ASM Sc. J., 12, Special Issue 5, 2019 for ICoAIMS2019, 57-64

A New Signature Scheme Define over a Class of Non-Abelian Group

Denis C.K. Wong

Lee Kong Chian Faculty of Engineering and Science, DMAS,
Universiti Tunku Abdul Rahman, Sungai Long, Malaysia

A signature scheme consists of three algorithms, which are, the key generation, signing and verification algorithms used for verifying the authenticity of digital messages or documents. Most existing signature schemes are constructed based on number theory based hard problems such as integer factorization problem, discrete logarithm problem, quadratic residue problem and etc. Furthermore, conventional signature schemes are mostly defined over abelian group deal to engineer preference. Our main objective is to construct a new signature scheme π by generalized the scheme to non abelian group. More precisely, we will use the dihedral group D_{2pq} of order $2pq$, where p and q are two distinct large primes. A new hard problem known as the exhaustion number search problem is introduced which relies on the difficulty of computing the exhaustion set in D_{2pq}. We show that the exhaustion number set problem is computationally equivalent to the well-known subset sum problem originated from the Knapsack set problem. Furthermore, we construct a new family of hash function h which is relied on the Cayley graph of the maximal cyclic subgroup $\langle r \rangle$ of D_{2pq}. Together with h, we will show that the proposed scheme π is secure against existential forgery under an adaptive chosen message attack.

Keywords: signature scheme; dihedral group; Cayley graph; exhaustion set

I. INTRODUCTION

Many public key encryption schemes are remained secure based on the hardness of some mathematical problems in a large and finite abelian group (more precisely, finite cyclic groups) (Fiat et al. 1986; Merkle et al. 1978). Some well studied hard problems that have been used are the integer factorization and discrete logarithm problems (Rivest et al. 1978; Zhang et al. 2004). However, deal to Shor's algorithm (Shor 1997), many conventional number theories based hard problems become feasible to solve. Hence, alternative hard problems must be proposed which avoid the attack by Shor's algorithm. In recent year, there are plenty of code-based, lattice-based and hash-based cryptographic primitives being constructed which might resist the Shor's attack. There are plenty of claims stated that the advent of quantum computers may cause many well-known hard problems used in various signature schemes to become vulnerable to various attacks. In this paper, we investigate an alternative direction, which is known as the group-based cryptography. In short, this direction of studies arise deal to the attempt to generalize current cryptographic primitives defined over abelian group to non abelian group (Ansel et al. 1999; Mahalanbis 2006; Paeng et al. 2001).

One of the most frequently used group-based hard problem is the conjugacy search problem (Ansel et al. 2001; Dehornoy 2004; Ko et al. 2000; Lee 2004). It is well known that this problem has a solution because one can recursively enumerate all conjugates of a given element, but the enumeration process can be very time consuming. Specific groups may or may not admit more efficient solutions, so the choice of the platform group is importance to ensure the constructed scheme is secure (Eick et al. 2008; Grigoriev et al. 2005}. For our construction, we choose the dihedral group as our platform group, and hence the security of the scheme is based on finding conjugator of certain elements in dihedral group. Although, conjugacy classes are well studies for dihedral group, we choose dihedral group for two main reasons:

1. the underlying algebraic properties of dihedral group is well studies; and
2. the constructed scheme using the dihedral group can be generalized easily to other groups such as

*Corresponding author's e-mail: deniswong@utar.edu.my

quasi-dihedral group, extra special $p-$ group, nilpotent group and etc.

Cryptographic primitives constructed by using non abelian group is not a new idea. Over the last decade, there has been an active line of research to develop and analyse new cryptosystems and key exchange protocols based on non commutative cryptographic platforms (Shpilrain 2006). More precisely, cryptographic primitives are constructed by using Braid group, linear group, modular group, polycyclic group and etc (Steinwandt 2004; Stickel 2004). Please refer to (Myasnilov et al. 2007) for a comprehensive introduction and survey.

In this paper, we propose a new hard problem, namely the exhaustion number search problem (ESP) which is originated from the combinatorics object called exhaustion set (ES) and is defined as follows:

"A subset S of D_{2pq} is called an exhaustion set provided $S^n = D_{2pq} + X$, where $X \in \mathbb{Z}[D_{2pq}]$."

