Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 6, pp. 1753–1760
DOI : 10.47974/JDMSC-1640

The Huff curve–ElGamal graphic public key cryptosystem

Batool Hatem Akar Alkfari *
Ruma Kareem K. Ajeena †
Department of Mathematics
Education College for Pure Sciences
University of Babylon
Babylon
Iraq

Abstract

A new graph for the cryptographic application is presented in this work. This graph is defined using the Huff curve over a prime field. The Huffs curve graph (HC_g) considered as an alternative graph of the Edwards curve graph (E_dCG).The HC_g is used to give another modified Version Public-key cryptosystem ElGamal (EPKC) the proposed HC-ElGamal graphic cryptosystem enhances the secure communication in compare with original EPKC.

Subject Classification: *62-09; 65S05.*

Keywords: *Cryptography, Graph theory, Huff curve, Security.*

1. Introduction

Algebra and number theory are used to solve several problems in mathematics and computer science and other fields especially in cryptography [1]. W. Diffie and M. Hellman used the discrete logarithm problem (DLP) in 1976 to calculate and distribute the private key to two users [2]. ElGamal public key that is proposed in 1985 is also based on DLP [3]. Wael Al Etaiwi [4] in 2014 used the graph theory ideas to encrypt and decrypt data. Shubham Agarwal and Anand Singh Uniyal [5] in 2015 came up with the idea of a prime weighted graph (PWG) as a way to make

* *E-mail:* batool.hatem.pure291@student.uobabylon.edu.iq
(Corresponding Author)
† *E-mail:* pure.ruma.k@uobabylon.edu.iq

communication more secure (PWG). Recently, in 2021, Ruma Ajeena [6] used the connected sub-graphs of undirected simple graph to proposed the soft graphic ISD (SG-ISD) method. Also, in 2021, Karrar Aljamaly and Ruma Ajeena [7] introduced a novel public key cryptosystem based on undirected complete graphs (UCG). And in [8], To develop a novel asymmetric encryption algorithm, they defined a new graph based on elliptic scalar multiplication over a prime field. In this work, a Huff curve graph (*HCg*) is defined as a new graph and a main point to work. The points on the *HC* graph are the points lie on the Huff curves that form a Huffs curves group over a prime field. A subgraph of the *HC* graph is defined as well. Using the HC subgraph, the matrix representation of the proposed algorithm enables quick computations and makes it simpler to implement. The HC graphic cryptosystem is more secure than the old asymmetric cryptosystem. So, the HC graphic asymmetric cryptosystem is seen as a new way to use Huffs curve cryptography.

2. Huff Curve Modulo *p*

Huff in 1948 [9] proposed an elliptic curve model to analyze a Diophantine issue. When dealing with elliptic curves, the Huff's model is provided by the following formula

$$HC{:}ax(y^2\text{-}1) = by(x^2\text{-}1) \pmod{p} \text{ with } a^2 \neq b^2$$

An addition and doubling of two points on HC are computed by

i. Dedicated addition. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on HC and $P_1 \neq P_2$. The addition $P_1 + P_2$ is computed by

$$P_1 + P_2 \equiv \left(\frac{(x_1 - x_2)(y_1 + y_2)}{(1 - x_1x_2)(y_1 - y_2)}, \frac{(y_2 - y_1)(x_1 + x_2)}{(x_1 - x_2)(1 - y_1y_2)} \right) (\mathrm{mod}\, p).$$

ii. Unified addition. The addition of the points P_1 and P_2 can be computed by alternative formula that is given by

$$P_1 + P_2 \equiv \left(\frac{(x_1 + x_2)(1 + y_1y_2)}{(1 + x_1x_2)(1 - y_1y_2)}, \frac{(y_2 + y_1)(1 + x_1x_2)}{(1 - x_1x_2)(1 + y_1y_2)} \right) (\mathrm{mod}\, p).$$

iii. Doubling. The doubling point $2P_1$ of the point P_1 is computed by

$$2P_1 \equiv \left(\frac{2x_1(1 + y_1)}{(y_1^2 - 1)(1 + x_1^2)}, \frac{2y_1(1 + x_1^2)}{(x_1^2 - 1)(1 + y_1^2)} \right) (\mathrm{mod}\, p),$$

where the identity element is (0, 0) and $-P = (-x, -y)$.

