

# Solutions to the Conjugacy Search Problem in Various Platform Groups <sup>★</sup>

Simran Tinani<sup>1</sup>[0000-0001-6886-4970],  
Carlo Matteotti<sup>2</sup>, and Joachim Rosenthal<sup>1</sup>[0000-0003-4545-3559]

<sup>1</sup> Institute of Mathematics, University of Zurich  
Winterthurerstrasse 190, 8057 Zurich  
`simran.tinani@math.uzh.ch`

<sup>2</sup> Eidgenössisches Departement VBS,  
Papiermühlestrasse 20, 3003 Bern  
`Carlo.Matteotti@vtg.admin.ch`

<sup>3</sup> `rosenthal@math.uzh.ch`

**Abstract.** Recently, the use of algorithmic problems over nonabelian groups was proposed for constructing quantum-secure cryptosystems. The most prominent such problem is the Conjugacy Search Problem (CSP), which requires the recovery of a conjugator  $x \in G$ , given  $g$  and  $h = x^{-1}gx$ . The best known protocols constructed based on the CSP are by Anshel, Anshel and Goldfeld, and Ko-Lee. The authors of these systems proposed as platforms the Braid groups, which were subsequently shown to be insecure. Thus, the search for a suitable nonabelian platform group is an active area of research. However, several existing attacks on nonabelian systems are protocol-specific, and focus on retrieving the private key without solving the CSP. So far, the true difficulty of the CSP in different platform groups has not been sufficiently investigated. In this paper, we study the CSP in some popularly proposed nonabelian platforms: some special polycyclic groups, extraspecial  $p$ -groups, and matrix groups over finite fields.

**Keywords:** Group-based Cryptography · Conjugacy Search Problem · Nonabelian groups.

## 1 Introduction

The construction and realization of cryptographic systems that resist quantum attacks presently constitutes an important area of research. Apart from lattice-based, multivariate, and code-based cryptography, it has been proposed recently to use the rich structure of nonabelian groups to construct quantum-secure protocols for public key exchange, message encryption, and authentication. Some recent surveys on this broad, emerging field, called group-based cryptography, can be found in [27] and [8].

The most prominent algorithmic problem employed for constructing nonabelian protocols has been the Conjugacy Search Problem (henceforth referred to as the CSP). While the Discrete Logarithm Problem (henceforth referred to as the DLP) in a group  $G$  requires the recovery of the exponent  $n$  when given the group elements  $g$  and  $h = g^n$ , the CSP requires the recovery of a conjugator  $x \in G$ , given the elements  $g$  and  $h = x^{-1}gx$ . To reflect this analogy, it is common to use the notation  $g^x := x^{-1}gx$  for  $g, x \in G$ , which we also adopt in this paper. If the conjugator is restricted to lie in a subgroup  $A \subseteq G$ , we refer to the problem as an  $A$ -restricted CSP, and more generally as a restricted CSP. Some problems similar to the CSP have also been proposed for use, for example, see [31], [2], [13], and [30]. However, this paper is majorly

---

<sup>★</sup> This research is supported by armasuisse Science and Technology.

concerned with the CSP. We note that conjugation is an action of a group on itself, and thus CSP-based protocols may be seen as special cases of the semigroup action-based construction in [22].

The first protocols constructed based on the CSP were by Anshel, Anshel and Goldfeld [1], and Ko–Lee [19]. The authors of both these systems proposed for use the Braid groups  $B_N$ . However, a number of attacks [15], [26], [33] show that the Braid groups are not suitable platforms. Nevertheless, the possibility of finding another nonabelian group that could serve as a platform for CSP-based protocols is still open. Some other popular nonabelian groups that have been proposed as cryptographic platforms are polycyclic groups, metabelian groups, some  $p$ -groups, Thompson groups, and matrix groups.

Attacks on other nonabelian protocols using different platforms have also been developed: several protocols have been cryptanalysed using polynomial time linear algebra attacks, for example, in [20], [25], [33], and [3]. However, many of these attacks are impractical to implement for standard parameter values, despite being polynomial time. Further, even though the linearity of a platform group renders a system vulnerable to these attacks, the computation of a linear representation may pose a serious roadblock for an adversary.

More importantly, such attacks are also typically protocol-specific, and focus on retrieving the private key without solving the CSP in the group. This always leaves open the possibility of constructing a different protocol, again based on the CSP, where the known attacks are avoided. So far, the true difficulty of the CSP in different platform groups has not been sufficiently investigated. In order to develop a cryptosystem based on the CSP, it is necessary to rule out platforms where there is a polynomial time solution or reduction to other known problems.

In this paper, we explore the CSP in three categories of groups: polycyclic groups with two generators (which we call 2-PC groups), extraspecial  $p$ -groups, and matrix groups over finite fields. More precisely, we show a reduction to one or more DLP’s in the cases of finite 2-PC groups and a special case of the CSP in matrix groups. For extraspecial  $p$ -groups, we show that the CSP has a polynomial time solution, by reducing it to a set of linear modular equations. Thus, while in full generality, the CSP seems to be a promising non-commutative replacement for the DLP, it seems to offer no novel security feature in several types of platforms and protocols. The algebraic reductions demonstrated in this paper may also prove useful in future cryptanalysis techniques for nonabelian protocols over different platform groups.

