Group-Based Key Exchange Protocol Based on Complete Decomposition Search Problem

Chang Seng Sin(✉) and Huey Voon Chen

Department of Mathematical and Actuarial Sciences,
Lee Kong Chian Faculty of Engineering and Science,
Universiti Tunku Abdul Rahman,
Bandar Sungai Long, 43000 Kajang, Selangor, Malaysia
Jaybao@1utar.my

Abstract. Let G be a finite non-abelian group. Let $A_1, \cdots, A_k$ be non-empty subsets of G, where $k \geq 2$ is an integer such that $A_i \cap A_j = \emptyset$ for integers $i, j = 1, \cdots, k$ $(i \neq j)$. We say that $(A_1, \cdots, A_k)$ is a complete decomposition of G if the product of subsets $A_{i_1} \cdots A_{i_k} = \{a_{i_1} ... a_{i_k} | a_{i_j} \in A_{i_j}; j = 1, \cdots, k\}$ coincides with G where the A_{i_j} are all distinct and $\{A_{i_1}, \cdots, A_{i_k}\} = \{A_1, \cdots, A_k\}$. The complete decomposition search problem in G is defined as recovering $B \subseteq G$ from given A and G such that $AB = G$. The aim of this paper is twofold. The first aim is to propose the complete decomposition search problem in G. The other objective is to provide a key exchange protocol based on the complete decomposition search problem using generalized quaternion group Q_{2^n} as the platform group for integer $n \geq 3$. In addition, we show some constructions of complete decomposition of generalized quaternion group Q_{2^n}. Further, we propose an algorithm that can solve computational complete decomposition search problem and show that the algorithm takes exponential time to break the scheme.

Keywords: Group-based key exchange protocol · Complete decomposition search problem · Nonabelian group

1 Introduction

A lot of study regarding group factorization theory of abelian group written additively had been conducted over the years. The study of group factorization was first initiated by Hajos in year 1938 [13]. He successfully solved a geometry problem that raised by Minkowski by using group theoretical equivalent [14]. This scenario attracted the attention of studying the factorization of a finite abelian group into not necessary subgroup factors [15]. Many type of algebraic structures were derived from group factorization. One of the algebraic structure is exhaustion number as defined in [6]. In [8], they investigated the exhaustion number of dihedral group of order $2p$, where p is an odd prime. Another type

S.-H. Heng and J. Lopez (Eds.): ISPEC 2019, LNCS 11879, pp. 413–422, 2019.
https://doi.org/10.1007/978-3-030-34339-2_23

of analogous of group factorization, namely complete decomposition is defined as follows: Let G be a finite non-abelian group. Let $A_1, \cdots, A_k$ be non-empty subsets of G, where $k \geq 2$ is an integer such that $A_i \cap A_j = \emptyset$ for integers $i, j = 1, \cdots, k$ $(i \neq j)$. We say that $(A_1, \cdots, A_k)$ is a complete decomposition of G if the product of subsets $A_{i_1} \cdots A_{i_k} = \{a_{i_1} ... a_{i_k} | a_{i_j} \in A_{i_j}; j = 1, \cdots, k\}$ coincides with G where the A_{i_j} are all distinct and $\{A_{i_1}, \cdots, A_{i_k}\} = \{A_1, \cdots, A_k\}$. The investigation of complete decomposition of some finites groups can be found in [5].

Computational hardness assumptions are essential elements in cryptography. They are building blocks of a cryptographic primitive. Generally, computer scientist relates the hardness of a new problem to a well-known hardness assumption by reduction. Researchers reviewed the proposed hardness problem continuously over the years [4,11,24,25]. There are many hardness problems proposed in the past, such as integer factorization problem, Rivest-Shamir-Adleman (RSA) problem, discrete logarithm problem, knapsack problem etc. In this paper, we proposed some group-based hardness problem. One of the well known group-based hardness problem proposed is the Conjugacy Search Problem (CSP) [20]. The similarity of our proposed hardness problem and CSP is the utilization of non-commutative properties of the underlying group.

