JONATHAN GRYAK, The Graduate Center, CUNY
On the Conjugacy Problem in Certain Metabelian Groups

Non-commutative cryptography seeks to develop cryptosystems that utilize algorithmic problems from group theory for their hardness assumptions. The security of such systems is contingent upon the computational complexity of the chosen algorithmic problem in the underlying platform group.

In this talk, we analyze the computational complexity of the conjugacy search problem in a certain family of metabelian groups. We prove that in general the time complexity of the conjugacy search problem for these groups is at most exponential. For a subfamily of groups we prove that the conjugacy search problem is polynomial. We also show that for some of these groups the conjugacy search problem reduces to the discrete logarithm problem.

This is a joint work with Delaram Kahrobaei and Conchita Martinez-Perez.