An algorithm to enhance elliptic curves scalar multiplication combining MBNR with point halving

ABSTRACT

Elliptic curves (EC) scalar multiplication over some finite fields, is an attractive research area, and it has been paid much attention by re- searchers in the recent years. Researchs still in progress to improve the imple- mentation of elliptic curves cryptography (ECC) and reducing its complexity. Elliptic curve point-halving algorithm proposed in [10], later double-base (DB) chain [3], and step multi-base representation (SMBR) [17] are among the ef- ficient techniques used in this field. The presented paper proposes a new algorithm combining SMBR and point halving. We extend the work done by [13], which combined DB chain with point halving technique. The experiment results show that our contribution can enhance EC scalar multiplication.

Keyword: Elliptic curves cryptography; Integer representation; Multinumber system; Point halving