Atelier « La sécurité informatique et la cryptographie »
12–16 avril 2010

Workshop on Computer Security and Cryptography
April 12–16, 2010

Choosing curves and coordinates for pairing computation

Michael Naehrig

Cryptography Group
Microsoft Research
One Microsoft Way
Redmond, WA 98052
USA

michael@cryptojedi.org

For almost a decade now, pairings are used in cryptographic protocols that provide special functionality. In the meantime, many improvements to Miller's algorithm for computing pairings on elliptic curves have led to remarkable increase in the efficiency of such protocols.

In this talk, we will discuss the options for choosing pairing-friendly elliptic curves and corresponding coordinate systems for implementing efficient pairing algorithms. We will include recent developments like pairings on Edwards curves and new explicit formulas for pairing functions on curves with high degree twists.