PQC Seminar

Nonabelian Groups in Cryptography

Simran Tinani[1]

University of Zürich

CYD Doctoral Fellow, Cyber-Defence Campus

September 28, 2021

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

Introduction to the Project

- The discrete logarithm and integer factorization problems comprise the most commonly employed algorithmic problems in current cryptographic protocols. However, these problems are solved in polynomial time with a quantum algorithm.
- The construction and realization of cryptographic systems that may resist quantum attacks comprise a pressing problem in cryptography.
- Apart from lattice-based, multivariate, and code-based cryptography, nonabelian group-based cryptography has been proposed recently as a viable post-quantum paradigm, and has gained significant traction as a research topic.

Potential role of non-commutativity

Definition (Hidden subgroup problem)

Let G be a group, X a finite set, and $f : G \to X$ a function that hides a subgroup $H \leq G$, i.e. for all $g_1, g_2 \in G$, $f(g_1) = f(g_2)$ if and only if $g_1 H = g_2 H$. Using information of the evaluations of f, given via its oracle, determine a generating set for H.

- Shor's quantum algorithms for factoring and discrete logarithm relies on the ability of quantum computers to solve the HSP for finite Abelian groups.
- An efficient algorithm for the HSP in a general nonabelian group is unknown.
- The existence of efficient quantum algorithms for HSPs for certain non-Abelian groups would imply efficient quantum algorithms for the graph isomorphism problem and certain shortest vector problems (SVPs) in lattices.

Background: Nonabelian Group-based Cryptography

- The use of infinite nonabelian groups in cryptography originates in the Magyarik-Wagner (1995) protocol based on word problem for finitely presented groups.
- Foremost introduction into mainstream cryptography discourse: Anshel, Anshel and Goldfeld (1999), and Ko-Lee (2000) protocols, based on the conjugacy search problem (CSP) in Braid groups.
- CSP was seen as a natural non-abelian extension of the DLP.

Definition (Conjugacy Search Problem (CSP))

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

- It has been shown that the conjugacy search problem in a braid group cannot provide adequate security.
- It is not known whether a class of groups exists where the AAG protocol, or more generally, conjugacy-based protocols, are secure enough for real-life applications.
- To use the CSP, one wants to identify non-abelian groups where the word problem has an easy (polynomial) solution but the conjugacy search problem is algorithmically difficult to solve.
- A computationally difficult problem in one group may be trivial in another, or another representation of the same group. Research is needed to identify suitable platform groups where the chosen problem is difficult, and where a practically efficient implementation is possible.

Linear Platform Groups

- Polycyclic and metabelian groups have been suggested as platforms for protocols based on the conjugacy search and other related problems.
- When choosing a platform group, linear representations play an important role, since it is often easy to solve the underlying algorithmic problems in linear/matrix groups.

Problem 1

What is the dimension of the smallest linear representation of a general polycyclic group and a metabelian group, as compared with the group orders? What is the (quantum) complexity of finding such representation?

- Some other related computational problems that have been employed so far are the simultaneous conjugacy problem, decomposition problem, factorization problem, and word problem.
- Group theoretic generalizations of the subset sum and knapsack problems have also been devised.
- However, evidence about the difficulty of these problems for the groups considered is so far insufficient.

Problem 2

What are the classical and quantum complexities of algorithmic problems relevant to cryptography (Eg. isomorphism search problem, twisted search conjugacy problem, power conjugacy problem, subgroup membership problem), in polycyclic groups?

Nonlinear Platforms Groups

- Examples: Thompson groups, some metabelian groups
- Length-based attacks are possible for infinite platform groups. Few other recent attacks also exist that do not depend on linearity.
- Claims of resilience to known and novel nonlinear attacks in nonlinear groups require further study.

Problem 3

What are the complexities of commonly employed algorithmic problems (such as the CSP, MSP, etc.) in Thompson groups? Are Thompson groups immune to known nonlinear attacks?

A starting point: Polycyclic groups

- Polycyclic groups were suggested in 2004 as suitable platforms for non-abelian cryptography (particularly, the AAG protocol) by Eick and Kahrobaei. Some experimental evidence was also offered.

Definition (Polycyclic Group)

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

- A variety of key exchanges, digital signature systems, and secret sharing schemes using polycyclic groups have been published.

- The CSP and some related algorithmic problems are believed to be difficult in certain classes of polycyclic groups.
- There is evidence of the ineffectiveness of length-based attacks and other heuristic methods which have been employed on braid groups.
- In 2014, Cavallo and Kahrobaei constructed a family of polycyclic groups where the CSP is claimed to be NP-complete.

