

Key Agreement and Authentication Schemes Using Non-Commutative Semigroups

M.M. Chowdhury

Abstract

We give a new two-pass authentication scheme, which is a generalisation of an authentication scheme of Sibert-Dehornoy-Girault based on the Diffie-Hellman conjugacy problem. Compared to the above scheme, for some parameters it is more efficient with respect to multiplications. We sketch a proof that our authentication scheme is secure.

1. Introduction

In recent years various cryptographic protocols using infinite non-abelian groups have been proposed. For example the seminal algebraic key establishment protocol given in [1], and Artin's braid groups have been popular choices for such protocols. Braid groups are a popular choice because they are not too complicated to work with and they are more complicated than abelian groups. In particular the conjugacy problem in braid groups is algorithmically difficult and hence gives a one-way function.

We give a new authentication scheme (by using equations (2) and (3) below which form a main part of this paper), which is a generalisation of the authentication scheme *I* of SDG (Sibert-Dehornoy-Girault) given in [10]. We do not claim that equations (2) and (3) are totally original; for example a simpler version of equation (3) is used in the authentication scheme in [14]. In this paper we refer to the authentication scheme *I* in [10] as the SDG scheme. Based on the proof of the SDG scheme given in [10] we sketch a proof that our new authentication scheme is a perfectly honest-verifier ZK interactive proof of knowledge of the prover's secret. Two other provably secure schemes which are scheme *II* and scheme *III* are given [10] and they differ from our authentication scheme because they are zero-knowledge in an theoretical infinite framework, and they are iterated three pass schemes. Other differences are that scheme *II* is based on different hard problems compared to our authentication scheme. We refer to [10] for further details of these schemes. Two related authentication schemes were proposed in [11] and it was shown in [12] one "authentication scheme" in [11] is totally insecure and the other authentication scheme as shown in [12] can be broken by solving a specialisation of the decomposition problem defined in [4] (see below). An authentication scheme is given in [14] which has security based on a generalisation of the discrete logarithm problem in non-abelian finite groups. The main difference of our authentication scheme from the authentication scheme in [14] and the unbroken scheme in [11], [12] is that it is based on our version of the Diffie-Hellman decomposition problem defined below.

2. Hard Problems in Non-Abelian Groups

We now define the following known hard problems. The notation $[I, J] = 1$ (resp. $[I, J] \neq 1$) means that the subsets I and J of a semigroup G commute

(resp. do not commute). We may consider $G = B_n$ (the braid group of index n) in the following known problems, because the problems are then hard and by hard we mean there is no known algorithm to solve the problem such that a cryptographic protocol based on the problem would be insecure for practical use. When $G = B_n$ then WLOG the usual choices for A and B are the braid subgroups LB_n and UB_n (defined in section 3) as these are the choices that are used in [2] and [6] but the choices of A and B may be different. For our protocol to be secure at the very least G should be non-commutative.

The **DP** (Decomposition Problem) [4] is defined as follows.

Public Information: G is a semigroup, A is a subset of G . $x, y \in G$ with $y = axb$.

Secret information: $a, b \in A$.

Objective: find elements $f, g \in A$ such that $fxg = y$.

The definition of the *DP* above generalises the definition of a less general version of the *DP* given in [6], [3] and [5]. The less general version only differs from the above definition of *DP* because G is a group and A is a subgroup. In our notation in all of this paper we omit the binary operation $*$ when writing products so for example $f * x * g$ is understood to mean fxg . We require that $*$ is efficiently computable.

The **CSP** (Conjugacy Search Problem) [1], [3] is defined as follows.

Public Information: G is a group. $x, y \in G$ with $y = f^{-1}xf$.

Secret Information: $f \in G$.

Objective: find an element $g \in G$ such that $g^{-1}xg = y$.

The **DH-DP** (Diffie-Hellman Decomposition Problem) [6], [3] is defined as follows.

Public Information: G is a group. A, B are subgroups of G with $[A, B] = 1$. $x, y_a, y_b \in G$ with $y_a = axb$, $y_b = cxd$.

Secret Information: $a, b \in A$, $c, d \in B$.

Objective: find the element $cy_ad (= ay_b b = acx b d)$.

The **DH-CP** (Diffie-Hellman Conjugacy Problem) is the specialisation of the DH-DP [6] with $a = b^{-1}$ and $c = d^{-1}$.

We now re-define the DP and DH-DP above as used in our authentication scheme. In the rest of this paper below the DP and DH-DP will mean their re-definitions.

The re-definition of the **DP** is as follows.

Public Information: G is a semigroup. A, B are subsets of G . $x, y \in G$ with $y = axb$.

Secret Information: $a \in A$, $b \in B$.

Objective: find elements $f \in A$, $g \in B$ such that $fxg = y$.

The re-definition of the **DH-DP** is as follows.

Public information: G is a semigroup. A, B, C, D are subsets of G . $x, y_a, y_b \in G$ with $y_a = axb$, $y_b = cxd$.

Secret Information: $a \in A$, $b \in B$, $c \in C$, $d \in D$.

Objective: find the element $cy_ad (= ay_b b = acxbd)$. So if we can find $f \in A$, $g \in B$ such that $fxg = y_a$ or $h \in C$, $i \in D$ such that $hxi = y_b$ then this is sufficient to break our schemes which have security based upon the DH-DP.

A variant of the above re-definition of the **DH-DP** which we refer to as the **DH-DP'** on which the security of our variant protocols is based upon is as follows.

Public information: G is a semigroup. A, B, C, D are subsets of G . $x, y_a, y_b \in G$ with $y_a = axb$, $y_b = caxbd$.

