Iraqi Journal of Communications and Computer Networks
e-ISSN: 3105-9252, p-ISSN: 3105-9244
Vol. (1), Iss. (1), September 2025
DOI: https://doi.org/10.58564/IJCCN.1.1.2025.5

https://ijccn.net/ **Research Article**

Colored Star Graph for Encryption Schemes

Ruma Kareem K. Ajeena [1*], Satea Hikmat Alnajjar [2], Sabah Mahmoud K. Al-Masoudi [3], Atheer Jawad Kadhim [4]

[1] Prof. Dr., Computer Science Department, College of Education for Pure Science Ibn Al- Haitham, University of Baghdad & Scientists Foundation for Development Baghdad, Iraq
[2] Asst. Prof. Dr., Network Engineering and Cyber security Department, College of Engineering, Al-Iraqia University, Baghdad, Iraq
[3] Head of Foundation, Scientists Foundation for Development, Baghdad, Iraq
[4] Researcher, Babylon Education Directorate, Babylon, Iraq

***Corresponding Author:** ruma.k.kh@ihcoedu.uobaghdad.edu.iq, scientists.ffd2019@gmail.com

Citation: Kareem K. Ajeena , R., Satea Hikmat Alnajjar, Sabah Mahmoud K. Al-Masoudi, & Atheer Jawad Kadhim. (2025). Colored Star Graph for Encryption Schemes. Iraqi Journal of Communications and Computer Networks (IJCCN), 1(1), 47–51.

ARTICLE INFO

Received: 11 Apr. 2025
Revised: 05 Jul. 2025
Accepted: 11 Jul. 2025

ABSTRACT

Graph theory as an essential area of mathematics for several applications. It uses for modeling many real life problems in various specializations, in engineering , computer science, banking, industry, transportation, as well as in cryptography and security to solve them. In this work, alternative symmetric encryption (SE) scheme are proposed based on new formula of shared secret key (SSK). This key is generated using the coloring star graph (CSG). The ciphertext of the plaintext, that is an English word or English sentence, is computed and sent in the channel as the CSG. The attackers here with the proposed SE scheme facing the difficulty to recover the secret key. New experimental result is presented with small parameters as a study case. So, the security of the proposed CSG-SE scheme depending on how to generate the secret key. Thus, the CSG-SE scheme considers as more secure SE scheme in compare with previous ones for communication.

Keywords: Cryptography, SE scheme, Graph theory, CSG, Security.

INTRODUCTION

Several problems in the real life are solved using the various mathematical methods [1,2]. Elliptic curves also have been employed to solve many problems in different area [3-6], especially in cryptography. On the other hand, graph theory is widely used as a tool for encryption due to its various properties and its easy representation on computers as a matrix. It is considered as an essential tool in many cryptographic applications. Most of them focused on applying various concepts of graph theory to design the symmetric encryption algorithms [7-11].

A new version of SE scheme has been proposed in this work which it depending on the CSG. The secret key is computed strongly based on the CSG. The ciphertext here is done for an English word as the CSG as well. The security level has been determined in compared with other SE schemes.

The outline of this paper consists of: Section II includes the SE scheme using the CSG. Section III discusses the computational result of the proposed encryption scheme that based on CSG. Section IV displays the security issues of the proposed CSG-SE scheme. Finally, Section V draws the conclusions.

Copyright © 2025 by Author/s and Licensed by IJCCN.
This is an open access article distributed under the This journal is licensed under a Creative Commons Attribution 4.0 International License.

THE SYMMETRIC ENCRYPTION SCHEME BASED ON CSG

Suppose the plaintext m can be taken as an English word or sentence which can write by

$$m = \{m_1, m_2, \ldots, m_n\} = \{m_i\}_{i=1,2,\ldots,n}.$$

The English alphabetic (EAVS) can replaced by the values:

$$A \rightarrow 0, B \rightarrow 1, C \rightarrow 2, \ldots, Z \rightarrow 25.$$

The letters of m, using the EAVs, are written as the numbers modulo 26. These numbers can be rewritten as the binary forms. Let K be a coloring star graph (CSG) that displayed in Figure (1).

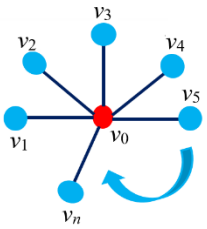

Figure 1. A coloring star graph (CSG).