Throughout, polynomial time algorithm in a group  $G$  refers to an algorithm with time complexity  $\mathcal{O}(\log|G|)$ . Many of the polynomial time algorithms referred to are, in fact, constant time, but we do not emphasize this fact or the exact complexities, since our primary goal is to rule out unsuitable platforms. We use terms like “ $X$  is difficult to compute” to mean that the best-known algorithms for computing  $X$  are exponential.

## 2 Polycyclic Groups

In [7], polycyclic groups were suggested as a potential platform for CSP-based cryptography. A survey of polycyclic group-based cryptography can be found in [12]. In this section, we demonstrate that if a 2-PC group  $G$  is finite, the CSP is at most as hard as a DLP, whereas the restricted CSP can be designed to be exactly equivalent to a DLP. We illustrate what the restricted CSP in some other special polycyclic groups looks like. We show also that in some specific polycyclic platforms like the generalized quaternion group, there is a reduction of the CSP and the decomposition problem ([30]) to a set of linear modular equations. We use this method to cryptanalyse the system in [32].

**Definition 1 (Polycyclic Group).** *Let  $G$  be a group with generators  $a_1, a_2, \dots, a_n$ . Let  $I \subseteq \{1, 2, \dots, n\}$  denote a list of indices and  $m_i > 1$  be integers corresponding to elements  $i \in I$ .  $G$  is polycyclic if and only*

if it has a presentation of the form

$$G = \langle a_1, a_2, \dots, a_n \mid a_i^{m_i} = w_{ii} \ (i \in I), \ a_j^{a_i} = w_{ij} \ (1 \leq i < j \leq n), \ a_j^{a_i^{-1}} = w_{-ij} \ (i < j, \ i \notin I) \rangle, \quad (1)$$

where  $w_{ij} = a_{|i|+1}^{l(i,j,|i|+1)} \dots a_n^{l(i,j,n)}$ , with  $l(i,j,k) \in \mathbb{Z}$ , and  $0 \leq l(i,j,k) < m_k$  if  $k \in I$ . Here  $|i|$  denotes the absolute value of the integer  $i$ .

We will refer to a polycyclic group with  $n$  generators as  $n$ -polycyclic or  $n$ -PC. Define  $G_i = \langle a_i, a_{i+1} \dots a_n \rangle$ ,  $1 \leq i < n$ ,  $G_{n+1} = \langle 1 \rangle$ . The presentation in (1) is called *consistent* if  $|G_i/G_{i+1}| = m_i$  whenever  $i \in I$ , and  $G_i/G_{i+1}$  is infinite whenever  $i \notin I$ .

**Definition 2 (Normal Form).** *Given a consistent polycyclic presentation (1) for a group  $G$ , every element  $a$  of  $G$  can be represented uniquely in the form  $a = a_1^{e_1} a_2^{e_2} \dots a_n^{e_n}$ , where  $e_i \in \mathbb{Z}$ ,  $0 \leq e_i < m_i$  for  $i \in I$ .*

Given a word  $w$  in the generators  $a_1, a_2, \dots, a_n$  of  $G$ , there exists an algorithm, called a collection algorithm, to convert  $w$  into normal form. Many different strategies for this process have been suggested, but the best-known performance in most cases is achieved by the Collection from the Left Algorithm [36], and its improvement in [10].

## 2.1 CSP in 2-PC groups

We consider the case  $n = 2$ , where we have two generators  $x_1$  and  $x_2$  with relations  $x_1^{-1}x_2x_1 = x_2^L$  and  $x_1x_2x_1^{-1} = x_2^D$  (the second is redundant if and only if  $x_1$  has finite order, in which case we have  $D = L^{\text{ord}(x_1)-1}$ ). If some nonzero power  $x_1^C$  of  $x_1$  lies in  $\langle x_2 \rangle$ , then we have a relation of the form  $x_1^C = x_2^E$ . If  $x_1$  has infinite order (mod  $\langle x_2 \rangle$ ) for simplicity we nevertheless retain this relation with  $C = E = 0$ . Thus for parameters  $C, L, D, E \in \mathbb{Z}$ ,  $L, D \neq 0$ , the group presentation is

$$\langle x_1, x_2 \mid x_1^C = x_2^E, x_2^{x_1} = x_2^L, x_2^{x_1^{-1}} = x_2^D \rangle \quad (2)$$

Throughout, we will write  $N_2 = \text{ord}(x_2)$ , which is allowed to be infinite. If  $N_2$  is finite then  $\gcd(L, N_2) = 1$ , since if not, writing  $L' = \gcd(L, N_2) \neq 1$ , we have  $x_1^{-1}x_2^{N_2/L'}x_1 = 1$ , or  $x_2^{N_2/L'} = 1$ , a contradiction.

