The Generalized Diffie-Hellman Key Exchange Protocol on Groups

Wachirapong Jirakitpuwapat[1] and Poom Kumam[2,3(✉)]

[1] Department of Mathematics, Faculty of Science, King Mongkuts University of Technology Thonburi (KMUTT), 126 Pracha-Uthit Road, Bang Mod, Thrung Khru, Bangkok 10140, Thailand
wachirapong.jira@hotmail.com

[2] KMUTT-Fixed Point Research Laboratory, Department of Mathematics, Room SCL 802 Fixed Point Laboratory, Science Laboratory Building, Faculty of Science, King Mongkuts University of Technology Thonburi (KMUTT), 126 Pracha-Uthit Road, Bang Mod, Thrung Khru, Bangkok 10140, Thailand
poom.kum@kmutt.ac.th

[3] KMUTT-Fixed Point Theory and Applications Research Group (KMUTT-FPTA), Theoretical and Computational Science Center (TaCS), Science Laboratory Building, Faculty of Science, King Mongkuts University of Technology Thonburi (KMUTT), 126 Pracha-Uthit Road, Bang Mod, Thrung Khru, Bangkok 10140, Thailand

Abstract. In this paper, we study key exchange protocol which is similar to Diffie-Hellman key exchange protocol. This key exchange protocol uses maximal abelian subgroup of automorphism of group. We give an example group is used for key exchange protocol.

Keywords: Diffie-Hellman key exchange · Cryptography · Group

Mathematics Subject Classification: Primary 94A62
Secondary 20F28

1 Introduction

In cryptography, keys exchange is a method to send a key between a sender and a recipient. The problems of the key exchange are how they send the message so that nobody else can understand the message except for the sender and the recipient. The procedure is one of the first public key cryptographic protocols used to build up a secret key between each other over insecure channel. The protocol itself is constrained to exchange of the keys for example: we are making a key together instead of sharing data while the key exchange. We implement algorithm for exchanging information over a public channel so that building up a mutual secret between two gatherings that can use for secret communication. Diffie-Hellman is suitable to use in information communication and less frequently use for information storage or archived over a long time period.

L. H. Anh et al. (eds.), *Econometrics for Financial Applications*, Studies in Computational Intelligence 760, https://doi.org/10.1007/978-3-319-73150-6_8

In cryptographic protocol has the key exchange is the first issue. For human development, people try to hide the data from other people so that composing structure. This is assumed that is the first and primitive type of encryption, but it is just only half section of cryptography. The other half is the capacity to reproduce the first message from its hidden structure. Cryptography is like a normal message but nobody except for the exact recipient will understand the message. By that time the huge majority of the cryptosystems were private of symmetric key cryptosystems. In this two clients Alice and Bob select a key, which is their private key then use the key in a private key cryptosystem to convey information over people in public channel. We investigate a public key cryptography regarding the Diffie-Hellman key Exchange Protocol, which is the most primitive thought behind a public key cryptography. In the Diffie-Hellman key exchange protocol, two clients unknown to one another can set up a private however arbitrary key for their symmetric key cryptosystem. The Diffie-Hellman key agreement protocol (1976) was the first practical method for setting up a shared secret over an insecure communication channel.

In modern cryptography, we assume that key is a only secret. Therefore if there are many keys, then the opponent hard break cryptosystem. We will generalized Diffie-Hellman key exchange protocol on groups. We choose key which is automorphism group in maximal abelian subgroup of automorphism group.

2 Preliminaries

In this section, we will introduce Diffie-Hellman Key Exchange and group.

2.1 Diffie-Hellman Key Exchange

The simple and original key exchance protocol uses the module p and $g \in \{1, \ldots, p-1\}$ where p is a prime in [1].

Example 1. Alice and Bob want to exchange key over an insecure channel.

1. Alice and Bob agree to use the module p and $g \in \{1, \ldots, p-1\}$ where p is a prime.
2. Alice choose a secret $a \in \{1, \ldots, p-1\}$. Then she sends $A = g^a \bmod p$ to Bob.
3. Bob choose a secret $b \in \{1, \ldots, p-1\}$. Then he sends $B = g^b \bmod p$ to Alice.
4. Alice compute $B^a \bmod p$.
5. Bob compute $A^b \bmod p$.
6. Alice and Bob have common secret key $A^b = B^a \bmod p$.

