New quintupling point arithmetic 5P formulas for Lŏpez-Dahab coordinate over binary elliptic curve cryptography

ABSTRACT

In Elliptic Curve Cryptography (ECC), computational levels of scalar multiplication contains three levels: scalar arithmetic, point arithmetic and field arithmetic. To achieve an efficient ECC performance, precomputed points help to realize a faster computation, which takes away the need to repeat the addition process every time. This paper introduces new quintupling point (5P) formulas which can be precomputed once and can be reused at the scalar multiplication level. We considered mixed addition in Affine and Lŏpez-Dahab since the mixed addition computation cost is better than the traditional addition in Lŏpez-Dahab coordinates over binary curve. Two formulas are introduced for the point quintupling which (Double Double Add) and (Triple Add Double), the cost of the two formulas are 17 multiplication+12 squaringand 23 multiplication+13 squaring respectively. The two formulas are proven as valid points. The new quintupling point can be implemented with different scalar multiplication methods.

Keyword: Elliptic Curve Cryptosystem (ECC); Scalar multiplication algorithm; Point arithmetic; Point quintupling; Lopez-Dahab (LD); Binary curve