DATA ANALYTICS AND APPLIED MATHEMATICS (DAAM)
e-ISSN: 2773-4854
VOL. 3, ISSUE 2, 13 – 17
DOI: https://doi.org/10.15282/daam.v3i2.8936

ORIGINAL ARTICLE

Some analysis on conjugacy search problem for Diffie-Hellman protocol

S.H. Jusoo[1], M.S. Mohamad[2], S.A. Sulaiman[3] and Faisal[4]

[1,2,3]Centre for Mathematical Sciences, Universiti Malaysia Pahang, Lebuh Persiaran Tun Khalil Yaakob, 26300 Kuantan, Pahang, Malaysia
[4]Mathematics Department, School of Computer Science, Bina Nusantara University, West Jakarta, Indonesia

ABSTRACT – The field in nonabelian group-based cryptosystem have gain attention of the researchers as it expected to offers higher security when confronted with quantum computational due to more complex algebraic structures. Hence, this paper intents to give an overview on Diffie-Hellman protocol considering the mathematically hard problem such as the conjugacy search problem in a group *G*. In this paper we provide examples for *G* of non abelian group particularly the group of *SL*(2,3).

ARTICLE HISTORY
Received: 20/07/2022
Revised: 20/09/2022
Accepted: 30/09/2022

KEYWORDS
Diffie-Hellman protocol
Nonabelian group
Conjugacy search problem

INTRODUCTION

The public key cryptography was firstly introduced by Diffie and Hellman in 1976 namely Diffie-Hellman key exchange [1]. The scheme is one of the most common public keys currently in use along with the RSA cryptosystem, the ElGamal cryptosystem and the elliptic curve cryptosystem. These public keys mainly based on the number theory and hence depend on the structure of abelian groups. With the increasing power of computing machinery and the realisation of quantum computers, the cryptosystem for both public and classical key becoming less secure and that means abelian groups are too easy to understand and becoming vulnerable for quantum computing. Hence the needs to improve the security and much attention to be put on the nonabelian groups from the algebraic point of view [2].

The classical Diffie-Hellman protocol as mentioned in [1], where such simplest and original implementation of this protocol uses Z_p^*, the multiplicative group of integers modulo p, where p is prime and g is the generator with modulo p. The Diffie-Hellman (*DH*) protocol as presented in [3] as follows: Let G be a cyclic group with g as the generating element in G.

1) Alice and Bob agree on a group G of order q and an element g in G.
2) Alice picks a random natural number $m < q$ and sends g^m to Bob.
3) Bob picks a random natural number $n < q$ and sends g^n to Alice.
4) Alice computes secret key, $K_A = (g^n)^m = g^{nm}$.
5) Bob computes secret key, $K_B = (g^m)^n = g^{mn}$.

The property of the multiplicative group of integers is commutative as in $mn = nm$, thus both Alice and Bob are now in possession of the same group element $K = K_A = K_B$, where it came out as the shared secret key. For the protocol to be considered secure, G and g are needed to be chosen properly. The difficulty of such problem lies on the recovery of g^{mn} from g, g^m, and g^n (publicly known) whereby it means to recover the shared secret key, K.

Essentially, the hardness of the well-known mathematical problem in number theory namely Integer Factorization Problem and Discrete Logarithm Problem are the ground to the problem in cryptography and the security of Diffie-Hellman protocol relies on the Diffie-Hellman problem or the Discrete Logarithm Problem which are defined as follows, respectively [4]:

Diffie-Hellman Problem: Let G be a group. If $g, g^x, g^y \in G$ are known, find the value of g^{xy}.

Discrete Logarithmic Problem: Let G be a group. If $h, g \in G$, such that $h = g^x$ and h, g are known. Find the integer x.

