Ratio Mathematica Volume 41, 2021, pp. 19-27

Encryption using semigroup action

Anooja I[*]
Vinod S[†]
Biju G.S[‡]

Abstract

An enciphering transformation is a function f that converts any plaintext message into a ciphertext message and deciphering transformation is a function f^{-1}, which reverse the process. Such a set-up is called a cryptosystem. In this paper, we extend a generalization of the original Diffie-Hellman key exchange and ElGamal cryptosystem in $(\mathbb{Z}/p\mathbb{Z})^*$ by constructing a semigroup action on a finite dimensional vector space T over F_2.

Keywords: semigroup action; enciphering; plaintext; ciphertext; cryptosystem
2010 AMS subject classifications: 94A60, 08A70, 08A62. [1]

[*] Department of Mathematics, CMS College Kottayam (Autonomous), Kottayam 686 001 Kerala, India; anoojai@gmail.com.

[†] Department of Mathematics, Government College for Women, Thiruvananthapuram, Kerala, India; wenod76@gmail.com.

[‡] Department of Mathematics, College of Engineering, Thiruvananthapuram-695016, Kerala, India; gsbiju@cet.ac.in.

[1] Received on August 23, 2021. Accepted on December 14, 2021. Published on December 31, 2021. doi: 10.23755/rm.v41i0.649. ISSN: 1592-7415. eISSN: 2282-8214. ©Anooja et al.
This paper is published under the CC-BY licence agreement.

1 Introduction

Recently there has been a lot of on-going research work to find more secure and efficient public key cryptosystems based on algebraic structures such as non-abelian groups, linear groups, semigroups and power series rings (see Anshel et al. [1999], Baumslag et al. [2006], Maze et al. [2007], Shpilrain and Zapata [2006]), and where the security is based on hard algorithmic problems from combinatorial group theory. The hard problems from combinatorial group theory include the conjugacy search problem, the decomposition search problem and the subgroup membership search problem. Most common public key cryptosystems and public key exchange protocols presently in use, such as the RSA algorithm, Diffie-Hellman, and elliptic curve methods are number theory based and hence depend on the structure of abelian groups.

The idea of using semigroups as platforms for public key cryptosystems has appeared in several papers. Yamamura [1998] has considered a group action of $Sl_2(\mathbb{Z})$. Blackburn and Galbraith [1999] have analyzed the system of Yamamura and they have shown that it is insecure. Maze et al. [2007] showed that the discrete logarithm problem over a group can be considered as a special case of an action by a semigroup on a set. They showed that every semigroup action by an abelian semigroup on a set gives rise to a Diffie-Hellman key exchange. By taking the action of the semigroup on itself, a semigroup can then be used as a platform for a public key cryptosystem. Kropholler et al. [2010] studied the potential of the semigroup $\langle a, b\,; a^p = b^r, a^q = b^s\rangle$ as platforms for the Diffie-Hellman key exchange protocol. Special instances of semigroup actions appears in Anshel et al. [1999], Shpilrain and Ushakov [2005], Ko et al. [2000] and Slavin [2007]. In this paper, we try to extend a generalization of the original Diffie-Hellman key exchange and ElGamal cryptosystem in $(\mathbb{Z}/p\mathbb{Z})^*$ by constructing a semigroup from a (p, q)-graph G and defining a semigroup action on a finite vector space of dimension q over the field F_2.

2 Notations and Basic Results

Most of the notations, definitions and results we mentioned here are standard and can be found in Menezes et al. [1996], Koblitz [1998], Lyndon and Schupp [1977], Maze et al. [2007] and Diffie and Hellman [1976].

Most of the public key cryptosystems and public key exchange protocols currently in use, like the Diffie and Hellman [1976] key exchange protocol, the ElGamal [1985] public key cryptosystem, the Digital Signature Algorithm (DSA) and the ElGamal's signature scheme, use the discrete logarithm problem as the basis of their security.

The discrete logarithm problem can be defined as follows.

