International J. of Math. Sci. & Engg. Appls. (IJMSEA)
ISSN 0973-9424, Vol. 9 No. II (June, 2015), pp. 115-128

INTEGER SUB-DECOMPOSITION ELLIPTIC SCALAR MULTIPLICATION ON KOBLITZ CURVES OVER BINARY EXTENSION FIELD

RUMA KAREEM K. AJEENA
Babylon University, Department of Mathematics,
Mathematics School, Babil city, Iraq

Abstract

In this work, the developed algorithm of the integer sub-decomposition (ISD) method used to compute a scalar multiplication kP on another class of elliptic curves is presented. These curve are called Koblitz curves E_a, with $a \in \{0, 1\}$, defined over a binary extension field F_{2^m} that have efficiently-computable endomorphisms ψ_j for $j = 1, 2$. ISD method on Koblitz curves E_a is used for speeding the computations of the endomorphisms ψ_j to compute kP. These endomorphisms are defined as the Frobenious maps over the endomorphism ring $\mathbb{Z}[\tau]$, where τ is a complex number. The endomorphism ring $\mathbb{Z}[\tau]$ in this case is embedded into an imaginary quadratic field $\mathbb{Q}(\sqrt{D})$, where $D = -7$ is a square-free number. Subsequently, the ISD sub-decomposition idea on Koblitz curves E_a is utilized to speed the representations of the sub-scalars k_{11}, k_{12}, k_{21} and k_{22} using τ-adic non-adjacent form (TNAF). On the curves E_a defined over F_{2^m}, computing the endomorphisms and τ-adic representations of ISD sub-scalars can be carried out without using any point doublings. This property is considered as a fundamental advantage to speed up the computation of complex multiplication kP. The ISD complex multiplication is defined by

$$kP = k_{11}P + k_{12}\psi_1(P) + k_{21}P + k_{22}\psi_2(P)$$

where k_{11}, k_{12}, k_{21} and $k_{22} \in \mathbb{Z}[\tau]$ and are defined by $k_{11} = u_{l_3-1}\tau^{l_3-1} + \cdots + u_1\tau + u_0$, $k_{12} = u_{l_4-1}\tau^{l_4-1} + \cdots + u_1\tau + u_0$, $k_{21} = u_{l_5-1}\tau^{l_5-1} + \cdots + u_1\tau + u_0P$ and $k_{22} = u_{l_6-1}\tau^{l_6-1} + \cdots + u_1\tau + u_0$. The endomorphisms in kP formula are defined by $\psi_1(P) = u_{l_1-1}\tau^{l_1-1}(P) + \cdots + u_1\tau(P) + u_0P$ and $\psi_2(P) = u_{l_2-1}\tau^{l_2-1}(P) + \cdots + u_1\tau(P) + u_0P$. The operations to compute ISD sub-scalars and the endomorphisms in ISD scalar multiplication kP are called complex multiplications by τ on E_a.

Key Words : *Elliptic Curve Cryptography, Koblitz curves, Complex Scalar Multiplication, ISD method, Efficiently computable endomorphism, Binary extension field.*

2000 AMS Subject Classification : Primary-11Dxx, 11Rxx, Secondary-20Gxx, 06Bxx.