ASM Sc. J., 13, 2020
https://doi.org/10.32802/asmscj.2020.sm26(5.11)

Encryption Scheme using Non-Abelian Group based on Conjugacy Search Problem

Y.X. Lee[1*], Denis C. K. Wong[2] and Wun-She Yap[3]

[1,2]*Department of Mathematical and Actuarial Sciences, LKC FES, Universiti Tunku Abdul Rahman, 43000 Kajang, Selangor, Malaysia*

[3]*Department of Electric and Electronic Engineering, LKC FES, Universiti Tunku Abdul Rahman, 43000 Kajang, Selangor, Malaysia*

Non-abelian group public key cryptography is a relatively new and exciting research field. As a result, we choose to work over a non-abelian group called Miller group in which its automorphism group is abelian. In this paper, we construct two new encryption schemes: we first propose a basic encryption scheme, which then we modified by adding a hash function in the second scheme. Both schemes are based on the hardness of solving the conjugacy search problem. Our proposed schemes resist the quantum attacks since there are no known efficient polynomial algorithms that can solve the conjugacy search problem. Furthermore, we prove that our schemes are semantically secure against indistinguishable chosen ciphertext attack.

Keywords: encryption, conjugacy search problem, post-quantum

I. INTRODUCTION

The security is an important issue in cryptography. We need a secure cryptosystem because a lot of transaction happening through internet such as internet shopping and electronics financial transfer which rely on the security of the system. Most common public key cryptosystems in use, such as the RSA algorithm (Rivest et al., 1978), El-Gamal scheme (El-Gamal, 1985)) and Diffie-Hellman scheme (Diffie & Hellman, 1976) are dependent on the structure of abelian groups. Since computing machinery and quantum computer has made this technique less secure, hence there has been some research to analyse new cryptosystems based on non-abelian groups. Constructing encryption schemes using a non-abelian group can be viewed as a generalization for most conventional schemes which is defined over abelian groups, refer to (Anshel et al., 1999; Mullan, 2011). One of the generalizations of discrete logarithm problem is called conjugacy search problem (CSP). There are several group-based public key protocols used the hardness of this problem in some particular groups for instance braid groups, refer (Hasapis et al., 2015; Ko et al., 2000; Myasnikov et al., 2008; Paeng et al., 2001) for more information. Anshel et al. (1999) proposed a protocol and shown that the conjugacy problem is unsolvable, and no known polynomial time algorithm can solve this problem. After that Ko et al. [7,8] proposed a one-way function, key agreement scheme which is based on the difficulty of conjugacy search problem. Wang et al. [15] proposed a cryptosystem based on a self-distributive system. Conjugacy search problem in non-abelian groups defines this cryptosystem. We formally stated the CSP as follows:

Conjugacy search problem. Given a recursive presentation of a group G and randomly pick two elements $g, h \in G$. Find an element $x \in G$ such that $x^{-1}gx = h$.

The remainder of the paper is organized as follows. We describe some preliminary concepts which will be needed later in Section II. We discuss our basic encryption schemes in Section III and analyse its security. In Section IV, we propose an encryption scheme by adding a hash function. We discuss the comparison with various encryption schemes

*Corresponding author's e-mail: leeyixuan0725@hotmail.com

in Section V. Finally, the summary will be given in Section VI.

II. PRELIMINARIES

A. Public Key Encryption

Definition II.1 *A (Gen, Enc, Dec) – public key encryption scheme is a tuple of probabilistic polynomial-time (PPT) algorithms such that*

1. *The randomized key generation algorithm Gen inputs the security parameter* 1^k *and outputs a pair of keys which are public key,* pk *and secret key,* sk*; written as* $(pk, sk) \leftarrow Gen\ (1^k)$.
2. *The randomized encryption algorithm* Enc*inputs a key* pk *and a plaintext message* $m \in \{0,1\}^*$*, and outputs a ciphertext* c*. We written this as* $c \leftarrow Enc_{pk}(m)$.
3. *The decryption algorithm* Dec *inputs a key* sk *and a ciphertext* c*, and outputs a message* m *or* $\perp$*. We written this as* $m \leftarrow Dec_{sk}(c)$.

