1092-11-21 **Dustin Moody*** (dustin.moody@nist.gov), 100 Bureau Drive, Stop 8930, Gaithersburg, MD 21703. *Applications of Edward Isogenies in Cryptography.* Preliminary report.

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 new post-quantum public key cryptosystems.

Moody and Shumow have presented a new isogeny formula for elliptic curves known as Edwards curves. This new formula is more efficient than using the standard Velu formula for isogenies. In this work, we examine applications of the Edwards isogeny formula in cryptography. (Received June 17, 2013)