1147-11-596 **David Jao*** (djao@uwaterloo.ca), 200 University Ave. W, Waterloo, Ontario N2L3G1, Canada.
The SIDH cryptosystem.

Isogeny-based cryptography represents one of the few number-theoretic approaches to cryptography that remains relevant in the context of post-quantum cryptosystems, schemes that are intended to be secure against adversaries with efficient universal quantum computers. Compared to other post-quantum cryptosystems, isogeny-based cryptography has smaller keys, and simple, straightforward parameter selection involving only one tunable security-sensitive parameter. In this talk, we survey one existing proposal for isogeny-based cryptography, the Supersingular Isogeny Diffie-Hellman (SIDH) proposal of Jao and De Feo, whose underlying hard problem is a variant of the Charles-Goren-Lauter cycle finding problem on Pizer's family of expander graphs. We demonstrate some explicit examples of SIDH computations, and discuss the current status of the security of the cryptosystem against classical and quantum adversaries. (Received January 26, 2019)