The main results of this section are as follows.

**Lemma 1.** *The conjugated word  $(x_1^c x_2^d)^{-1} (x_1^a x_2^b) (x_1^c x_2^d)$  can be collected to  $x_1^g x_2^h$  with  $g = a$  and*

$$h = \begin{cases} -dL^a + bL^c + d; & \text{if } c, a \geq 0 \\ -dL^a + bD^{-c} + d; & \text{if } c < 0, a \geq 0 \\ -dD^{-a} + bL^c + d; & \text{if } c \geq 0, a < 0 \\ -dD^{-a} + bD^{-c} + d; & \text{if } c, a < 0 \end{cases}$$

**Theorem 1.** *If  $N_2 = \text{ord}(x_2)$  is finite, the CSP has a polynomial time solution in  $G_2$ .*

*Proof.* Suppose that we are given an instance of the CSP, i.e. the equation  $(x_1^c x_2^d)^{-1} (x_1^a x_2^b) (x_1^c x_2^d) = x_1^e x_2^f$ , where we want to solve for unknowns  $c$  and  $d$ . Then, from Lemma 1,  $a = e \pmod C$  and the CSP is reduced to solving a modular equation for unknowns  $c$  and  $d$ .

If  $a \geq 0$ , we have  $f + d(L^a - 1) = bL^c$ , or  $f + d(L^a - 1) = bD^{-c}$ . Writing  $b_1 = \gcd(b, N_2)$ , we see that a solution for  $L^c$  (resp  $D^{-c}$ ) exists if and only if  $d(L^a - 1) = -f \pmod{b_1}$ . Writing  $a_1 = \gcd(b_1, L^a - 1)$ , a solution  $d$  for  $d(L^a - 1) = -f \pmod{b_1}$  exists if and only if  $a_1 \mid f$ . By construction, a solution  $(c, d)$  exists, so both these conditions are satisfied. Further, a solution  $d$  to  $d(L^a - 1) = -f \pmod{b_1}$  is given by  $d = -(f/a_1)((L^a - 1)/a_1)^{-1} \pmod{b_1/a_1}$ . Write  $d = -(f/a_1)((L^a - 1)/a_1)^{-1} + Mb_1/a_1$  for some  $M \in \mathbb{Z}$  which we may choose. Then, the following equalities hold  $\pmod{N_2}$

$$M(L^a - 1)/a_1 = (f + d(L^a - 1))/b_1 = \begin{cases} (b/b_1)L^c, & c \geq 0 \\ (b/b_1)D^{-c}, & c < 0 \end{cases}.$$

Writing  $A = (b/b_1)^{-1}((L^a - 1)/a_1)$  (clearly  $\gcd(A, N_2) = 1$ ), we may take  $M = A^{-1} \pmod{N_2}$ , so that a solution is given by  $c = 0$ . Then  $d = (L^a - 1/a_1)^{-1}(-f + b/a_1)$ .

Similarly, a solution can be obtained for the case  $a < 0$ . Thus, in both cases, a solution of the CSP involves a fixed number of applications of the Euclidean algorithm, and so has polynomial time complexity.

*Remark 1.* If  $N_2 = \infty$ , then the CSP in  $G_2$  reduces to an exponential Diophantine integer equation  $f = -dL^a + bL^c + d$  which possesses at least one solution. There is no known standard technique for solving such equations, and trial and error would perhaps be the best method (for a general reference see [29]).

**Theorem 2.** *If  $N_2 = \text{ord}(x_2)$  is finite, the  $\langle x_1 \rangle$ -restricted CSP in  $G_2$  reduces to a DLP. Further, the elements can be chosen so that it is exactly equivalent to a DLP  $\pmod{N_2}$ .*

Observe that the example of 2-PC groups demonstrates that a well-chosen restricted CSP can be notably more complex than the regular CSP. This complexity may grow with the number of generators, as suggested by the following special cases.

## 2.2 Cases of the CSP in some other polycyclic groups

**Proposition 1.** *Consider the 3-PC group  $\langle s, t_1, t_2 \rangle$ . Let  $\theta_i$  be the order of  $t_i$  for  $i = 1, 2$ . Write  $s^{-1}t_1s = t_1^{a_1^{(1)}} t_2^{a_2^{(1)}}$ ,  $s^{-1}t_2s = t_1^{a_1^{(2)}} t_2^{a_2^{(2)}}$ . Then we have  $s^{-i}t_1^A t_2^B s^i = t_1^{A_i} t_2^{B_i}$  where  $(A_0, B_0) = (A, B)$  and for  $i \geq 0$*

$$(A_{i+1}, B_{i+1}) = \left( a_1^{(1)} A_i + a_1^{(2)} B_i \pmod{\theta_1}, a_2^{(1)} L^{A_i a_1^{(2)}} \frac{L^{A_i a_1^{(1)}} - 1}{L^{a_1^{(1)}} - 1} + a_2^{(2)} \frac{L^{B_i a_1^{(2)}} - 1}{L^{a_1^{(2)}} - 1} \pmod{\theta_2} \right).$$