For some existence results of exhaustion 2 −subsets in D_{2p} which can be extended to D_{2pq}, refer to (Wong et al. 2017). We shown that ESP over dihedral group is computationally equivalent to the well-known Knapsack set problem.

Despite in most of the conventional signature schemes, their message and key spaces are chosen from the cyclic group $\mathbb{Z}_{pq}$, but we propose to employ a dihedral group D_{2pq} of order $2pq$ as the platform group for our proposed scheme. Unlike $\mathbb{Z}_{pq}$, we see that D_{2pq} containing two cyclic subgroups, which are $\langle r \rangle$ of order pq and $\langle s \rangle$ of order 2. Clearly, there exists some elements in $\langle r \rangle s$ which do not commute and so the computation involves in both signing and verification phases are more complicated. The usage of non abelian group such as dihedral group as a platform group is two folds. On one hand, the property of non commutativeness does improve the security of the scheme in some sense. On the other hand, the computational time of the proposed scheme will be definitely increased due to the property of non commutativeness.

Main Contribution. The main contributions of this paper are summarized as follows:

(1) Propose a new hard problem which is known as the ESP, and hence show that the ESP is equivalent to the subset sum problem (SSP),

(2) Use a systematically way to construct a collision resistant hash function from the directed Cayley graph based on dihedral group of order $2pq$.

(3) Construct a signature scheme by using the dihedral group of order $2pq$ as the platform group based on the hardness of ESP.

Paper Organization. The rest of this paper is organized as follows. In Section 2, we discussed some preliminary concepts and the exhaustion set problem in dihedral groups, and then we setup a linkage for showing that the exhaustion number search problem is computationally equivalent to subset sum problem. In Section 3, we proposed a construction of hash function based on directed Cayley graph and proposed a new signature scheme based on ESP together with its security analysis. We conclude in Section 4.

II. PRELIMINARIES

A. Syntax and Definition of Signature Scheme

The formal definition of a signature scheme (see (Steinwandt 2004; Myasnikov et al. 2007)) is given as follows:

A **Signature Scheme** π is a tuple of three probabilistic polynomial-time algorithms $(Gen, Sign, Ver)$ satisfying the following:

The Key-Generation Algorithm: Gen takes as input a security parameter 1^n and outputs a pair of keys (pk, sk), which are the public key and the private key, respectively.

The Signing Algorithm} $Sign$ takes as input a private key sk and a message $m \in \{0,1\}^*$. It outputs a signature σ, denoted as $\sigma \leftarrow Sign_{sk}(m)$.

The Verification Algorithm: Ver takes as input a public key pk, a message m, and a signature σ. It outputs a bit b, with $b = 1$ meaning valid and $b = 0$ meaning invalid. We write this as $b := Ver_{pk}(m, \sigma)$.

It is required that for every n, every (pk, sk), output by $Gen(1^n)$, and every $m \in \{0,1\}^*$, it holds that $Ver_{pk}(m, Sign_{sk}(m) = \sigma) = 1$.

Let $\pi = (Gen, Sign, Ver)$ be a signature scheme. We follow the standard security model as given in (Rivest et al. 1978; Mahalanbis 2008; Paeng et al. 2001; Dehornoy 2004; Lee 2004). Consider the following experiment for an adversary $\mathbb{A}$ and parameter n. The signature experiment $Sign-forge_{\mathbb{A},\pi}(n)$:

- $Gen(1^n)$ is run to obtain keys (pk, sk).

- Adversary $\mathbb{A}$ is given pk and oracle access to $Sign_{sk}$. This oracle returns a signature σ for any message m of the adversary's choice. The adversary then output (m, σ). Let Q denote the set of messages whose signatures were requested by $\mathbb{A}$ during its execution.
- The output of the experiment is defined to be 1 if and only if (1) $Ver_{pk}(m, \sigma) = 1$ and (2) $m \notin Q$.