Secret Information: $a \in A$, $b \in B$, $c \in C$, $d \in D$. (a, b have an inverse).

Objective: find the element $a^{-1}y_b b^{-1} (= cxd, y_a = axb)$. So if we can find $f \in A$, $g \in B$ $h \in C$, $i \in D$ such that $hxi = cxd$ or $f^{-1}y_b g^{-1} = cxd$, $fxg = y_a$ then this is sufficient to break our schemes which have security based upon the DH-DP'.

In all of this paper for our authentication scheme the DP, DH-DP and DH-DP' are considered with commutativity conditions such as (2) and (3) defined below. We assume the DP, DH-DP and DH-DP' are hard. The connection between the DH-DP and the DP is similar to the one between the Diffie-Hellman problem and the discrete logarithm problem. The DH-DP, DH-DP' is obviously reducible to the DP, but we assume that it is as hard for general G . Hence checking that the DP is hard for x is supposed to ensure that the DH-DP also is.

The security of the modified key exchange protocol on page 2 of [4] is based on the DP with the additional condition that $[A, B] = 1$ and its security is also based on the DH-DP.

3. The Sibert-Dehornoy-Girault Authentication Scheme

All the details of implementation in braid groups for the SDG authentication scheme I are given in [10] so we do not reproduce them all here; we restrict to the details we require. For $n \geq 2$, B_n is defined to be the group with the presentation with $n - 1$ generators (plus the identity e), denoted σ_i for $i = 1, 2, \dots, n - 1$ and the defining relationships

$$\begin{aligned} \sigma_i \sigma_j &= \sigma_j \sigma_i & |i - j| > 1 \\ \sigma_i \sigma_j \sigma_i &= \sigma_j \sigma_i \sigma_j & |i - j| = 1 \end{aligned} \tag{1}$$

We refer the reader to any textbook about braids, for instance [13]; each element of B_n has the geometrical interpretation by an n -strand braid in the usual sense. This geometrical interpretation is that any n -strand braid diagram can be first sliced into a concatenation of elementary diagrams with one crossing each and then each elementary diagram can be used to give an encoding of the braid diagram as a word in one of the letters σ_i or σ_i^{-1} . σ_i is used for the diagram where the i th strand crosses under the $(i + 1)$ st one, and σ_i^{-1} is used for the diagram where the i th strand crosses over the $(i + 1)$ st one.

LB_n and UB_n are the two commuting subgroups of B_n generated by the Artin generators $\sigma_1, \dots, \sigma_{\lfloor n/2 \rfloor - 1}$ and $\sigma_{\lfloor n/2 \rfloor}, \dots, \sigma_{n-1}$ [10]. The SDG authentication is as follows. Following [10] we require that the DH-CP and CSP are

hard in G as the security of the authentication is based on these problems, let $G = B_n$, $A = LB_n$, $B = UB_n$ in the DH-CP and CSP. Let G' be a non-abelian group, let $w \in G'$ be a publicly known word which has a secret word as one of its factors (an attacker may attempt to recover this secret word from w), let S be a function which maps w to an equivalent word, S is called a scrambling function, the security of the protocol is based on the difficulty of recovering the above secret word from the word $S(w)$ [10]. A choice for the scrambling function can be a normal form for w [10]. All braids are expressed in rewritten form using the scrambling function such that the DH-CP and CSP are hard.

- Phase 1. Key generation
 - i) Choose a public $b \in B_n$.
 - ii) $A(\text{lice})$ chooses a secret braid $s \in LB_n$, her private key; she publishes $b' = sb s^{-1}$; the pair (b, b') is the public key.
- Phase 2. Authentication phase
 - i) $B(\text{ob})$ chooses $r \in UB_n$ and sends the challenge $t = rbr^{-1}$ to A .
 - ii) A sends the response $y = h(sts^{-1})$ to B , and B checks $y = h(rb'r^{-1})$.

h is a fixed collision-free hash function from braids to sequences of 0's and 1's or, possibly, to braids, for which this choice for h , G must have an efficient solution for the word problem for use in phase 2ii).

A proof that the above authentication scheme is a perfectly honest-verifier ZK interactive proof of knowledge of s is given in [10]. There is a linear algebraic algorithm to solve the DH-CP but the attack is not efficient enough to break the public-key cryptosystem with the proposed parameters of [2] in real time [6]. The SDG scheme has a similar structure to the public-key cryptosystem in [2] because both algorithms are based on the DH-CP. Hence the parameters of the SDG scheme are based on considerations of the parameters of the above public-key cryptosystem [10]. Hence parameters can be chosen for the SDG scheme so that it cannot be broken in real time by using the attack on the DH-CP in [6].

4. New Authentication Scheme

The new authentication scheme is as follows. Let G be a (infinite or finite) non-commutative semigroup. We define the scrambling function as in the SDG scheme, for our scheme, but with the modification that it is defined over the semigroup G instead of only a group. All elements in G in this section are rewritten using the scrambling function and parameters are chosen such that the DH-DP and DP are hard, as the security of our authentication scheme is based on these problems.

- Phase 0. Initial setup
 - i) G is chosen and is publicly known. The users publicly agree on which method first, second or third (described below) will be used to select the subsets and publicly agree on which of the commutativity conditions (2) or (3) will be used.
- A first method to select the parameters is to select publicly known subsets

L_A, L_B, R_A, R_B and Z of G are chosen for which either property a) below is true or property b) below is true. Let $z \in Z$ with z the publicly known element which is the value of x in the definition of the DH-DP used in the example of the DH-DP in our new authentication scheme.

