has been done in [20] and the choice of the above parameters is considered insufficient for practical use. According to the cryptanalysis discussed in [20], if the above parameters are used, then a complete session key can be recovered easily. Therefore, the parameters choices prescribed in [11] is not suggested for practical use and further research is required to achieve a good bound with better choice of parameters.

4.2 Formal security model of cryptographic schemes based on SAP

In [21] Stolbunov presented the security model of the key-exchange protocol and the ElGamal encryption scheme based on SAP. For defining the security of the key-exchange protocol, he used the security model proposed by Canetti and Krawczyk in [2].

The security of the ElGamal encryption scheme is defined using the indistinguishability of encryptions in chosen plain-text attack. The computational Diffie–Hellman group action problem (CDHAP), decisional Diffie–Hellman group action problem (DDHAP) and DDHAP assumption are presented in the paper for defining the security of scheme (defined in Section 3).

The following two theorems are proved in the paper [21] for defining the security of the key-exchange protocol and the ElGamal encryption scheme.

Theorem 4.1. *If the DDHAP assumption holds for a finite abelian group G acting on the set S, then the key agreement protocol is semantic secure in the adversarial model.*

Theorem 4.2. *If the DDHAP assumption holds for a finite abelian group G acting on the set S and the hash family H is entropy smoothing, then the public-key encryption scheme is secure against IND−CPA.*

5 Some work based on action of algebraic structure

In [17] Sakaluskas proposed a signature scheme based on the semiring action problem. To define this scheme he used two hard problems in his paper, which can be treated as one-way function, one is the multiple factor's search problem (MFSP) and the other is the operator and operand search problem (OOPS). He also used two operand search problems as an one-way function, denoted as $*$ and $\oplus$. It is proved in the paper that the scheme has provable security. He postulated three kind of attacks in his paper covering other possible attacks on the proposed signature scheme.

In [18] a digital signature scheme is defined using the action of infinite ring over module. The scheme is defined to be secure against data forgery, signature repudiation and existential forgery.

In [16] a digital signature scheme is defined using the Gaussian monoid. The proposed scheme is based on different hard problems which are linked to an one way function. The scheme is proved to be secure against existential forgery, data implied forgery and data implied forgery in module action level.

In [22] a bi-semigroup action problem (BSAP) is proposed and using this computational hard problem a new key exchange protocol is defined. In [8] some properties of semigroups are discussed which are useful for designing the public key cryptosystem. In [3] an efficient quantum algorithm is described by using Shor's algorithm [19] for computing discrete logarithms in semigroups. It is shown that some generalizations of DLP are hard in semigroups but easy in groups. It is discussed in the paper how SAP for a cyclic semigroup action can be considered as an instance of shifted DLP.

6 Future scope of SAP

It is explained in the previous sections how SAP can be considered the generalization of DLP. The semigroup action problem (SAP) is considered to be more secure because the structures used to define it do not contain invertible elements, and the semirings used to define the extension of SAP are simple, which reduces the probability of applying the Pohlig–Hellman attack. Therefore, using such algebraic structures, SAP can be used to define other public-key cryptographic schemes also, like authentication scheme, zero knowledge undeniable signature scheme, signcryption scheme etc.

7 Conclusion

In this paper, we have explained the SAP and summarized the work related to it. It is explained that how SAP is extended on different algebraic structures like semirings, semimodule, quotient semirings, quotient semimodule etc. To the best of our knowledge, in our paper we have covered almost all the work proposed in the literature related to cryptography based on SAP.

References

[1] R. E. Atani, S. E. Atani and S. Mirzakuchaki, Public key cryptography using semigroup actions and semirings, *J. Discrete Math. Sci. Cryptogr.* **11** (2008), no. 4, 437–445.

[2] R. Canetti and H. Krawczyk, Analysis of key-exchange protocols and their use for building secure channels, in: *Advances in Cryptology—EUROCRYPT 2001*, Lecture Notes in Comput. Sci. 2045, Springer, Berlin (2001), 453–474.

[3] A. M. Childs and G. Ivanyos, Quantum computation of discrete logarithms in semigroups, *J. Math. Cryptol.* **8** (2014), no. 4, 405–416.

[4] W. Diffie and M. E. Hellman, New directions in cryptography, *IEEE Trans. Inform. Theory* **IT-22** (1976), no. 6, 644–654.

[5] R. Ebrahimi Atani, S. Ebrahimi Atani and S. Mirzakuchaki, Public key cryptography based on semimodules over quotient semirings, *Int. Math. Forum* **2** (2007), no. 49–52, 2561–2570.

[6] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Trans. Inform. Theory* **31** (1985), no. 4, 469–472.

[7] A. Kendziorra, *Computational aspects of finite simple semirings*, Ph.D. thesis, University College Dublin, 2012.

[8] P. H. Kropholler, S. J. Pride, W. A. M. Othman, K. B. Wong and P. C. Wong, Properties of certain semigroups and their potential as platforms for cryptosystems, *Semigroup Forum* **81** (2010), no. 1, 172–186.

[9] G. Maze, *Algebraic Methods for Constructing One-way Trapdoor Functions*, ProQuest LLC, Ann Arbor, 2003; Thesis (Ph.D.)–University of Notre Dame.

[10] G. Maze, C. Monico and J. Rosenthal, Public key cryptography based on semigroup actions, preprint (2005), https://arxiv.org/abs/cs/0501017v2.

[11] G. Maze, C. Monico and J. Rosenthal, Public key cryptography based on semigroup actions, preprint 2007, https://arxiv.org/abs/cs/0501017v4.

[12] G. Maze, C. Monico, J. Rosenthal and J. J. Climent, Public key cryptography based on simple modules over simple rings, in: *Proceedings of the 15th International Symposium of the Mathematical Theory of Networks and Systems—MTNS*, University of Notre Dame, Paris (2002).

[13] C. J. Monico, *Semirings and Semigroup Actions in Public-key Cryptography*, ProQuest LLC, Ann Arbor, 2002; Thesis (Ph.D.)–University of Notre Dame.

[14] S. C. Pohlig and M. E. Hellman, An improved algorithm for computing logarithms over GF(p) and its cryptographic significance, *IEEE Trans. Inform.* **IT-24** (1978), no. 1, 106–110.

[15] R. L. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Comm. ACM* **21** (1978), no. 2, 120–126.

[16] E. Sakalauskas, New digital signature scheme in Gaussian monoid, *Informatica (Vilnius)* **15** (2004), no. 2, 251–270.

[17] E. Sakalauskas, One digital signature scheme in semimodule over semiring, *Informatica (Vilnius)* **16** (2005), no. 3, 383–394.

[18] E. Sakalauskas and T. Burba, Digital signature scheme based on action of infinite ring, *Inform. Technol. Control.* **31** (2004), no. 2, DOI 10.5755/j01.itc.31.2.11849.

[19] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J. Comput.* **26** (1997), no. 5, 1484–1509.

[20] R. Steinwandt and A. Suárez Corona, Cryptanalysis of a 2-party key establishment based on a semigroup action problem, *Adv. Math. Commun.* **5** (2011), no. 1, 87–92.

[21] A. Stolbunov, Reductionist security arguments for public-key cryptographic scheme based on group action, The Norwegian Information Security Conference, 2009.

[22] I. D. Trendafilov and M. I. Durcheva, Discrete logarithm in finite fields some algorithms for computing new public key cryptosystem, *AIP Conf. Proc.* **1293** (2010), DOI 10.1063/1.3515599.

[23] J. Zumbřagel, *Public-key cryptography based on simple semirings*, Ph.D. thesis, University of Zürich, 2008.