An even and odd situation for the multiplier of scalar multiplication with pseudo τ-adic non-adjacent form

ABSTRACT

An algorithm was developed for elliptic scalar multiplication (SM) on Koblitz curve where the multiplier of SM is in the form of Pseudo Ű-adic Non-Adjacent Form (pseudoTNAF). This expansion is equivalent to Ű-adic Non-Adjacent Form (TNAF) and Reduced Ű-adic Non-Adjacent Form (RTNAF) that was produced by Solinas in the year 1997 and 2000 respectively. Some properties for the multiplier of SM was proposed in order to guess the secret message. For the same reason, the objective of this paper is to give five new properties for such multiplier.

Keyword: Koblitz curve; Scalar multiplication; Ű-adic Non-Adjacent Form (pseudoTNAF)