Introduction to Cryptography via Braid Groups

Eonkyung Lee
(Sejong University, eonkyung@sejong.ac.kr)

Abstract

This talk introduces modern cryptology via braid groups. First, we see cryptographic schemes, especially designed using braid groups. In braid groups, the conjugacy problem is known as a pretty hard problem to solve. Based on variants of this problem, there have been proposed key agreement protocols, public-key encryption schemes, pseudorandom number generator, pseudorandom synthesizer, entity authentication schemes, and so on.

Second, we see cryptanalysis of these schemes in two steps. At the first step, we see attacks mounted on them. Here, we notice that these attacks are different from the prior attacks in finite abelian groups. Usually, probability argument is used in many cases when analyzing attacks. However, it is not in braid-group-based cryptanalysis. This motivates to need a kind of analysis tools. Therefore, at the second step, we see such a tool and how to concretely analyze attacks in braid groups by using it.