Using the K graph, the SSK is created by

$$k \equiv n * \text{the color} \pmod{26},$$

where n is a number of the vertices in CSG except the color of the center vertex. The colored vertices have been represented as the decimal numbers using the EAVs. The binary expansions of these decimals are formed. Computing theciphertext C of m is done by

$$C \equiv m + k \pmod{2}.$$

Namely,

$$c_i \equiv m_i + k_i \pmod{2}, \text{ for } i = 1,2, \ldots, n.$$

The ciphertext string C = (c1, c2,..., cn) is created as the CSG as shown in Figure (2) which has been sent to second user.

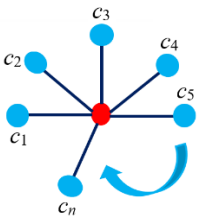

Figure 2. The ciphertext of the CSG.

The ciphertext has been send to second user as the CSG. He/She uses the CSG to determine the vertices of CSG. These vertices will be rewritten as the decimal representations depending on the EAVs. The binary forms of these decimal numbers is created. On the other hand, the SSK is computed based on the CSG vertices (which can be selected by red color for example) by

$$k \equiv n * \text{ the color (say red)} \pmod{26}.$$

Hence, the computation of the plaintext is done by

$$m_i \equiv c_i - k_i \pmod 2, \text{ for } i = 1,2, \ldots, n.$$

Namely,

$$m = \{m_1, m_2, \ldots, m_n\}.$$

RESULTS AND DISCUSSION

Study Case Using the CSG for SE Scheme

A plaintext m is chosen as the word Ali which is represented by

$$m = \{m_1, m_2, m_3\} = \{A, l, i\}.$$

Based on the EAVs, the letters of m_1, m_2 and m_3 are written by

$$m = \{0, 11, 8\}.$$

The numbers 0, 11 and 8 are rewritten in binary form by

$$0 \rightarrow 00000,\ 11 \rightarrow 01011,\ 8 \rightarrow 01000.$$

Now, suppose the K is a CSG that is given by

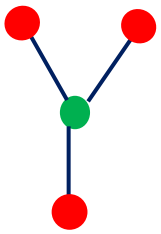

Figure 3. The CSG with a 3-red color vertices.

Based on the K graph, first user computes his /her SSK by

$$k = 3 * \text{red} \pmod{26}$$

where 3 is the red color vertices and red is a color of the vertices except the center vertex of the CSG. Now, the decimal representations of the letters r, e, d in the red word are done based the EAVs. So,

$$r \rightarrow 17,\ e \rightarrow 4 \text{ and } d \rightarrow 3.$$

Thus,

$$\begin{aligned} k &\equiv 3 * \{r, e, d\} \pmod{26} \\ &\equiv \{3*17, 3 * 4, 3 * 3\} \pmod{26} \\ &\equiv \{25, 12, 9\}. \end{aligned}$$

The numbers 25, 12, 9 are rewritten as binary strings:

$$25 \rightarrow 11001 = k_1,\ 12 \rightarrow 01100 = k_2,\ 9 \rightarrow 01001 = k_3.$$

The ciphertext C of m is calculated by

$$c_i \equiv m_i + k_i \pmod 2, \text{ for } i = 1,2,3.$$

In more details,

$$\begin{aligned} c_1 &\equiv m_1 + k_1 \pmod 2 \equiv 00000 + 11001 = 11001 \\ c_2 &\equiv m_2 + k_2 \pmod 2 \equiv 01011 + 01101 = 00111 \\ c_3 &\equiv m_3 + k_3 \pmod 2 \equiv 01000 + 01001 = 00001. \end{aligned}$$

So,

$$C = \{11001, 00111, 00001\}$$
$$= \{25, 7, 1\}$$
$$= \{Z, H, B\}.$$

The CSG of C is formed by

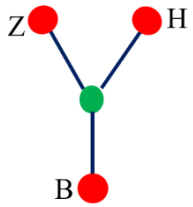

Figure 4. The ciphertext of CSG with a 3-red color vertices.

First user sends the CSG to the receivers. Second user (receiver) receives the ciphertext CSG. The CSG vertices is determined firstly by v_1= Z, v_2 = H and v_3= B.

