Hard problems in elliptic curve scalar multiplication

Natarajan Vijayarangan *
Innovation Labs
Tata Consultancy Services (*TCS*)
No. 17, Cathedral Road
Chennai 600 086, India

Abstract

Number Theory and Cryptography are based on mathematical problems that are considered difficult to solve. "Difficult" in this case refers more to the computational requirements in finding a solution than to the conception of the problem. These problems are formally called "hard" problems. Some of the most well known examples are factoring large numbers, finding the discrete logarithms, theorem-proving, and the Traveling Salesman Problem. In the theory of *Double Base Number System* (DBNS)/*Multiple Base Number System* (MBNS), finding the best approximation for a given integer is a hard problem. This approximation can be used to compute Elliptic curve scalar multiplication in an efficient way. In this paper, we have come up with an algorithm for DBNS, which expresses any integer n in the form of DBNS with decreasing order of exponents.

Keywords and phrases : *EC scalar multiplication, double base number system (DBNS), multiple base number system (MBNS), digital signature schemes, ECDSA, ECC.*

Introduction

Elliptic Curve Cryptography (ECC) was proposed by N. Koblitz [1], and V. Miller [2] independently. ECC has obtained a lot of applications because of smaller key-length and increased theoretical robustness. In ECC, scalar multiplication (or point multiplication) is the operation of calculating an integer multiple of an element in additive group of elliptic curve. In other words, it is a computation of kP for any integer k and a point P on the elliptic curve. To compute EC scalar multiplications, one can easily adapt historical exponentiation methods to scalar multiplication, replacing multiplication by addition and squaring by doubling. Recently, DBNS [4] and MBNS [8] methods have been used to reduce

E-mail: n.vijayarangan@tcs.com

Journal of Discrete Mathematical Sciences & Cryptography
Vol. 13 (2010), No. 5, pp. 445–452