1147-11-168 **Shahed Sharif*** (ssharif@csusm.edu), Dept. of Mathematics, 333 S. Twin Oaks Valley Rd., San Marcos, CA 92069. *Multiparty Non-Interactive Key Exchange From Isogenies on Elliptic Curves.*

We describe 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, which is believed to be difficult. We describe an open mathematical problem which is the only obstruction to a working protocol; namely, an efficiently computable isomorphism invariant of a product of isogenous elliptic curves. (Received January 06, 2019)