*Thus, the  $\langle s \rangle$ -restricted conjugation action on  $\langle t_1, t_2 \rangle$  can be described as a recurrence relation in  $\mathbb{Z}/\theta_1\mathbb{Z} \times \mathbb{Z}/\theta_2\mathbb{Z}$ . Solving this restricted CSP constitutes finding  $N$  from the  $N^{\text{th}}$  terms of this recurrence relation.*

**Proposition 2.** *Consider the  $(n+1)$ -PC group  $\langle s, t_1, \dots, t_n \rangle$  where  $T := \langle t_1, \dots, t_n \rangle$  is abelian. Representing the elements of  $T$  as column vectors  $(r_1, \dots, r_m)$ , we can describe the conjugation action of  $s$  on  $T$  by the linear map*

$$\mathbb{Z}_{o_1} \times \mathbb{Z}_{o_2} \times \dots \times \mathbb{Z}_{o_m} \rightarrow \mathbb{Z}_{o_1} \times \mathbb{Z}_{o_2} \times \dots \times \mathbb{Z}_{o_m}$$

$$(r_1, \dots, r_m) \rightarrow \begin{bmatrix} a_1^{(1)} & \dots & a_1^{(m)} \\ a_2^{(1)} & \dots & a_2^{(m)} \\ \vdots & \dots & \vdots \\ a_m^{(1)} & \dots & a_m^{(m)} \end{bmatrix} \cdot \begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_m \end{bmatrix}$$

*Here, the restricted CSP constitutes recovering  $N$  from the  $N^{\text{th}}$  power of the above matrix.*

Note that the above problem is not the same as the matrix group DLP because the entries of each column actually lie in separate groups.

### 2.3 Using matrix representations of polycyclic groups

It is known that every polycyclic group is linear, and thus embeds faithfully into a matrix group over some field. This subsection discusses the possibility of disguising the polycyclic group structure with matrices for use in cryptosystems. In this scenario, the adversary who wants to solve the CSP is faced with the additional problem: given the public matrix generators  $M_1, \dots, M_n$ , the public base matrix  $X$ , and a public key matrix  $Y$  (which represents  $A^{-1}XA$ ), find exponents  $(i_1, \dots, i_n), (j_1, \dots, j_n)$  such that  $X = M_1^{i_1} \dots M_n^{i_n}$ ,  $Y = M_1^{j_1} \dots M_n^{j_n}$ . Once this is done, the problem reduces back to finding the conjugator in the words of the group  $G$ .

Such a problem has been discussed in [18], and is called the Generalized Discrete Logarithm Problem (GDLP). It is not known whether a general square root attack exists for the GDLP in any finite group. The thesis [16] discusses some square-root type algorithms for finite matrix groups. However, in a 2-PC group, represented by generator matrices  $M_x$  and  $M_y$ , the adversary must solve the GDLP in two variables to obtain back the group presentation version of the problem. Square root algorithms solving this case of the GDLP have been discussed in [24] and [17] reducing it to at most two DLP's over a matrix group. In [23], it was shown that the DLP over  $GL_r(\mathbb{F}_q)$  reduces to a DLP over a small extension of  $\mathbb{F}_q$ . Therefore, while the overall security of the protocol may be enhanced, introducing the matrix representation does not offer any novel security feature.

### 2.4 Examples

**Generalized Quaternion Groups** A generalized quaternion group is given by the presentation

$$Q_{2^n} = \langle x, y \mid x^N = 1, y^2 = x^{N/2}, yx = x^{-1}y, N = 2^{n-1} \rangle. \quad (3)$$

Writing  $y = x_1, x = x_2$ , we have the relations  $x_1^2 = x_2^{N/2}, x_2^{x_1} = x_2^{-1}$ . So, these groups are (finite) polycyclic. Clearly, any element in this group has a normal form  $x^i y^j$ , where  $0 \leq i \leq N, 0 \leq j \leq 1$ .

For an instance of the CSP  $(x^i y)^{-1} (x^a y) (x^i y) = x^A y$  the exponent  $i$  is easily seen to be found by solving the modular equation  $2i - a + N/2 = A \pmod{N}$ . Note that  $(x^i y)^{-1} (x^a) (x^i y) = y^{-1} x^a y = x^{-a}$ , so in this case any value of  $i$  is a valid solution. In fact, the same method can be used to solve problems related to the CSP, such as the decomposition problem, introduced in [30]. Given  $a, A, b$  and  $B$ , solving the decomposition problem  $(x^i y^j)(x^a y^b)(x^k y^l) = x^A y^B$  for  $i, j, k, l \in \mathbb{Z}$  in  $Q_{2^n}$  reduces to solving the following set of linear modular equations for  $i, j, k, l$ :

$$\begin{aligned} i + (-1)^j a + (-1)^{j+b} k &= A \pmod{N} \\ j + l &= B - b \pmod{2}, \end{aligned}$$

which, in turn, can be done in polynomial time.

