Séminaire des doctorants en Théorie des Nombres
"Jouve-Pazuki"

Bordeaux, IMB - Jeudi 7 Février 2013 - Salle 2 - 15h15-16h15

Pairing-friendly Elliptic Curves.

Min Sha

Pairings on elliptic curves over finite fields have been used to construct many novel cryptographic systems for which no other practical implementation is known. We call those elliptc curves suitable for implementing pairing-based systems pairing-friendly elliptic curves. In this talk, first I will give a concise survey of pairing-friendly elliptic curves, then I will talk about some of my recent work, such as a new upper bound for the number of isogeny classes of such curves and heuristic analysis about the Cocks-Pinch method, which is a very popular construction of pairing-friendly elliptic curves