Problem 2.1. *(Discrete Logarithm Problem) Let G be a group and $a, b \in G$. Find an integer $n \in \mathbb{N}$ such that $a^n = b$.*

Problem (2.1) has a solution if and only if $b \in \langle a \rangle$, the cyclic group generated by a. If $b \in \langle a \rangle$ then there is a unique integer n satisfying $1 \leq n \leq ord(a)$ such that $a^n = b$. This unique integer is called the discrete logarithm of b with base a and denote it by $\log_a b$. Discrete Logarithm Problem plays important role in the Diffie-Hellman key agreement and the ElGamal public key cryptosystem, the digital signature algorithm and ElGamal's signature scheme. Currently the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$ of integers modulo n where n is a prime is widely used as the platform group.

Protocol 2.1. *(Diffie-Hellman Key Exchange Protocol) Let G be a group.*

1. *Alice and Bob publicly agree on an element $g \in G$.*
2. *Alice chooses $n \in \mathbb{N}$ and computes g^n . Alice's private key is n, her public key is g^n.*
3. *Bob chooses $m \in \mathbb{N}$ and computes g^m . Bob's private key is m, his public key is g^m.*
4. *Their common secret key is then g^{mn}.*

The ElGamal public key cryptosystem works as follows:

Alice chooses $n \in \mathbb{N}$, $a, b \in G$ where $b = a^n$. The private key of Alice is (a, b, n), the public key is (a, b). Bob chooses a random integer $r \in \mathbb{N}$ and he applies the encryption function

$$\begin{aligned} \varphi &: G \to G \times G \\ m &\to (c_1, c_2) = (a^r, mb^r) \end{aligned}$$

Alice computes m from the ciphertext (c_1, c_2) by $m = c_2(c_1^n)^{-1}$.

3 Construction of a semigroup from a (p, q)- graph

Let G be a finite (p, q)-graph and H be a subgraph of G. Let x_H denote a vector corresponding to H such that $x_H = (x_1, x_2, \ldots, x_q)$ where

$$x_i = \begin{cases} 1 & \text{if } e_i \text{ is in } H \\ 0 & \text{otherwisef} \end{cases}$$

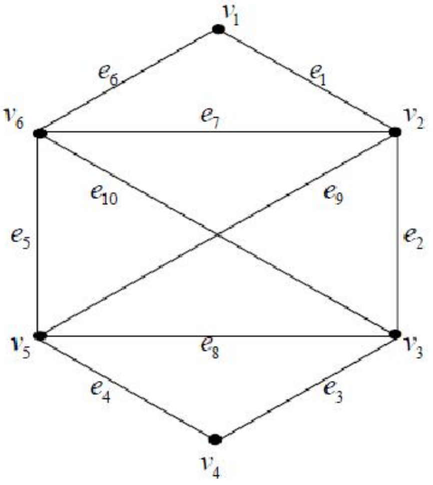

Figure 1: Graph G

Let S be a set of such vectors. Then S is a semigroup under the operation defined by

$$\begin{aligned} x_H\, y_K &= (x_1, x_2, \ldots, x_q)(y_1, y_2, \ldots, y_q) \\ &= (x_1y_1, x_2y_2, \ldots, x_qy_q) \end{aligned}$$

We shall illustrate this with the following example.

Example 3.1. *Consider the graph G with $p = 6$ and $q = 10$ given in Figure 1. Let us consider seven subgraphs of G, which are displayed in Figure 2. Let x_{H_1}, $x_{H_2}, \ldots$,x_{H_7} be the vectors corresponding to the subgraphs H_1, $H_2, \ldots$, H_7 respectively. Let $S = \{x_{H_1}, x_{H_2}, \ldots, x_{H_7}\}$. Then*

$$\begin{aligned} x_{H_1} &= (1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \\ x_{H_2} &= (1, 1, 0, 0, 0, 1, 1, 0, 0, 0) \\ x_{H_3} &= (1, 1, 1, 0, 0, 0, 0, 0, 1, 0) \\ x_{H_4} &= (1, 0, 0, 0, 0, 1, 0, 0, 0, 0) \\ x_{H_5} &= (1, 0, 1, 0, 0, 0, 0, 0, 1, 0) \\ x_{H_6} &= (1, 1, 0, 0, 0, 0, 0, 0, 0, 0) \\ x_{H_7} &= (1, 0, 0, 0, 0, 0, 0, 0, 0, 0) \end{aligned}$$