We say that for all (pk, sk) *outputs by Gen, all* $m \in \{0,1\}^*, Dec_{sk}(Enc_{pk}(m)) = m$.

Next, below is the standard definition of security against adaptive chosen ciphertext attack.

A public key encryption scheme is secure against adaptive chosen ciphertext attack (CCA secure) if the advantage of adversary A *in the following game is negligible:*

1. $Gen(1^k)$ *outputs* (pk, sk)*.Challenger gives*1^k *and* pk *to the adversary* A.
2. *Adversary can make polynomial many queries to a decryption oracle, Dec().*
3. A *outputs two messages* m_0, m_1*. Challenger randomly choose a bit* b *and gives the challenge ciphertext,*$c^* \leftarrow Enc_{pk}(m_b)$ *to the adversary.*
4. A *continue to query its decryption oracle* $Dec()$ *except that it may not request the decryption of* c^*.
5. *Finally,* A *outputs a guess* b'.

We say that A *win the game if* $b' = b$*. We denote the probability of this game by* $Pr_A[Succ]$*. The advantage of the adversary win this game is defined to be*$|Pr_A[Succ] - 1/2|$.

B. Notations of Group Theory

In this section, we state several results from group theory which will be needed later. Let G be a group and$a, b \in G$. Then, a is said to be the conjugate of $b \in G$ if there exists $g \in G$ such that $a = gbg^{-1}$. The conjugacy class of any element $b \in G$ is denoted by $cl(b)$ and is defined as$cl(b) = \{gbg^{-1} : g \in G\}$. It is clear from the property of commutativeness of an abelian group, every conjugacy class of every element in an abelian group is a singleton set.

Definition 1. *Let* G *be a group. An isomorphism of groups from* G *to* G *is called an automorphism. The set of automorphisms of* G *forms a group under composition is called the automorphism group of* G *and written as* $Aut(G)$.

Definition 2. *A group* G *is called a Miller group if it has an abelian automorphism group, in other words, if* $Aut(G)$ *is commutative then the group* G *is Miller.*

Han and Ma (2010) constructed an authentication scheme and signature scheme from Miller group. More details of Miller group can refer to (Earnley, 1976; Miller, 1913). Next, we state some facts that are important in the Miller group. We prove the following Corollary.

Corollary 1. Suppose G is a Miller group and $x, g, h \in G$. Then, $x^{gh} = x^{hg}$.

Proof Suppose $\phi_g, \phi_h \in Inn(G)$, then ϕ_{gh}=ϕ_{hg}. Thus, we see that $\phi_{gh}(x) = \phi_{hg}(x)$ for all $x \in G$. It follows that $x^{gh} = x^{hg}$.

III. BASIC ENCRYPTION SCHEME

We proposed a basic encryption scheme in this section. We defined the scheme by describing the three algorithms: Key Generation, Encryption and Decryption. Suppose $r \in G$, we use r in the encryption algorithm to ensure that the scheme is probabilistic.

1. **Key Generation.** Let G be a Miller group. Choose $g, x \in G$ and form $g^x = h \in G$. The public key is (g, h) and the private key is x.

2. **Encryption.** To encrypt a plaintext $m \in G$, we first randomly pick $r \in G$ and then $Enc(m) = (g^r, h^r m)$.
3. **Decryption.** To decrypt the ciphertext$(c_1, c_2) \in G \times G$, $Dec(c_1, c_2) = (c_1^x)^{-1} c_2$.

By using Corollary 1, the correctness of the scheme is shown as follows:

$$\begin{aligned} Dec\big(Enc(m)\big) &= Dec(g^r, h^r m) \\ &= [(g^r)^x]^{-1} h^r m \\ &= [(g^r)^x]^{-1} (g^x)^r m \\ &= m \end{aligned}$$

Security. Next, we study the security of the basic scheme. The IND-CPA model is same as IND-CCA model but without decryption oracle.

Theorem 1. The basic encryption scheme is IND-CPA secure.