Following [5] let $g \in G$ for G a group, $C_G(g)$ is the centraliser of g , we describe the modifications to the authentication scheme (and these apply to the key agreement protocol described below) to give two further methods to select the subgroups as follows. Publicly known subsets or privately known L_A, L_B, R_A, R_B and Z of G are chosen for which either property 2) below is true or property 3) below for the second and third methods below.

Using the above first method the security of the protocol is based on the DH-DP. We now give the two further methods to select the subsets which result in two modifications to the protocol when the first method is used. The second method to select the subgroups is A chooses $(a_1, a_2) \in G \times G$ and publishes the subgroups as a set of generators of the centralisers $L_B, R_B, L_B \subseteq C_G(a_1), R_B \subseteq C_G(a_2), L_B = \{\alpha_1, \dots, \alpha_k\}$ etc. B chooses $(b_1, b_2) \in L_B \times R_B$, and hence can compute x below etc. Following [5] there is no explicit indication of where to select a_1, b_1 and/or a_2, b_2 from. Hence before attempting something like a length based attack in this case the attacker has to compute the centraliser of L_B and/or R_B .

So a third method (this method is given for the key agreement protocol in [5]) to select the subgroups is

A chooses $L_A = G, a_1 \in G$, and publishes $L_B \subseteq C_G(a_1), L_B = \{\alpha_1, \dots, \alpha_k\}$,
 B chooses $L_B = G, b_2 \in G$, and publishes $R_A \subseteq C_G(b_2), R_A = \{\beta_1, \dots, \beta_k\}$,

Hence A chooses $(a_1, a_2) \in G \times C_G(b_2)$ and publishes the subgroup(s) as a set of generators of the centralisers B chooses $(b_1, b_2) \in C_G(a_1) \times G$, and hence can compute x etc. Again there is no explicit indication of where to select a_1 and/or b_2 from. Hence before attempting a length based attack in this case the attacker has to compute the centraliser of L_B and/or R_B .

The above three methods are examples of the following method, in general if a user A or B selects an element a_i or b_i respectively as their secret element (which multiplies the public element z at the left WLOG) key then the other user selects an element of the $C_G(a_i)$ or $C_G(b_i)$ respectively as their secret key for the corresponding secret commuting element to left multiply WLOG, and in general an attacker has no explicit indication of where to select a_i and/or b_i from. A potential disadvantage of using the above third method to select the subgroups is one user chooses the other users subgroups and this may aid the user who has selected the subgroup to find the others users secret key, and this secret key may be of use in say another attack. Hence before attempting a length based attack in this case the attacker has to compute the centraliser of $C_G(a_i)$ and/or $C_G(b_i)$. Note if the subgroups are selected in this in the second or third way (using centraliser computations) then its security is based on a variant of the DP, DH-DP and the difficulty of computing centralisers, for example if the third method above is used to select the subsets then following the attack given

in [5] the security of the protocol to find A or B 's private key may be found as follows

Attack on A 's Key. Find an element a'_1 which commutes with every element of the subgroup L_B and an element $a'_2 \in R_B$ such that $z' = a'_1 z a'_2$ where $a'_1 z a'_2$ above may be rewritten using a normal form. The pair (a'_1, a'_2) is equivalent to the pair (a_1, a_2) , because $a'_1 z a'_2 = a_1 z a_2$ this means an attacker can authenticate as Alice. The attack applies to the key exchange protocol below with the modification $K_A = a'_1 z a'_2$ instead of $z' = a'_1 z a'_2$ this gives a equivalent secret key for A used to get the common secret key.

Attack on B 's Key in the key exchange protocol in the section below. Find an element b'_2 which commutes with every element of the subgroup R_A and an element $b'_1 \in L_B$ such that $K_B = b'_1 z b'_2$ where $a'_1 z a'_2$ above may be rewritten using a normal form. The pair (b'_1, b'_2) is equivalent to the pair (b_1, b_2) , because $b'_1 z b'_2 = b_1 z b_2$ this means an attacker can find the common secret key when this set up is used as part of a key exchange algorithm as described below.

Then (following [5]) the most obvious way to recover Bob private key (the attack for A is similar)

B1. Compute the centraliser of $R_A, R_A \subseteq C_G(b_2)$.

B2. Solve the search version of the membership problem in the double coset $< L_B > \cdot z \cdot C_G(R_A)$.

So for the protocol to be secure we want both the above problems to be computationally hard, for the problem B2 to be hard it is required the centraliser $C_G(L_A)$ should be large enough to resist a brute force attack. The key exchange protocol in section 5 has security based upon the above problem. The above attack can be used to attack the authentication scheme or recover B 's secret elements with the modification $x = b'_1 z' b'_2$ instead of $K_B = b'_1 z b'_2$ (x is used instead of K_B and z' is used instead of z etc.).

The attacks above are considered with commutativity condition for the DH-DP such as (2) and (3) below. A similar attack is discussed when the second method is used to choose the subsets. Hence the platform group G should satisfy the requirements given in the security analysis in section 6.

a) If $z \neq e$ we require the following conditions

$$\begin{aligned} [L_A, L_B] &= 1, & [R_A, R_B] &= 1, \\ [L_B, Z] &\neq 1, & [L_A, Z] &\neq 1, \\ [R_B, Z] &\neq 1, & [R_A, Z] &\neq 1, \\ [L_A, R_A] &\neq 1, & [L_B, R_B] &\neq 1. \end{aligned} \tag{2}$$

All the above conditions for $z \neq e$ can arise by generalising from properties of subgroups used in either the SDG scheme or CKLHC scheme for example the second and third conditions in (2) arise from the observations that in general $[LB_n, B_n] \neq 1, [LB_n, UB_n] = 1$.

b) If $z = e$ we require the following conditions

$$\begin{aligned} [L_A, L_B] &= 1, & [R_A, R_B] &= 1, \\ [L_A, R_A] &\neq 1, & [L_B, R_B] &\neq 1, \\ [L_B, R_A] &\neq 1, & [L_A, R_B] &\neq 1. \end{aligned} \tag{3}$$

We were unable to show that the DH-DP using conditions (2) or (3) was easy. Hence we assume that the DH-DP is hard with condition with the above conditions. Note condition (3) is condition (2) but with conditions of the form of a subset not commuting with Z omitted (because $z = e$) and the additional conditions $[L_B, R_A] \neq 1, [L_A, R_B] \neq 1$. The above additional conditions are required so the DH-DP is not easy and hence our authentication scheme is secure.

