Generalizing equivalent elliptic divisibility sequence for elliptic net scalar multiplication

ABSTRACT

Elliptic Net is a powerful method to compute cryptographic pairings or scalar multiplication. The elliptic net rank one originated from the nonlinear recurrence relations, also known as the elliptic divisibility sequence. In this paper, a generalization of equivalent sequences is defined. Combining the new generalization with a few restrictions on the initial value, the paper further proposes and discusses an elliptic net scalar multiplication of rank one for Weistrass equation and non-singular elliptic curve.

Keyword: Equivalence; Net; Divisible; Polynomials