Tripling formulae of elliptic curve over binary field in Lopez-Dahab model

ABSTRACT

In elliptic curve cryptosystem (ECC), scalar multiplication is the major and most costly operation. Scalar multiplication involves with point operations such as point addition, point doubling, and point tripling. Scalar multiplication can be improved by using efficient point operations. This research focuses on point tripling operation for elliptic curves over the binary field in Lopez-Dahab (LD) model. Currently, there is no existing tripling formula for this model. Traditionally, tripling is computed using one doubling followed by one addition (i.e. 3P=2P+P) with cost of 18M+8S, where M is field multiplication and S is field squaring. In this paper, we proposed tripling formulae with cost of 12M+7S. We proved the formulae and proposed its algorithm. The tripling saved 6M+1S which contribute to cost reduction in multiplication and squaring by 33% and 12.5% respectively when compared with the traditional method. For National Institute of Standards and Technology (NIST) curve (i.e. where a = 1), the cost of the tripling is further reduced to 10M+7S which saved 8M+1S from the traditional one. Further cost reduction in multiplication and squaring by 44% and 12.5% respectively.

Keyword: Elliptic curve over binary field, scalar multiplication, point tripling, Lopez-Dahab