Scalar multiplication via elliptic nets with application to cryptography

ABSTRACT

The net theory based on elliptic sequences is widely used as a computational tool in cryptographic pairing. The theory of this net is originated from non-linear recurrence relations which also known as elliptic divisibility sequences. In this study, at first we review the history of elliptic net such as recurrence sequences and elliptic divisibility sequences with the important properties. Next, we address scalar multiplication in elliptic curve cryptography. We further with division polynomials used in the elliptic net and followed by an elliptic net scalar multiplication. Finally, this study stated the future research directions of elliptic net and its scalar multiplication. The findings from this study will help other researchers to explore and to expand recent topics of applied mathematical sequences in cryptography.

Keyword: Divisibility; Elliptic; Polynomial; Rank; Scalar