1125-11-903 **David Jao*** (djao@uwaterloo.ca), 200 University Ave. W, Waterloo, Ontario N2L3G1, Canada.

Post-quantum public-key cryptography based on isogenies between supersingular elliptic curves.

According to our current knowledge of quantum mechanics, computers based on quantum phenomena can potentially solve certain problems much more quickly than is possible on any classical computer, including most of the mathematical problems upon which current public-key cryptosystems are based. In response, researchers have developed *post-quantum cryptosystems* — alternative cryptosystems based on new mathematical problems which are hard to solve even on a quantum computer. Mainstream post-quantum cryptosystems can be categorized into several broad families: lattice-based, code-based, hash-based, and schemes based on multivariate polynomials. A fifth family of cryptosystems, based on isogenies between supersingular elliptic curves, offers a promising alternative to these schemes. Compared to other schemes, isogeny-based cryptosystems are unique in the following ways: they achieve the smallest possible public key size; they are based on number-theoretic complexity assumptions; implementations can leverage existing elliptic curve cryptography libraries; and the security level has a simple linear relationship to the key size. In this presentation we survey existing constructions of isogeny-based cryptosystems and present recent results on key sizes, performance, and security. (Received September 13, 2016)