Improved arithmetic on elliptic curves over prime field

ABSTRACT

A fast point doubling and point addition operations on an elliptic curve over prime field are proposed. This occur when we use a special coordinates system (to represent any point on elliptic curve over prime field. Using this system improved the elliptic curve point arithmetic by reducing the computation cost for point doubling and point addition operation.

Keyword: Elliptic curve cryptosystem; Point arithmetic of elliptic curve; Affine coordinates; Projective coordinates; Jacobian coordinates