Elliptic Curve Scalar Multiplication Algorithm Using ZOT Structure

Hani Mimi*, Azman Samsudin, Shahram Jahani

Al-Zaytoonah University of Jordan, Universiti Sains Malaysia

hani_mimi@zuj.edu.jo, Azman@cs.usm.my, Jahani2001@yahoo.com

Abstract: *The computation of kP over elliptic curves is the dominant operation. It depends on the representation of the scalar k. The binary method is the standard unsigned method that is used to compute the elliptic curve point $Q = kP$. Researchers found that it is not the most efficient way for implementing elliptic curve computations. Other recoding methods such as CR, NAF, and MOF were presented in order to enhance the efficiency of EC computations. Our ZOTEC method that is based on ZOT recoding method was proposed to accelerate the EC computations. ZOTEC can be computed right-to-left or left-to-right. The recoding process is also faster than NAF and as fast as CR and MOF if the binary conversion included or excluded. ZOTEC method is more efficient than BIN, CR, MOF, and NAF methods in terms of field complexity and time complexity whenever a field inversion is more expensive than 6 multiplications for BIN, CR, and MOF, and 8.3 for NAF.*

Keywords *Elliptic curve arithmetic, point multiplication, single scalar multiplication, non-window recoding methods, signed binary representation.*