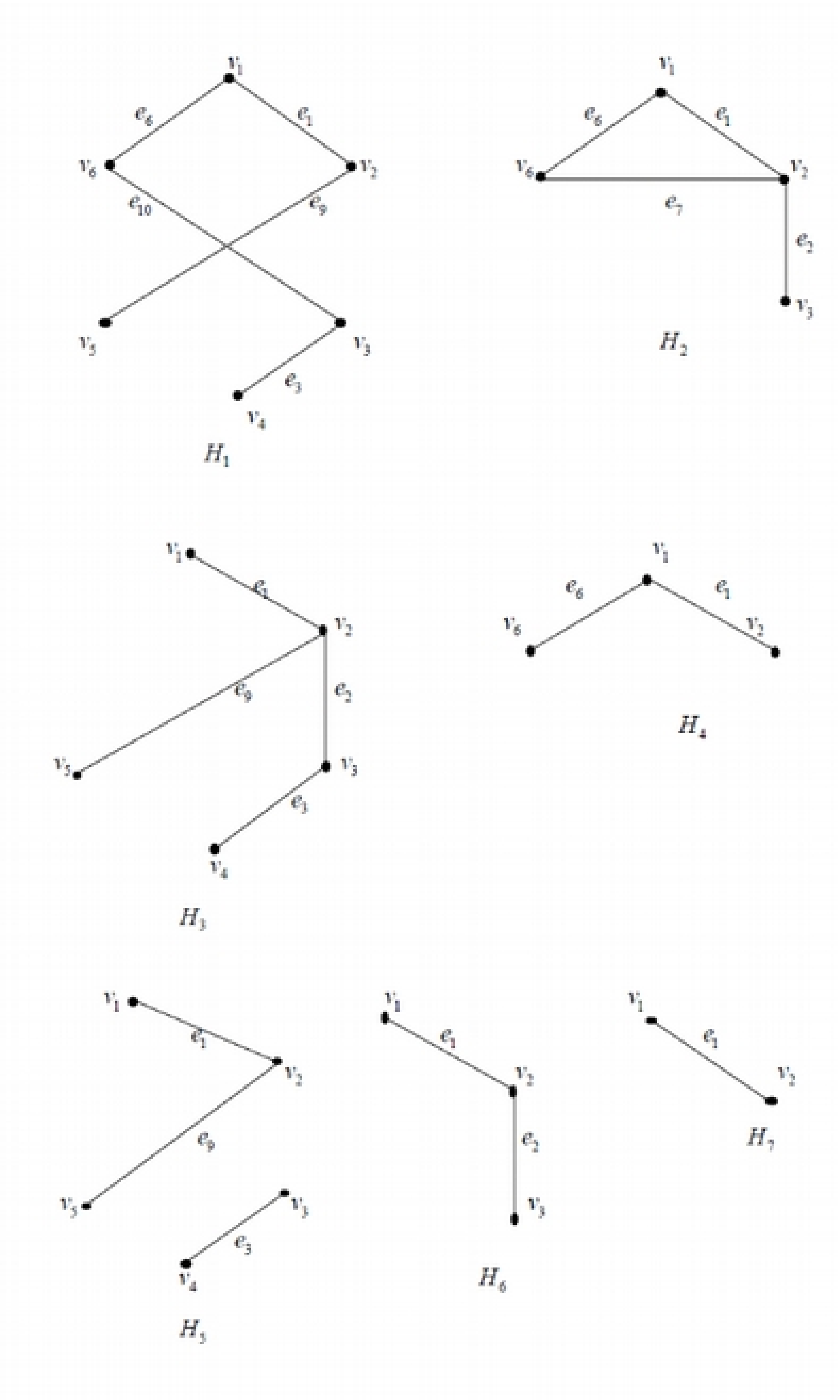

Figure 2: Subgraphs of the graph G

Now,

$$\begin{array}{llll}
x_{H_1}x_{H_2} = x_{H_4}, & x_{H_1}x_{H_3} = x_{H_5}, & x_{H_1}x_{H_4} = x_{H_4}, & x_{H_1}x_{H_5} = x_{H_5}, \\
x_{H_1}x_{H_6} = x_{H_7}, & x_{H_1}x_{H_7} = x_{H_7}, & x_{H_2}x_{H_3} = x_{H_6}, & x_{H_2}x_{H_4} = x_{H_4}, \\
x_{H_2}x_{H_5} = x_{H_7}, & x_{H_2}x_{H_6} = x_{H_6}, & x_{H_2}x_{H_7} = x_{H_7}, & x_{H_3}x_{H_4} = x_{H_7}, \\
x_{H_3}x_{H_5} = x_{H_5}, & x_{H_3}x_{H_6} = x_{H_6}, & x_{H_3}x_{H_7} = x_{H_7}, & x_{H_4}x_{H_5} = x_{H_7}, \\
x_{H_4}x_{H_6} = x_{H_7}, & x_{H_4}x_{H_7} = x_{H_7}, & x_{H_5}x_{H_6} = x_{H_7}, & x_{H_5}x_{H_7} = x_{H_7}, \\
x_{H_6}x_{H_7} = x_{H_7} & & &
\end{array}$$

Also,

$$x_{H_i}(x_{H_j}x_{H_k}) = (x_{H_i}x_{H_j})x_{H_k}, \quad i, j, k = 1, 2, \ldots, 7.$$

Hence S is a semigroup.

4 Key Exchange using S-action

Let T be a q dimensional vector space over F_2. Define the left action of S on T, $\varphi : S \times T \to T$ such that $\varphi(x, t) = xt$. We call this action as an S-action on the vector space T. The right action is similarly defined.

Let G be a (p, q)-graph, S an abelian semigroup associated with the graph G, T be a q dimensional vector space over F_2, and an S-action on T as defined above.

Diffie-Hellman key exchange using S-action is as follows:

1. Alice and Bob agree on an element $t \in T$.
2. Alice chooses $x \in S$ and computes xt. Alice's private key is x, her public key is xt.
3. Bob chooses $y \in S$ and computes yt. Bobss private key is y, his public key is yt.
4. Their common secret key is then $x(yt) = (xy)t = (yx)t = y(xt)$.

Example 4.1. *Consider the semigroup S in the example 3.1. Let T be a 10 dimensional vector space over F_2. Suppose Alice and Bob want to agree on a key. Suppose they choose $t = (0, 1, 1, 0, 1, 0, 1, 1, 0, 0) \in T$. Then Alice chooses $x_{H_1} = (1, 0, 1, 0, 0, 1, 0, 0, 1, 1) \in S$ and computes $x_{H_1}t = (0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$. Then send it to Bob. Similarly, Bob chooses $x_{H_6} = (1, 1, 0, 0, 0, 1, 0, 0, 1, 1) \in S$ and computes $x_{H_6}t = (0, 1, 0, 0, 0, 0, 0, 0, 0, 0)$. Then send it to Alice. Their common key is $x_{H_1}(x_{H_6}t) = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$.*