In [32], a key exchange protocol based on the group  $Q_{2^n}$  was proposed, based on a problem that the authors call complete decomposition problem. This is similar to the decomposition problem in [30], but the base word  $a$  is kept secret. However, the same method reduces the key retrieval to a set of linear equations.

**Proposition 3.** *Retrieving the secret keys in the protocol of [32] reduces to solving a system of six linear equations in six unknowns over  $\mathbb{Z}_N$ ,  $N \in \mathbb{Z}$  and thus can be done in polynomial time.*

*Matrix Representations of Quaternions* In groups like  $Q_{2^n}$ , it is easy to see that disguising the elements as matrices simply introduces a single DLP into the security of the protocol. Suppose that the elements  $x$  and  $y$  correspond respectively to invertible matrices  $M_x$  and  $M_y$  in  $GL_r(\mathbb{F}_q)$ . The adversary sees matrices of the form  $A = M_x^i M_y$ . However, since  $M_y$  is known, the exponent  $i$  can be recovered by solving the DLP  $AM_y^{-1} = M_x^i$ .

**Holomorphs of cyclic groups** Let  $G$  be the holomorph  $G = C_p \rtimes \text{Aut}(C_p)$  of a cyclic group of prime order, where each element in  $C_p = \langle g \rangle$  is represented as  $g^n$ ,  $n \in \mathbb{Z}$ . We have  $\text{Aut}(C_p) \cong \mathbb{Z}_p^\times$ , which is also cyclic. Thus,  $\text{Hol}(G)$  is a 2-PC group. The action of  $\mathbb{Z}_p^\times$  on  $C_p$  is written as a conjugation, and given by  $k^{-1}h^i k = h^{ik}$ ,  $k \in \mathbb{Z}_p^\times$ ,  $i \in \mathbb{Z}$ . Given elements  $g_1 = h^l k_1$ ,  $g_2 = h^n k_2$  in  $G$ , to solve the CSP we have to find  $g = h^m k$  such that  $g^{-1}g_1 g = g_2$ . It may be verified that  $(h^m k)^{-1}(h^l k_1)(h^m k)$  simplifies to  $h^W k_1$  with  $W = k((-m + l) + mk_1^{-1}) \pmod p$ . Thus, one needs to solve  $n = k((k_1^{-1} - 1)m + l) \pmod p$  for  $m$  and  $k$ , which is doable in polynomial time.

### 3 $p$ -Groups

A finite group with order a power of a prime  $p$  is called a  $p$ -group. Among these, some interesting and well-studied (overlapping) subclasses are the special, extraspecial, and Miller  $p$ -groups. Since  $p$ -groups constitute a vast and important class of nonabelian groups, and often form building blocks for other nonabelian groups, it is worth examining the difficulty of the CSP in them. In fact, some authors have already proposed them as potential platforms for cryptography. For example, in [14], authentication and signature schemes using the CSP were proposed, and  $p$ -Miller groups were suggested as platforms. In [21] automorphisms of extraspecial  $p$ -groups were used.

Several  $p$ -groups are constructed by combining smaller  $p$ -groups by taking direct, semidirect and central products (see, for example, [4], [6]). While it is clear that given a direct product  $G = H \times K$ , an instance of the CSP in  $G$  reduces to two separate instances of the CSP in  $H$  and  $K$ , we show similar reductions for some special central products. We use these to show that the CSP in any extraspecial  $p$ -group has a polynomial time solution. These results also demonstrate that while considering a group for a CSP-based system, care must be taken to ensure that an easy decomposition as a central product is not possible.

#### 3.1 Central products

**Definition 3.** A group  $G$  is said to be a central product of its subgroups  $H$  and  $K$  if every element  $g \in G$  can be written as  $hk$ , with  $h \in H, k \in K$  (i.e.  $G = HK$ ), and we have  $hk = kh \forall h \in H, k \in K$ .

For a subset  $S$  and an element  $x$  of a group  $G$  we use the notations  $xS := \{xz \mid z \in S\}$  and  $Sx := \{zx \mid z \in S\}$ . For any  $x \in G$ , denote by  $C_x := \{g^{-1}xg \mid g \in G\}$  the conjugacy class of  $x$ . For subsets  $S_1$  and  $S_2$ , the product  $S_1 S_2$  denotes the set  $\{s_1 s_2 \mid s_1 \in S_1, s_2 \in S_2\}$ . We introduce the following property, which is relevant to central products and the CSP.

**Definition 4.** A group  $G$  is said to be efficiently  $C$ -decomposable if for any elements  $h, k, x, y \in G$  with  $hC_x \cap kC_y \neq \emptyset$ , an element of  $hC_x \cap kC_y$  can be found in polynomial time.