*CORRESPONDING AUTHOR | M.S. Mohamad | ✉ mohdsham@ump.edu.my

However, both Integer Factorization Problem and Discrete Logarithm Problem would be efficiently solved on the realisation of the quantum computer, hence the emergence of numerous group-based cryptosystem in recent times has raised the attention of researchers. In other words, some mathematical problems involving non-commutative groups are substantially harder to solve when the quantum computation algorithm applied [5]. Thus, this paper mainly concerned with group-based cryptography particularly the attention is directed towards the nonabelian groups [6]. Some examples on the matrix groups are provided as well in the preliminaries section.

The rest of the paper is structured as follows. In the preliminary section, the basic notions used for the research are provided. The next section is the main part where the proofs for the results obtained are presented and then followed by concluding remark in the last section.

PRELIMINARIES

In this section, some definitions that are important in the research are stated. The definiton of Conjugacy Search Problem is given in the Definition 2.1 as follows:

Definition 2.1 [7] (Conjugacy Search Problem): Let G be nonabelian group. For $g, x \in G$, then the relation of the conjugate of g by x, that is $g^x = xgx^{-1}$.

The task is to find some $x \in G$ in the above relation, thus it is known as Conjugacy Search Problem (CSP). The hardness of the Conjugacy Search Problem upon the group is taken into consideration other than assuming that the group's elements are easily stored and manipulated. In Definition 2.2 and 2.3, the definition of the conjugacy class and center of a group are defined respectively as follows.

Definition 2.2 [8] (Conjugacy Class): If G is a group, then the equivalence class of $a \in G$ under the relation "y is conjugate of x in G" is called the conjugacy class of a; it is denoted by a^G.

The conjugacy class a^G is the set of all the conjugates of a in G. [9]

Definition 2.3 [10] (Center): The set of all elements of G which commute with every element of G is a center of a group G, that is

$$C = \{a \in G \mid ax = xa, \ \forall x \in G\}.$$

Next, proposition with the condition for the element to be the center of the group is provided.

Proposition 2.4 [10]: If a is the only element of order k in G, then a is in the center of G.

In this paper, the group of $SL(2,3)$ is studied and the elements of the group are classified according to its conjugacy classes. In particular, $SL(2,3)$ is a nonabelian group of order 24 is given as Example 2.5 as follows.

Example 2.5: The group $SL(2,3)$ is the multiplicative group of two-by-two invertible matrices of determinant 1 with entries from the field $Z_3 = \{0,1,-1\}$ under addition and multiplication modulo 3 [8]. More detail of the elements with the order in the respective conjugacy class provided in the table in Table 1. By Definition 2.1, there are seven conjugacy classes in $SL(2,3)$ that has been identified as provided in Table 1.

Likewise, the elements of $SL(2,3)$ with respect to Diffie-Hellman protocol are provided and it is identified that such elements in the same conjugacy classes will not necessarily generate the same shared secret key. Example 2.6 shows an example for this case.

Example 2.6: Let us consider the elements in conjugacy Class III in Table 1. Then, let the generator be g_{15} and choose the private keys from the Class III where $x = g_9$ and $y = g_{21}$. Then compute $g^x = g_9 g_{15} g_9^{-1}$ and it simplified to g_4. Similarly, we compute $g^y = g_{21} g_{15} g_{21}^{-1}$ and it simplified to g_4 as well. We then compute $K_A = g_9 g_4 g_9^{-1}$ and $K_B = g_{21} g_4 g_{21}^{-1}$ and it give the outcome of $K_A = g_{24}$ and $K_B = g_{11}$ which are not the common secret key. Next, we consider example where the elements in the same conjugacy class generate the same shared secret key. Let the generator be g_2 and the elements in Conjugacy Class I where $x = g_{11}$ and $y = g_{20}$ are considered. Computing $g^x = g_{11} g_2 g_{11}^{-1}$ giving us g_{18} meanwhile $g^y = g_{20} g_2 g_{20}^{-1}$ simplified to g_{19}. Both $K_A = g_{11} g_{19} g_{11}^{-1}$ and $K_B = g_{20} g_{18} g_{20}^{-1}$ generate the same shared secret key g_{12}.