3. The Graphic Representation of HC over Prime Field

The Huff points over a prime field have been used to define an alternative graph of the Edwards curve graph (E_dCG) [10]. This graph is called a Huff curve graph (HC_g) which is defined as follows.

Definition 3.1: Let $HC(F_p)$ be a Huff curve group. If $P + Q = (0, 0)$, where $(0, 0)$ is the identity element and $Q = -P$ such that P and Q are two different points in $HC(F_p)$, then P and Q are adjacent or can be joined by an edge in the graph. In addition, every Huffs point is adjoined with the identity element. Then it is possible to form the HC graph $HC_g(F_p)$ that is corresponding to $HC(F_p)$.

For instance, if $HC : x(y^2 - 1) = 3y(x^2 - 1) (\mathrm{mod}\, 7)$ is a Huff curve. The point on HC form a set $HC(F_p) = (0, 0), (1, 1), (1, 6), (6, 1), (6, 6)\}$. The $HC_g(F_p)$ is shown in Figure (1).

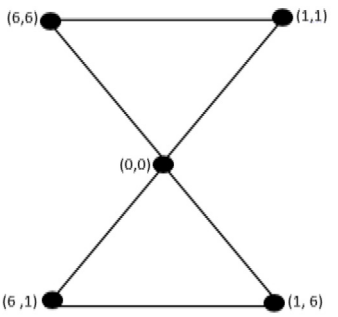

Figure 1

The $HC_g(F_p)$ of $HC(F_p)$.

4. The HC- ElGamal Graphic Cryptosystem

This section presents alternative version of EPKC using the Huff curve points and the HC_g graph. The public parameters are a Huff curve group $HC(F_p)$ and the matrix $T \in GL_n(F_p)$. The proposed HC- ElGamal graphic cryptosystem is explained through the following algorithm.

Algorithm. The HC- ElGamal Graphic Cryptosystem

Key Generation [9]:

Input. A prime number p and the matrix $T \in GL_n(F_p)$.

Output. The public key A, where $A \in GL_n(F_p)$.

1. Alice selects the value a as her private key, where a $\in$ {2, ..., p – 1}.
2. She generates a public key $A = T^a \pmod{p}$.
3. Alice's keys (A, a).

Encryption:

Input. The matrices $T \in GL_n(F_p)$ and a public key A.

Output. The ciphertext (C_1, C_2), where C_1 and C_2 are two matrices.

1. Bob chooses his plaintext M which is the Huffs curve subgroup of $HC_s(F_p)$ such that if (x, y) $\in$ M then (-x, -y) $\in$ M.
2. He represents his plaintext M by subgraph $HC_s(F_p)$.
3. He converts the $HC_s(F_p)$ into a weighted graph. This converting is done through computing the weights for all edges, if (x, y) and (–x, -y) two points between any edge then the weight of this edges is W = min {x, –x}, if (x, y) and (0, 0) two points between any edge then the weight of this edges is w = 0.
4. A weighted graph converted into another graph after deleting one of the triangles that have the same weights and It is represented by an adjacent matrix B.
5. He selects his secret key $b \in \{2, 3, ..., p - 1\}$.
6. Two square matrices are used to calculate the ciphertext. $C_1 \equiv T^b \pmod{p}$ and $C_2 \equiv A^b M \pmod{p}$.
7. Bob sends Alice the pair of ciphertexts (C1, C2).

Decryption:

Input. A prime p and a ciphertext (C_1, C_2).

Output. The plaintext M which is the Huff curve subgroup of $HC(F_p)$.

1. Alice computes $(C_1{}^a)^{-1} \pmod{p}$.
2. She computes the multiplication matrix $(C_1^a)^{-1} \times C_2 \pmod{p}$.
3. She represents matrix B by a weighted graph.
4. She gets the Huffs points by using the weights of all edges that give the original plaintext.

