Computing Pairings via Elliptic Nets

Emmanuel Fouotsa[1]

The University of Bamenda, Uba
Higher Teacher Training College, Bambili
P.O;Box 39 Bambili (Cameroon)
emmanuelfouotsa@yahoo.fr

Abstract. pairings are bilinear maps defined over groups of points of an elliptic curves. They enables many applications in cryptography and the Miller algorithm is the main tool for their computation. In this talk, we explain an alternative way of computing these maps based on the work of K. Stange and then study some recent optimizations.
Key words: Pairings-Miller Algorithm-Elliptic Nets.

References:

1. Katherine Stange. "Tate pairing via elliptic nets". Pairing Conference 2007, LNCS 4575. pp. 329-348, (2007).
2. N.Ogura, N. Kanayama, S. Uchiyama and E. Okamoto. Cryptotographic pairings on Elliptic nets, IWSEC 2011, LNCS 7038, pp. 6578, 2011