Student Exchange Event

The Conjugacy Search Problem and Cryptographic Applications

Simran Tinani[1]

University of Zürich

CYD Doctoral Fellow, Cyber-Defence Campus

November 30, 2021

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

Introduction to the Project

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

Background: Abelian Groups in Cryptography

Definition (Discrete Logarithm Problem)

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

- Popularly used platforms for the DLP are **multiplicative groups of finite fields** and **elliptic curve groups over finite fields**.
- The best classical algorithms for the DLP in a general finite group of order N have complexity $\mathcal{O}(\sqrt{N} \log N)$. Shor's algorithm provides a polynomial-time quantum solution.
- Shor's quantum algorithms for factoring and and the DLP rely on the ability of quantum computers to solve the "Hidden Subgroup Problem" for finite Abelian groups.

Why look to 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 $g_1H = g_2H$. Using information of the evaluations of f, given via its oracle, determine a generating set for H.

- 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

- Foremost introduction of nonabelian groups into mainstream cryptography discourse: Anshel, Anshel and Goldfeld (1999), and Ko-Lee (2000) protocols, based on the conjugacy search problem in Braid groups.
- The CSP can be seen as a natural non-abelian extension of the DLP. To reflect this analogy, it is common to use the notation $g^x := g^{-1}xg$ for $g, x \in G$.

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.

Protocol 1 (Ko-Lee protocol)

G is a suitable finitely generated group, with subgroups A and B that commute element-wise, i.e. $ab = ba \; \forall \; a \in A, \; b \in B$. A base element $w \in G$ is chosen. The parameters G, A, B, and w are made public.

- *Alice chooses a secret element $a \in A$, and publishes $w^a = a^{-1}wa$.*
- *Bob chooses a secret element $b \in B$, and publishes $w^b = b^{-1}wb$.*
- *Alice computes $K_A = (w^b)^a$, and Bob computes $K_B = (w^a)^b$.*

Since a and b commute, we have a common shared secret $K_A = K_B = a^{-1}b^{-1}wab$.

- The security of the CSP in a Braid group has been shown to be inadequate. It is unknown whether a class of groups exists where the CSP is secure enough for real-life applications.
- Several attacks such as the linear decomposition, nonlinear decomposition, and cryptanalysis via algebraic spans have been devised which retrieve the private keys without solving the underlying algorithmic problems. However, the actual difficulty of the CSP has not been sufficiently investigated.
- Some popular nonabelian platforms are **polycyclic groups, metabelian groups, some *p*-groups, Thompson groups, and matrix groups.**
- In this presentation we discuss conditional reductions of and solutions to the CSP in three classes of groups, namely **2-polycyclic, extraspecial *p*-groups, and matrix groups**.

Polycyclic groups

- Polycyclic groups were suggested in 2004 as suitable platforms for non-abelian cryptography by Eick and Kahrobaei. 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.

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

Definition (Polycyclic Group)

A G be a group with generators $a_1, a_2, \ldots, a_n$ and $I \subseteq \{1, 2, \ldots, n\}$ is called polycyclic if it has a presentation of the form

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

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 $k \in I$.

Every element a of G can be represented uniquely in a **normal form**, $a = a_1^{e_1} a_2^{e_2} \ldots a_n^{e_n}$, where $e_i \in \mathbb{Z}$, $0 \leq e_i \leq m_i$ for $i \in I$.

2-Polycyclic Groups

In the case $n = 2$, with two generators x_1 and x_2 with two relations $x_1^{-1}x_2x_1 = x_2^L$ and $x_1x_2x_1^{-1} = x_2^D$. The group presentation is

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

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

Theorem 1

If $c,\ a > 0$, the 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 $g = a \mod C$ and $h = -dL^a + bL^c + d \mod N_2$.

Theorem 2

If $N_2 = \mathrm{ord}(x_2)$ is finite, solving the CSP is at most as hard as solving a DLP $\mod N_2$. If $N_2 = \infty$, the CSP reduces to an exponential Diophantine equation over $\mathbb{Z}$.

p–groups

- A finite group with order a power of a prime p is called a p-group.
- 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 old and newly conceived cryptographic protocols.

Example: Extra Special p-groups of order p^3

In extra special 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 3

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 $B - b = -ka + ic \mod p$. Thus, the CSP has a polynomial time solution in $M(p)$ and $N(p)$.

p-groups

- Several p-groups are constructed by combining smaller p-groups by taking direct, semidirect and central products.
- Recall that the Pohlig-Hellman algorithm “decomposes" the DLP in a group of smooth order to several smaller prime DLP’s.
- Algorithmic problems can usually be decomposed when a direct product decomposition product is available.
- For the CSP, semidirect and central products also allow this. Our results show that a selected platform must be “atomic", or have a decomposition that is difficult to compute.

Central and Semidirect Decompositions

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

Theorem 4

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.

Definition

A group G is said to be a ***semidirect product*** *of its subgroups H and K if H is normal in G, and $G = HK$. Equivalently, G may be seen as the set $H \times K$ equipped with the operation $(h_1, k_1) \cdot (h_2, k_2) = (h_1 \cdot k_1 h_2 k_1^{-1},\ k_1 k_2)$. We will write $G = H \rtimes K$ to denote such a semidirect product.*

Theorem 5

Let G be a semidirect product $G = H \rtimes K$, where H is a finite abelian group and K is any group. Then, the CSP in G reduces in polynomial time to a set of DLP's in H and a CSP in K.

Matrix Groups

- Matrix groups over finite fields have played an important role in cryptography. The DLP in $GL_n(\mathbb{F}_q)$ was studied by Menezes-Wu and Freeman and shown to be no more difficult than the DLP over a small extension of $\mathbb{F}_q$.

- 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 $Y = Z^{-r}XZ^r$ and $Z^{-s}XZ^s$, 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.

Matrix Groups

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 by Menezes-Wu) such that $J_Z = PZP^{-1}$, where J_Z is the Jordan Normal form of Z.

Theorem 6

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 $\mathbb{F}_{q^k}$.

This method gives a solution to a special case of the Anshel–Anshel–Goldfeld and Ko–Lee protocols over $GL_n(\mathbb{F}_q)$.

Conclusion

- 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 (like extraspecial p–groups) as platforms, and a minimum complexity of a protocol designed based on the CSP. For instance, Theorem 6 implies that for a protocol over a matrix group, conjugators must be picked from a subgroup with at least two generators.
- A selected platform must be "atomic", or have a decomposition that is difficult to compute.
- The CSP in a 2–polycyclic group may already have reasonable difficulty, and suggests that with more than two generators a polycyclic group may indeed offer promising security levels.

Key Background Literature I

Iris Anshel, Michael Anshel, and Dorian Goldfeld.
An algebraic method for public-key cryptography.
Math. Res. Lett., 6(3-4):287–291, 1999.

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

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

David Freeman.
The discrete logarithm problem in matrix groups.
2004.

Key Background Literature II

- 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.

- Alfred Menezes and Yihong Wu.
  The discrete logarithm problem in $GL(n, q)$.
  Ars Comb., 47, 1997.

- 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.

Key Background Literature III

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

Vitaliĭ Roman'kov.
A nonlinear decomposition attack.

Thank you!