AWM Research Symposium 2022

Complexity of Conjugacy Search in some Platform Groups

Simran Tinani

Based on joint work with Carlo Matteotti and Joachim Rosenthal[1]

University of Zurich UZH

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

June 16, 2022

[1] This research is supported by armasuisse Science and Technology.

Introduction

- The discrete logarithm problem (DLP) and integer factorization are the most widely used algorithmic problems for public key cryptography. However, they are solved in polynomial time with a quantum algorithm.
- Shor's quantum algorithms rely on the solution of the *Hidden Subgroup Problem* for finite abelian groups.
- Apart from lattice-based, multivariate, code-based, and isogeny-based cryptography, it has been proposed recently to use nonabelian group theoretic computational problems.

Background: Nonabelian Group-based Cryptography

Definition (Discrete Logarithm Problem (DLP))

Given $g, h \in G$ with $h \in \langle g \rangle$, find $n \in \mathbb{Z}$ such that $h = g^n$.

Definition (Conjugacy Search Problem (CSP))

Given $g, h \in G$, find an element x of G such that $h = x^{-1}gx$, given that it exists. We adopt the notation $g^x := x^{-1}gx$.

- Anshel, Anshel, and Goldfeld, 1999 and Ko et al., 2000, built the first protocols based on the CSP in braid groups.
- Several attacks (Hofheinz and Steinwandt, 2002), (Myasnikov, Shpilrain, and Ushakov, 2006) show that braid groups are not suitable platforms. Proposed alternatives: polycyclic groups, p-groups, Thompson groups, matrix groups.

Motivation

- For linear platform groups (i.e. those that embed faithfully into a matrix group over a field), several polynomial time attacks exist (Kreuzer, Myasnikov, and Ushakov, 2014), (Myasnikov and Roman'kov, 2015), (Tsaban, 2015), (Ben-Zvi, Kalka, and Tsaban, 2018).
- Often impractical to implement for standard parameter values.
- Computation of an efficient linear representation may pose a serious roadblock for an adversary.
- Protocol-specific and focus on retrieving the private shared key without solving the CSP
- So far, the true difficulty of the CSP in different platforms has not been sufficiently investigated.

Motivation

Definition (A-restricted CSP)

Given a subgroup $A \leq G$ and elements g and h of a group G, find an element $x \in A$ such that $h = x^{-1}gx$, given that it exists.

We are specifically interested in the case where A is cyclic.

- In Ko-Lee, commutativity of conjugators is needed. Interesting abelian subgroups of several proposed platforms are cyclic.
- In AAG, the amount of information the adversary has is "proportional" to the number of generators of A.
- Case A cyclic is most basic, reductions to it may be possible

Polycyclic groups

- Suggested as platforms for CSP in (Eick and Kahrobaei, 2004).
- There is evidence of the ineffectiveness of length-based attacks and other heuristic methods for braid groups.

Definition (Polycyclic Group)

A polycyclic group is a group G with a subnormal series $G = G_1 > G_2 > \ldots > G_{n+1} = 1$ with cyclic quotient G_i/G_{i+1}.

$$\begin{aligned} G = \langle a_1, a_2, \ldots, a_n \mid a_i^{m_i} &= w_{ii},\ i \in I, \\ a_j^{a_i} &= w_{ij},\ 1 \leq i < j \leq n, \\ a_j^{a_i^{-1}} &= w_{-ij},\ 1 \leq i < j \leq n, i \notin I \rangle, \end{aligned}$$

for some $I \subseteq \{1, 2, \ldots, n\}$, where $w_{ij} = a_{|i|+1}^{l(i,j,|i|+1)} \ldots a_n^{l(i,j,n)}$, with $l(i,j,k) \in \mathbb{Z}$, and $0 \leq l(i,j,k) < m_k$ if $k \in I$.

Polycyclic Groups with two generators

In the case $n = 2$, we the group presentation

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

Here, collection, multiplication, conjugation can be performed with a single application of a formula.

Lemma 1

The conjugated word $(x_1^c x_2^d)^{-1}(x_1^a x_2^b)(x_1^c x_2^d) = x_1^g x_2^h$ *with* $g = a$,

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

CSP in 2-Polycyclic Groups

Theorem 1

If $N_2 = \mathrm{ord}(x_2)$ is finite, the CSP has a polynomial time solution.

Theorem 2

If $N_2 = \mathrm{ord}(x_2)$ 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 in $(\mathbb{Z}/N_2\mathbb{Z})^*$.

If $N_2 = \infty$, the CSP reduces to the Diophantine integer equation $f = -dL^a + bL^c + d$. The $\langle x_1 \rangle$-restricted CSP $f = bL^c$ here is easily solved by taking the real number base-L logarithm of $f/b \in \mathbb{Z}$.

