Bilinear pairings computation using the extended double-base chains algorithm

ABSTRACT

Elliptic curve (EC) pairings have been the focus of attention of researchers and cryptographers, especially after identity-based cryptosystems(IBC) were proposed in 2001. The Weil and Tate pairing is considered as the most important pairings used in cryptographical protocols and their applications. The computation efficiency of the Weil and Tate pairings mainly depends on the efficiency of the EC scalar multplications algorithms used. In this paper, we compute the Tate pairing using multi-base number representation(MBNR) system in scalar multiplication instead of using binary representation as used in Miller's algorithm and in the double-base (DB) chain used by Changan Zhao et al. We show that using doubling, tripling and quintupling in scalar multiplication, computation of the Tate pairing and its applications can be significantly enhanced.

Keyword: Bilinear pairing; Tate pairing; Miller's algorithm; Elliptic curves cryptography; Multi-number representation system