Definition (Power-Conjugate Presentation)

Let G be a group with generators $a_1, a_2, \ldots, a_n$. Let $I \subseteq \{1, 2, \ldots, n\}$ denote a list of indices and $m_i > 1$ be integers corresponding to elements $i \in I$. A power-conjugate presentation is a group presentation of the form

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

where the words w_{ij} are of the form $w_{ij} = a_{|i|+1}^{l(i,j,|i|+1)} \ldots a_n^{l(i,j,n)}$, with $l(i,j,k) \in \mathbb{Z}$, and $0 \leq l(i,j,k) < m_k$ if $k \in I$.

- G is polycyclic if and only if it has a polycyclic presentation.

Theorem 1 (Auslander, 1967)

Every polycyclic group has a faithful representation in $SL(n, \mathbb{Z})$ for some n.

An $n \times n$ matrix (a_{ij}) is called uni-triangular if $a_{ij} = 0$ for $j < i$ and $a_{ii} = i$ for all i. These form a nilpotent subgroup $T_n(Z)$ of $GL(n, \mathbb{Z})$

Theorem 2 (Mal'cev, 1951)

Every polycyclic group has a faithful representation in $T_n(\mathbb{Z})$ for some n.

Theorem 3 (Swan, 1967)

Every solvable subgroup of $GL(n, Z)$ is polycyclic.

Definition (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* $e_i \in \mathbb{Z}$, $0 \leq e_i \leq m_i$ *for* $i \in I$.

- Computations in polycyclic groups are done by a process called *collection*. The best known method for this process is collection from the left (Gebhardt, 2002). However, the general complexity of this process has not been determined.
- Multiplication, exponentiation and conjugation in polycyclic groups are captured by a set of recursive functions.
- For some classes of polycyclic groups, these functions may have easy to compute closed forms.

- Finite p-groups: For tuples $x = (x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n)$ and the notation $g^x = g_1^{x_1} \ldots g_n^{x_n}$, denote by $m(x, y)$ the function describing the multiplication $g^x g^y = g^{m(x,y)}$. Then, in any finite p-group, $m(x, y)$ is a polynomial in x and y (Eick, 2011).

- In general, exponents in the normal form after multiplication, exponentiation, and conjugation may blow up exponentially.

- Existing bounds for collection are dependent on several unknown constants of the intermediate stages of the algorithm, and are observed to be highly pessimistic when compared to empirical results.

Case: Two generators, x_1 and x_2

For $x, y \in G$ we use the notation $x^y := y^{-1}xy$. The group presentation is

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

In this case, collection, multiplication, exponentiation, and conjugation can be performed with a single application of a formula.

Theorem

Suppose we have $(x_1^c x_2^d)^{-1} x_1^a x_2^b (x_1^c x_2^d) = x_1^e x_2^f$. *Then the left hand side can be collected to* $x_1^g x_2^h$ *with* $g = a$ *and*

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

Case: Two generators

Theorem

Thus, $a = e \mod \text{ord}(x_1)$ *and the conjugacy search problem is reduced to solving one of the modular equations for unknowns* c *and* d*:*

$$-Dd^a + bL^c + d = f \mod \text{ord}(x_2) \text{ if } c, d > 0$$

$$-dL^a + bL^c + d = f \mod \text{ord}(x_2) \text{ if } c > 0,\ d < 0$$

$$-dD^a + bD^c + d = f \mod \text{ord}(x_2) \text{ if } c < 0,\ d > 0$$

$$-dL^a + bD^c + d = f \mod \text{ord}(x_2) \text{ if } c, d < 0$$

Example: Extra Special Group $G = (C_p \times C_p) \rtimes C_p$

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

G can also be seen as the subgroup of $Mat_3(\mathbb{F}_p)$ with 1's along the diagonal, where x corresponds to $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, y corresponds to $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, and z corresponds to $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$.