2.2 Groups

Definition 1. For a nonempty G, a function $\cdot : G \times G \to G$ is called a *binary operation*. Image of $(a, b) \in G$ is denoted by ab. G with binary operation is a *group* if it has properties

1. Associativity, $\forall a, b, c \in G, (a \cdot b) \cdot c = a \cdot (b \cdot c)$,
2. Identity $\exists e \in, \forall a \in G, a \cdot e = a = e \cdot a$,
3. Inverse $\forall a \in G \exists b \in G, a \cdot b = e = b \cdot a$.

Definition 2. A group G is commutative if $\forall a, b \in G, ab = ba$. A commutative group is called *abelian group.*

Definition 3. Let G and H be groups. A *homomorphism* from G to H is a map $\phi : G \to H$ which satisfy

$$\forall a, b \in G, \phi(ab) = \phi(a)\phi(b).$$

An *isomorphism* is a homomorphism which is injection and surjection. We write $G \cong H$. An *automorphism* is a isomorphism from G to G. The automorphism group of G is denoted by $Aut(G)$.

Theorem 1 [2]**.** *Let G be a finite abelian group. Then G is isomorphic to a product of groups of the form*

$$H_p = \mathbb{Z}_{p^{n_1}} \times \cdots \times \mathbb{Z}_{p^{n_m}},$$

in which p is a prime number and $n_1 \leq \cdots \leq n_m$ are positive integers.

Theorem 2 [2]**.** *Let H and K be finite groups with relatively prime orders. Then*

$$Aut(H) \times Aut(K) \cong Aut(H \times K).$$

Theorem 3 [2]**.** *Let $H_p = \mathbb{Z}_{p^{n_1}} \times \cdots \times \mathbb{Z}_{p^{n_m}}$ be a group which p is a prime number and $n_1 \leq \cdots \leq n_m$ are positive integers. Setting $d_k = \max\{\ell : n_\ell = n_k\}$ and $c_k = \min\{\ell : n_\ell = n_k\}$. Then*

$$|Aut(H_p)| = \prod_{k=1}^{m}(p^{d_k} - p^{k-1}) \prod_{j=1}^{m}(p^{{n_j}^{(m-d_j)}}) \prod_{i=1}^{m}(p^{{n_i-1}^{(m-c_i+1)}}).$$

Lemma 1. *A abelian group $G = H_{p_1} \times \cdots \times H_{p_k}$ which $p_1 < \cdots < p_k$ are prime numbers, $H_p = \mathbb{Z}_{p^{n_1}} \times \cdots \times \mathbb{Z}_{p^{n_m}}$ and $n_1 \leq \cdots \leq n_m$ are positive integers has*

$$Aut(G) = \prod_{i=1}^{k} |Aut(H_{p_i})|.$$

Proof. It's obvious by Theorems 2 and 3.

Theorem 4 [4]**.** *Let n be a positive integer such that $n \geq 3$ and let $k = 2n^{n-1}$. Let $G = <x, y, z, u>$ with defined by*

1. $x^{2n} = y^2 = z^2 = u^2 = [x, z] = [x, u] = [z, u] = [y, z] = 1$,
2. $yxy = x^{k+1}$,
3. $yuy = zu$.

The $Aut(G)$ is abelian group. It is isomorphic to $\mathbb{Z}_{2^6} \times \mathbb{Z}_{2^{n-2}}$. The order of G is 2^{n+3}.

3 Key Exchange Protocol

Alice and Bob want to exchange key over an insecure channel that is similar in [3].

3.1 Key Exchange Protocol I

1. Alice and Bob choose group G and an element $g \in G$ in public information. Note that G and g are public information.
2. Alice and Bob choose automorphism ϕ_A and ϕ_B from maximal abelian subgroup S of $Aut(G)$, respectively. Note that ϕ_A and ϕ_B are private information.
3. Alice and Bob compute $\phi_A(g)$ and $\phi_B(g)$ respectively and exchange them. Note that $\phi_A(g)$ and $\phi_B(g)$ are public information.
4. Both of them compute $\phi_A(\phi_B(g)) = \phi_B(\phi_A(g))$ from their private information, which is their common secret key.

In Example 1 is special case when $\phi_A(g) = g^a$, $\phi_B(g) = g^b$ and $\phi_A(\phi_B(g)) = g^{ab}$.

Remark. The opponent hard compute $\phi_A(\phi_B(g))$ from $G, g, \phi_A(g), \phi_B(g)$.

Example 2. Alice and Bob want to exchange key over an insecure channel.