CSP in a finite $(n+1)$-PC group; n generators commute

$$G = \langle s, t_1, \ldots, t_n \mid t_i^{\theta_i} = 1, t_i t_j = t_j t_i,\ t_i{}^s = t_1^{a_i^{(1)}} \ldots t_n^{a_i^{(n)}}, 1 \leq i,j \leq n \rangle$$

Representing elements of T as column vectors $(r_1 \ldots, r_n)$, we can describe the conjugation action of s on T by the map

$$\mathbb{Z}_{o_1} \times \mathbb{Z}_{o_2} \times \ldots \times \mathbb{Z}_{o_n} \to \mathbb{Z}_{o_1} \times \mathbb{Z}_{o_2} \times \ldots \times \mathbb{Z}_{o_n}$$

$$(r_1, \ldots, r_n) \to \begin{bmatrix} a_1^{(1)} & \ldots & a_1^{(n)} \\ a_2^{(1)} & \ldots & a_2^{(n)} \\ \vdots & \ldots & \vdots \\ a_n^{(1)} & \ldots & a_n^{(n)} \end{bmatrix} \cdot \begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{bmatrix}$$

The $\langle s \rangle$-restricted CSP constitutes recovering N from the N^{th} power of the above matrix.

Matrix Groups

- The DLP in $GL_n(\mathbb{F}_q)$ was studied in (Menezes and Wu, 1997) and (Freeman, 2004) and shown to be no more difficult than the DLP over a small extension of $\mathbb{F}_q$.

- Most known nonabelian platform groups are linear. If a faithful representation and its inverse can efficiently be computed, the security of the system depends on that of the matrix CSP rather than that in the original platform.

- Let $X \in Mat_n(\mathbb{F}_q)$, $Z \in GL_n(\mathbb{F}_q)$ and $Y = Z^{-r}XZ^{r}$ be public matrices. The $\langle Z \rangle$-restricted CSP comprises finding $r \in \mathbb{Z}$.

$\langle Z \rangle$-restricted CSP in $GL_n(\mathbb{F}_q)$

There is an extension $\mathbb{F}_{q^k}$ of $\mathbb{F}_q$ and a unique matrix $P \in GL_n(\mathbb{F}_{q^k})$, both computable in polynomial time (Menezes and Wu, 1997)), such that $J_Z = PZP^{-1}$, where J_Z is the Jordan Normal form of Z.

$$\text{Define } M := PXP^{-1}, \; N := PYP^{-1}, \; \theta_Z := \mathrm{ord}_{\mathrm{GL}_n(\mathbb{F}_q)}(Z).$$

Clearly, $Z^{-r}XZ^r = Y \iff J_Z^{-r}MJ_Z^r = N$.

Theorem 3

If J_Z is diagonal then the retrieval of $r \pmod{\theta_Z}$ reduces to solving at most n^2 DLPs over $\mathbb{F}_{q^k}$.

$\langle Z \rangle$-restricted CSP in $GL_n(\mathbb{F}_q)$

Proposition 1

The value of $r' := r \pmod p$ can be computed in polynomial time.

Proposition 2

Computing $r \pmod{\operatorname*{lcm}_{1 \leq i \leq s} \operatorname{ord}(\lambda_i)}$ reduces in polynomial time to solving at most s^2 DLPs in $\mathbb{F}_{q^k}$.

Theorem 4

Let J_Z be non-diagonal, and composed of s Jordan blocks. Then, the computation of r is polynomial time reducible to a set of s^2 DLPs over $\mathbb{F}_{q^k}$.

p–groups

- A p-group is a finite group with order a power of a prime p.
- Several p-groups are constructed by combining smaller p-groups by taking direct, semidirect and central products
- 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.
- Every extraspecial p-group has order p^{1+2n} and is a central product of n extraspecial groups of order p^3.

Definition

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 $hk = kh \; \forall \; h \in H, \; k \in K$.*

Definition

A finite group G is ***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. Here $C_x := \{g^{-1}xg \mid g \in G\}$.*

Theorem 5

Let G be efficiently C-decomposable and $H, K \leq G$ be such that $G = HK$ is a central product. Then, solving the CSP in G is polynomial time reducible to solving 2 separate CSPs in H and K.