**Theorem 3.** Let  $G$  be an efficiently  $C$ -decomposable group and  $H$  and  $K$  be subgroups of  $G$  such that  $G$  is the central product of  $H$  and  $K$ . Then, solving the CSP in  $G$  is polynomial time reducible to solving two separate CSP's in  $H$  and  $K$ .

### 3.2 CSP in extraspecial $p$ -groups

**Definition 5 (Extraspecial  $p$ -group).** A  $p$ -group  $G$  is called extraspecial if its center  $Z(G)$  is cyclic of order  $p$ , and the quotient  $G/Z(G)$  is a non-trivial elementary abelian  $p$ -group.

Throughout this section,  $C_p$  denotes the cyclic group of order  $p$ , and  $A \rtimes B$  denotes the semidirect product of groups  $A$  and  $B$ . It is well-known that there are precisely two isomorphism classes for the extraspecial group of order  $p^3$ :  $M(p) = C_{p^2} \rtimes C_p$  and  $N(p) = (C_p \times C_p) \rtimes C_p$ , where the latter may be represented as triangular matrices over the finite field of order  $p$ , with 1's on the diagonal. Further, every extraspecial  $p$ -group has order  $p^{1+2n}$  for some positive integer  $n$ , and conversely for each such number there are exactly two extraspecial groups up to isomorphism. Every extraspecial group of order  $p^{1+2n}$  can be written as a central product of either  $n$  copies of  $M(p)$  or  $n - 1$  copies of  $M(p)$  and 1 copy of  $N(p)$ . A standard reference for these results is [11]. Further, a central product decomposition of any extraspecial  $p$ -group is computable in polynomial time by the result in [37].

It is well known (refer, for example, to [5]) that  $M(p)$  and  $N(p)$  have the following presentations:

$$\begin{aligned} M(p) &= \langle x, y \mid x^{p^2} = 1, y^p = 1, yxy^{-1} = x^{1+p} \rangle \\ N(p) &= \langle x, y, z \mid x^p = y^p = z^p = 1, xy = yx, yz = zy, zxz^{-1} = xy^{-1} \rangle. \end{aligned}$$

The following results demonstrate solutions for the CSP in  $M(p)$  and  $N(p)$ .

**Lemma 2.** Two elements  $g = x^a y^b$  and  $g' = x^A y^B$  in  $M(p)$  are conjugates if and only if  $a = A \pmod p$  and  $B = b \pmod p$ . In this case, a conjugator  $h = x^i y^j$  such that  $g' = h^{-1}gh$  can be found by solving  $(A - a)/p = (aj - ib) \pmod p$ . Consequently, the CSP has a polynomial time solution in  $M(p)$ .

**Lemma 3.** Two elements  $g = x^a y^b z^c$  and  $g' = x^A y^B z^C$  in  $N(p)$  are conjugate if and only if  $a = A \pmod p$  and  $C = c \pmod p$ . In this case,  $h = x^i y^j z^k$  is a conjugator such that  $g' = h^{-1}gh$  if and only if  $(i, k)$  satisfies  $B - b = -ka + ic$ . Consequently, the CSP has a polynomial time solution in  $N(p)$ .

**Proposition 4.** Any central product  $G$  of finitely many copies of  $N(p)$  and  $M(p)$  is efficiently  $C$ -decomposable.

As a direct consequence of the above results, we have below the main result of this section.

**Theorem 4.** The CSP in an extraspecial  $p$ -group has a polynomial time solution.

## 4 Matrix Groups

Throughout this section, we use  $q$  to denote a power of a prime  $p$ .

Matrix groups over finite fields have played an important role in cryptography. In [23] and [9], the DLP over the matrix group  $GL_n(\mathbb{F}_q)$  was studied and shown to be no more difficult than the discrete logarithm problem over a small extension of  $\mathbb{F}_q$ , and in fact, less efficient in terms of key sizes for the same security level. In this section, we study the CSP in  $Mat_n(\mathbb{F}_q)$  in the special case when the conjugator is known to lie in a cyclic subgroup of  $GL_n(\mathbb{F}_q)$ . More precisely, suppose that  $X \in Mat_n(\mathbb{F}_q)$  and  $Z \in GL_n(\mathbb{F}_q)$  are public matrices. The public keys of the system are of the form  $Y = Z^{-r} X Z^r$  and  $Z^{-s} X Z^s$ , where the integers  $r$

and  $s$  are secrets. The shared secret is  $Z^{-r-s}XZ^{r+s}$ , and so it is enough to solve the CSP, i.e. find any one of the integers  $r$  and  $s$ . We will show that the retrieval of  $r \in \mathbb{Z}$  from  $X, Z$ , and  $Y$  reduces to a set of DLP's. This analysis enables a full cryptanalysis of the system proposed in [35].

