Improvement to scalar multiplication on Koblitz curves by using pseudo τ-adic non-adjacent form

ABSTRACT

Pseudo Ű-adic non-adjacent form (pseudoTNAF) for elliptic scalar multiplication on Koblitz Curve was developed by Faridah et al. since 2012. This is analog to binary method and alternative to Ű-adic non-adjacent form (TNAF) and reduced Ű-adic non-adjacent form (RTNAF) methods that was produced by Solinas at the year 1997 and 2000 respectively. The objective of this paper is to improve the scalar multiplication algorithm with pseudoTNAF that was published earlier. Consequently, to prove that the density of the pseudoTNAF Hamming weights (HW) is less four percents than the HW of both TNAF and RTNAF.

Keyword: Hamming weight; Koblitz curve; Non adjacent form; PseudoTNAF; Scalar multiplication