Table 1. Conjugacy Classes for $SL(2,3)$

Class	List of all elements of conjugacy class.	Conjugacy class size	Order of the elements in conjugacy class
I	$g_7 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	1	1
II	$g_{16} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	1	2
III	$g_3 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, g_9 = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}, g_{10} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, g_{21} = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$	4	3
IV	$g_{13} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, g_{23} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, g_8 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, g_6 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$	4	3
V	$g_{19} = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}, g_{12} = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}, g_{18} = \begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix}, g_2 = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$	4	6
VI	$g_{22} = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}, g_{14} = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, g_{17} = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}, g_5 = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$	4	6
VII	$g_4 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, g_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, g_{11} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, g_{20} = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, g_{15} = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}, g_{24} = \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}$	6	4

RESULTS AND ANALYSIS

The public key exchange protocol in the spirit of Diffie-Hellman protocol are provided and examined on any nonabelian group.

In this case, general protocol is specialised as follows:

$$g^x = xgx^{-1} \text{ for any element } g, x \in G.$$

1) Alice and Bob agree on a group G and public elements $g, g^x, g^y \in G$.
2) Alice selects private elements x and Bob selects y as the private elements.
3) Alice computes $g^x = xgx^{-1}$ and send the element to Bob and similarly Bob computes $g^y = ygy^{-1}$ and send the element to Alice.
4) Alice compute secret key, $K_A = xg^y x^{-1}$ and Bob compute secret key, $K_B = yg^x y^{-1}$.

Since $\left(g^x\right)^y = \left(g^y\right)^x$, we should have $K_A = K_B = K$ be the common shared secret key.

In the subsequent propositions, some conditions given to be satisfied for nonabelian group in Diffie-Hellman protocol namely Proposition 3.1 and 3.2.

Proposition 3.1: Suppose $x, y \in G$ be the private keys where G is nonabelian group in Diffie-Hellman protocol using Conjugacy Search Problem. If it holds true for $xy = yx$, then the shared secret key exist.

Proof: Let the public key generated by Alice is $g^x = xgx^{-1}$ then will be passed to Bob and the public key generated by Bob is $g^y = ygy^{-1}$ then will be passed to Alice. The shared secret key given by $\left(g^x\right)^y = \left(g^y\right)^x$ or equivalently $\left(xgx^{-1}\right)^y = \left(ygy^{-1}\right)^x$. The public key is then inserted into the Conjugacy Search Problem equation and give Alice's secret key, $K_A = xygy^{-1}x^{-1}$ and Bob's secret key, $K_B = yxgx^{-1}y^{-1}$. Since $xy = yx$, then

$$\begin{aligned} K_A &= xygy^{-1}x^{-1} \\ &= (xy)g(xy)^{-1} \\ &= (yx)g(yx)^{-1} \\ &= yxgx^{-1}y^{-1} \\ &= K_B. \end{aligned}$$

giving us the common shared secret key.

Proposition 3.2: Suppose $x, y \in G$ be the private keys where G is nonabelian group in Diffie-Hellman protocol using Conjugacy Search Problem. If it holds true for $(xy) = (yx)^{-1}$, then the shared secret key exist.

Proof: Let the public key generated by Alice is $g^x = xgx^{-1}$ then will be passed to Bob and the public key generated by Bob is $g^y = ygy^{-1}$ then will be passed to Alice. The shared secret key given by $\left(g^x\right)^y = \left(g^y\right)^x$ or equivalently $\left(xgx^{-1}\right)^y = \left(ygy^{-1}\right)^x$. The public key is then inserted into the Conjugacy Search Problem equation and give Alice's secret key, $K_A = xygy^{-1}x^{-1}$ and Bob's secret key, $K_B = yxgx^{-1}y^{-1}$. Since $(xy) = (yx)^{-1}$ then $K_A = xygy^{-1}x^{-1} = (yx)^{-1}g(xy)^{-1} = (yx)^{-1}g(yx)$ and $K_B = yxgx^{-1}y^{-1} = (yx)g(yx)^{-1} = (yx)g(yx)^{-1}$.
Without loss of generality,

$$\begin{aligned} xy &= (yx)^{-1} \\ xy &= x^{-1}y^{-1} \\ xxy &= xx^{-1}y^{-1} \\ x^2yy &= y^{-1}y \\ (xy)^2 &= 1. \end{aligned}$$