5. Study case of the *HCg* cryptosystem

Suppose HC is a Huff curve defined by HC: $20x(y^2\text{-}1) = 5y(x^2\text{-}1)$ over the prime field F_{103}. A set $HC(F_{103})$ of all points lying on HC is computed by

$$HC(\mathrm{F}_{103}) = \{(1, 1), (1, 102), (2, 11), (2, 28)...(0, 0)\}$$

which forms an abelain group under addition. This group is called Huff group and it has prime order $n = 117$. The public matrix

$$T = \begin{pmatrix} 31 & 41 & 101 & 55 & 23 \\ 23 & 67 & 78 & 90 & 3 \\ 56 & 89 & 18 & 23 & 7 \\ 76 & 33 & 101 & 13 & 23 \\ 12 & 34 & 67 & 17 & 99 \end{pmatrix} \in GL_5(F103).$$

Alice chooses her privet key $a = 4$ and compute her puplic key A by

$$A = T^4 (\mathrm{mod}103) = \begin{bmatrix} 49 & 33 & 59 & 30 & 99 \\ 23 & 55 & 59 & 16 & 48 \\ 38 & 82 & 62 & 41 & 38 \\ 66 & 53 & 87 & 10 & 61 \\ 33 & 83 & 100 & 25 & 3 \end{bmatrix}.$$

Bob chooses his plaintext M by

$M = \{(31, 43), (72, 60), (46, 73), (19, 31), (84, 72), (93, 43), (10, 60), (0, 0)\}$.

M is a subset of a Huff curve set $HC_s\ (F_{103})$ is a plaintext which is represented by Huff curve weighted subgraph $HC_s\ (F_{103})$ as shown in Figure (2).

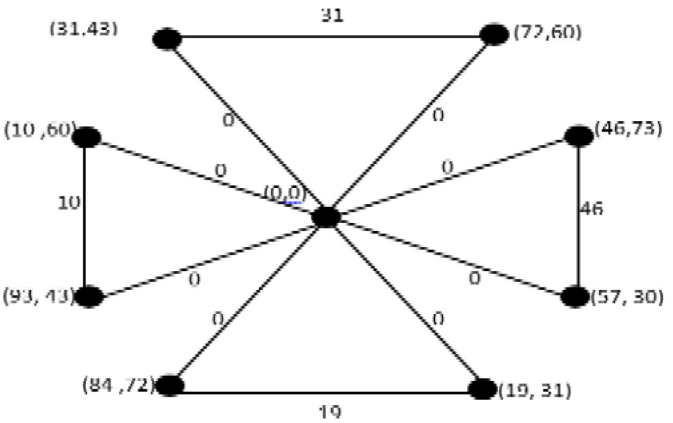

Figure 2

The Huff curve weighted subgraph $HC_s(F_{103})$.

Bob converts Huff curve weighted subgraph $HC_s(F_{103})$ into another Huff curve graph $HC_s^*(F_{103})$ as seen in Figure (3).

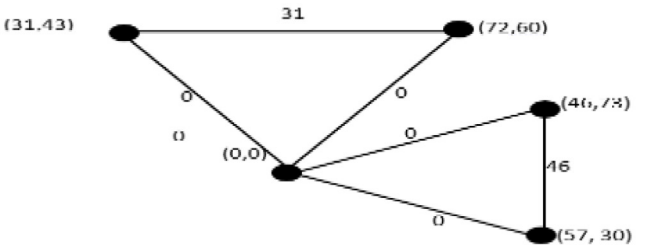

Figure 3

The Huff curve weighted subgraph $HC_s^*(F_{103})$.

An adjacent matrix B of $HC_s^*(F_{103})$ is computed by

$$B = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 31 & 0 & 0 \\ 0 & 31 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 46 \\ 0 & 0 & 0 & 46 & 0 \end{bmatrix}.$$

Bob chooses a secret key $b = 3$ and computes the ciphertext (C_1, C_2) by

$$C_1 = T^3 (\mathrm{mod}\, 103) = \begin{bmatrix} 67 & 35 & 52 & 65 & 55 \\ 50 & 38 & 69 & 63 & 66 \\ 51 & 38 & 99 & 96 & 59 \\ 3 & 23 & 37 & 90 & 35 \\ 17 & 67 & 61 & 11 & 34 \end{bmatrix} \text{ and}$$

$$C_2 = A^3 \times B (\mathrm{mod}\, 103) \equiv \begin{bmatrix} 0 & 9 & 95 & 54 & 33 \\ 0 & 13 & 21 & 37 & 4 \\ 0 & 93 & 28 & 86 & 4 \\ 0 & 42 & 22 & 50 & 29 \\ 0 & 53 & 84 & 38 & 99 \end{bmatrix}.$$

He sends the pair of ciphertexts (C_1, C_2) to Alice.