Proof Let A be an IND-CPA adversary. Define the following experiment.

Query: A randomly pick r^* and send to the challenger, C. Upon receivedr^*, C run the encryption algorithm and send the partial ciphertext g^{r^*} to A.

Challenge: A outputs two plaintexts m_0 and m_1 to C. C will produce the following ciphertexts by running the encryption algorithm: $Enc(m_0) = \big(g^{r^*}, X\big)$ and $Enc(m_1) = (g^s, Y)$.

Then C send g^{r^*} or g^s to A.

Guess:A upon received g^{r^*} or g^s, need to guess whether g^{r^*}correspond to m_0 or m_1(respectively, whether g^s correspond to m_0 or m_1).

$$\Pr[A\ win] = \Pr\big[Enc(m_0) = g^{r^*} \big|\ A\ received\ g^{r^*}\big]$$
$$= \Pr[Enc(m_1] = g^s |\ A\ received\ g^s].$$

Consider the experiment, instead of giving $h^{r^*} m_0$, we give $A\ X$, where $X = x m_0$, where x is a uniform element. Since x, h are given, then solving $x = h^{r^*}$ is equivalent to solve the CSP to obtain r^*. As we assume CSP is hard, then by looking at $h^{r^*} m_0$ and $x m_0$, we obtain no information on r^*. Consider $Enc(m_0) = (g^{r^*}, h^{r^*} m_0)$ and $Enc(m_1) = (g^s, h^s m_1)$, if $h^{r^*} m_0 = h^s m_1$ and $g^{r^*} = g^s$, then from both equations we know that $r^* = s$. This implies that $m_0 = m_1$, which is absurd.If we assume $h^{r^*} m_0 \neq h^s m_1$and $g^{r^*} \neq g^s$ then we let$g^{r^*} g^{-s} = \alpha$, where $\alpha \in G$. If $r^* = s$, then we have $\alpha = 1$ which is absurd. This implies that $m_0 \neq m_1$. Since A cannot guess the way $h^{r^*}$is computed fromr^*. The only way A distinguished r^* and $s$is if he r^*queries to C and sees that the answer is different from the answer he queries s to C.

Pr (A queries r^* in experiment)
= Pr (A queries r^* in actual attack)
= Pr (A get $r^* | C$ provide g^{r^*})
= Pr (A does not get m)
= Pr (A guesses m_0 or m_1)
= Pr [$Enc(m_0) = g^{r^*} | A$ received g^{r^*}]
= Pr [A win]

IV. ENCRYPTION SCHEME II

In this section, we generalized from the basic encryption scheme to construct an IND-CCA secure scheme. We added hash function in this scheme, it is because hash function is irreversible. The following algorithm gives our proposed encryption scheme.

1. **Key generation.** Randomly select $g, x \in G$ and from $g^x = h \in G$ and choose two cryptographic hash functions $H_1 : G \to \{0,1\}^*$ and $H_2 : G \times \{0,1\}^* \to \{0,1\}^*$ which will be viewed as random oracle in our security proof. The public key is (g, h, H_1, H_2) and private key is x.
2. **Encryption.** To encrypt a plaintext $m \in \{0,1\}^*$, we first randomly pick $r \in G$, then $Enc(m) = \big(g^r, H_1(h^r) \oplus m, H_2(m, g^r)\big)$.
3. **Decryption.** To decrypt the ciphertext $c_1, c_2, c_3 \in G \times \{0,1\}^* \times \{0,1\}^*$, compute $m' = H_1(c_1^x) \oplus c_2$. Check $c_3 = H_2(m', c_1)$ if so return m, else return $\perp$.

The correctness of the scheme is shown as follows:

$$\begin{aligned} m' &= H_1(c_1^x) \oplus c_2 \\ &= H_1((g^r)^x) \oplus H_1(h^r) \oplus m \\ &= H_1(h^r) \oplus H_1(h^r) \oplus m \\ &= m \end{aligned}$$

Since $m' = m$, then $c_3 = H_2(m, c_1)$, so return m.