π is existentially unforgeable under an adaptive chosen-message attack if for all probabilistic polynomial-time adversaries $\mathbb{A}$, there exists a negligible function $negl$ such that $Pr[Sign - forge_{\mathbb{A},\pi}(n) = 1] \leq negl(n)$.

B. Exhaustion Set Problem in Dihedral groups

In a non-abelian group G, two elements $x, y \in G$ are conjugate to each other, written $x \sim y$ if $y = a^{-1}xa$ for some $a \in G$. Here, a or a^{-1} is called a conjugator and the pair (x, y) is said to be conjugate. We note that $\sim$ is an equivalence relation and the corresponding equivalence classes are called the conjugacy classes. The conjugacy problem was identified by Max Dehn in 1911 as one of the fundamental problems in group theory together with another two problems; the word problem and the isomorphism problem. It is known that the conjugacy problem is infeasible for many classes of groups. We next introduce two version of the conjugacy problems.

Conjugacy Decision Problem: Determine whether $x \sim y$ for a given instance $x, y \in G$.

Conjugacy Search Problem: Find $a \in G$ such that $y = a^{-1} xa$ for a given instance $x, y \in G$ such that $x \sim y$.

Clearly, conjugacy problem is a generalized version of the well-known number theory based discrete logarithm problem which is usually defined over multiplicative cyclic groups.

In the following discussion, we introduce a new hard problem analogous to the conjugacy problem in non abelian group. To use a group efficiently for cryptography purposes, we need to carefully choose the underlying group and the most important criteria is the group must be able to describe by a presentation. In short, a presentation of a group is a set of generators and defining relations.

From now onward, we let p and q be distinct large prime numbers. A dihedral group D_{2pq} of order $2pq$ is a non abelian group describes by the following presentation

$$D_{2pq} = \langle r, s \mid r^{pq} = s^2 = 1, sr = r^{-1}s \rangle.$$

One of the most distinguishable differences between $\mathbb{Z}_{pq}$ and D_{2pq} is D_{2pq} is non-abelian group. The computation involves elements from D_{2pq} is undoubtedly more complicated as not all elements are commuted, hence it can be treated as a new security layer against outside attack by opponents. However, the multiplication of elements in D_{2pq} does increase the cost of computations.

We would like to emphasize that groups containing a subgroup isomorphic to the generalized linear group are not useful in cryptography due to plenty of well-developed tools in linear algebra. On the other hand, since there is only the "multiplicative" operation in our chosen platform group, the dihedral group, then, for instance, to construct a El-Gamal like scheme we need the "addition" operation as well. To do this, we introduce the concepts of group ring.

Let R be a commutative ring with unity 1 and G be a multiplicative group with identity 1. The group ring $R[G]$ of G with coefficients in R is the set

$$R[G] = \left\{ \sum_{g \in G} a_g \, g : a_g \in R \right\}.$$

Addition and multiplication in $R[G]$ are defined as follows: $\sum_{g \in G} a_g \, g + \sum_{g \in G} b_g \, g = \sum_{g \in G} (a_g + b_g) \, g$ and $\sum_{g \in G} a_g \, g \sum_{h \in G} b_h \, h = \sum_{g \in G} \sum_{h \in G} a_g b_h \, gh$.

We next introduce a new hard problem in dihedral group, called the exhaustion number search problem (ESP), (Wong et al. 2017). This problem is formulated based on the existence of exhaustion set (ES), which is formally defined as follows:

Definition 1. Let S be a nonempty subset of D_{2pq} with $1 < |S| < 2pq$. The **exhaustion number** of S is defined by $e(S) = min\{ t : S^t = D_{2pq} + Y \}$. If $e(S)$ exists, then S is called the $|S|$ **−exhaustion set** in D_{2pq} and Y is called the **dummy set** of T.

To ensure exhaustion set can be applied in our proposed scheme, we further insists that if $e(S) = t$, then the following equation holds: $S^t = \alpha \, D_{2pq} + X$, where $\alpha \geq 1, X \in \mathbb{Z}[D_{2pq}]$ is nontrivial with D_{2pq} is not a subset $of \; X$. Under this assumption, X is unique for a given S and the corresponding exhaustion number t is also unique as shown in the following proposition.

