1125-14-596 **Dustin Moody*** (dustin.moody@nist.gov), NIST, 100 Bureau Drive, Computer Security Division, Gaithersburg, MD 20877, and **Daniel Shumow**, Microsoft. *Isogenies of Edwards Curves.*

Isogenies are the structure preserving maps between elliptic curves. As such, isogenies play a key role many areas of elliptic curve cryptography. For example, they have been proposed as a mathematical primitive in the construction of hash functions, pseudo-random generators, as well as post-quantum public key cryptosystems. In this work, we present a new isogeny formula for elliptic curves known as Edwards curves. The new formula is twice as efficient than using the standard Velu formula for isogenies. We examine the potential applications of the Edwards isogeny formula in cryptography. (Received September 12, 2016)