After receiving the ciphertext pair (C_1, C_2) to Alice, she wants to decrypt and recover the original plaintext. She computes first

$$(C_1^4)^{-1} (\mathrm{mod}\, 103) \equiv \begin{bmatrix} 6 & 51 & 8 & 27 & 21 \\ 28 & 15 & 27 & 51 & 102 \\ 77 & 32 & 6 & 14 & 28 \\ 85 & 42 & 0 & 18 & 64 \\ 63 & 40 & 0 & 97 & 27 \end{bmatrix}$$

$$(C_1^4)^{-1} \times C_2 (\text{mod} 103) = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 31 & 0 & 0 \\ 0 & 31 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 46 \\ 0 & 0 & 0 & 46 & 0 \end{bmatrix} = B.$$

Alice represents a matrix B by a weighted graph in Figure (2) and gets the original plaintext

M = {(31, 43), (72, 60), (46, 73), (19, 31), (84, 72), (93, 43), (10, 60), (0, 0)}

by using the weighted of edges graph.

6. The Security Consideration of Huffs Curve Graphic Cryptosystem

The concepts of graph theory are viewed here as an indispensable instrument for enhancing security. The security of the proposed *HC* graphic cryptosystem depends on the random choice of the HC subgraph that corresponds to the HC subgroup of an *HC* group $HC(F_p)$. With a large prime number p, the *HC* graph has a large number of the vertices. Thus, it is possible to form a large number of the *HC* subgraphs. Choosing one of these subgraph randomly to represent a plaintext gives more secure to communicate using the proposed *HC* graphic cryptosystem. Eve needs to compute many cases to reach the correct choice of the *HC* subgraph. Thus, the *HC* graphic cryptosystem is more secure and suitable for Huffs cryptographic communication schemes.

7. Conclusions

This paper suggested a new graph HCg using the Huff curve defined over a prime field. This graph is used to modify the original EPKC. On the proposed HC-ElGamal graphic cryptosystem the security issues are determined. The HC-ElGamal graphic cryptosystem is considered as a more secure communication encryption scheme in compare with the original one.

References

[1] Hashim, Hashim Madlool, and Ruma Kareem K. Ajeena. "The Computational Complexity of the Elliptic Curve Factorization Algorithm over Real Field." *Journal of Physics: Conference Series*. Vol. 1897. No. 1. IOP Publishing, 2021.

[2] Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE transactions on Information Theory,* 22(6), 644-654.

[3] ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on Information Theory,* 31(4), 469-472.

[4] Al Etaiwi, W. M. (2014). Encryption algorithm using graph theory, *Journal of Scientific Research and Reports,* 2519-2527.

[5] Agarwal, Shubham, and Anand Singh Uniyal. Prime Weighted Graph in cryptographic System For Secure Communication. I*nternational Journal of Pure and Applied Mathematics,* 105(3), (2015), 325-338.

[6] R. Ajeena, "The soft graphic integer sub-decomposition method for elliptic scalar multiplication," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 24, no 6 pp. 1751-1765, 2021.

[7] K. Aljamaly, and R. Ajeena, "Undirected Complete Graph to Design New Public Key Cryptosystem," *Journal of Physics: Conference Series*. vol. 1897, no. 1, IOP Publishing, 2021.

[8] K. Aljamaly, and R. Ajeena, "The elliptic scalar multiplication graph and its application in elliptic curve cryptography," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 24, no 6 pp. 1793-1807, 2021.

[9] R. Ajeena, and K. Aljamaly, The Edwards Curve Graphic Encryption Scheme, *Journal of Discrete Mathematical Sciences and Cryptography*, in press, 2022.

[10] G. B. Huff. Diophantine problems in geometry and elliptic ternary forms. *Duke Math. J.*, 15:443–453, 1948.

Received May, 2022

Revised June, 2022