S-action Problem

Let G be a (p, q)-graph and S be a semigroup associated with the graph G, acting on a q dimensional vector space T over F_2.

Given elements $t \in T$ and $y \in S$, find $x \in S$ such that $xt = y$.

4.1 Diffie-Hellman Problem using S-action

Let G be a (p, q)-graph, S be a semigroup associated with the graph G, T be a q dimensional vector space over F_2 and φ be an S-action on T.

Given $r, s, t \in T$ with $s = xr$ and $t = yr$ for some $x, y \in S$, find $(xy)r \in T$.

5 Cryptosystem using S-action

Let G be a (p, q)-graph, S be a semigroup associated with the graph G, T be a q dimensional vector space over F_2, T is an additive abelian group and an action on T as defined above.

ElGamal cryptosystem using S-action is as follows:

1. Alice chooses elements $t \in T$ and $x \in S$. Alice's public key is (t, xt).
2. Bob chooses a random element $y \in S$ and encrypts a message m using the encryption function $(m, y) \mapsto (yt, (y(xt)) + m) = (c_1, c_2)$.
3. Alice can decrypt the message using

$$\begin{aligned} m &= (y(xt))^{-1} + (y(xt)) + m \\ &= (xc_1)^{-1} + c_2 \end{aligned}$$

Note: Message m is also represented as vectors. Each letter in the message represents a vector $(x_1, x_2, \ldots, x_q)$, $q \geq 26$ such that

$$x_i = \begin{cases} 1 & \text{if the corresponding letter is in } i^{th} \text{ position of the alphabet} \\ 0 & \text{otherwise} \end{cases}$$

Example 5.1. *Let G be any (p, q)-graph with $q = 26$. Let T be a 26 dimensional vector space over F_2, T be an additive abelian group and S be the semigroup associated with the graph G. The action of S on T is as defined earlier. Suppose Alice wants to receive a message.*

1. *Alice chooses* $t = (0,1,1,0,1,0,1,1,0,\dots,0) \in T$. *Then chooses* $x = (1,0,1,0,1,0,1,0,1,0,\dots,0) \in S$ *corresponding to one subgraph* H_1 *of* G *and compute* $xt = (0,0,1,0,1,0,1,0,0,\dots,0)$. *Her public key is* (t, tx).

