Twenty years of attacks on unipotent elements

Şükrü Yalçınkaya
İstanbul University

Abstract

A *black box group* is a black box (or an oracle, or a device, or an algorithm) operating with binary strings of uniform length which encrypt (not necessarily in a unique way) elements of some finite group. Group operations, taking inverses and deciding whether two strings represent the same group elements are done by the black box. In this context, a natural task is to find a probabilistic algorithm which determines the isomorphism type of a group within given arbitrarily small probability of error. More desirable algorithms, *constructive recognition algorithms*, are the ones producing an isomorphism between a black box copy of a finite group and its natural copy.

In this talk, I will discuss the recognition problem for the black box groups of Lie type and a solution of a twenty year old problem in the computational group theory, that is, a construction of a unipotent element in a black box group encrypting PSL_2 leading to a recognition of the black box groups PSL_2. This is a joint work with Alexandre Borovik.