Proposition 2. The dummy set X corresponding to an exhaustion set S in D_{2pq} is unique.

Proof. Suppose we can write $S^t = \alpha D_{2pq} + X$ and $S^t = \beta D_{2pq} + X'$ with D_{2pq} is not a subset of X and D_{2pq} is nota subset of X'. Then, we see that $\alpha D_{2pq} + X = \beta D_{2pq} + X'$ which implies $(\alpha - \beta)D_{2pq} = X' - X$. If $\alpha > \beta$, then we can write $\alpha = \beta + \theta$ for some $\theta > 0$. Thus, $\theta D_{2pq} = X' - X$ which contradicts that D_{2pq} is not a subset of X and D_{2pq} is not a subset of X'. Similarly, we see that the case $\beta > \alpha$ is also impossible. Therefore, we conclude that $\alpha = \beta$ and so $X = X'$.

We are interested to find the exhaustion number t and the dummy set X. The computational and decision versions of the problem is given as follows:

Exhaustion Number Search Problem (ESP):
Given $S \subset D_{2pq}$. Find t such that $S^t = \alpha D_{2pq} + X$, where α and X with properties in Proposition 2.

Exhaustive Decision Problem (EDP):
Given $S \subset D_{2pq}$. Determine whether t satisfies $S^t = \alpha D_{2pq} + X$, where α and X with properties in Proposition 2.

The following corollary follows directly from Proposition 2.2.

Corollary 3. The output for ESP is unique.

Suppose $e(S) = t$. Then $S^t = \alpha D_{2pq} + X$. Let $R = \alpha D_{2pq} + X \in \mathbb{Z}[D_{2pq}]$. We rewrite $S^t = R$ as $S \sim R$. Similarly, for any $g_1, g_2 \in D_{2pq}$, if there exists an integer t such that $g_1^t = g_2$, then we write $g_1 \sim g_2$. Note that we use the same notation " $\sim$ " as in conjugacy class for exhaustion set. A subsets pair (S, R) is said to be ESP-hard if $S \sim R$ and ESP is infeasible for the instance (S, R). The security of our proposed scheme is depended on the hardness of solving the ESP.

The subset sum problem (SSP) is a well-known problem (Mathews 1897) and is the basis for the security of the Merkle-Hellman Knapsack scheme, refer (Merkle et al. 1978). The SSP given below is stated as a computational problem and is proven to be NP-hard, refer (Caprara et al. 2004; Gens et al. 1994; Kellerer et al. 2003; Martello et al. 1984; Martello et al. 1985).

Subset Sum Problem (SSP):
Given a set of positive integers $\{a_1, a_2, \dots, a_n\}$ which is called a Knapsack set, and a positive integer s. Find $x_i \in \{0,1\}, 1 \leq i \leq n$, such that $\sum_{i=1}^{n} a_i x_i = s$ provided that such x_i exist.

We are interested in the case when the underlying subset in SSP is form from elements in D_{2pq}. We convert the SSP to the following problem which is defined over D_{2pq}.

Subset Sum Problem in D_{2pq} (SSPD):
Given a subset $\{a_1, a_2, \dots, a_n\} \subset D_{2pq}$ and an element $s \in D_{2pq}$. Find $x_i \in \{0,1\}, 1 \leq i \leq n$ such that $\prod_{i=1}^{n} a_i^{x_i} = s$ provided that such x_i exist.

The SSPD can be solved by using the following Algorithm 1 which is modified from the Naive algorithm, see (Cormen et al. 2001; Martello et al. 1990). Note that Algorithm 1 takes $O(2^n)$ steps to produce an answer and, hence, is inefficient.

Algorithm 1: Solve SSPD
Input: $\{a_1, a_2, \dots, a_n\} \subset D_{2pq}$ and $s \in D_{2pq}$.
Output: $x_i \in \{0,1\}, 1 \leq i \leq n$ such that $\prod_{i=1}^{n} a_i^{x_i} = s$, provided x_i exist.
For each possible vector $(x_1, x_2, \dots, x_n) \in D_{2pq}$, compute $\prod_{i=1}^{n} a_i^{x_i} = l$.
If $l = s$, then return a solution $(x_1, x_2, \dots, x_n)$.
Return (no solution exists).