Diffie and Hellman [9] first developed the idea of asymmetric key exchange protocol. The security of Diffie-Hellman key exchange protocol depended on the hardness of the discrete logarithm problem (DLP). Two years later, Rivest, Shamir and Aldeman applied the hardness of integer factorization problem (IFP) to propose an encryption scheme which known as RSA encryption scheme [17]. However, Shor [18] proposed an algorithm that can feasibly solve many conventional number theory based problem. Therefore, the security of public-key cryptosystems that relied on some well-studied hardness problem such as DLP and IFP become questionable. Thus, researchers start looking into code-based, lattice-based, hash-based and group-based cryptographic primitives that suspected to remain secure under post-quantum attack [3].

Numerous studies regarding group-based cryptography had been conducted over the years [10]. The idea of constructing some cryptographic primitives based on the non-commutative group has been discussed in [19]. There are some constructions of cryptographic primitives based on the braid group by applying the conjugacy search problem (CSP) [1,7,16]. Baba et al. [2] constructed a relevant analogy from the integer factorization problem to the factorization problem over non-abelian groups. Gu and Zheng proposed several conjugated problems related to the factorization problem over non-abelian groups and showed three constructions of cryptographic primitives based on these conjugacy systems [12]. The idea that using the complexity of infinite non-abelian groups in cryptography was first proposed by Wagner and Magyarik [23]. They devised a public-key protocol based on unsolvability of the word problem in 1985. Search problems are the most suggested protocols and they are variants of decision problems of group theory. They are suitable for the general paradigm of a public key protocol. Some of the key exchange protocols related to non-commutative groups were proposed in [21,22].

Our Contribution. The main contribution of this paper is to propose a new hardness problem called Complete Decomposition Search Problem (CDSP). We construct a key exchange protocol based on CDSP. We choose generalized quaternion group Q_{2^n} as our platform group. We also provide some constructions of complete decomposition of Q_{2^n} to show that the CDSP can be practically applied. Besides, we compare the performance of our scheme with the Diffie-Hellman key exchange protocol. Finally, we present some simple security analysis of the proposed scheme.

2 Some Constructions of Complete Decomposition of Q_{2^n}

The generalized quaternion group Q_{2^n} is a finite non-abelian group with group presentation $\langle x, y | x^{2^{n-1}} = 1, y^2 = x^{2^{n-2}}, yx = x^{2^{n-1}-1}y \rangle$ for integer $n \geq 3$. In this section, we first introduce some of the multiplication rules for the elements in the generalized quaternion group Q_{2^n}. Then, we provide a construction of complete decomposition of Q_{2^n}.

Lemma 1. *Let i, n be some integers such that $1 \leq i \leq 2^{n-1} - 1$ and $n \geq 3$. Then the following properties holds:*

(i) $x^i y = y x^{2^{n-1}-i}$;
(ii) $\langle x \rangle y x^i = \langle x \rangle y$.

Proof. Note that $\langle x \rangle = \{1, x, x^2, \ldots, x^{2^{n-1}-1}\}$ and $\langle x \rangle y = \{y, xy, \ldots, x^{2^{n-1}-1}y\}$. By employing induction on i, the basic step $xy = yx^{2^{n-1}-1}$ for $i = 1$ holds. Assume that it is true when $i = k$ for some positive integers k, then $x^k y = yx^{2^{n-1}-k}$. Now, we show that the case $i = k + 1$ is true. For $i = k + 1$, we have $x^{k+1}y = x^k xy = x^k yx^{2^{n-1}-1} = yx^{2^{n-1}-k}x^{2^{n-1}-1} = yx^{2^{n-1}}x^{2^{n-1}-(k+1)}$. Since $x^{2^{n-1}} = 1$, it follows that $yx^{2^{n-1}}x^{2^{n-1}-(k+1)} = yx^{2^{n-1}-(k+1)}$ as required. For part (ii), we see that $\langle x \rangle y x^i = \{1, x, \ldots, x^{2^{n-1}-1}\}x^{2^{n-1}-i}y = \{x^{2^{n-1}-i}y, x^{2^{n-1}}y, \ldots, x^{2^n-i-1}y\}$. Since $|\{x^{2^{n-1}-i}y, x^{2^{n-1}}y, \ldots, x^{2^n-i-1}y\}| = 2^{n-1}$, it follows that $\{x^{2^{n-1}-i}y, x^{2^{n-1}}y, \ldots, x^{2^n-i-1}y\} = \langle x \rangle y$.