- Phase 1. Key generation
 - i) Choose a public $z \in Z$.
 - ii) A chooses secret elements $a_1 \in L_A, a_2 \in R_A$, her private key; she publishes $z' = a_1 z a_2$; the pair (z, z') is the public key.
- Phase 2. Authentication phase
 - i) B chooses $b_1 \in L_B, b_2 \in R_B$ and sends the challenge $x = b_1 z b_2$ to A .
 - ii) A sends the response $w = H(a_1 x a_2)$ to B , and B checks $w = H(b_1 z' b_2)$.

H is a fixed collision-free hash function from elements of G to sequences of 0's and 1's or, possibly, to elements of G , for which this choice of H, G must have an efficient solution for the word problem for use in phase 2ii)

Proposition 4.1

Our Authentication Scheme is a perfectly honest-verifier ZK interactive proof of knowledge of a_1 and a_2 .

Proof. (*Sketch*) *Completeness.* Assume that, at step 2(ii) w' is sent by A . Then B accepts A 's key if and only if $w' = H(b_1 z' b_2)$ which is equivalent to

$$w' = H(b_1(a_1 z a_2)b_2). \tag{4}$$

By hypothesis $a_1 \in L_A, a_2 \in R_A, b_1 \in L_B, b_2 \in R_B$, so $b_1 a_1 = a_1 b_1, b_2 a_2 = a_2 b_2$ holds and (4) is equivalent to $w = H(a_1(b_1 z b_2)a_2)$ i.e. $w' = w$.

Soundness. Assume cheater A' is accepted with non-negligible probability. This means A' can compute $H(b_1 z' b_2)$ with non-negligible probability. Since H is supposed to be an ideal hash function, this means that A' can compute the element q satisfying $H(q) = H(b_1 z' b_2)$ with non-negligible probability and this is because of two possibilities. The first possibility is that $q = b_1 z' b_2$ which contradicts the hypothesis that the DH-DP is hard. The second possibility is $q \neq b_1 z' b_2$ which means that A' and B are able to find a collision for H which contradicts that H is a collision free hash function.

Honest-verifier zero knowledge. Consider the probabilistic Turing machine defined as follows: it chooses random elements b_1 and b_2 using the same drawing as the honest verifier, and outputs the instances $(b_1, b_2, H(b_1 z' b_2))$. So the

instances generated by this simulator follow the same probability distribution as the ones generated by the interactive pair (A, B) . \square

4.1 Comparison of Our Authentication Scheme with the Sibert-Dehornoy-Girault Authentication Scheme

The generalisation (not the variants) specialises to the SDG scheme (hence our authentication scheme can be as secure as the SDG authentication scheme) with the parameters $H = h, G = B_n, Z = B_n, L_A = R_A = LB_n, L_B = R_B = UB_n, b_1 = r, b_2 = r^{-1}, a_1 = s, a_2 = s^{-1}, z = b, z' = b', x = t, w = y$, the first method is used to select the subsets and conditions (2) (or property a) is true) are used.

If $z = e$ then this implies the following. Condition (3) do not allow the subgroups used in the SDG scheme to be used in our authentication scheme, because if these subgroups are used as the incorrect choices for L_A, L_B, R_A and R_B in our authentication scheme then it is easy to see the DH-DP is easy and hence our authentication scheme is insecure. There is more control of the public parameters (the choices of the subsets) compared to the SDG scheme and this may be useful for selecting secure public keys. Compared to the SDG scheme, potentially our authentication scheme requires less memory and fewer multiplications to compute the challenge of B and the public key of A . This is because the identity element may take little memory (compared to $b \neq e$) to represent depending on the representation of G . Alternatively we can omit the implementation of using Z completely because x and z' can be computed using two multiplications.

4.2 A Variant of the Authentication Scheme

A variant of the above authentication scheme is as follows

- Phase 0. Initial Setup. The phase 0 is the same as phase 0 of the authentication scheme in section 4.
- Phase 1. Key generation
 - i) Choose a public $z \in Z$.
 - ii) A chooses (invertible) secret elements $a_1 \in L_A, a_2 \in R_A$, her private key; she publishes $z' = a_1 z a_2$; the pair (z, z') is the public key.
- Phase 2. Authentication phase
 - i) B chooses $b_1 \in L_B, b_2 \in R_B$ and sends the challenge $x = b_1 z' b_2$ to A .
 - ii) A sends the response $w = H(a_1^{-1} x a_2^{-1})$ to B , and B checks $w = H(b_1 z b_2)$, if the check is true he accepts if the check is false he rejects.

H is a fixed collision-free hash function from elements of G to sequences of 0's and 1's or, possibly, to elements of G , for which this choice of H, G must have an efficient solution for the word problem for use in phase 2ii). The above variant authentication scheme has security based on the DH-DP'.