Theorem 2. The encryption scheme II is IND-CCA secure. From the definition, a scheme is IND-CCA secure if adversary has a negligible advantage in winning the above game.

Proof Let A be an IND-CCA adversary. Define the following experiment.

Key generation: Challenger, C gives A the Miller group system parameter (g, h, r).

Phase 1 decryption query: The adversary queries the decryption oracle. Let $c_{1_i}, c_{2_i}, c_{3_i}$ be decryption query and send to the challenger, C. C run the decryption algorithm and compute $m' = H_1(c_1^x) \oplus c_2$, check whether $c_3 = H_2(m', c_1)$ if yes return m' else return $\perp$. The resulting decryption is given to A which is m' or $\perp$.

Challenge: A outputs two plaintexts m_0 and m_1 to C. C choose a bit $b \in \{0,1\}^*$and produce the following ciphertexts by running the encryption algorithm. $Enc(m_b) = \left(g^{r'}, H_1\left(h^{r'}\right) \oplus m_b,\ H_2\left(m_b, g^{r'}\right)\right)$. Then C send $c^* = (g^{r'}, H_1\left(h^{r'}\right) \oplus m_b, H_2\left(m_b, g^{r'}\right))$ to A.

Phase 2 decryption query: We answer as the decryption query in phase 1 except that it may not request the decryption of c^*.

Consider the experiment, adversary compute $m' = H_1((g^{r_i})^x \oplus H_1(h^{r_i}) \oplus m_i)$ then check $H_2(m_i, g^{r_i}) = H_2(m', g^{r_i})$. If true, then return $m_i = m'$. To obtain $m' = m_i$, it is equivalent to have $H_1((g^{r_i})^x) = H_1(h^{r_i})$. Noted that $H_i: G \to \{0,1\}^*$ and $H_1(y) \in \{0,1\}^*$. We have 2^n of hash values for some $n \in Z$ and it can be done in 2^n ways. By comparing the hash values, adversary have

$$(g^{r_i})^x = h^{r_i}$$
$$x(g^{r_i})x^{-1} = r_i h\, {r_i}^{-1}$$
$$xr_i g r_i^{-1} x^{-1} = r_i h\, {r_i}^{-1}$$
$$r_i^{-1} x r_i g r_i^{-1} x^{-1} r_i = h$$
$$(r_i^{-1} x r_i) g \left(r_i x r_i^{-1}\right)^{-1} = h$$
$$x^{r_i^{-1}} g \left(x^{r_i^{-1}}\right)^{-1} = h$$
$$g^{x^{r_i{}^{-1}}} = h.$$

Since $g, h \in G$ are given to adversary, knowing g, h to solve $g^{x^{r_i{}^{-1}}} = h$ for $x^{r_i{}^{-1}}$ is equivalent to solve CSP which is impossible. Suppose adversary get $x^{r_i{}^{-1}} = \alpha_i$ for some $\alpha_i \in G$, then if CSP is solvable, knowing x and α_i can recover the randomly chosen r_i. It is because by solving CSP we can obtain the master secret key, and use it to recover the randomly chosen element in encryption. However, all these can't happen as CSP is computationally infeasible to solve. Thus, the advantage of the adversary win the game is negligible. According to the definition, since the adversary has a negligible advantage in winning the above game, thus the scheme is secure under IND-CCA attack.

V. COMPARISON WITH VARIOUS TYPES OF ENCRYPTION SCHEME

We list out the security model and the hardness problem for different types of encryption schemes in the table below.

Table I: Comparison between the encryption schemes

Public key encryption scheme	Security model	Hardness problem
El-Gamal cryptosystem [4]	IND-CPA	DLP
MOR cryptosystem [9]	Central commutator attack	DLP
Ko-Lee et al. encryption scheme [7]	Brute force attack	Conjugacy problem
Wang et al. encryption scheme [15]	IND-CCA	CSP