Extraspecial p-groups of order p^3

In extraspecial p-groups of order p^3, it is always possible to reduce the CSP to a set of linear modular equations.

$$M(p) = \langle x, y \mid x^{p^2} = 1, y^p = 1, yxy^{-1} = x^{1+p} \rangle$$

$$N(p) = \langle x, y, z \mid x^p = y^p = z^p = 1, xy = yx, yz = zy, zxz^{-1} = xy^{-1} \rangle.$$

Theorem 6

For $g = x^a y^b$ and $g' = x^A y^B$ in $M(p)$, an element $h = x^i y^j$ satisfies $g' = h^{-1}gh$ if and only if $(A - a)/p = (aj - ib) \mod p$. For $g = x^a y^b z^c$ and $g' = x^A y^B z^C$ in $N(p)$ an element $h = x^i y^j z^k$ satisfies $g' = h^{-1}gh$ if and only if $B - b = -ka + ic \mod p$.

Theorem 7

Any extraspecial p-group G is efficiently C-decomposable. Thus, the CSP in G has a polynomial time solution.

Applications

- Protocol in (Sin and Chen, 2019) based on a "decomposition problem" in (polycyclic) generalized quaternion groups Q_{2^n} is broken by collection and solving linear equations $\pmod{N}$.

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

- Protocol in (Valluri and Narayan, 2016) is based on the a $\langle Z \rangle$-restricted CSP over quaternions mod p, H_p.

$$H_p = \{a_1 + a_2 i + a_3 j + a_4 k \mid a_i \in \mathbb{Z}_p\}.$$

  There is an explicit isomorphism with efficiently computable inverse $H_p \cong Mat_2(\mathbb{Z}/p\mathbb{Z})$ (Tsopanidis, 2020).

- "Subgroup CSP" in (Gu and Zheng, 2014) corresponds exactly to the A-restricted CSP for A cyclic. Suggested platforms are $\mathrm{GL}_n(\mathbb{F}_q)$, a subgroup of it, and a braid group.

Thank you!

References I

Anshel, Iris, Michael Anshel, and Dorian Goldfeld (1999). "An algebraic method for public-key cryptography". In: *Math. Res. Lett.* 6.3-4, pp. 287–291.

Ben-Zvi, Adi, Arkadius Kalka, and Boaz Tsaban (2018). "Cryptanalysis via algebraic spans". In: *Annual International Cryptology Conference*. Springer, pp. 255–274.

Eick, Bettina and Delaram Kahrobaei (2004). "Polycyclic groups: a new platform for cryptology?" In: *arXiv preprint math/0411077*.

Freeman, David (2004). "The Discrete Logarithm Problem in Matrix Groups". In:

Gu, Lize and Shihui Zheng (2014). "Conjugacy Systems Based on Nonabelian Factorization Problems and Their Applications in Cryptography". In: *J. Appl. Math.* 2014, 630607:1–630607:10.

References II

Hofheinz, Dennis and Rainer Steinwandt (2002). "A Practical Attack on Some Braid Group Based Cryptographic Primitives". In: *Public Key Cryptography — PKC 2003*. Ed. by Yvo G. Desmedt. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 187–198. ISBN: 978-3-540-36288-3.

Ko, Ki Hyoung et al. (2000). "New public-key cryptosystem using braid groups". In: *Annual International Cryptology Conference*. Springer, pp. 166–183.

Kreuzer, Martin, Alexey D Myasnikov, and Alexander Ushakov (2014). "A linear algebra attack to group-ring-based key exchange protocols". In: *International Conference on Applied Cryptography and Network Security*. Springer, pp. 37–43.

Menezes, Alfred and Yihong Wu (1997). "The Discrete Logarithm Problem in $GL(n,q)$". In: *Ars Comb.* 47.

References III

Myasnikov, Alexei and Vitali Roman'kov (2015). "A linear decomposition attack". In: *Groups Complexity Cryptology* 7.1, pp. 81–94.

Myasnikov, Alexei, Vladimir Shpilrain, and Alexander Ushakov (2006). "Random Subgroups of Braid Groups: An Approach to Cryptanalysis of a Braid Group Based Cryptographic Protocol". In: *Public Key Cryptography - PKC 2006*. Ed. by Moti Yung et al. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 302–314. ISBN: 978-3-540-33852-9.

Sin, Chang Seng and Huey Voon Chen (2019). "Group-Based Key Exchange Protocol Based on Complete Decomposition Search Problem". In: *Information Security Practice and Experience*. Springer International Publishing.

References IV

Tsaban, Boaz (2015). "Polynomial-time solutions of computational problems in noncommutative-algebraic cryptography". In: *Journal of Cryptology* 28.3, pp. 601–622.

Tsopanidis, Nikolaos (2020). "The Hurwitz and Lipschitz Integers and Some Applications". PhD thesis. Universidade do Porto.

Valluri, Maheswara Rao and Shailendra Vikash Narayan (2016). "Quaternion public key cryptosystems". In: *2016 World Congress on Industrial Control Systems Security (WCICSS)*, pp. 1–4.