1125-14-1127 **Kristin E. Lauter*** (klauter@microsoft.com). *The Future of Curves in Cryptography (?).*

Over the last decade, the use of Elliptic Curve Cryptography (ECC) has become standard across the industry, used for example for digital signatures to assure identity and authenticity, and for key exchange to set up secure browser sessions. ECC was proposed 3 decades ago, but widespread adoption was prompted by government-issued Suite B requirements in 2006. In the meantime, practical aspects of using higher genus curves for cryptography have also been explored, and it has been demonstrated that Jacobians of genus 2 curves can even match the performance of ECC at the same security levels. But recently, government-issued recommendations (CNSA Suite) have shifted to require larger key sizes for RSA and ECC-based systems based on the threat of quantum attacks, while awaiting the outcome of an international competition to select new "Post-Quantum" Cryptographic (PQC) systems. This talk will discuss ongoing work on assessing security of ECC and higher genus curves against both quantum and classical attacks. (Received September 15, 2016)