In the El-Gamal cryptosystem, the encryption algorithm requires two exponentiations. However, these exponentiations are independent of the message and can be computed ahead of time if need be. In decryption algorithm it only requires one exponentiation. It depends on the hardness of discrete logarithm problem and is IND-CPA secure. MOR cryptosystem is a generalization of El-Gamal cryptosystem. It is using automorphism instead of exponential. The security model is central commutator attack based on the discrete logarithm problem (DLP). El-Gamal can be defined in any cyclic group but for MOR cryptosystem it is using group of unitriangular matrix. Conjugacy problem is to determine whether there exists an

element z of G such that $y = zxz^{-1}$. However, for CSP is to find out the z such that that $y = zxz^{-1}$. The conjugacy problem can be described as a decision version and a computational version, CSP is an example of a computational version. The decision version is known as conjugacy decision problem (CDP). In Ko-Lee scheme, braid group is used to construct the scheme. It involved a hash function and two inversions in encryption algorithm, however in decryption algorithm involved a hash function and one inversion. The security model used in this scheme is the brute force attack based on the hardness of conjugacy problem. We know that there are not many researchers using CSP to construct their scheme. One of the researchers using this hardness problem is Wang et al. (2009). They are using braid group to construct the scheme. In the encryption algorithm involved one inversion while in decryption algorithm involved two inversions. However, we are using CSP together with the Miller group. Note that our scheme is resisting quantum attacks since there are no known efficient polynomial algorithms that can solve the CSP.

VI. CONCLUSION

In this paper, we have proposed two encryption schemes by using the Miller group whose security is based on the hardness of conjugacy search problem. As a realization of the Miller group is proposed, whose allows us to carry out a detailed analysis showing the cryptosystem. The results shown in Theorem IV.1 stated that the adversary has a negligible advantage in winning the game, as desired, imply that the encryption scheme is secure against the attacks of chosen ciphertext.

VII. ACKNOWLEDGEMENT

The authors thank for the support by FRGS. This paper is supported by Malaysia Fundamental Research Grant Scheme with project code FRGS/2017/STG/UTAR/02/2.

VIII. REFERENCES

Anshel I., Anshel M., Goldfield D. (1999). An algebraic method for public key cryptography, Math. Res. Lett. 6, 287-291.

Diffie, W., & Hellman, M. (1976). New directions in cryptography. IEEE transactions on information theory, 22(6), 644-654.

Earnley, B. E. (1976). On finite Groups whose group of automorphisms is abelian. PhD thesis, Wayne State University.

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

Hasapis, S. D., Panagopoulos, D., &Raptis, E. (2015). A Survey of Group-based Cryptography. Journal of Applied Mathematics & Bioinformatics, 5(3), 73-96.

Han, G., & Ma, C. (2010). A new authentication and signature scheme based on the conjugacy search problem. In Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010 Second International Conference on (2), 317-320. IEEE.

Ko, K. H., Lee, S. J., Cheon, J. H., Han, J. W., Kang, J. S., & Park, C. (2000). New public key cryptosystem using braid groups. In Annual International Cryptology Conference 166-183. Springer, Berlin, Heidelberg.

Ko, K. H., Choi, D. H., Cho, M. S., & Lee, J. W. (2002). New Signature Scheme Using Conjugacy Problem. IACR Cryptology ePrint Archive, 168, 1-13.

Mahalanobis, A. (2008). A simple generalization of the ElGamal cryptosystem to non-abelian groups. Communications in Algebra, 36(10), 3878-3889.

Miller, G. A. (1913). A non-abelian group whose group of isomorphism is abelian. Messenger Math, 43, 124-125.

Mullan, C. (2011). Some Results in Group-based cryptography (Doctoral dissertation, University of London).

Myasnikov, A., Shpilrain, V., & Ushakov, A. (2008). Group-based cryptography. Springer Science & Business Media.

Paeng, S. H., Ha, K. C., Kim, J. H., Chee, S., & Park, C. (2001). New public key cryptosystem using finite non-Abelian groups. In Annual International Cryptology Conference 470-485. Springer, Berlin, Heidelberg.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126.

Wang, L., Wang, L., Cao, Z., Okamoto, E., & Shao, J. (2009). New Cryptosystems From CSP-Based Self-Distributive Systems. IACR Cryptology ePrint Archive, 2009, 566.