A Survey on Single Scalar Point Multiplication Algorithms for Elliptic Curves over Prime Fields

Mohammad Rasmi	Ahmad Abu Sokhon	Mohammad Sharif	Hani Almimi
Zarqa University, Jordan	*Al-Zaytoonah University of Jordan*	*Al Ain University of Science and Technology, UAE*	*Al-Zaytoonah University of Jordan*
mr77mr@hotmail.com	ahmad.abusukhon@zuj.edu.jo	m2sharief@yahoo.co.uk	hani.mimi@zuj.edu.jo

Abstract— **Elliptic Curve Cryptography (ECC) is an attractive field of research since it requires a shorter key length compared to other public-key cryptosystems such as RSA. A shorter key reduces the required computations, power consumption, and storage. The major time-consuming operation in ECC is the point multiplication, kP. Therefore, a lot of research has been carried out to improve the efficiency of ECC implementations. Composite Elliptic Curve (EC) operations and recoding methods are two factors that affect the efficiency of EC scalar multiplication. Deciding which composite EC operation to be used in an ECC system helps to improve the computational efficiency. In addition, finding a method that accelerates the EC computations, which depends on a new recoding method and employing the most efficient composite operations, is considered a pressing need. In this a research, a survey of EC single scalar multiplication methods is introduced. Therefore, a comprehensive information related to EC multiplication methods will be provided in order to facilitate literature review for researchers who would like to conduct a research in this area of science.**

Keywords— **Elliptic Curve Cryptography, recoding methods, EC multiplication**