Analysis of the conjugacy search problem of the Diffie-Hellman protocol based on the SL(2,3) subgroup.

Siti Hasanah Jusoo[1*], *Mohd Sham* Mohamad[1], *Sahimel Azwal* Sulaiman[1], and *Fatin Hanani* Hasan[1]

[1]Centre for Mathematical Sciences, Universiti Malaysia Pahang Al-Sultan Abdullah, Lebuh Persiaran Tun Khalil Yaakob, 26300 Kuantan, Pahang, Malaysia

Abstract. The purpose of the Diffie-Hellman key exchange is to establish a shared secret key given that the protocol works in an abelian group setting. In this paper, conditions are presented to attain a shared secret key over a nonabelian group for the well-known Diffie-Hellman method. To attain the shared secret key, a subgroup of a nonabelian group will be presented in the abelian configuration by incorporating group theory concept such as normal subgroup and cyclic subgroup. The protocol introduced on the nonabelian group, namely the special linear group, addresses the conjugacy search problem, aiming to enhance the security of the existing protocol. Examples in special linear group $\mathrm{SL}(2,3)$ are presented to illustrate the implementation of Diffie-Hellman key exchange protocol.

1 Introduction

Essentially, the study of public key cryptography is based on the algebraic structure of abelian groups. One of the common public key cryptography implementing the abelian structure is the Diffie-Hellman key exchange which was introduced by Diffie and Hellman in 1976 [1]. The security of the Diffie-Hellman key exchange relies on the difficulty of solving a discrete logarithm problem where the exponents commute. As stated in [2], the security of the cryptographic scheme is based on the one-way function where computing the function $f(x)$ is straight forward, yet the inverse function is computationally infeasible. It is widely known that the two popular one-way function used in the cryptographic scheme are the integer factorization and discrete logarithm problem. Likewise, in the Diffie-Hellman cryptosystem, given the element of g and x, it is relatively easy to compute g^x but it is infeasible to compute the inverse, i.e: to find x given g and $g^x \bmod p$ where p is large enough. The most challenging aspect of a cryptographic scheme often lies in computing its inverse function. The current security of the Diffie-Hellman method relies on the difficulty of solving the discrete logarithm problem (DLP) in certain abelian groups. However, due to the emergence of the quantum computers and the escalating capabilities of computing devices, the security of this cryptosystem over the abelian group has become vulnerable to future

[*]Corresponding author: mohdsham@ump.edu.my

attacks. Cryptosystems using nonabelian groups are actively being studied to enhance their future security, see [3] and [4]. Certain research has explored the use of nonabelian groups in public key exchange. Here, we briefly mention a few examples without going into details. The authors in [5], [6] and [7] propose to use the braid group for their respective protocols as the platform group. In their work [3], the suggested cryptosystem is based on the automorphism defined by the conjugation operation. They highlight the challenge of identifying the conjugate element in finite nonabelian groups as a basis for security in their scheme. In [8], a finite nonabelian group namely the Thompson group is used to develop a public key cryptosystem model.

In this paper, the Diffie-Hellman key exchange protocol over nonabelian groups are considered with some conditions presented to gain the common shared secret key. The special linear group $\mathrm{SL}(2,3)$ is suggested as the platform for the execution of the protocol. The nonabelian nature of the elements imply the inequality $\left(a^{x}\right)^{y} \neq \left(a^{y}\right)^{x}$ presenting a challenge to attain the common Diffie-Hellman key. While growing computational power requires larger key sizes for security, finding methods to decrease key sizes that have more complex algebraic structure is crucial. Hence, the use of conjugation instead of exponentiation in Diffie-Hellman key exchange protocol serves as a more complex problem in finding the secret key. The conjugacy search problem will be the basis for the key agreement scheme as suggested in [9] and the Diffie-Hellman protocol will be studied over the nonabelian group as proposed in this paper. The Conjugacy Search Problem can be defined as follows:

Conjugacy search problem: Given a recursive presentation of a group $G,$ two elements $g, g^{x} \in G$ are randomly picked. Find element $x \in G$ such that $g^{x} = xgx^{-1}.$

The fundamental concepts for the research are presented in the paper's preliminary section. In the following section some conditions necessary for the existence of the shared secret key are presented. Finally, the last section presents as our concluding remarks.