2.1 Construction of Complete Decomposition of Q_{2^n}

Let A, B be the subsets of Q_{2^n}. To show that the complete decomposition of generalized quaternion group Q_{2^n} is not trivial, we first show an example where (A, B) is not a complete decomposition of Q_{2^n}.

Example 1. Let $A = \{1, x, \ldots, x^{2^{n-1}-1}\}$ and $B = \{y, xy, \ldots, x^{2^{n-1}-1}y\}$ be the subsets of Q_{2^n}. Clearly, $A = \langle x \rangle \subseteq Q_{2^n}$ and $B = \langle x \rangle y \subseteq Q_{2^n}$. Since $AB \subseteq \langle x \rangle y$, it follows that (A, B) is not a complete decomposition of Q_{2^n}.

Next, we provide a construction of complete decomposition of generalized quaternion group Q_{2^n} for integer $n \geq 4$. For practical reason, the selection of subsets A and B are restricted to the condition where $A \cup B \subsetneq Q_{2^n}$.

Proposition 1. *Let* $A = \{1, x, x^2, \ldots, x^{2^{n-1}-3}\} \cup \{x^{2^{n-1}-2}y, x^{2^{n-1}-1}y\}$ *and* $B_i = (\{y, xy, \ldots, x^{2^{n-1}-3}y\} \cup \{x^{2^{n-1}-2}, x^{2^{n-1}-1}\}) \setminus \{xy, x^3y, \ldots, x^iy\}$ *be the subsets of* Q_{2^n}*, where* $i \in \{1, 3, \ldots, 2^{n-1} - 5\}$, $|A| = 2^{n-1}$ *and* $2^{n-2} + 2 \leq |B_i| \leq 2^{n-1} - 1$. *Then* (A, B_i) *is a complete decomposition of* Q_{2^n} *for integer* $n \geq 4$.

Proof. To show that (A, B_i) is a complete decomposition, we first consider the case when $i = 2^{n-1} - 5$. We have $B_{2^{n-1}-5} = \{y, x^2y, \ldots, x^{2^{n-1}-6}y, x^{2^{n-1}-4}y\} \cup \{x^{2^{n-1}-3}y\} \cup \{x^{2^{n-1}-2}, x^{2^{n-1}-1}\}$ with size $2^{n-2} + 2$. We compute the product of sets $\{1, x, x^2, \ldots, x^{2^{n-1}-3}\} \subseteq A$ and $\{y, x^2y, \ldots, x^{2^{n-1}-4}y\} \subseteq B_{2^{n-1}-5}$ as follows:

$$\begin{aligned}&\{1, x, x^2, \ldots, x^{2^{n-1}-3}\}\{y, x^2y, x^{2^{n-1}-4}y\}\\ &= \langle x\rangle y.\end{aligned}$$

Then, we compute the product of sets $\{x^{2^{n-1}-2}y, x^{2^{n-1}-1}y\} \subseteq A$ and $\{y, x^2y, \ldots, x^{2^{n-1}-4}y\} \subseteq B_{2^{n-1}-5}$ as follows:

$$\begin{aligned}L_1 =&\{x^{2^{n-1}-2}y, x^{2^{n-1}-1}y\}\{y, x^2y, \ldots, x^{2^{n-1}-4}y\}\\ =&\{x^{2^{n-1}+2^{n-2}+2}, x^{2^{n-1}+2^{n-2}+3}, \ldots, x^{2^{n-1}+2^{n-2}+2^{n-1}-1}\}\end{aligned}$$

where $|L_1| = 2^{n-1} - 2$. Then, we compute the product of sets $\{x^{2^{n-1}-2}y, x^{2^{n-1}-1}y\} \subseteq A$ and $\{x^{2^{n-1}-3}y\} \subseteq B_{2^{n-1}-5}$ as follows:

$$L_2 = \{x^{2^{n-1}-2}y, x^{2^{n-1}-1}y\}\{x^{2^{n-1}-3}y\} = \{x^{2^{n-1}+2^{n-2}+1}, x^{2^{n-1}+2^{n-2}+2}\}.$$