First observe that there exists an extension  $\mathbb{F}_{q^k}$  of  $\mathbb{F}_q$  and a unique matrix  $P \in GL_n(\mathbb{F}_{q^k})$  (computable in polynomial time, by the algorithm in [23]) such that  $J_Z = PZP^{-1}$ , where  $J_Z$  is the Jordan Normal form of  $Z$ . Writing  $M = PXP^{-1}$  and  $N = PYP^{-1}$ , we then have  $Z^{-r}XZ^r = Y \iff J_Z^{-r}MJ_Z^r = N$ . The integer  $r$  can then be recovered from the latter of these two equations, using a set of algebraic manipulations. The following theorem summarizes the main result of this section.

**Theorem 5.** *If  $J_Z$  is diagonal, the retrieval of  $r$  reduces to a set of at most  $n^2$  simultaneous DLP's over  $\mathbb{F}_{q^k}$ . If  $J_Z$  is not diagonal and composed of  $s > 1$  Jordan blocks, recovering  $r$  reduces to  $s^2$  instances each of a linear equation over  $\mathbb{F}_q$  and a simultaneous DLP over  $\mathbb{F}_{q^k}$ .*

#### 4.1 An application to cryptanalysis

In [35], a protocol based on the above-discussed special case of the CSP (i.e. where the conjugators are all in a cyclic subgroup) described above was proposed for a ring  $R = H_p$  called quaternions mod  $p$ . For a prime  $p$ , the authors define  $H_p$  as the set  $\{a = a_1 + a_2i + a_3j + a_4k \mid a_i \in \mathbb{Z}_p\}$ . Arithmetic is defined in the usual way for quaternions, but over  $\mathbb{Z}_p$  (for a detailed exposition on quaternion sets, see [34]). We observe that by Proposition 3.3 in [34], we have an explicit isomorphism (with an explicit inverse) between  $H_p$  and  $Mat_2(\mathbb{Z}/p\mathbb{Z})$ . Thus, in effect, the protocol in [35] may be treated as if it is over  $Mat_2(\mathbb{F}_p)$ , and then Theorem 5 gives a full reduction to at most 4 DLP's.

## 5 Conclusion

In this paper, we described conditional reductions of and solutions to the CSP in three classes of groups, namely polycyclic, extraspecial  $p$ -groups, and matrix groups. We found that the CSP may often be reduced to a set of DLP's or even to an easier problem, like a set of linear modular equations. Our results imply the non-availability of some classes of groups as platforms, and a minimum complexity of a protocol designed based on the CSP. For instance, Theorem 5 implies that for a protocol over a matrix group, conjugators must be picked from a subgroup with at least two generators. In particular, this method gives a solution to a special case of the Anshel–Anshel–Goldfeld and Ko–Lee protocols over  $GL_n(\mathbb{F}_q)$ . The section on  $p$ -groups showed that extraspecial  $p$ -groups are unsuitable platforms. The result on central products can be seen as an analogy to the Pohlig–Hellman algorithm [28] for the CSP, and shows that a selected platform must be “atomic”, or have a central decomposition that is difficult to compute. The section on polycyclic groups shows that the CSP in the case with only two generators may already have reasonable difficulty, and suggests that with more than two generators the CSP may indeed offer promising security levels.



