Arithmetic on Abelian and Kummer varieties

Damien Robert (INRIA, Bordeaux)

Abstract:

In the use of elliptic curves and abelian varieties for public key cryptography, the speed of the arithmetic play a preponderent role in the efficiency of the cryptosystem. Currently it seems that Kummer surfaces (represented by a theta model of level 2) have a slight edge against elliptic curves.

In this talk I will discuss the arithmetic of Abelian and Kummer varieties given by theta models of level 4 and 2. In the first part I will outline a brief review of Mumford’s theory of algebraic theta functions. We will see how a geometric condition, like the fact that a model is projectively normal, can actually help for the arithmetic. In the second part I will adopt a more elementary point of view to explain how we can use the mathematical tools described above to speed-up the arithmetic of Kummer and Abelian varieties in practice.

This is a joint work with David Lubicz.