Observe that $L_1 \cup L_2 = \{x^{2^{n-1}+2^{n-2}+1}, x^{2^{n-1}+2^{n-2}+2}, \ldots, x^{2^{n-1}+2^{n-2}+2^{n-1}-1}\}$ with the size $|L_1 \cup L_2| = 2^{n-1} - 1$. We notice that $\langle x\rangle \setminus (L_1 \cup L_2) = \{x^{2^{n-1}+2^{n-2}+2^{n-1}}\}$. Next, we compute the product of sets $\{1, x, \ldots, x^{2^{n-1}-3}\} \subseteq A$ and $\{x^{2^{n-1}-2}, x^{2^{n-1}-1}\} \subseteq B_{2^{n-1}-5}$ as follows:

$$\begin{aligned}L_3 =&\{1, x, \ldots, x^{2^{n-1}-3}\}\{x^{2^{n-1}-2}, x^{2^{n-1}-1}\}\\ =&\{x^{2^{n-1}-2}, x^{2^{n-1}-1}, \ldots, x^{2^{n-1}+2^{n-1}-4}\}\end{aligned}$$

where $|L_3| = 2^{n-1} - 1$. From here, we see that $\langle x\rangle \setminus L_3 = \{x^{2^{n-1}+2^{n-1}-3}\}$. To show that $(L_1 \cup L_2 \cup L_3) = \langle x\rangle y$, we need to show that $x^{2^{n-1}+2^{n-2}+2^{n-1}} \neq x^{2^{n-1}+2^{n-1}-3}$. Clearly $2^{n-1}+2^{n-2}+2^{n-1} \neq 2^{n-1}+2^{n-1}-3$ for any integer $n \geq 4$ which implies $x^{2^{n-1}+2^{n-2}+2^{n-1}} \neq x^{2^{n-1}+2^{n-1}-3}$. Thus, $(L_1 \cup L_2 \cup L_3) = \langle x\rangle y$. Therefore, we say that $(A, B_{2^{n-1}-5})$ is a complete decomposition of Q_{2^n}. Since $B_{2^{n-1}-5} \subseteq B_{2^{n-1}-7} \subseteq \cdots \subseteq B_1$ and $(A, B_{2^{n-1}-5})$ is a complete decomposition of Q_{2^n}, it follows that (A, B_i) is a complete decomposition of Q_{2^n} for $n \geq 4$ and $i \in \{1, 3, \ldots, 2^{n-1} - 5\}$.

3 Application on Cryptography

In this section, we first propose two problems, namely Decisional Complete Decomposition Search Problem and Computational Complete Decomposition Search Problem for arbitrary finite nonabelian group G. We provide a key exchange protocol based on the hardness problem proposed. Finally, we analyze the performance and security of the proposed scheme.

3.1 Complete Decomposition Search Problem (CDSP)

We define two problems as follows:

Decisional Complete Decomposition Search Problem (DCDSP): Let G be a finite non-abelian group. Given A, B and G. Determine whether B satisfies $AB = G$, where $A, B \subseteq G$ and $A \cap B = \emptyset$.

Computational Complete Decomposition Search Problem (CCDSP): Let G be a finite non-abelian group. Given A and G. Find B such that $AB = G$, where $A, B \subseteq G$ and $A \cap B = \emptyset$.

