Pseudo r - Adic Non Adjacent Form for Scalar Multiplication on Koblitz Curves

ABSTRACT

In ECC, scalar multiplication is the dominant operation, namely computing nP from a point P on an elliptic curve where the multiplier n is an integer, defined as the point resulting from adding P + P + … + P , n times. The □-NAF proposed by Solinas, is one of the most efficient algorithms to compute scalar multiplications on Koblitz curves. In this paper, we introduced an equivalent multiplier to T-NAF namely pseudoTNAF. It is based on the idea of transforming the T-NAF expression to a reduced T-NAF that has been done by some researchers. It can eliminate the elliptic doublings in scalar multiplication method, and double the number of elliptic additions. We provide the formula for obtaining a total of lattice points in Voronoi region of modulo r + st where r + st an element of ring Z (T). This helps us to find all the multipliers n that based on T-NAF. We also discuss the estimation of operational costs when using pseudoTNAF as a multiplier of scalar multiplication.

Keyword: Scalar multiplication; Koblitz curve; Density; Voronoi region; Hamming weight