2 Preliminaries

The Diffie-Hellman key exchange protocol can be generalised by using the conjugacy relation in this way:

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

1. Two parties which are Alice and Bob agree on a group G and public elements $g, g^{x}, g^{y} \in G.$
2. The private element x and y are selected by Alice and Bob respectively.
3. Alice computes $g^{x} = xgx^{-1}$ and sends the element to Bob and similarly Bob computes $g^{y} = ygy^{-1}$ and sends the element to Alice.
4. Alice computes secret key, $K_{a} = xg^{y}x^{-1}$ and Bob computes secret key, $K_{b} = yg^{x}y^{-1}.$

Since $\left(g^{x}\right)^{y} = \left(g^{y}\right)^{x}$, then the shared secret key, K where it is also expressed as $K = K_{a} = K_{b}$ being the same key.

Subsequently, some conditions along with the proofs are provided based on the generalization of the above protocol to attain the common shared secret key for suggested special linear group $\mathrm{SL}(2,3)$.

Additionally, some important notions and basic definitions used in the study are presented. The definition of the special linear group is defined as follows:

Definition 2.1 [10]: The special linear group, denoted by $\mathrm{SL}\,(2, Z_p)$, is the multiplication group of 2×2 over the field $¢_p$ with the determinant equal to 1and has the presentation:

$$\mathrm{SL}(2, Z_p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}; a, b, c, d \in Z_p, ad - bc = 1 \right\}.$$

This paper focuses on the special linear group, $\mathrm{SL}(2,3)$ with entries of $\{-1, 0, 1\}$ as the example for the Diffie-Hellman protocol.

Figure 1 below illustrates the lattice of subgroups for the group $\mathrm{SL}(2,3)$.

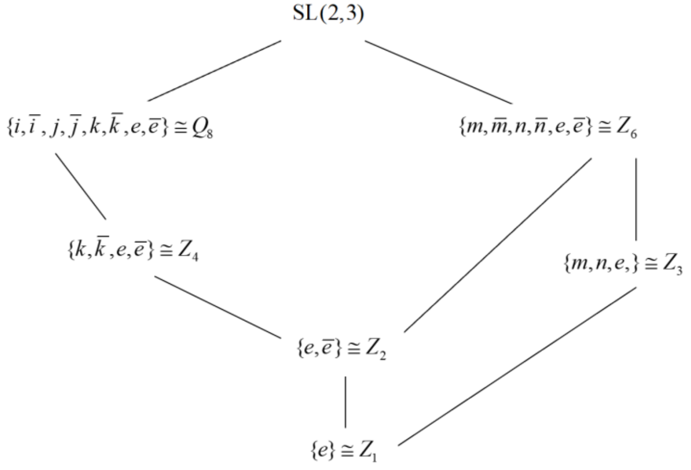

Fig. 1. Lattice of subgroups for $\mathrm{SL}(2,3)$

The elements of $\mathrm{SL}(2,3)$ in Figure 1 are denoted as follows:

$$m = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},\ \bar{m} = \begin{bmatrix} -1 & -1 \\ 0 & -1 \end{bmatrix},\ n = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix},\ \bar{n} = \begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix}$$

$$i = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},\ \bar{i} = \begin{bmatrix} -1 & -1 \\ -1 & 1 \end{bmatrix},\ j = \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix},\ \bar{j} = \begin{bmatrix} 1 & -1 \\ -1 & -1 \end{bmatrix}$$

$$k = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},\ \bar{k} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix},\ e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ \bar{e} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

In Figure 1, it is given that the subgroups Z_1, Z_2, Z_3, Z_4 and Z_6 are all cyclic except for Q_8, the subgroup that is isomorphic to the quaternion group.

The definition of centre and the order of a group are defined in Definition 2.2 and Definition 2.3 respectively as follows.

Definition 2.2 [11]**:** The set of all elements of $Z(G)$ that commute with each element of G is the *centre* of the group G, that is

$$Z(G)=\{a \in G : ax = xa \ \forall \ x \in G\}.$$

The centre $Z(G)$ is a normal subgroup of G. For $G=\mathrm{SL}(2,3)$, the elements of $e,\bar{e}$ are the only elements that commute with all the other elements. In Figure 1, Z_2 is identified as the normal subgroup for the group $\mathrm{SL}(2,3)$.

Definition 2.3 [12]**:** The order of $\mathrm{SL}\,(2,¢_{p})$ is $p(p-1)(p+1)$.

From Proposition 2.3, it can be deduced that the order of SL $(2,3)$ is 24.

Next, Propositions 2.1 and 2.2 in [13] state the conditions for a private key to achieve the same shared secret key for a nonabelian group.

