Contemporary algebraic and geometric techniques
in coding theory and cryptography
Summer school — July 18-22, 2022
Università degli Studi della Campania "Luigi Vanvitelli"

Group-based cryptography: from algorithmic problems to cryptographic applications

Marialaura Noce

University of Salerno
Italy

Abstract

In cryptography most famous protocols (RSA, Diffie-Hellman, and elliptic curve methods) depend on the structure of commutative groups and they are related to the difficulty to solve integers factorization and discrete logarithms. In 1994 Shor provided a quantum algorithm that solves these problems in polynomial time. For this reason, researchers were motivated to find alternative methods for constructing cryptosystems. One of them is based on non-commutative cryptography, which does not operate over the integers. Hence, for security reasons, in the last decade new cryptosystems and key exchange protocols based on non-commutative cryptographic platforms have been developed and the complexity of algorithmic problems have made available families of groups as platform groups for cryptographic protocols.
The purpose of this talk is on the one hand to survey some algorithmic problems in group theory motivated by cryptography. On the other hand, to present the actual state of some group based cryptography. We will mainly focus on the class of Engel groups and braid groups, presenting new results and some open problems with a view towards applications to cryptography (see [1, 2, 3]). For this reason, in the following we will explain more in details algorithmic problems in groups, Engel groups, and braid groups.

Algorithmic problems in groups

The area of group theory that studies group as combinatorial objects (using group presentation with generators and relators) is called *combinatorial group theory*, and it has been studied in order to find solutions to *decision problems* (problems with "yes" or "no" answer). To understand better this, we first need some preliminary definitions.

Let $X = \{x_1, \ldots, x_n\}$ and $X^{-1} = \{x_1^{-1}, \ldots, x_n^{-1}\}$. A word w in the set $X \cup X^{-1}$ is *freely reduced* over X if it contains no adjacent symbols xx^{-1} or $x^{-1}x$. The free reduction of a word w on $X^{\pm}$ is obtained by replacing all subwords xx^{-1} or $x^{-1}x$ from w by the empty string to form its free reduction. The resulting word is called the *free reduction of* w. Given two words w, w' on $X^{\pm}$, we write $w \sim w'$ to denote that the free reductions of w and w' are the same. For example: $abb^{-1}b \sim aa^{-1}ab^{-1}bb \sim ab$.

We define the free group $F(X)$ by the set of freely reduced words on $X^{\pm}$, where the multiplication of two elements $w_1, w_2 \in F(X)$ is the free reduction of the word $w_1 w_2$. The identity element in $F(X)$ is the empty string ε. Given a set R of words from $F(X)$, we let $\langle\langle R \rangle\rangle$ denote the subgroup of $F(X)$ generated by all conjugates of the elements from R. We say that a group G has the presentation $\langle X \mid R \rangle$ if it is isomorphic to the quotient group $F(X)/\langle\langle R \rangle\rangle$. We write $G = \langle X \mid R \rangle$. The elements from R are called the *relations of the presentation*. If both X and R are finite then we say that $\langle X \mid R \rangle$ is a *finite presentation*. Roughly speaking, the presentation $\langle X \mid R \rangle$ indicates that we can take words from $F(X)$ and delete or insert subwords from $\langle\langle R \rangle\rangle$ without changing the element of the word represents in G.

With this in mind, given a group $G = \langle X \mid R \rangle$, we can define the following three decision problems introduced by Dehn in 1911:

- Word Problem: For any $g \in G$, determine if g is the identity element of G.
- Conjugacy Problem: For any $x, y \in G$, determine if x and y are conjugate.
- Isomorphism Problem: Let G and G' be groups given by finite presentations, determine if G is isomorphic to G'.

The above Dehn decision problems have a dual in the form of a *search problem*, that is a problem in which the solution gives an element of the group as a witness to the positive answer. For example, given a group G and $a, b \in G$ where a is a conjugate of b, the *conjugacy search problem* is the problem to find an element $c \in G$ such that $a^c = c^{-1}ac = b$.