Suppose that we are given elements $g = x^a y^b z^c$ and $g\prime = x^A y^B z^C$ and $h = x^i y^j z^k$ in G. One derives the relation $z^k(x^a y^b)z^{-k} = x^a y^{-ka+kb}$.

$$\begin{aligned} g\prime = g^h &\iff x^A y^B z^C = (x^i y^j)z^k(x^a y^b z^c)z^{-k} y^{-j} x^{-i} \\ &\iff g\prime = x^i y^j x^a y^{-ka+b} z^c y^{-j} x^{-i} \\ &\iff g\prime = x^a y^{-ka+b} x^i z^c x^{-i} \\ &\iff x^A y^B z^C = g\prime = x^a y^{-ka+b+ic} z^c \end{aligned}$$

Thus, $g = x^a y^b z^c$ and $g\prime = x^A y^B z^C$ are conjugate if and only if $a = A \mod p$ and $C = c \mod p$, and the conjugacy decision problem is solved by simply checking these modular equalities. Similarly, the conjugator is easily found in polynomial time by finding a solution (i, k) to this modular equation.

Case: 3 and more generators

- A formula for $x_1^{-1}x_2^A x_3^B x_1$ can be derived and stored. Then, $x_1^{-K}x_2^A x_3^B x_1^K$ can be derived in $\mathcal{O}(\log K)$ applications of a square-and-multiply method.
- Thus, the complexity of multiplying two words with exponents bounded above by K is $\mathcal{O}(\log K)$ steps, and for r words it is $\mathcal{O}((r-1)\log K)$.

Theorem

In a finite polycyclic group of exponent K, two words in x_0, $x_1, \ldots, x_j$ can be multiplied in $\mathcal{O}(\frac{(j)!}{2}(\log K)^{2(j-2)})$ word multiplications in x_1, x_2, x_3.

Case: 3 and more generators

- On computing the exponents C and D in the normal form of $x_1^{-2}(x_2^A x_3^B)x_1^2 = x_2^C x_3^D$ explicitly, one observes that the relationship between D and the initial constants is already complicated.
- Unlike in the two generator case, a closed form for collection looks difficult to obtain, and the function involved needs to be computed recursively.
- In fact, when G is infinite, D grows exponentially in A and B, while C grows linearly with A and B. Thus in the next step, i.e. the computation of $x_1^{-4}x_2^A x_3^B x_1^4$, both the final exponents in the normal form grow exponentially with both A and B.

Classes of groups where CSP is easy

- In extra special p-groups of order p^3, it is always possible to reduce the CSP to a set of linear modular equations.
- Similarly, the system in the paper "Key Exchange Based on Complete Decomposition Problem", which uses the generalized quartenion groups, is easily broken using the relators in the group presentation, again via reduction to a system of linear modular equations in the exponents.

Problem 4

What kind of relators in a polycyclic group render collection and/or the CSP efficiently solvable?

Challenges and research scope

- Despite the availability of apparently difficult algorithmic problems, a secure cryptographic protocol using a nonabelian group is yet to be constructed.
- Several attacks such as the linear decomposition (Myasnikov and Romankov, 2015), nonlinear decomposition (Roman'kov, 2016), and cryptanalysis via algebraic spans (Ben-Zvi, Kalka and Tsaban, 2018) have been devised which retrieve the private keys without solving the underlying algorithmic problems.
- Numerous problems and methods need addressing in the area of nonabelian group-based systems before it may be considered as a viable post-quantum solution for cryptography.

Key Background Literature I

Louis Auslander.
On a problem of philip hall.
Annals of Mathematics, 86:112, 1967.

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

Bren Cavallo and Delaram Kahrobaei.
A family of polycyclic groups over which the uniform conjugacy problem is np-complete.
International Journal of Algebra and Computation, 24(04):515–530, 2014.

Key Background Literature II


Bettina Eick.
Collection by polynomials in finite p-groups.
01 2012.


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


Benjamin Fine, Maggie Habeeb, Delaram Kahrobaei, and Gerhard Rosenberger.
Aspects of nonabelian group based cryptography: a survey and open problems.


Volker Gebhardt.
Efficient collection in infinite polycyclic groups.
J. Symb. Comput., 34(3):213–228, September 2002.

Key Background Literature III


A. I. Mal'tsev.
On some classes of infinite soluble groups.
Mat. Sb. (N.S.), 28(70):567–588, 1951.


Alexei Myasnikov and Vitalĭ Roman'kov.
A linear decomposition attack.


Alexei Myasnikov, Vladimir Shpilrain, and Alexander Ushakov.
Group-based cryptography.
Springer Science & Business Media, 2008.


Alexei Myasnikov, Vladimir Shpilrain, and Alexander Ushakov.
Non-Commutative Cryptography and Complexity of Group-Theoretic Problems.
American Mathematical Society, USA, 2011.

Key Background Literature IV


Vitaliĭ Roman'kov.
A nonlinear decomposition attack.


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.


R. Swan.
Representations of polycyclic groups.
1967.

Thank you!