The above variant authentication scheme specialises to the authentication scheme in [14]. The above variant protocol specialises to the authentication scheme in [14] with the parameters, conditions (3) are used, G a finite non-abelian group, Bob is user B in our protocol, Alice is user A in our protocol $z = \text{identity element}$, L_A, R_B are publicly known and is generated by a , R_B is generated by b , $L_B = L_A, R_B = R_A$ B selects the secret element which is depends on the secret exponents $0 < r < n_1, 0 < s < n_2$, $a^r \in L_A, b^s \in R_B$, A selects the secret element which is depends on the secret exponents $0 < v < n_1, 0 < w < n_2$, $a^v \in L_A, b^w \in R_B$, so the common secret key is $z' = a^v b^w$, where the notation e, f , is used in [14].

5. New Key Agreement Protocol

The setup for the authentication protocols in the above section can be used for key agreement as follows.

- Phase 0. Initial Setup. The phase 0 is the same as phase 0 of the authentication scheme in section 4.
- Choose $z \in G$. Phase 1.
 - ii) $A(\text{lice})$ chooses a secret elements $a_1 \in L_A$, $a_2 \in R_A$, her private key; she publishes $K_A = a_1 z a_2$; the pair (z, K_A) is the public key.
 - i) $B(\text{ob})$ chooses a secret elements $b_1 \in L_B$, $b_2 \in R_B$, her private key; she publishes $K_B = b_1 z b_2$; the pair (z, K_B) is the public key.
 - iii) A and B can compute the common shared secret key κ as $\kappa = a_1 K_B a_2$ and $\kappa = b_1 K_A b_2$ respectively. Optionally the alternative computation $\kappa = h(a_1 K_B a_2)$ and $\kappa = h(b_1 K_A b_2)$ can be done.

h is a fixed collision-free hash function from braids to sequences of 0's and 1's or, possibly, to braids, for which this choice for h . Again the above protocol is considered with the commutativity conditions 2 or 3. Note the elements K_A and K_B are rewritten for example a normal form to make the protocol secure.

Because phase 0 is the same as the authentication scheme again its security is based on a variant of the DP, DH-DP and the difficulty of computing centralisers.

Our protocol specialises to the CKLHC protocol in [8] is the above protocol with the parameters G the braid group, A and B commuting defined by LB_n and UB_n are the two commuting subgroups of B_n generated by the Artin generators $\sigma_1, \dots, \sigma_{\lfloor n/2 \rfloor - 1}$ and $\sigma_{\lfloor n/2 \rfloor}, \dots, \sigma_{n-1}$, the first method in phase 0 is used and the DH-DP uses the condition (2). The publicly transmitted information is rewritten using the left canonical form. The KLCHKP protocol [2] is the specialisation of the CKLHC protocol with $a_2 = a_1^{-1}$ and $b_2 = b_1^{-1}$ and hence our protocol generalises the KLCHKP protocol.

Our protocol specialises to the key agreement protocol given on page two of [4] with the parameters $L_A = R_B$, $L_B = R_A$, $[L_A, L_B] = 1$, and commutativity condition (2), G is a semi-group or G is the Thompson group, the first method

in phase 0 is used and hence our protocol generalise the protocol given in [4]. Using the notation used in [4] this is $L_A = A, L_B = B, z = w$. So the left and right secrets are taken from different subgroups the protocol.

Our protocol specialises to the key agreement protocol given in [5] when G is a group, A and B are subgroups in the parameters of the DH-DP, using the third method in phase 0 to select the subsets/ modify the key agreement protocol described above, commutativity condition 2, $L_B \subseteq C_G(a_1), L_B = \{\alpha_1, \dots, \alpha_k\}, R_A \subseteq C_G(b_2), R_A = \{\beta_1, \dots, \beta_k\}, K_A$ and K_B are rewritten using a normal form, using the notation given in [5] this is $K_A = P_A, K_B = P_B, B = L_B, A = R_A$.

Hence we get new variants (which use less multiplications) of the protocols [4], [5], [2],[8] if we consider the parameters that our key agreement protocol above specialises to the protocols above but using condition (3) instead of conditions (2), for example if we consider the second method in phase 0 to modify the protocol with the parameters above to specialise, then compared to using the third method in phase 0 the advantage of this protocol is that user A does not have to wait for B to select the subgroup and so for example can create the certificate to prove that the public key of A belongs to A .

5.1 Variant of Key Exchange

A variant of the key exchange is as follows

The above setup can be used for key agreement as follows the details are as follows.

- Phase 0. Initial Setup. The phase 0 is the same as phase 0 of the authentication scheme in section 4.
- Choose $z \in G$.
 - ii) A (lice) chooses a secret invertible elements $a_1 \in L_A, a_2 \in R_A$, her private key; she publishes $K_A = a_1 z a_2$; the pair (z, K_A) is the public key.
 - i) B (ob) chooses a secret braid $b_1 \in L_B, b_2 \in R_B$, his private key; he publishes $K_B = b_1 K_A b_2$; the pair (K_A, K_B) is the public key.
 - iii) A and B can compute the common shared secret key κ as $\kappa = a_1^{-1} K_B a_2^{-1}$ and $\kappa = b_1 z b_2$ respectively. Optionally the alternative computation $\kappa = h(a_1^{-1} K_B a_2^{-1})$ and $\kappa = h(b_1 K_A b_2)$ can be done.

h is a fixed collision-free hash function from braids to sequences of 0's and 1's or, possibly, to braids, for which this choice for h . Again the above protocol is considered with the commutativity conditions 2 or 3. Note the elements K_A and K_B are rewritten for example a normal form to make the protocol secure.

