Topics in Cryptography:
Pairing Based Cryptography

Instructor: David Jao, djao@math.uwaterloo.ca, MC 5038, x32493.

Description: Introduction to the mathematics of elliptic curve cryptography, with emphasis on cryptographic pairings and pairing based cryptography. Topics to be covered include definitions, proofs of basic properties, curve construction, implementation issues, and protocol design.

Course outline:

- *Mathematics of elliptic curves:* Divisors, linear equivalence
- *Definition of pairings:* Weil pairing, Tate pairing
- *Construction of pairings:* Curve selection, embedding degree
- *Implementation of pairings:* Miller's algorithm, precomputation optimizations
- *Protocols:* Identity based encryption, short signatures, group signatures, key agreement

Prerequisites: Knowledge of finite fields is assumed. Familiarity with elliptic curve cryptography is helpful but not required.

Textbook: No textbook.

Evaluation: Grades will be based on final projects consisting of a class presentation and a written report. No exams.