1. Alice and Bob agree to use group $G = \mathbb{Z}_{p^n} \times \mathbb{Z}_{q^m}$ where p, q are prime and $g = (g_1, g_2) \in G$.
2. Alice choose $a = (a_1, a_2)$ where $gcd(a_1, n) = gcd(a_2, m) = 1$. Her automorphism is $\phi_A(g') = (g_1'^{a_1}, g_2'^{a_2})$. Bob choose $b = (b_1, b_2)$ where $gcd(b_1, n) = gcd(b_2, m) = 1$. His automorphism is $\phi_B(g') = (g_1'^{b_1}, g_2'^{b_2})$.
3. Alice and Bob compute $\phi_A(g)$ and $\phi_B(g)$ respectively and exchange them.
4. Both of them compute $\phi_A(\phi_B(g)) = \phi_B(\phi_A(g))$ from their private information, which is their common secret key.

3.2 Key Exchange Protocol II

1. Alice and Bob choose group G in public information.
2. Alice chooses automorphism ϕ_A from maximal abelian subgroup S of $Aut(G)$ and she choose an element $g \in G$. Then she sends $\phi_A(g)$ to Bob. Note that g and ϕ_A are private information but $\phi_A(g)$ is public information.
3. Bob chooses automorphism ϕ_B from maximal abelian subgroup S of $Aut(G)$. Then he send $\phi_B(\phi_A(g))$ to Alice. Note that ϕ_B is private information but $\phi_B(\phi_A(g))$ is public information.
4. Alice compute $\phi_A^{-1}(\phi_B(\phi_A(g))) = \phi_B(g)$. Next Alice choose automorphism ϕ_H from maximal abelian subgroup S of $Aut(G)$ and compute $\phi_H(g)$. Then she sends $\phi_H(\phi_B(g))$ to Bob. Note that ϕ_H is private information but $\phi_H(\phi_B(g))$ is public information.
5. Bob compute $\phi_B^{-1}(\phi_H(\phi_B(g))) = \phi_H(g)$, which is their common secret key.

Remark. The opponent hard compute $\phi_A(\phi_B(g))$ from $G, \phi_A(g), \phi_B(\phi_A(g))$, $\phi_H(\phi_B(g))$.

Example 3. Alice and Bob want to exchange key over an insecure channel.

1. Alice and Bob agree to use group $G = \mathbb{Z}_{p^n} \times \mathbb{Z}_{q^m}$ where p, q are prime.
2. Alice chooses $a = (a_1, a_2)$ where $gcd(a_1, n) = gcd(a_2, m) = 1$. Her automorphism is $\phi_A(g') = (g_1'^{a_1}, g_2'^{a_2})$. She choose an element $g \in G$. Then she sends $\phi_A(g)$ to Bob.
3. Bob chooses $b = (b_1, b_2)$ where $gcd(b_1, n) = gcd(b_2, m) = 1$. His automorphism is $\phi_B(g') = (g_1'^{b_1}, g_2'^{b_2})$. Then he send $\phi_B(\phi_A(g))$ to Alice.
4. Alice compute $\phi_A^{-1}(\phi_B(\phi_A(g))) = \phi_B(g)$. Next Alice choose $c = (c_1, c_2)$ where $gcd(c_1, n) = gcd(c_2, m) = 1$. Her automorphism is $\phi_H(g') = (g_1'^{c_1}, g_2'^{c_2})$. Then she sends $\phi_H(\phi_B(g))$ to Bob.
5. Bob compute $\phi_B^{-1}(\phi_H(\phi_B(g))) = \phi_H(g)$, which is their common secret key.

Acknowledgements. This project was supported by the Theoretical and Computational Science (TaCS) Center under Computational and Applied Science for Smart Innovation Cluster (CLASSIC), Faculty of Science, KMUTT. The third author would like to thanks the Petchra Pra Jom Klao Ph.D. Research Scholarship for financial support.

References

1. Diffie, W., Hellman, M.: New directions in cryptography. IEEE Trans. Inf. Theory **22**, 644–654 (1976)
2. Hillar, C.J., Rhea, D.L.: Automorphism of finite abelian groups. Am. Math. Mon. **114**, 917–923 (2007)
3. Mahalanobis, A.: The Diffie-Hellman Key Exchange protocal and non-abelian groups. Israel J. Math. **165**, 161–187 (2008)
4. Struik, R.R.: Some non-abelian 2-groups with abelian automorphism groups. Arch. Math. **39**, 299–302 (1982)