Mathematics of Post-Quantum Cryptography

Algebraic Cryptography Center at Stevens Institute of Technology

Nelly Fazio

(The City College of New York)

Group-Theoretic Cryptography: *Respice, Adspice, Prospice*

Abstract:

This talk outlines an ongoing research effort towards a probabilistic framework for the application of infinite groups to cryptography.

We start by analyzing a classical group-theoretic construction for public-key cryptosystems from a complexity-theoretic perspective. We then suggest a way of casting some of the standard computational problems from group theory in terms of probabilistic cryptographic assumptions---an essential ingredient for a formal security analysis. Next, we present a new group-theoretic assumption, inspired by recent advances in lattice-based cryptography. Our assumption is based on a problem that we term ``Learning Homomorphisms from Images with Errors" (LHIE), which can be viewed as a generalization of the ``Learning With Errors" (LWE) problem from the setting of vector spaces and linear transformations to the setting of groups and homomorphisms. We conclude by discussing a new group-theoretic public-key cryptosystem, whose security is based on the hardness of the LHIE problem.

Algebraic
Cryptography
Center

STEVENS
Institute of Technology