World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:12, No:06, 2018

Implementation of Integer Sub-Decomposition Method on Elliptic Curves with J-Invariant 1728

Authors : Siti Noor Farwina Anwar, Hailiza Kamarulhaili

Abstract : In this paper, we present the idea of implementing the Integer Sub-Decomposition (ISD) method on elliptic curves with j-invariant 1728. The ISD method was proposed in 2013 to compute scalar multiplication in elliptic curves, which remains to be the most expensive operation in Elliptic Curve Cryptography (ECC). However, the original ISD method only works on integer number field and solve integer scalar multiplication. By extending the method into the complex quadratic field, we are able to solve complex multiplication and implement the ISD method on elliptic curves with j-invariant 1728. The curve with j-invariant 1728 has a unique discriminant of the imaginary quadratic field. This unique discriminant of quadratic field yields a unique efficiently computable endomorphism, which later able to speed up the computations on this curve. However, the ISD method needs three endomorphisms to be accomplished. Hence, we choose all three endomorphisms to be from the same imaginary quadratic field as the curve itself, where the first endomorphism is the unique endomorphism yield from the discriminant of the imaginary quadratic field.

Keywords : efficiently computable endomorphism, elliptic scalar multiplication, j-invariant 1728, quadratic field
Conference Title : ICNTP 2018 : International Conference on Number Theory and Physics
Conference Location : Paris, France
Conference Dates : June 25-26, 2018