Again because phase 0 is the same as the authentication scheme we have sketched its security is based on a variant of the DP, DH-DP' and/or the difficulty of computing centralisers.

The above variant protocol specialises to the key exchange in [9] with the parameters, conditions (2) or (3) are used, G a finite non-abelian group, Bob is user B in our protocol, Alice is user A in our protocol, $z = e, L_A$ is publicly

known and is generated by a , R_B is generated by b , $L_B = L_A, R_B = R_A$ B selects the secret element which is depends on the secret exponents $0 < r < n_1, 0 < s < n_2, a^r \in L_A, b^s \in R_B$, A selects the secret element which is depends on the secret exponents $0 < v < n_1, 0 < w < n_2, a^v \in L_A, b^w \in R_B$, so the common secret key is $\kappa = f = a^v b^w$, where the notation e, f is used in [9].

5.1.1 Groups With No Efficient Normal Form

If there is no efficient algorithm for a canonical form in G then the secret elements such as Alice's secret key must be disguised in another way such as using a scrambling function. The algorithm in [1] for when G is a group, and there is no efficient normal form in G but there is an efficient algorithm for the word problem in G , can be used to find a common shared secret key can be found as follows using the algorithm in [1] which is. Fix b as $b = 0$ or $b = 1$.

1. B sends a rewritten form of κ which is r for $r = \kappa$ or a random word for $r, r \neq \kappa$.
 2. User A checks if $k = r$ then this determines the bit b , otherwise the bit is $1 - b$.
 3. The steps 1 and 2 are repeated m times so an m bit key is exchanged.
- As stated in [1] the protocol is probabilistic and slower compared to using a canonical form.

6. Security Analysis

The attacks below are considered with commutativity condition for the DH-DP such as (2) and (3) below.

6.1 Attacks When Second Method is used to Choose Subsets in Authentication Scheme and Key Exchange Scheme

If the second method above is used to select the subsets then following the attack given in [5] the security of the protocol to find A or B 's private key may be found as follows

Attack on A 's Key. Find an element a'_1 which commutes with every element of the subgroup L_B and an element $a'_2 \in R_B$ which commutes with every element of the subgroup R_B such that $z' = a'_1 z a'_2$ where $a'_1 z a'_2$ above may be rewritten using a normal form. The pair (a'_1, a'_2) is equivalent to the pair (a_1, a_2) , because $a'_1 z a'_2 = a_1 z a_2$ this means an attacker can authenticate as Alice. The attack applies to the key exchange protocol (when the second method is used to choose the subsets) with the modification $K_A = a'_1 z a'_2$ instead of $z' = a'_1 z a'_2$ this gives an equivalent secret key for A used to get the common secret key.

Then (following [5]) the most obvious way to do the above attack Alice's private key

A1. Compute the centraliser of $R_B, R_B \subseteq C_G(a_2)$ and compute the centraliser of $L_B, L_B \subseteq C_G(a_1)$

A2. Solve the search version of the membership problem in the double coset $\langle C_G(L_B) \rangle \cdot z \cdot \langle C_G(R_B) \rangle$.

So for the protocol to be secure we want both the above problems to be computationally hard, for the problem A1 to be hard it is required both the centralisers $C_G(L_B)$ and $C_G(R_B)$ be large enough to resist a brute force type attack. The above attack can be used to attack the authentication scheme or recover A 's secret elements with the modification $z' = a'_1 z a'_2$ instead of $K_A = a'_1 z a'_2$ (z' is used instead of K_A etc.) so this can be used to impersonate A .

Attack on B 's Key in the key exchange protocol. Find an element $b'_1 \in L_B$ and an element $b'_2 \in R_B$ such that $K_B = b'_1 z b'_2$ where $b'_1 z b'_2$ above may be rewritten using a normal form. The pair (b'_1, b'_2) is equivalent to the pair (b_1, b_2) , because $b'_1 z b'_2 = b_1 z b_2$ this means an attacker can find the common secret key when this set up is used as part of a key exchange algorithm as described below.

Then (following [5]) the most obvious way to do the above attack, Bob private key

B1. Solve the search version of the membership problem in the double coset $\langle L_B \rangle \cdot z \cdot \langle R_B \rangle$.

So for the protocol to be secure we want the above problem to be computationally hard, for the problem B1 to be hard it is required that the elements cannot of L_B , R_B all be tested (for an equivalent key pair b'_1, b'_2) so to resist a brute force attack the possible values for b'_1, b'_2 should be large enough. The above attack can be used to attack the authentication scheme or recover B 's secret elements with the modification $x' = b'_1 z' b'_2$ instead of $K_B = b'_1 z b'_2$ (x' is used instead of K_B and z' is used instead of z etc.) so this can be used to impersonate A .

6.2 Attack When Second Method is used to Choose Subsets in the Variant Authentication Scheme and Variant Key Exchange Scheme

If the second method above is used to select the subsets then following variant of the attack given in [5] the security of the protocol to find A or B 's private key may be found as follows

Attack on A 's Key. Find an element a'_1 which commutes with every element of the subgroup L_B and an element $a'_2 \in R_B$ which commutes with every element of the subgroup R_B such that $z' = a'_1 z a'_2$ where $a'_1 z a'_2$ above may be rewritten using a normal form and a'_1, a'_2 are both invertible elements.