III. CONSTRUCTIONS

A. Proposed Hash Functions

In this section, we construct a special types of hash function that will be used as a hash oracle in our proposed scheme. Suppose $G = \langle r \rangle$ is the cyclic subgroup of D_{2pq} of order pq. Since G is isomorphic to the additive group of integers modulo $pq, \mathbb{Z}_{pq}$, so we may identity G with $\mathbb{Z}_{pq}$. We now present a method of hashing variable length texts over binary field $\mathbb{F}_2 = \{0, 1\}$ by modifying the method described in (Zemor 1994). The same method of hashing variable length texts can be defined over arbitrary finite field by using the following construction.

First, we choose a set S of generators of $\mathbb{Z}_{pq}$ with $|S| = |\mathbb{F}_2| = 2$, together with a one-to-one mapping f from $\mathbb{F}_2$ to S. For ease of implementation, we choose $S = \left\{1, \frac{1+pq}{2}\right\}$, whereby in general, we may choose arbitrary S. Next, we define the following function $f: \mathbb{F}_2 \to S$ as $0 \mapsto 1$ *and* $1 \mapsto \frac{1+pq}{2}$. The hash function h associated to G, S and f, is constructed as follows:

For any text $x \in \mathbb{F}_2^k$, associate the corresponding string of elements of S, and compute the sum in G to obtain the hashed value

$$h : \mathbb{F}_2^k \to \mathbb{Z}_{pq},$$

$$x = x_1 x_2 \dots x_k \mapsto h(x) = \sum_{i=1}^{k} f(x_i).$$

Denote by $X(\mathbb{Z}_{pq}, S)$ the directed Cayley graph associated with $\mathbb{Z}_{pq}$ and S. This means that the set of vertices of X is $\mathbb{Z}_{pq}$, and there is a directed edge between vertices v and w if and only if $w = v + s$ for all $s \in S$.

Suppose x is a text of length n. We can identity x as a directed path in the graph X, with the identity vertex as starting point, and its endpoint is precisely the hashed value $h(x)$. Note that two texts yielding the same hashed value correspond to two paths with the same starting and endpoints. We would like to minimize this instance to happen, and this turn out to construct X with large girth, refer (Zemor 1994). Roughly speaking, the girth of a graph is the length of a shortest cycle contained in the graph. Therefore, we choose $x \in \mathbb{F}_2^k$ with k strictly less than the girth of X which is $\frac{1+pq}{2}$. For instance, if $p = 11$ and $q = 13$ are the two distinct largest 4-bit primes, then we may choose $x \in \mathbb{F}_2^k$ for $k < 72$ to avoid collisions. Note that the hash function h constructed above is easily computed since the value can always be read from the directed Cayley graph and is computationally difficult to find collisions.

To use h in our proposed scheme, once we obtained the hashed value $h(x) \in \mathbb{Z}_{pq}$, we form

$$\begin{cases} r^{h(x)}, & h(x) \equiv 0 (mod\ 2) \\ r^{h(x)}s, & else \end{cases}$$

We emphasize that throughout the rest of this paper, s will always be multiplied on the right-hand side. For signature scheme, sometime we need to consider a hash function H in the form $H: \mathbb{F}_2^{k_1} \times \dots \times \mathbb{F}_2^{k_w} \to \mathbb{Z}_{pq}$. For this case, the hash function H is defined naturally as follows: $H(x_1, \dots, x_w) = \sum_{i=1}^{w} h(x_i) = \sum_{i=1}^{w} \sum_{j=1}^{k_i} h(x_{i_j})$, where $x_i = \left(x_{i_1}, x_{i_2}, \dots, x_{i_{k_i}}\right) \in \mathbb{F}_2^{k_i}$ for $i = 1,2, \dots, w$. By following the argument as in previous paragraph, we then multiply $r^{H(x_1,\dots,x_w)}$ with s to form $r^{H(x_1,\dots,x_w)}s \in D_{2pq}$. It follows that h is computationally infeasible to find collisions if and only if H is computationally infeasible to find collisions.