Proposition 2.1 [13]**:** *Suppose G is a nonabelian group in the Diffie-Hellman protocol where $x,y \in G$ are the private keys and using the Conjugacy Search Problem. If the condition $xy = yx$ is satisfied, then the secret key is the same.*

Proposition 2.2 [13]**:** *Suppose G is a nonabelian group in the Diffie-Hellman protocol where $x,y \in G$ are the private keys and using the Conjugacy Search Problem. If the condition $(xy)=(yx)^{-1}$ is satisfied, then the secret key is the same.*

In the next section, the conditions necessary for the group to be satisfied in achieving the same shared secret key are provided.

3 Results and analysis

Some propositions are given in this section which must be satisfied for the nonabelian group G to achieve the same shared secret key for the Diffie-Hellman key exchange protocol.

Proposition 3.1: Suppose private keys $x,y \in H$ where $H \leq G$ and H is cyclic, then the secret key generated is the same.

Proof: Consider the public keys computed by Alice and Bob be $g^x = xgx^{-1}$ and $g^y = ygy^{-1}$ respectively. Then, g^x will be handed to Bob to generate the common secret key $K_b=\left(g^x\right)^y=\left(xgx^{-1}\right)^y=yxgx^{-1}y^{-1}$. Since x,y are from the same cyclic group satisfying the commutativity property $xy=yx$, the shared secret key generated by Alice is $K_a=(xy)g(y^{-1}x^{-1}) \ =(yx)g(x^{-1}y^{-1})=K_b$ which is equivalent to Bob's secret key.

Proposition 3.2: Let G be a group and $H_1,H_2 \leq G$. We suppose the private keys $x \in H_1$, $y \in H_2$ where H_1 is cyclic and $H_1 \leq H_2$, then the secret key generated is the same.

Proof: Suppose $x \in H_1$ and any element of H_1 commutes with every element in $y \in H_2$ such that $xy = yx$, then the shared secret key generated by Alice and Bob are equivalent which are $K_A = (xy)g(y^{-1}x^{-1}) = (yx)g(x^{-1}y^{-1}) = K_B$.

Proposition 3.3: Suppose private keys $x, y \in G$ are taken from any normal subgroup of H, then the shared secret key exists.

Proof: From Definition 2.2, given that the set of all the elements in normal subgroup $Z(G)$, is centre of the group and commute with every element of H. For any $x, y \in Z(G)$, $\left(g^x\right)^y = \left(g^y\right)^x$ hence the shared secret key exists.

Subgroup Q_8 is selected as an additional example due to its nonabelian structure and given its group presentation of $Q_8 = \left\langle a, b \mid a^4 = e, a^2 = b^2, ba = a^{-1}b \right\rangle$. The elements denoted with the bar are inverses, e.g: $\overline{g}$ in Q_8 is the inverse for g except for e and $\overline{e}$ where their inverses are themselves.

Elements in Q_8	Inverse of element
$i = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$	$\overline{i} = \begin{bmatrix} -1 & -1 \\ -1 & 1 \end{bmatrix}$
$j = \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}$	$\overline{j} = \begin{bmatrix} 1 & -1 \\ -1 & -1 \end{bmatrix}$
$k = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$	$\overline{k} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$

Theorem 3.4: Suppose private keys $x, y \in Q_8$. Any element of $g \in G$, then the common shared secret key is established.

Proof: Let the private key for Alice $x = i$, the inverse $x^{-1} = \overline{i}$ and for Bob $y = j$, the inverse $y^{-1} = \overline{j}$. The public keys generated by Alice and Bob are $g^x = ig\overline{i}$ and $g^y = jg\overline{j}$ respectively.

Alice uses the public key g^y to generate the shared secret key

$$\left(g^y\right)^x = ijg\overline{j}\ \overline{i} = ijgj^{-1}i^{-1} = ijg\left(ij\right)^{-1},$$

Bob uses the public key g^x to generate the shared secret key

$$\left(g^x\right)^y = jig\overline{i}\ \overline{j} = jigi^{-1}j^{-1} = jig\left(ji\right)^{-1}.$$

From Proposition 2.2, it is stated that $ij = (ji)^{-1}$, thus giving us $ijg\left(ij\right)^{-1} = jig\left(ji\right)^{-1}$. Hence, they will generate the same shared secret key $K_A = K_B$.

Proposition 3.5: Any private keys $x, y \in G$, such that $x^2 = y^2 = -e$ where e is the identity, will generate the same shared secret key $K_A = K_B$.

