Using Abelian Varieties for Multiparty non-Interactive Key Exchange

Alice Silverberg, University of California, Irvine

We give a framework for constructing an efficient non-interactive key exchange protocol for n parties for any $n \geq 2$. Our approach is based on the problem of computing isogenies between isogenous elliptic curves. Our obstruction to obtaining a working protocol is the open mathematical problem of finding an efficient algorithm that takes as input an abelian variety presented as a product of isogenous elliptic curves, and outputs an isomorphism invariant of the abelian variety. This is joint work with Dan Boneh, Darren Glass, Daniel Krashen, Kristin Lauter, Shahed Sharif, Mehdi Tibouchi, and Mark Zhandry.