Maximum and minimum norms for τ-NAF expansion on Koblitz Curve

ABSTRACT

Background/Objectives: The scalar multiplication in Elliptic Curve Cryptosystem (ECC) is the dominant operation of computing integer multiple for an integer n and a point P on elliptic curve. In 1997, Solinas[4] introduced the τ-adic non-adjacent form (τ-NAF) expansion of an element n of ring Z(τ) on Koblitz Curve. However in 2000, Solinas estimated the length of τ-NAF expansion by using maximum and minimum norms that obtained by direct evaluation method. In 2014, Yunos et al.9 introduced the formula of norm for every τ-NAF to improve this method. However, a lot of combination of norm should be considered when length of expansion is more than 15. So, the objective of this paper is to built the formulas to calculate the number of maximum and minimum norms for τ-NAF occurring among of all elements in Z(τ). Application/Improvement: With these formulas, we can estimate the length of τ-NAF expansion more accurately.

Keyword: τ-adic non-adjacent form (τ-NAF); Koblitz Curve; Maximum and minimum norms