In this paper, we choose our platform group G as generalized quaternion group Q_{2^n}. We construct an algorithm to solve CCDSP in Q_{2^n} below for integer $n \geq 4$. Since $A \cap B = \emptyset$ and $|Q_{2^n}| = 2^n$, it follows that the total combination of subsets B given $|A|$ is $\binom{2^n-|A|}{|B|}$. Let $\{B_j | j = 1, 2, \ldots, \binom{2^n-|A|}{|B|}\}$ represents all the possible subsets of B. The algorithm computes the products $AB_1, AB_2, \ldots, AB_{\binom{2^n-|A|}{|B|}}$ and return B_j if $AB_j = G$ for integer $1 \leq j \leq \binom{2^n-|A|}{|B|}$.

Algorithm 1. Solve CCDSP in Q_{2^n}

- **Input**: $A, |B|, n$.
- **Output**: All possible subsets of B_j for $j = 1, 2, \ldots, \binom{2^n-|A|}{|B|}$.
- For each possible subset $B_j \subseteq Q_{2^n}$, where $1 \leq j \leq \binom{2^n-|A|}{|B|}$, compute $AB_j = D$.
- If $D = G$, then return a solution B_j.
- Return (no solution exists).

3.2 Our Proposed Scheme

Let $A, B \subseteq Q_{2^n}$. In this section, we propose a key exchange protocol based on the computational complete decomposition search problem (CCDSP) in Q_{2^n} between Alice and Bob. Suppose Alice holds a shared key B and wants to share with Bob. They can proceed as follows:

1. **Preparation Step** A and Q_{2^n} are selected and published, where $AB = Q_{2^n}$. Two subsets $A_1, A_2 \subseteq \langle x \rangle$ are selected and kept secretly. Alice chooses $a \in A$ and two distinct elements $b_1, b_2 \in A_1$ secretly. Bob chooses $c \in Q_{2^n}$ and two distinct elements $d_1, d_2 \in A_2$ secretly.
2. **Sharing private key** a
   (a) Alice computes $b_1 a b_2$.
   (b) Bob computes $d_1 b_1 a b_2 d_2$.
   (c) Alice computes $b_1^{-1} b_1 d_1 a d_2 b_2 b_2^{-1}$.
   (d) Bob computes $d_1^{-1} d_1 a d_2 d_2^{-1} = a$.
3. **Sharing private key** c
   (a) Bob computes $d_1 c d_2$.
   (b) Alice computes $b_1 d_1 c d_2 b_2$.
   (c) Bob computes $d_1^{-1} d_1 b_1 c b_2 d_2 d_2^{-1} = b_1 c b_2$.
   (d) Alices computes $b_1^{-1} b_1 c b_2 b_2^{-1} = c$.
4. **Exchange shared key** B
   (a) Alice and Bob compute $ac = b$.
   (b) Alice computes $E = Bb$.
   (c) Bob computes $x = (ac)^{-1} = c^{-1} a^{-1}$.
   (d) Bob computes $Ex = Bbx = Bacc^{-1}a^{-1} = B$.

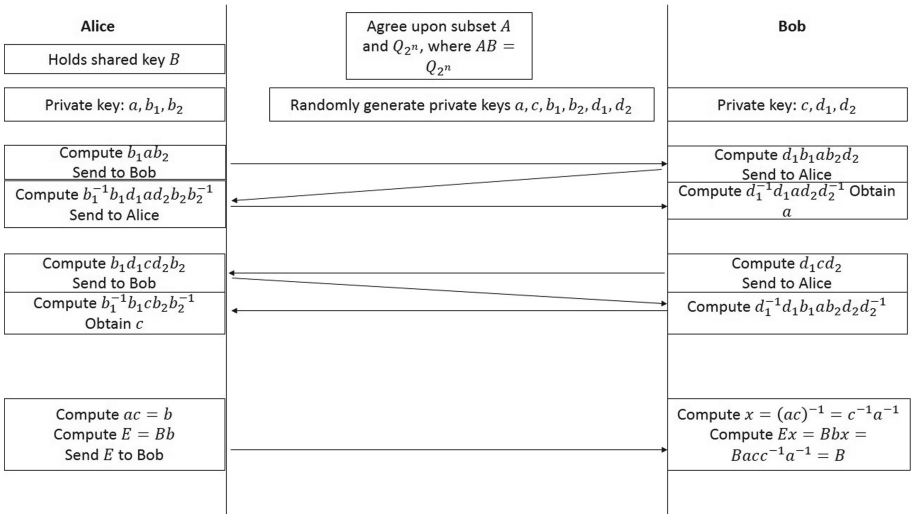

Fig. 1. Proposed key exchange protocol

3.3 Performance Analysis

For our proposed scheme which constructed using finite non-abelian generalized quaternion group, the steps involved are expected to be longer compare to other group-based key exchange protocol which constructed based on the abelian

