1046-68-1974 **Nelly Fazio*** (fazio@cs.ccny.cuny.edu), Department of Computer Science, The City College of New York, 160 Convent Ave, NAC 8/206, New York, NY 10031. *Bilinear Groups and Algebraic Cryptography.* Preliminary report.

The discovery of bilinear groups—that is, cryptographic groups equipped with a bilinear map—has enabled the resolution of long-standing open problems in cryptography, while at the same time opening the way to a variety of novel applications. Despite their power and versatility, however, essentially all known bilinear groups are based on the algebraic structure of a single mathematical construct, namely elliptic (or hyperelliptic) curves.

In this talk, we start by taking a closer look at how bilinearity can be exploited to achieve the range of cryptographic properties required by the many applications of bilinear groups. Next, we discuss some preliminary efforts in investigating the feasibility of constructing bilinear groups based on alternative algebraic structures in combinatorial group theory. (Received September 16, 2008)