1060-20-223 **Nelly Fazio** (fazio@cs.ccny.cuny.edu), Department of Computer Science, 160 Convent Avenue, Shepard Hall 279, New York, NY 10031, and **William Skeith*** (wes@cs.ccny.cuny.edu), Department of Computer Science, 160 Convent Ave, NAC Room 8 206, New York, NY 10031.

Group-Theoretic Cryptography: Respice, Adspice, Prospice.

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 outline a new approach for finding cryptographically-suitable group-theoretic assumptions, inspired by recent advances in lattice-based cryptography. The framework relies on a new 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 how this assumption yields group-theoretic public-key cryptosystems, and describe some of the remaining challenges in this effort. (Received March 30, 2010)