Engel group-based cryptography

Engel groups play an important role in group theory since these groups are closely related to the Burnside problems. We recall that an element g of a given group G is said to be *right Engel* if for every $x \in G$ there exists an integer $n = n(g,x) \geq 1$ such that $[g, {}_n x] = 1$, where the commutator $[g, {}_n x]$ is

defined recursively by the rules $[g,x] = g^{-1}g^x$ and

$$[g,_n x] = [g,x,\overset{n}{\ldots},x] = [[g,x,\overset{n-1}{\ldots},x],x]$$

if $n > 1$. Similarly, g is a *left Engel* element if the variable x appears on the left. A group is said to be an *Engel group* if all its elements are right Engel or, equivalently, left Engel.
We will present the state of the art of Engel group-based cryptography and propose several open problems.

Braid group-based cryptography

Braid groups were first defined by Artin in 1947. A braid group $\mathscr{B}_n$ on n strands is the group with the following presentation:

$$\mathscr{B}_n = \left\langle \sigma_1, \sigma_2, \ldots, \sigma_{n-1} \;\middle|\; \begin{array}{ll} \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j, & |i-j| = 1 \\ \sigma_i\sigma_j = \sigma_j\sigma_i, & |i-j| > 1 \end{array} \right\rangle.$$

Graphically a braid on n strands can be seen as a collection of n paths in a cylinder joining n distinguished points at the top of the cylinder with n points at the bottom, with the restrictions that the paths do not touch each other and run monotonically in the vertical direction. We can obtain the product of two braids by gluing the bottom of the first braid cylinder with the top of the second braid cylinder. In this setting, a generator σ_i is the braid in which only the strands i and $i+1$ cross once, and its inverse σ_i^{-1} is the braid in which the strands i and $i+1$ cross in the opposite sense. (See Figure 1).

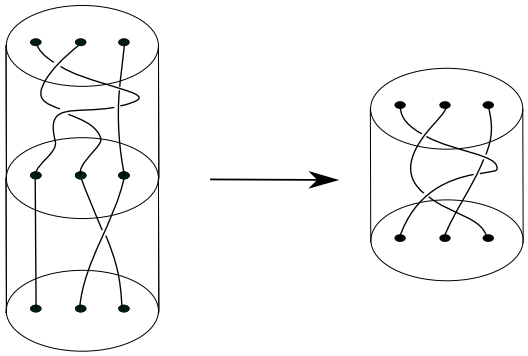

Figure 1: How to multiply the braids $\sigma_1\sigma_2^{-2}\sigma_1$ and σ_2.

In the past decades, braid groups attracted a lot of attention in cryptography, in particular for authentication schemes and digital signatures. Among others, we will present some protocols based on the root extraction problem in

braids. The root problem is a decision problem that asks whether given a braid β and an integer k, there exists a braid α such that $\alpha^k = \beta$. We will first go through an historical overview of the approaches to this problem and then we will describe the proposed cryptosystems that claim to be based on this problem. We will see that some of them can be attacked without solving the root extraction problem and that others are not safe if the parameters are not carefully chosen.

References

[1] M. Cumplido, D. Kahrobaei, M. Noce, The root extraction problem in braid group-based cryptography, submitted, available at `arxiv.org/pdf/2203.15898` (2022).

[2] D. Kahrobaei, R. Flores, M. Noce, Group-based Cryptography in the Quantum Era, accepted in *Notices of the American Mathematical Society*, available at `arxiv.org/abs/2202.05917` (2022).

[3] D. Kahrobaei, M. Noce, Algorithmic problems in Engel groups and cryptographic applications, *International Journal of Group Theory* **9** no. 4 pp. 231-250 (2020).

Keywords: Algorithmic problems in groups, Engel groups, braid groups