group. From Fig. 1, we see that sharing private key a and c between Alice and Bob involved 8 mathematical computation in total. For the step involving calculating the shared key B, there is a total of 4 mathematical computations required. The computations involved in our proposed scheme are mainly on multiplication between the group elements, which can be done easily due to the well-studied structure of the generalized quaternion group Q_{2^n}.

Comparing with Diffie-Hellman Key Exchange Protocol in Term of Performance. Now, we compare the performance of our proposed scheme with the pioneer of the key exchange protocol, which is Diffie-Hellman key exchange protocol. The parameters used in Diffie-Hellman key exchange protocol are a prime numbers p and q (generator of p). For computation wise, Diffie-Hellman key exchange protocol involved of 4 steps. Besides, only one communication required between Alice and Bob to obtain the shared key. Clearly our proposed scheme takes more steps in term of computation and communication compare to Diffie-Hellman key exchange protocol, however Diffie-Hellman Problem (DHP) might become vulnerable under the post-quantum attack.

3.4 Security of the Scheme

In Sect. 2.1, we show a construction of (A, B) is a complete decomposition of generalized quaternion group Q_{2^n}, where $|A| = 2^{n-1}$ and $2^{n-1} - 2 \leq |B| \leq 2^{n-1} - 1$ for integer $n \geq 4$. We first discuss the security of the scheme by using Algorithm 1 proposed in Sect. 3.1 and consider the case where $|A| = 2^{n-1}$ and $|B| = 2^{n-1} - 2$.

Theorem 1. *Let A, B be the subsets of Q_{2^n}, where $|A| = 2^{n-1}$ and $|B| = 2^{n-1} - 2$ for $n \geq 4$. Adversary takes at least exponential time E to solve Computational Complete Decomposition Search Problem using subsets A, B in Algorithm 1.*

Proof. Note that $|B| = \frac{|Q_{2^n}|}{|A|}$, $A \cap B = \emptyset$ and $|Q_{2^n}| = 2^n$. Since $A \cap B = \emptyset$, we can exclude the elements in subset A and hence left with the remaining $2^n - |A|$ elements. To search for subset B, one will try for different subset B_i, where the choice of elements for B_i comes from $2^n - |A|$ remaining elements. Thus, the worst case for one to obtain such subset B require $\binom{2^n - |A|}{|B|}$ attempts. Next, we show that Algorithm 1 need at least exponential time E to break our scheme. We compare the value between $\binom{2^n - |A|}{|B|}$ and 2^n as follows:

$$\begin{aligned}\binom{2^n - |A|}{|B|} &= \binom{2^{n-1}}{2^{n-1} - 2} \\ &= \frac{2^{n-1}!}{2!(2^{n-1} - 2)!} \\ &= \frac{1 \cdot 2 \cdots 2^{n-1}}{2(1 \cdot 2 \cdots (2^{n-1} - 2))}\end{aligned}$$

$$
\begin{aligned}
&= \frac{(2^{n-1}-1)2^{n-1}}{2} \\
&= (2^{n-1}-1)2^{n-2} \\
&= 2^{2n-3} - 2^{n-2} \geq 2^n
\end{aligned}
$$

Clearly, $(2^{n-1}-1)2^{n-2} \geq 2^n$ for $n \geq 4$. Since $\binom{2^n-|A|}{|B|} \geq 2^n$ for $n \geq 4$, it follows that Adversary takes at least exponential time E to break our scheme using Algorithm 1.