B. Proposed Signature Scheme

Suppose ESP is infeasible and EDP is feasible. Our proposed signature scheme π defined over D_{2pq} is described as follows:

First, two distinct large odd primes p and q are randomly picked, and form the platform group, i.e., the dihedral group D_{2pq}. Furthermore, use the hash function constructed in previous section.

Key-Generation: Choose $A \in \mathbb{Z}[D_{2pq}]$ with $e(A) = t$ and $A \sim B$. Public key is (A, B) and the private key is t.

Sign: Given a message $m \in \{0,1\}^*$, compute $y = h(m) \in D_{2pq}$ and the signature is $\sigma = y^t$.

Verify: Upon received the signed message (m, σ), we first computes $y = h(m)$ and check whether $Ay = yA$. If yes, then we check whether $\sigma \sim y$ and check whether $B\sigma \sim A\,y$. If both yes, then (m, σ) is a valid signed message.

Correctness. The correctness of the proposed scheme is shown as follows:

Given a message m, use the hash function h to compute $y = h(m)$. With the public key A, the signer will check whether $Ay = yA$. Next by using the private key to compute y^t and together with the signature σ, check whether $\sigma \sim y$ and

$$B\sigma = A^t\, y^t = (Ay)^t.$$

Hence, $B\sigma \sim Ay$.

C. Security Proof

In the following game, we consider an adversary $\mathbb{A}$ which are given the instances of ESP to find a solution for the ESP by preforming an interactive game with a challenger C.

With the system parameter and the knowledge of the dihedral group D_{2pq}, C generates the public key (A, B) and the private key t, where t is kept in secret and (A, B) will be given to $\mathbb{A}$. Next, $\mathbb{A}$ randomly selected some plaintexts $m_1, m_2, \dots, m_r \in \{0,1\}^*$ gives to the challenger C, then C queries the hash oracle h to obtain $h(m_1) = h_1$, $h(m_2) = h_2, \dots, h(m_r) = h_r \in D_{2pq}$ and also queries the sign oracle

to obtain $h_1^t = \sigma_1, h_2^t = \sigma_2, \dots, h_r^t = \sigma_r$, and hence return $\sigma_1, \sigma_2, \dots, \sigma_r$ to $\mathbb{A}$.

The adversary will maintenance the following list of valid signed messages:

$$(m_1, \sigma_1 = h_1^t)$$
$$(m_2, \sigma_2 = h_2^t)$$
$$\dots$$
$$(m_r, \sigma_r = h_r^t)$$

Next, $\mathbb{A}$ uses the verification algorithm to obtain and check the validity of the signed messages. The adversary proceed as follows:

$y_1 = h_1$	$Ay_1 = y_1 A$	$\sigma_1 = y_1^t$	$\sigma_1 \sim y_1$	$B\sigma_1 \sim A\, y_1$
$y_2 = h_2$	$Ay_2 = y_2 A$	$\sigma_2 = y_2^t$	$\sigma_2 \sim y_2$	$B\sigma_2 \sim A\, y_2$
...	...	...	...	...
$y_r = h_r$	$Ay_r = y_r A$	$\sigma_r = y_r^t$	$\sigma_r \sim y_r$	$B\sigma_r \sim A\, y_r$

With all these information, $\mathbb{A}$ compute $y_1\, y_2 \dots y_r = h_1\, h_2 \dots h_r$ and suppose that $h_1\, h_2 \dots h_r$ is the hashing of a message m_{r+1}, that is, $h(m_{r+1}) = h_1\, h_2 \dots h_r$. Let $y_{r+1} = y_1\, y_2 \dots y_r$, then check that $A\, y_{r+1} = y_{r+1} A$. Next, compute $\sigma_{r+1} = y_{r+1}^t$ and so $\sigma_{r+1} \sim y_{r+1}$.

Finally, we perform the following verification:

$$B\sigma_{r+1} = B\, y_{r+1}^t = A^t\, y_{r+1}^t = (Ay_{r+1})^t,$$

which implies that $B\, \sigma_{r+1} \sim A\, y_{r+1}$.