The pair (a'_1, a'_2) is equivalent to the pair (a_1, a_2) , because $a'_1 z a'_2 = a_1 z a_2$ this means an attacker can authenticate as Alice because the attacker can compute $a_1^{-1} x a_2^{-1}$. The above attack applies to the key exchange protocol with the modification $K_A = a'_1 z a'_2$ instead of $z' = a'_1 z a'_2$ this gives an equivalent secret key for A used to get the common secret key which can be computed as $\kappa = a_1^{-1} K_B a_2^{-1}$. (Another attack call this attack B, is to find elements a'_1, a'_2 such that $a_1^{-1} z' a_2^{-1} = z$, a'_1, a'_2 can be used instead of a_1, a_2 to get the common secret key, the attack is similar for the key agreement protocol with K_A used in place of z').

Then (following [5]) the most obvious way to do the above attack Alice's private key

A1. Compute the centraliser of $R_B, R_B \subseteq C_G(a_2)$ and compute the centraliser of $L_B, L_B \subseteq C_G(a_1)$

A2. Solve the search version of the membership problem in the double coset $\langle C_G(L_B) \rangle \cdot z \cdot \langle C_G(R_B) \rangle$ and/or $\langle C_G(L_B) \rangle \cdot K_B \cdot \langle C_G(R_B) \rangle$.

(For attack B we do the search $\langle C_G(L_B) \rangle \cdot z' \cdot \langle C_G(R_B) \rangle$ there is a variant of attack B when the third method is used to choose the subsets doing a search of the form $\langle L_B \rangle \cdot z' \cdot \langle C_G(R_B) \rangle$) So for the protocol to be secure we want both the above problems to be computationally hard, for the problem A1 to be hard it is required both the centralisers $C_G(L_B)$ and $C_G(R_B)$ to be large to resist a brute force type attack.

Attack on B 's key in the key exchange protocol. Find an element $b'_1 \in L_B$ and an element $b'_2 \in R_B$ such that $K_B = b'_1 z b'_2$ where $b'_1 z b'_2$ above may be rewritten using a normal form. The pair (b'_1, b'_2) is equivalent to the pair (b_1, b_2) , because $b'_1 z b'_2 = b_1 z b_2$ this means an attacker can find the common secret key when this set up is used as part of a key exchange algorithm as described below.

Then (following [5]) the most obvious way to do the above attack, Bob private key

B1. Solve the search version of the membership problem in the double coset $\langle L_B \rangle \cdot z \cdot \langle R_B \rangle$ and/or $\langle L_B \rangle \cdot K_A \cdot \langle R_B \rangle$.

So for the protocol to be secure we want the above problem to be computationally hard, for the problem B1 to be hard it is required that the elements of L_B, R_B cannot all be tested (for an equivalent key, pair b'_1, b'_2) so to resist a brute force attack. The above attack can be used to attack the authentication scheme or recover B 's secret elements with the modification $x = b'_1 z' b'_2$ instead of $K_B = b'_1 z b'_2$ (x' is used instead of K_B and z' is used instead of z etc.) so this can be used to impersonate A .

6.3 Attack When Third Method is used to Choose Subsets in the Variant Authentication Scheme and Variant Key Exchange Scheme

Attack on A 's Key. Find an element a'_1 which commutes with every element of the subgroup L_B and an element $a'_2 \in R_B$ such that $z' = a'_1 z a'_2$ where $a'_1 z a'_2$ above may be rewritten using a normal form and a_1, a_2 are both invertible elements. The pair (a'_1, a'_2) is equivalent to the pair (a_1, a_2) , because $a'_1 z a'_2 = a_1 z a_2$ this means an attacker can authenticate as Alice the attack applies to the key exchange protocol with the modification $K_A = a'_1 z a'_2$ instead of $z' = a'_1 z a'_2$ is solved this gives a equivalent secret key for A used to get the common secret key by computing $\kappa = a'^{-1}_1 K_B a'^{-1}_2$.

Then (following [5]) the most obvious way to do the above attack Alice's private key

A1. Compute the centraliser of $L_A, L_A \subseteq C_G(a_1)$.

A2. Solve the search version of the membership problem in the double coset $\langle C_G(L_A) \rangle \cdot z \cdot \langle R_A \rangle$ and/or $\langle C_G(L_A) \rangle \cdot K_B \cdot \langle R_A \rangle$.

Attack on B 's key in the key exchange protocol is below. Find an element b'_2 which commutes with every element of the subgroup R_A and an element $b'_1 \in L_B$ such that $K_B = b'_1 z b'_2$ where $b'_1 z b'_2$ above may be rewritten using a normal form. The pair (b'_1, b'_2) is equivalent to the pair (b_1, b_2) , because $b'_1 z b'_2 = b_1 z b_2$ this means an attacker can find the common secret key.

Then (following [5]) the most obvious way to recover Bob private key

B1. Compute the centraliser of R_A , $R_A \subseteq C_G(b_2)$.

B2. Solve the search version of the membership problem in the double coset $\langle L_B \rangle \cdot z \cdot C_G(R_A)$.

So for the protocol to be secure we want both the above problems to be computationally hard, for the problem B2 to be hard it is required the centraliser $C_G(R_A)$ to be large enough to resist a brute force attack. The key exchange protocol in section 5 has security based upon the above problem. The above attack can be used to attack the authentication scheme or recover B 's secret elements with the modification $x = b'_1 z' b'_2$ instead of $K_B = b'_1 z b'_2$ is solved (x is used instead of K_B and z' is used instead of z etc.) so this can be used to impersonate Alice.

6.4 Requirements of the of Platform Group

Hence the platform group G should satisfy at least the following properties in order for our key establishment protocol to be efficient and secure, we have taken the requirements from [5] so the properties are the same as given in [5] with the relevant modifications. At least one of property P7, P8, or P9 is true depending on the choice of protocol used.

