“Computational/Algorithmic Problems in Geometric Group Theory and their applications in Post-quantum Cryptography”

Abstract: The National Security Agency (NSA) in August 2015 announced plans to transition to post-quantum algorithms “Currently, Suite B cryptographic algorithms are specified by the National Institute of Standards and Technology (NIST) and are used by NSA’s Information Assurance Directorate in solutions approved for protecting classified and unclassified National Security Systems (NSS). Below, we announce preliminary plans for transitioning to quantum resistant algorithms.” [https://www.nsa.gov/ia/programs/suiteb_cryptography/]

Shortly after the National Institute of Standardization and Technology (NIST) announced a call to select standards for post-quantum public-key cryptosystems.

The academic and industrial communities have suggested as the quantum-resistant primitives: Lattice-based, Multivariate, Code-based, Hash-based, Isogeny-based and group-based primitives.

In this talk I will focus on some ideas of group-based primitives. The one which was proposed to NIST is by SecureRF company based in Connecticut, among its founders there is a number theorists (Goldfeld) and two group theorists (Anshel and Anshel). They proposed a digital signature using a hard algorithmic problem in braid groups, namely conjugacy problem.

I will then give a survey of some other suggested group-based cryptosystems that could be claimed as post-quantum cryptosystems. I particularly focus on Right Angel Artin groups (a.k.a. RAAGs), which has been of central attention to geometric group theorists recently. Such groups are defined using graphs, and therefore some of their algorithmic problems could be equivalent to graph theoretic problems, for example isomorphism problem and homomorphism problem. I will present a joint work with Flores and Koberda, in which we work on complexity of algorithmic problems in RAAGs and give applications to cryptography.