Therefore, $\sigma_{r+1} = \sigma_1\, \sigma_2 \dots \sigma_r$ is a valid signature on m_{r+1}. However, this is equivalent to the fact that we can find a $(B\sigma_{r+1}, Ay_{r+1})$-pair which is ESP-hard.

In the following theorem, we establish a condition on solving ESP in D_{2pq}.

Theorem 4. Solving ESP in D_{2pq} implies SSP in D_{2pq}. Conversely, solving SSP in D_{2pq} implies solving ESP in D_{2pq} provided the size of ES is more than or equal to $log_2\,(pq)$.

Proof. Let $T = \{a_1, a_2, \dots, a_n\} \subset D_{2pq}$. Note that $T^t = (a_1 + a_2 + \cdots + a_n)^t$. Since D_{2pq} is a nonabelian group, we cannot apply the multinomial theorem. However, by expanding each term manually (for instance, refer (Wong et Al. 2017)), we see that each term in the expansion can be written in the form $a_1^{x_1}\, a_2^{x_2} \dots a_n^{x_n}$, where $x_1 + x_2 + \cdots + x_n = t$. Assume that we have a solution for ESP in D_{2pq}, then T is an ES and so $T^t = \alpha\, D_{2pq} + X$ which implies that we can find t such that $a_1^{x_1}\, a_2^{x_2} \dots a_n^{x_n} = s$ for all $s \in D_{2pq}$. Hence, we can solve SSP in D_{2pq}. On the other hand, suppose we have a solution for SSP in D_{2pq}, by modify Algorithm 1, we can produce a solution for ESP in D_{2pq}. The modified algorithm is as follows:

Algorithm 2: Modified Solve SSP in D_{2pq}

Input $\{a_1, a_2, \dots, a_n\} \subset D_{2pq}$ and $s \in D_{2pq}$.

For each possible vector $(x_1, x_2, \dots, x_n) \in \mathbb{F}_2^n$

do compute $\prod_{i=1}^n a_i^{x_i} = s$.

Return (s).

This algorithm return 2^n of $s \in D_{2pq}$. To produce an ES for D_{2pq}, we must have $2^n \geq |D_{2pq}| = 2pq$, which is equivalent to said that $n \geq log_2\,(pq)$.

Since SSP is NP-hard, then we see that SSP in D_{2pq} is NP-hard and so we conclude that ESP in D_{2pq} is also NP-hard. This provides an evidence of the intractability of ESP in D_{2pq}. Therefore, breaking our proposed scheme is as hard as solving ESP in D_{2pq} and so finding a ESP-hard pair is infeasible.

IV. CONCLUSION

In this work, we propose a new signature schemes based on the hardness of ESP which is proven to be NP-hard. We show that ESP is computationally equivalent to the well-known subset sum problem. However, there are some questions that remain to be answered. Although ESP can increase the security of the proposed scheme, but it may also increase the computational complexity for executing the dihedral group multiplication and hence might affect the performance of the scheme.

V. ACKNOWLEDGEMENT

This work was supported by the Fundamental Research Grant Scheme (FRGS), project No. FRGS/1/2017/ STG06/UTAR/02/2.

VI. REFEREENCES

Anshel, I, Anshel, M & Goldfeld, D 1999, 'An algebraic method for public-key cryptography', *Mathematical Research Letters*, Vol. 6, pp. 287-291.

Anshel, I, Anshel, M, Fisher, B & Goldfeld, D 2001, 'New key agreement protocols in braid group cryptography', *in Cryptology- CT-RSA'01*, Springer-Verlag, LNCS 2020, pp. 144-156.

Caprara, A & Pferschy. U 2004, 'Worst-case analysis of the subset sum algorithm for bin packing', *Operations Research Letters*, 32: pp. 159-166.

Cormen, TH, Leiserson, CE, Rivest, RL & Stein, C 2001, 'Introduction to Algorithms', MIT Press, second edition.

Dehornoy, P 2004, 'Braid-based cryptography', *contemporary Mathematics*, Vol. 360, pp. 5-33.