(P1) G should be a non-commutative group of at least exponential growth. The latter means that the number of elements of length n in G is at least exponential in n ; this is needed to prevent attacks brute force type attacks on the key space.

(P2) This property may be optional. There should be an efficiently computable normal form for elements of G .

(P3) It should be computationally easy to perform group operations (multiplication and inversion) on normal forms.

(P4) It should be computationally easy to generate pairs $(a, \{a_1, \dots, a_k\})$ such that $aa_i = a_i a$ for each $i = 1, \dots, k$. (Clearly, in this case the subgroup generated by a_1, \dots, a_k centralizes a).

(P5) For a generic set $\{g_1, \dots, g_k\}$ of elements of G it should be difficult to compute $C(g_1, \dots, g_n) = C(g_1) \cap \dots \cap C(g_k)$.

(P6) This property may be optional. Even if $H = C(g_1, \dots, g_n)$ is computed, it should be hard to find $x \in H$ and $y \in H_1$ (where H_1 is some fixed subgroup given by a generating set) such that $xy = w'$, i.e., to solve the membership search problem for a double coset.

(P7) This property may be optional. Even if $H = C(g_1, \dots, g_n)$ is computed, and $H_1 = C(g'_1, \dots, g'_m)$ (g' is a generator as usual) is computed and it should

be hard to find $x \in H$ and $y \in H_1$ such that $xwy = w'$, i.e., to solve the membership search problem for a double coset.

(P8) This property may be optional. Given H and H_1 is some fixed subgroups given by a generating sets, and it should be hard to find $x \in H$ and $y \in H_1$ such that $xwy = w'$, i.e., to solve the membership search problem for a double coset.

(P9) This property may be optional. Which is there should be an efficiently algorithm for the word problem in G .

6.5 Braid groups

We now consider braid groups as a possible platform group. Here we consider the properties (P1)-(P6) from the previous section.

(P1) For $n > 2$, braid groups B_n are non-commutative groups of exponential growth.

(P2) There are several known normal forms for elements of B_n , including Garside normal form (see [8]). The Garside normal form is efficiently computable.

(P3) There are efficient algorithms to multiply or invert normal forms of elements of B_n [8].

(P4) It is not so easy to compute the whole centralizer of an element g of G [5]. The number of steps required to compute $C_G(g)$ is proportional the size of the SSS (super summit set) of g . Generally speaking the “super summit set” is not of polynomial size in n and the braid length. Nevertheless, there are approaches to finding “large parts” of $C_G(g)$, e.g. one can generate a sufficiently large part of $SSS(g)$.

(P5) For a generic subgroup A there is no efficient algorithm to compute $C_G(A)$.

(P6), (P7) and (P8) There is no known solution to the membership search problem for double cosets HwH' in braid groups.

(P9) There are efficient algorithms for the word problem in braid groups, such as the practical handle reduction algorithm for the word problem described in [10].

7. Conclusion

We have presented new two-pass authentication schemes and key exchange protocols. This paper is a work in progress, because further work we plan to do for our authentication scheme is to investigate potential semigroups (apart from braid groups) and parameters for which it is secure, when its security is based on the DH-DP or variants of the DH-DP.

References

- [1] I. Anshel, M. Anshel, D. Goldfeld. An Algebraic Method for Public-key Cryptography, Mathematical Research Letters, 6, 1999, pp. 287-292.

- [2] K.K. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J.S. Kang, C. Park. New public-key cryptosystem using braid groups. CRYPTO 2000. LNCS, 1880, 2000, pp. 166-183.
- [3] K. H. Ko, Tutorial on Braid Cryptosystems 3, PKC 2001, Korea, February 13-15, 2001. Available at www.ipkc.org/pre_conf/pkc2001/PKCtp_ko.ps
- [4] V. Shpilrain and A. Ushakov, "Thompson's group and public key cryptography", LNCS, 3531, Springer-Verlag, 2005, pp. 151-164.
- [5] V. Shpilrain and A. Ushakov, A new key exchange protocol based on the decomposition problem, available at <http://eprint.iacr.org/2005/447.pdf> (Accessed 20/05/2006)
- [6] J. Cheon and B. Jun, "A Polynomial Time Algorithm for the Braid Diffie Hellman Conjugacy Problem", *Proceedings of Crypto 2003*, LNCS, 2729, Springer-Verlag, 2003, pp. 212-215.
- [7] T. Thomas and A. K. Lal, Group Signature Schemes Using Braid Groups, arXiv:cs.CR/0602063, 2006
- [8] J.C. Cha, K.H. Ko, S.J. Lee, J.W. Han, J.H. Cheon, An efficient implementation of braid groups, *Advances in cryptology: Proceedings of ASIACRYPT 2001*, Lecture Notes in Computer Science, Springer-Verlag, 2248, pp.144-156, 2001
- [9] E. Stickel, A New Method for Exchanging Secrets, *Proceedings of the Third International Conference on Information Technology and Applications*, 2005
- [10] H. Sibert, P. Dehornoy, M. Girault, "Entity Authentication Schemes Using Braid Word Reduction", *Discrete Applied Mathematics*, 154, 2006, pp. 420-436
- [11] Lal and Chattervedi. Authentication schemes using braid groups, arxiv preprint, July 2005
- [12] B. Tsaban, On an authentication scheme based on the root problem in the braid groups, ArXiv preprint, September 2005
- [13] K. Murasugi and B. Kurpita, *A Study of Braids*, Kluwer Academic Publishers, The Netherlands, 1999.
- [14] Stickel, A new public-key cryptosystem non-abelian groups, In *proceedings of the 13th International Conference on Information Systems Development*. Vilnius Technika, Vilnius 2004, September 2004