Next, we discuss the security of the scheme by assuming that adversary knows some of the private information related to the scheme. Firstly, suppose adversary knows $A_1 \subseteq \langle x \rangle$, where $|A_1| = t$. Then, adversary can guess two distinct elements $b_1, b_2 \in A_1$ correctly with the probability $Pr(Adv\ guess\ b_1, b_2) = \frac{1}{t}(\frac{1}{t-1})$. From here, adversary is able to compute a from $b_1 a b_2$ by using b_1, b_2. However, adversary has no information about $c \in Q_{2^n}$. Secondly, suppose adversary knows $A_2 \subseteq \langle x \rangle$, where $|A_2| = u$. Then, the probability of adversary guesses two distinct elements $d_1, d_2 \in A_2$ correctly is $Pr(Adv\ guess\ d_1, d_2) = \frac{1}{u}(\frac{1}{u-1})$. By using d_1 and d_2, adversary can compute c from $d_1 c d_2$. However, the information about a remains unknown to adversary. Finally, suppose that adversary knows $A_1, A_2 \subseteq \langle x \rangle$, then adversary is able to compute a, c with the probability $Pr(Adv\ guess\ b_1, b_2, d_1, d_2) = \frac{1}{t}(\frac{1}{t-1}) + \frac{1}{u}(\frac{1}{u-1})$. Adversary can use a, c to compute $c^{-1}a^{-1}$ then followed by shared key B. To summarize this, adversary is not able to compute the shared key B if he knows either A_1 or A_2 but not both. If adversary knows A_1, A_2, where $|A_1| = t, |A_2| = u$, then the probability of adversary computes shared key B correctly is $\frac{1}{t}(\frac{1}{t-1}) + \frac{1}{u}(\frac{1}{u-1})$. Thus, if t and u are large integers, then $\lim_{t\to\infty} \frac{1}{t} = \lim_{t\to\infty} \frac{1}{t-1} = \lim_{u\to\infty} \frac{1}{u} = \lim_{u\to\infty} \frac{1}{u-1} = 0$. Hence, the probability of adversary to compute shared key B correctly is negligible and the scheme is secured. We summarize the results in the following Table 1.

Table 1. Security of the scheme with the assumption that the adversary knows some information

Information that adversary knows	Can adversary computes a correctly from the given information?	Can adversary computes c correctly from the given information?	Can adversary computes shared key B correctly from the given information?
A_1 with size t	Yes, with the probability of $\frac{1}{t}(\frac{1}{t-1})$	No	No
A_2 with size u	No	Yes, with the probability of $\frac{1}{u}(\frac{1}{u-1})$	No
A_1 and A_2	Yes, with the probability of $\frac{1}{t}(\frac{1}{t-1})$	Yes, with the probability of $\frac{1}{u}(\frac{1}{u-1})$	Yes, with the probability of $\frac{1}{t}(\frac{1}{t-1}) + \frac{1}{u}(\frac{1}{u-1})$

3.5 Open Questions

For future research direction, researchers should analyze which assumptions can be reduced from Complete Decomposition Search Problem as proposed in this paper. We believe that there exists a relation between CDSP and Subset Sum Problem which known to be NP-hard. However, we are not able to provide any formal proof for this statement here. For the implementation of the proposed scheme in a real work scenario, one can investigate on the value of security parameter, for instance the size of subsets A and B to be used so that it provides the same security level like 2048 bit or 4098 bit Diffie Hellman key exchange. Besides, formal security proof or generic model of the proposed scheme should be considered.

Acknowledgments. The project was funded by the Fundamental Research Grant Scheme (FRGS), project number FRGS/1/2017/STG06/UTAR/02/3.