2. *Bob wishes to send a message* $m =$ *MEET ME TOMORROW to Alice. He send it letter by letter. So, first he wants to send the letter* $M = m_1(m) = (0,0,\dots,0,0,1,0,0,\dots,0,0)$.

   For, he chooses $y = (0,0,1,0,1,0,0,1,1,0,0,\dots,0,0) \in S$ *that is a vector corresponding to one subgraph*H_2 *of* G *and compute*

   $$\begin{aligned} yt &= (0,0,1,0,1,0,0,1,0,0,\dots,0,0) = c_1 \\ y(xt) &= (0,0,1,0,1,0,0,\dots,0,0) \end{aligned}$$

   and

   $$y(xt) = (0,0,1,0,1,0,0,0,0,0,0,0,1,0,\dots,0,0) = c_2$$

   Then he sends (c_1, c_2) *to Alice.*

3. *After receiving this, Alice decrypt the message by computing* $(xc_1)^{-1} + c_2$.

   $$\begin{aligned} xc_1 &= (0,0,1,0,1,0,0,\dots,0,0) \\ (xc_1)^{-1} &= (0,0,1,0,1,0,0,\dots,0,0) \\ (xc_1)^{-1} + c_2 &= (0,0,0,\dots,0,0,1,0,\dots,0,0) \\ &= m_1(m) = M \end{aligned}$$

Similarly, they transfer each letter in the message.

References

Iris Anshel, Michael Anshel, and Dorian Goldfeld. An algebraic method for public key cryptography. *Mathematical Research Letters*, 6(3–4):287–291, 1999.

Gilbert Baumslag, Benjamin Fine, and Xiaowei Xu. Cryptosystems using linear groups. *Applicable Algebra in Engineering, Communication and Computing*, 17(3):205–217, 2006.

Simon R Blackburn and Steven Galbraith. Cryptanalysis of two cryptosystems based on group actions. In *International Conference on the Theory and Application of Cryptology and Information Security*, volume 3531, pages 52–61. Springer, 1999.

Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE transactions on Information Theory*, 22(6):644–654, 1976.

Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory*, 31(4):469–472, 1985.

Ki Hyoung Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Ju-sung Kang, and Choonsik Park. New public-key cryptosystem using braid groups. In *Annual International Cryptology Conference*, pages 166–183. Springer, 2000.

Neal Koblitz. *Algebraic methods of cryptography*. Berlin Heidelberg New York: Springer, 1998.

PH Kropholler, SJ Pride, WAM Othman, KB Wong, and PC Wong. Properties of certain semigroups and their potential as platforms for cryptosystems. In *Semigroup Forum*, volume 81, pages 172–186. Springer, 2010.

Roger C Lyndon and Paul E Schupp. *Combinatorial group theory*. Berlin Heidelberg New York: Springer, 1977.

Gérard Maze, Chris Monico, and Joachim Rosenthal. Public key cryptography based on semigroup actions. *Advances of Mathematics of Communications*, 1 (4):489–507, 2007.

Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. *Handbook of Applied Cryptography. Discrete Mathematics and Its Applications*. CRC press, New York, 1996.

Vladimir Shpilrain and Alexander Ushakov. Thompson's group and public key cryptography. In *International Conference on Applied Cryptography and Network Security*, pages 151–163. Springer, 2005.

Vladimir Shpilrain and Gabriel Zapata. Combinatorial group theory and public key cryptography. *Applicable Algebra in Engineering, Communication and Computing*, 17(3):291–302, 2006.

Keith R Slavin. Public key cryptography using matrices. 2007. US Patent 10260818, http://www.patentstorm.us/patents/7184551-fulltext.html.

Akihiro Yamamura. Public-key cryptosystems using the modular group. In *International Workshop on Public Key Cryptography*, pages 203–216. Springer, 1998.