Second user converts these vertices into decimal representations by

$$Z \rightarrow 25, H \rightarrow 7 \text{ and } B \rightarrow 1.$$

He/She computes the binary representation of these numbers

$$Z \rightarrow 25 \rightarrow 11001, H \rightarrow 7 \rightarrow 00011 \text{ and } B \rightarrow 1 \rightarrow 00001.$$

Using the CSG, he /she determines the SSK. Based on the color of vertices in CSG is a red and the number of them is 3, so, the SSK generates by

$$k \equiv 3 * \text{red} \pmod{26}.$$

Since

$$r \rightarrow 17, e \rightarrow 4 \text{ and } d \rightarrow 3.$$

So,

$$k \equiv 3 * \{17, 4, 3\} \pmod{26}$$
$$= \{25, 12, 9\}.$$

In other words,

$$25 \rightarrow 11001, 12 \rightarrow 01100 \text{ and } 9 \rightarrow 01001.$$

The original plaintext is calculated by

$$m \equiv C - k \pmod{2}.$$

Namely,

$$m_1 \equiv c_1 - k_1 \pmod{2} = 11001 - 11001 = 00000 \rightarrow 0 \rightarrow A,$$
$$m_2 \equiv c_2 - k_2 \pmod{2} = 00111 - 01100 = 01011 \rightarrow 11 \rightarrow l,$$
$$m_3 \equiv c_3 - k_3 \pmod{2} = 00001 - 01001 = 01000 \rightarrow 8 \rightarrow i.$$

Therefore, the original plaintext is the word Ali.

SECURITY ISSUES

A strong generating of the SSK in the proposed CSG-SE scheme considers as a prominent point to increase the security. The CSG is used to generate the SSK as well as the ciphertext. Using the proposed scheme, discovering the SSK by attackers is difficult problem comparing to the previous SE scheme. The correct sequence of the SSK needs to find by attackers. More probabilities require to find it. The total probabilities are

$$C_s^{26} = \binom{26}{s} = \frac{26!}{s!\,(26-s)!}$$

where s is the letters word number in the of the CSG. According to example in the study case, with alphabet = 26 and s = 3, then $C_s^{26} = 2600$.

So, with small values of parameters, the attackers need to generate 2600 sequences of the SSK, one of them is the correct. Thus, for large parameters values, recovering the plaintext is a more secure.

CONCLUSION

A new SE scheme version which is named by the CSG-SE scheme has been proposed. The CSG is employed to generate the SSK of two entities using the strong formula. The plaintext in CSG-SE scheme is encrypted and sent as the CSG. New computational result is discussed to explain the CBG-SE scheme through using the parameters with small values. The security issues of CSG-SE scheme are determined. The CSG -SE scheme is more secure for cryptographic communications comparing to previous ones.

REFERENCES

[1] L. N. M. Tawfiq, and I. N. Abood, "Persons Camp Using Interpolation Method ," Journal of Physics: Conference Series. Vol. 1003, No. 1, 2018, pp. 012055.

[2] W. A. Shukur, K. J. Khalid, and K. O. Luheb, "A Proposed Hybrid Text Cryptographic Method Using Circular Queue," IJCET, Vol. 9, No. 7, 2018, pp. 1123-1132.

[3] S. J. Yaqoob, and R. K. K. Ajeena, "The Multi-Primes Lanstra's Elliptic Curve Factorization Algorithm," In 2020 6th International Engineering Conference "Sustainable Technology and Development"(IEC), 2020, pp. 141-145.

[4] Q. M. Luhaib, and R. K. K. Ajeena, "Elliptic curve matrices over group ring to improve elliptic curve–discrete logarithm cryptosystems," Journal of Discrete Mathematical Sciences & Cryptography, Vol. 26, No. 6, 2023, pp.1699 – 1704.

[5] R. K. K. Ajeena, and H. Kamarulhaili, "On the distribution of scalar k for elliptic scalar multiplication," AIP Conference Proceedings, Vol. 1682, No. 1, 2015.

[6] M. Amara, and A. Siad, "Elliptic curve cryptography and its applications," In International workshop on systems, signal processing and their applications, WOSSPA (pp. 247-250), 2011.

[7] T. Fujita, "Analytical study on Ultrafilter in Digraph: Directed Tangle and Directed Ultrafilter," Asian Research Journal of Mathematics 21, No. 5 (2025), pp. 132-146.

[8] T. Fujita, "Linear-branch-decomposition of digraph," Theory and Applications of Graphs, submitted (2025).

[9] P. Amudha, A. C. Sagayaraj, and A. S. Sheela, "An application of graph theory in cryptography," International Journal of Pure and Applied Mathematics, Vol. 119, No. 13, 2018, pp. 375-383.

[10] P. Amudha, A. C. Sagayaraj, and A. S. Sheela, "An application of graph theory in cryptography," International Journal of Pure and Applied Mathematics, Vol. 119, No. 13, 2018, pp. 375-383.

[11] R. Nandhini, V. Maheswari, and V. Balaji, "A Graph Theory Approach on Cryptography," Journal of Computational Mathematica, Vol. 2, No. 1, 2018, pp. 97-104.