A Mathematical Analysis of Elliptic Curve Point Multiplication

Ravi Kishore Kodali

Department of Electronics and Communication Engineering,
National Institute of Technology, Warangal,
Warangal, 506004 India

Abstract. This work presents a mixed-coordinate system based elliptic curve point multiplication algorithm. It employs the width-w Non-Adjacent Form (NAF) algorithm for point multiplication and uses the Montgomery trick to pre-compute the odd points $P_i = iP$ for $i = 1, 3, \cdots, 2^w - 1$ with only one field inversion.

Keywords: Non-Adjacent Form, Point Multiplication, Elliptic Curve.

1 Introduction

With the advent of the world wide web, huge amount of data by various applications/ nodes is being shared. With information sharing hitting unprecedented levels, security of the information being shared becomes paramount. While the data being exchanged among the nodes using the Internet it is necessary to make use of various cryptographic techniques and secure the data so as to reduce the risks associated. RSA, one of the asymmetric key cryptographic techniques, is being widely used over the Internet. However, this technique requires large key sizes and is compute intensive. Alternately, Elliptic Curve Cryptography (ECC)proposed by Koblitz [9] and Miller [13] can also be used as ECC provides similar security levels by making use of lesser key sizes as compared to the RSA. ECC, standardized by ISO [1], IEEE [15] and NIST [14], has been gaining its acceptance recently. However, ECC involves repeated application of compute intensive elliptic curve based point multiplication operation. This work primarily focusses on speeding up point multiplication.

2 Elliptic Curve Cryptography

ECC uses elliptic curves as given by equation 1.

$$y^2 = (x^3 + ax + b), \tag{1}$$

where $(a, b, x, y) \in F_p$, a prime field and p is a prime number and satisfying the condition $4a^3 + 27b^2 \neq 0$. Consider two points, P and Q lying on the elliptic curve (EC), $E_p(a, b)$ [10].

J. Lloret Mauri et al. (Eds.): SSCC 2014, CCIS 467, pp. 192–200, 2014.

The addition of these two points resulting in R, another point lying on the EC $E_p(a, b)$ is given by equation

$$R(x_R, y_R) = P + Q, \tag{2}$$

where

$$x_R = (\lambda^2 - x_P - x_Q) \tag{3}$$

$$y_R = (\lambda(x_P - x_R) - y_P) \tag{4}$$

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P} \tag{5}$$

The point doubling operation may be considered as being P = Q, R = 2P, the λ is to be computed by

$$\lambda = \frac{3x_P^2 + a}{2y_P} \tag{6}$$

The point multiplication can be achieved by using point addition and doubling operations repeatedly. One of the algorithms for point multiplication, double and add method is given by algorithm 1.

Algorithm 1. Double and add algorithm

Input: k (binary representation), P (a point on the EC)
Output $Q = k \times P$
A. Q = ϕ (point of infinity).
B. for $i = t - 1$ downto 0
    Q = 2Q.
    if $k_i = 1$, Q = Q+P.
C. Return Q

3 Related Work

For a given point, $P(x, y)$, the negative of P is given by $-P = (x, -y)$ for an elliptic curve over a prime field. The subtraction of points over a prime field may be considered as R = P - Q = P + (-Q) [7]. In order to achieve efficiency while carrying out point multiplication, a sliding window method is used [17]. The window size, the corresponding computational complexity and Fuzzy optimization are given in [8]. While representing the scalar values, various radices have also been used such as radix -2 and radix -3 have been used [4]. A multi-base non-adjacent form (mbNAF) technique is used to represent integers using different bases [12]. An improved method based on the width-w NAF multiplication, where $P_i = iP$ for $i = 1, 3, \cdots, 2^w - 1$ are pre-computed using double and add method and are stored, is presented. This method performs multiplication faster, when compared to the double and add method. This work focusses