Eick, B & Kahrobaei, D, 'Polycyclic groups: A new Platform for cryptology'. (http:// www-public.tubs.de:8080/beick/ publ/crypto.ps)

Fiat, A & Shamir, A 1986, 'How to prove yourself: Practical solutions to identification and signature problems', *In Advances in Cryptology - CRYPTO*'86, Springer, pp. 186-194.

Gens, G & Levner, E 1994, 'A fast approximation algorithm for the subset-sum problem', *Information Systems and Operational Research*, 32: pp. 143-148.

Grigoriev, D & Ponomarenko, I, 'Constructions in public-key crytography over Matrix groups'. (http:// arxiv.org /abs /math/0506180).

Kellerer, H, Mansini, R, Pferschy, U & Speranza, M 2003, 'An efficient fully polynomial approximation scheme for the subset-sum problem', *Journal of Computer and System Sciences*, 66: pp.349-370.

Ko, KH, Lee, SJ, Cheon, JH, Han, JW, Kang, JS & Park, CS 2000, 'New public-key cryptosystem using braid groups', *in cryptology: Proceedings of Crypto'00*, Springer-Verlag, LNCS 1880, pp.166-183.

Kumar, P & Garde, RJ 1989, 'Potentials of water hyacinth for sewage treatment', *Research Journal of Water Pollution Control Federation*, vol. 30, no. 10, pp. 291–294.

Lee, E 2004, 'Braid groups in cryptology', *IEICE transactions on fundamentals*, Vol. E87-A, no. 5, pp. 986-992.

Mahalanbis, A, 'Diffie-Hellman Key Exchange Protocol and Non Abelian Nilpotent groups'. (http://arxiv.org/abs/math.GR/0602282).

Martello, S & Toth, P 1985, 'Approximation schemes for the subset-sum problem: survey and experimental results', *European Journal of Operational Research*, 22: pp.56-69.

Martello, S & Toth, P 1984, 'Worst-case analysis of greedy algorithms for the subset-sum problem', *Mathematical Programming*, 28: pp. 198-205.

Martello, S & Toth, P 1990, 'Knapsack Problems: Algorithms and Computer Implementations', Wiley, Chichester, UK.

Mathews, GB 1897, 'On the partition of numbers', *Proceedings of the London Mathematical Society*, 28: pp. 486-490.

Merkle, RC & Hellman, ME 1978, 'Hiding information and signatures in trapdoor knapsacks', *IEEE Trans. Inform. Theory*, IT-24, pp. 525-530.

Myasnikov, AG, Shpilrain, V & Ushakov, A 2007, Group-based cryptography, Adv. Courses in Math., CRM Barcelona.

Paeng, SH, Ha, KC, Kim, JH, Chee, S & Park, C 2001, 'New public key cryptosystem using finite non abelian groups', *Advances in Cryptology*: *Proceedings of Crypto'01*, springer-Verlag, LNCS 2139, pp. 470-485.

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

Shor, PW, 1997 'Polynomial-time algorithm for prime factorization and discrete logarithms on quantum computer', *SIAM Journal on computing*, 26 (5), pp. 1484-1509.

Shpilrain, V & Ushakov, A, 'Thompson's group and public key cryptography'. (http:// arxiv.org/abs/ math.GR/00505487)

Steinwandt, R 2004, 'Non-abelian groups in public key cryptography'. (http://www.cms.math.ca/Events/winter04/abs/Plen.html).

Stickel, E 2004, 'A new public-key cryptosystem in non abelian groups', in *proceedings of the thirteen International conference on information systems development*, Vilnius Technika, pp. 70-80,.

Wong, Denis CK, Wong, KW & Yap, Wun-She 2017, 'Exhaustion 2-subsets in dihedral groups of order 2p', *Asian-European Journal of Mathematics*, In press, DOI:

10.1142/S179355711850047X.

Zemor. G 1994, 'Hash functions and Cayley graphs', *es. Codes Cryptography*, 4(4): p. 381-394.

Zhang, F, Safavi-Naini, R & Susilo, W 2004, 'An efficient signature scheme from bilinear pairings and its applications', in: *Public Key Cryptography*, PKC 2004, Springer, pp. 277-290.