This proves that xy has an order 2 which by Corollary 3.3, is a center and commute with all elements in G. Hence, we can say that $xy = (xy)^{-1}$ or equivalently $xy = yx$. By Proposition 3.1, $K_A = K_B$ and prove that the shared secret key exist.

Such element from previous example with an order of 2 is shown to be the center of the group in the following Corollary 3.3. Then, in Proposition 3.4, such shared secret key achieved given the stated condition.

Corollary 3.3: If a is the only element in G of order 2, then the element is in the center of the group.

Proof: By Proposition 2.4, a is the center of the group and will commute with any element in G.

Proposition 3.4: Let $g \in G$ be generator and the only element of order 2, then it will generate the shared secret key the same element as g in G.

Proof: In order to prove the shared secret key is exist, we need to prove that $\left(g^x\right)^y = \left(g^y\right)^x$. Suppose that $g \in G$ be generator of order 2. Thus, g will commute with any $x, y \in G$,i.e $xy = yx$. By Proposition 3.1, the secret shared key is exist and the key is $\left(g^x\right)^y = x(ygy^{-1})x^{-1} = gxyy^{-1}x^{-1} = gxx^{-1} = g$.

CONCLUSION

The Diffie-Hellman key exchange protocol is presented based on non-abelian group in particular the mathematically hard problem that is Conjugacy Search Problem is considered for the nonabelian group. Some of the proofs for some cases in nonabelian groups that will work for the Diffie-Hellman key exchange are provided as well. Our protocol can be based on any nonabelian group though in this paper the group $SL(2,3)$ is given as an example.

ACKNOWLEDGEMENTS

The authors would like to thank International Islamic University Malaysia for their support and Universiti Malaysia Pahang for the financial funding through IIUM-UMP Sustainable Research Collaboration Grant 2022 (Project ID: RDU223214) and not to be forgotten the financial support from DRS scheme fund of UMP endowment.

REFERENCES

[1] A. Shamir, *New Directions in Croptography*. Berlin, Germany: Springer, 2001, pp. 159.

[2] G. Baumslag, B. Fine and X. Xu, "Cryptosystems using linear groups," Applicable Algebra in Engineering, Communication and Computing, vol. 17, no. 3–4, pp. 205–217, 2006.

[3] N. Rahman and V. Shpilrain, "MAKE: A matrix action key exchange," Journal of Mathematical Cryptology, vol. 16, no. 1, pp. 64–72, 2022.

[4] T. Lin, "A Study of Non-Abelian Public Key Cryptography," International Journal of Network Security, vol. 20, no. 2, pp. 278–290, 2018.

[5] G. H. J. Lanel, T. M. K. K. Jinasena and B. A. K. Welihinda, "A Survey of Public-Key Cryptography over Non-Abelian Groups," International Journal of Computer Science and Network Security, vol. 21, no. 4, pp. 289-300, 2021.

[6] C. Mullan, "Some results in group-based cryptography," Ph.D. dissertation, Department of Mathematics, University of London, Surrey, England, 2011.

[7] S. R. Blackburn, C. Cid and C. Mullan, *Group Theory in Cryptography.* Somerset, United Kingdom: University in Bath, 2011 pp. 133–149.

[8] E. T. Whittaker, "The Mathematical Association," Mathematical Gazette, vol. 10, no. 145, pp. 17–19, 1920.

[9] J.J Rotman, An Introduction to the Theory of Groups. Illinois, United States of America: Springer, 1995.

[10] C.C. Pinter, A Book of Abstract Algebra. New York, United States of America: Courier Corporation, 2010.