Proof: According to Proposition 2.2, we know that $xy = x^{-1}y^{-1}$ gives $x^2y^2 = xx^{-1}y^{-1}y,$ which means $x^2y^2 = 1,$ Since $x^2 = -e$ and $y^2 = -e,$ thus satisfying the equation $-e\cdot -e = 1,$ then $K_A = K_B.$

Proposition 3.6: Let G be a group. Any private key $x, y \in G,$ such that $x^{4n} = y^{4n} = e$ where e is the identity, will generate the same shared secret key.

Proof: From Proposition 2.2, since $x^2y^2 = 1$, it follows that $x^3y^3 = xy$ and $x^4y^4 = x^2y^2 = 1.$ From this result one can conclude that $x^{2n}y^{2n} = 1.$ Now consider $x^{4n} = e$ and $y^{4n} = e.$ Halving the exponent will give $x^{2n} = -e$ and $y^{2n} = -e$ satisfying the condition $x^{2n}y^{2n} = 1.$ Thus, we can say that for any x, y with order of $4n$, the same shared secret key $K_A = K_B$ will be generated.

Example: Let $n = 1,$ with element x, y of order 4 such that $x^4 = e,\ y^4 = e,$ then let $x = i, y = j$ and $g = \bar{n}.$ The public key $g^x = i\bar{n}\bar{i} = \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$ and $g^y = j\bar{n}\bar{j} = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}$. Then the shared secret keys generated for Alice and Bob are $K_A = ig^y\bar{i} = \begin{bmatrix} -1 & 0 \\ -1 & -1 \end{bmatrix}$ and $K_B = jg^x\bar{j} = \begin{bmatrix} -1 & 0 \\ -1 & -1 \end{bmatrix}$ respectively which shows that the common shared secret keys are equivalent.

4 Conclusion

Here we have considered the well-known Diffie-Hellman protocol generalised to the nonabelian group. The conditions that must be satisfied to attain the same shared secret for the nonabelian group were presented. The subgroups in this paper are the cyclic group, normal subgroup and the subgroup that is isomorphic to quaternion group. However, this study is primarily focused on exploring the abelian properties within the subgroup of the nonabelian group. Future research could expand upon this by investigating the noncyclic subgroup or normal subgroup with a nilpotency class n, offering broader insights into the group's characteristics.

The authors are very grateful for the financial support from the International Islamic University Malaysia and Universiti Malaysia Pahang Al-Sultan Abdullah under the IIUM-UMP Sustainable Research Collaboration Grant 2022 (Project ID:RDU223214). They would also like to thank the UMP endowment's DRS programme fund for their financial support.

References

1. A. Shamir, New directions in croptography, Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), **2162**, 159 (2001)
2. C. Paar, J. Pelzl. Understanding cryptography: a textbook for students and practitioners. (Springer Science & Business Media, 2009)

3. S. H. Paeng, K. C. Ha, J. H. Kim, S. Chee, C. Park, New public key cryptosystem using finite non Abelian groups, Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), **2139,** 470 – 485 (2001)
4. V. Shpilrain, G. Zapata, Appl. Algebr. Eng. Commun. Comput., **17**, 291 – 302, (2006)
5. I. Anshel, M. Anshel, D. Goldfeld, Math. Res. Lett., **6**(3), 287 – 291 (1999)
6. K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. S. Kang, C. Park, New public-key cryptosystem using braid groups, Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), **1880**, 166 – 183 (2000)
7. K. H. Ko, J. W. Lee, T. Thomas, Des. Codes, Cryptogr., **45**(3), 317 – 333 (2007)
8. V. Shpilrain A. Ushakov, Contemp. Math., Amer. Math. Soc. **418**(2), 161 – 167 (2006)
9. S. D. Hasapis, D. Panagopoulos, E. Raptis, “A Survey of Group-based Cryptography,” J. Appl. Math. Bioinform., **5**(3), 73 – 96 (2015)
10. G. Baumslag, B. Fine, M. Kreuzer, G. Rosenberger, A Course Math. Cryptogr., **1**, 183 – 216, (2015)
11. C. Pinter, A book of abstract algebra. Courier Corporation, **161**, 4097, (Dover Publications, 2010)
12. E. T. Whittaker, Math. Gaz., **10**(145), 17 – 19 (1920)
13. S. H. Jusoo, M. S. Mohamad, S. A. Sulaiman, Faisal, Data Anal. Appl. Math., **3**(2), 13 – 17 (2022)