The end of paring based cryptography using small characteristic finite fields

Gora Adj
Departamento de Computación del CINVESTAV
gora@computacion.cs.cinvestav.mx

Abstract

A necessary condition for the security of a cryptosystem based on bilinear pairings over elliptic or hyperelliptic curves is that the discrete logarithm problem in the subjacent curve subgroups and the finite fieldsubgroup must be hard.

In recent years, there have been several dramatic improvements in algorithms for computing discrete logarithms in small characteristic finite fields, that consequently placed the security of the small-characteristic pairing-based cryptography in a state of uncertainty.

In this talk, we will discuss these new algorithms and tell how they drastically impact the security of cryptosystems based on pairings that utilize finite fields of small characteristic.