References

1. Anshel, I., Anshel, M., Goldfeld, D.: An algebraic method for public-key cryptography. Math. Res. Lett. **6**, 287–291 (2001)
2. Baba, S., Kotyada, S., Teja, R.: A non-abelian factorization problem and an associated cryptosystem. Cryptology Eprint Archive Report 2011/048 (2011)
3. Bernstein, D.J., Lange, T.: Post-quantum cryptography dealing with the fallout of physics success. IACR Cryptology Eprint Archive/2017/314 (2017)
4. Boudot, F.: On improving integer factorization and discrete logarithm computation using partial triangulation. Cryptology Eprint Archive Report 2017/758 (2017)
5. Chin, A.Y.M., Chen, H.V.: Complete decompositions of finite abelian groups. AAECC **30**, 263–274 (2018)
6. Chin, A.Y.M.: Exhaustion numbers of maximal sum-free sets of certain cyclic groups. Matematika **15**(1), 57–63 (2009)
7. Dehornoy, P.: Braid-based cryptography. Contemp. Math. **360**, 5–33 (2004)
8. Wong, C.K.D., Wong, K.W., Yap, W.S.: Exhaustion 2-subsets in dihedral groups of order $2p$. Asian Eur. J. Math. World Sci. Publ. Co. **11**(3), 1–13 (2018)
9. Diffie, W., Hellman, M.E.: New direction in cryptography. IEEE Trans. Inf. Theory **22**(6), 644–654 (1976)
10. Fine, B., Habeeb, M., Kahrobaei, D., Rosenberger, G.: Aspects of nonabelian group based cryptography: a survey and open problems. JP J. Algebra Number Theorie Appl. **21**, 1–40 (2011)
11. Goldwasser, S., Kalai, Y.T.: Cryptographic Assumptions: A Position Paper. TCC, pp. 505–522 (2015)
12. Gu, L., Zheng, S.: Conjugacy systems based on nonabelian factorization problems and their applications in cryptography. J. Appl. Math. **52**(2), 1–9 (2014)
13. Hajos, G.: Covering multidimensional spaces by cube lattices. Mat. Fiz. Lapok **45**, 171–190 (1938)
14. Hajos, G.: Uber Einfache und Mehrfache Bedeckung des n-dimensionalen Raumes Mit Einem Urfelgitter. Math. Zeit. **47**, 427–467 (1942)
15. Hajos, G.: Sur la Factorisation des Groupes Abeliens. Casopis Pes. Mat. Fys. **74**, 157–162 (1949)

16. Ko, K.H., Lee, S.J., Cheon, J.H., Han, J.W., Kang, J., Park, C.: New public-key cryptosystem using braid groups. In: Bellare, M. (ed.) CRYPTO 2000. LNCS, vol. 1880, pp. 166–183. Springer, Heidelberg (2000). https://doi.org/10.1007/3-540-44598-6_10
17. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2), 120–126 (1978)
18. Shor, P.W.: Polynomial-time algorithm for prime factorization and discrete logarithms on quantum computer. SIAM J. Comput. **26**(5), 1484–1509 (1997)
19. Shpilrain, V., Ushakov, A.: Thompson's group and public key cryptography. In: 3rd International Conference on Applied Cryptography and Network Security, ACNS 2005, pp. 151–163 (2005)
20. Shpilrain, V., Ushakov, A.: The conjugacy search problem in public key cryptography: unnecessary and insufficient. Appl. Algebra Eng. Commun. Comput. **17**, 285–289 (2006)
21. Ustimenko, V., Klisowski, M.: On noncommutative cryptography and homomorphism of stable cubical multivariate transformation groups of infinite dimensional affine spaces. Cryptology Eprint Archive Report 2019/593 (2019)
22. Ustimenko, V.: On inverse protocol of post quantum cryptography based on pairs of noncommutative multivariate platforms used in tandem. Cryptology Eprint Archive Report 2019/897 (2019)
23. Blakley, G.R., Chaum, D. (eds.): CRYPTO 1984. LNCS, vol. 196. Springer, Heidelberg (1985). https://doi.org/10.1007/3-540-39568-7
24. Yana, K., Yulia, K.: Merkle-Hellman knapsack cryptosystem in undergraduate computer science curriculum. FECS, pp. 123–128 (2010)
25. Zhu, H.: Survey of computational assumptions used in cryptography broken or not by shor's algorithm. Master in Science, Mc Gill University Montreal (2001)