## Bibliography

- [1] Iris Anshel, Michael Anshel, and Dorian Goldfeld. An algebraic method for public-key cryptography. *Math. Res. Lett.*, 6(3-4):287–291, 1999.
- [2] Iris Anshel, Michael Anshel, Dorian Goldfeld, and Stephane Lemieux. Key agreement, the algebraic eraser™, and lightweight cryptography. *Contemporary Mathematics*, 418:1–34, 2007.
- [3] Adi Ben-Zvi, Arkadius Kalka, and Boaz Tsaban. Cryptanalysis via algebraic spans. In *Annual International Cryptology Conference*, pages 255–274. Springer, 2018.
- [4] A. Caranti. A module-theoretic approach to abelian automorphism groups. *Israel Journal of Mathematics*, 205:235–246, 2015.
- [5] Keith Conrad. Groups of order  $p^3$ . *Expository papers on group theory*, 2014.
- [6] M. J. Curran. Direct products with abelian automorphism groups. *Communications in Algebra*, 35(1):389–397, 2006.
- [7] Bettina Eick and Delaram Kahrobaei. Polycyclic groups: a new platform for cryptology? *arXiv preprint math/0411077*, 2004.
- [8] Benjamin Fine, Maggie Habeeb, Delaram Kahrobaei, and Gerhard Rosenberger. Aspects of nonabelian group based cryptography: a survey and open problems. *arXiv preprint arXiv:1103.4093*, 2011.
- [9] David Freeman. The discrete logarithm problem in matrix groups. 2004.
- [10] Volker Gebhardt. Efficient collection in infinite polycyclic groups. *Journal of Symbolic Computation*, 34(3):213–228, 2002.
- [11] D. Gorenstein. *Finite Groups*. AMS Chelsea Publishing Series. American Mathematical Society, 2007.
- [12] Jonathan Gryak and Delaram Kahrobaei. The status of polycyclic group-based cryptography: A survey and open problems. *Groups Complexity Cryptology*, 8(2):171–186, 2016.
- [13] Lize Gu and Shihui Zheng. Conjugacy systems based on nonabelian factorization problems and their applications in cryptography. *Journal of Applied Mathematics*, 2014, 2014.
- [14] Guangguo Han and Chuanguui Ma. A new authentication and signature scheme based on the conjugacy search problem. In *2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing*, volume 2, pages 317–320, 2010.
- [15] Dennis Hofheinz and Rainer Steinwandt. A practical attack on some braid group based cryptographic primitives. In Yvo G. Desmedt, editor, *Public Key Cryptography — PKC 2003*, pages 187–198, Berlin, Heidelberg, 2002. Springer Berlin Heidelberg.
- [16] Ilic. *Discrete logs in arbitrary finite groups*. PhD thesis, Florida Atlantic University, 2008.
- [17] Sunil Kumar Kashyap, Birendra Sharma, and Amitabh Banerjee. A cryptosystem based on  $\text{DLP } \gamma = \alpha^a \beta^b \pmod p$ . *International Journal of Network Security*, 3:95–100, 01 2006.
- [18] Lee C Klingler, Spyros S Magliveras, Fred Richman, and Michal Sramka. Discrete logarithms for finite groups. *Computing*, 85(1-2):3, 2009.
- [19] Ki Hyoung Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Ju-sung Kang, and Choonsik Park. New public-key cryptosystem using braid groups. In *Annual International Cryptology Conference*, pages 166–183. Springer, 2000.
- [20] Martin Kreuzer, Alexey D Myasnikov, and Alexander Ushakov. A linear algebra attack to group-ring-based key exchange protocols. In *International Conference on Applied Cryptography and Network Security*, pages 37–43. Springer, 2014.
- [21] Ayan Mahalanobis. The mor cryptosystem and extra-special p-groups. *Journal of Discrete Mathematical Sciences and Cryptography*, 18(3):201–208, 2015.

- [22] Gérard Maze, Chris Monico, and Joachim Rosenthal. Public key cryptography based on semigroup actions. *Adv. in Math. of Communications*, 1(4):489–507, 2007.
- [23] Alfred Menezes and Yihong Wu. The discrete logarithm problem in  $GL(n, q)$ . *Ars Comb.*, 47, 1997.
- [24] Chandrashekhhar Meshram. A cryptosystem based on double generalized discrete logarithm problem. *Int. J. Contemp. Math. Sciences*, 6:285–297, 01 2011.
- [25] Alexei Myasnikov and Vitaliĭ Roman’kov. A linear decomposition attack. *Groups Complexity Cryptology*, 7(1):81–94, 2015.
- [26] Alexei Myasnikov, Vladimir Shpilrain, and Alexander Ushakov. Random subgroups of braid groups: An approach to cryptanalysis of a braid group based cryptographic protocol. In Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, and Tal Malkin, editors, *Public Key Cryptography - PKC 2006*, pages 302–314, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.
- [27] Alexei Myasnikov, Vladimir Shpilrain, and Alexander Ushakov. *Group-based cryptography*. Springer Science & Business Media, 2008.
- [28] S. Pohlig and M. Hellman. An improved algorithm for computing logarithms over  $GF(p)$  and its cryptographic significance (corresp.). *IEEE Transactions on information Theory*, 24(1):106–110, 1978.
- [29] T. N. Shorey and R. Tijdeman. *Exponential Diophantine Equations*. Cambridge Tracts in Mathematics. Cambridge University Press, 1986.
- [30] Vladimir Shpilrain and Alexander Ushakov. A new key exchange protocol based on the decomposition problem. *arXiv preprint math/0512140*, 2005.
- [31] Vladimir Shpilrain and Alexander Ushakov. An authentication scheme based on the twisted conjugacy problem. In *International Conference on Applied Cryptography and Network Security*, pages 366–372. Springer, 2008.
- [32] Chang Seng Sin and Huey Voon Chen. Group-based key exchange protocol based on complete decomposition search problem. In *Information Security Practice and Experience*. Springer International Publishing, 2019.
- [33] Boaz Tsaban. Polynomial-time solutions of computational problems in noncommutative-algebraic cryptography. *Journal of Cryptology*, 28(3):601–622, 2015.
- [34] Nikolaos Tsopanidis. *The Hurwitz and Lipschitz Integers and Some Applications*. PhD thesis, Universidade do Porto, 2020.
- [35] Maheswara Rao Valluri and Shailendra Vikash Narayan. Quaternion public key cryptosystems. In *2016 World Congress on Industrial Control Systems Security (WCICSS)*, pages 1–4, 2016.
- [36] Michael R. Vaughan-Lee. Collection from the left. *J. Symb. Comput.*, 9:725–733, 1990.
- [37] James B. Wilson. Finding central decompositions of  $p$ -groups. *Journal of Group Theory*, 12(6):813–830, 2009.