IMPLEMENTATION OF SIGNATURE SCHEME WITH PROJECTIVE COORDINATES ON ELLIPTIC CURVE CRYPTOSYSTEM

P. Anuradha Kameswari, L. Praveen Kumar

Department of Mathematics, Andhra University,
Visakhapatnam - 530003, Andhra Pradesh, India.

Department of Mathematics, Andhra University,
Visakhapatnam - 530003, Andhra Pradesh, India.

ABSTRACT

In this paper we implement a signature scheme on cryptosystem with elliptic curves by using the formulas for the projective coordinates obtained by generalizing the ideas of Montgomery to Weierstrass equation of elliptic curves. This arithmetic with projective coordinates is more efficient and avoid many inversions in the computations. We also propose a fast computing method evaluating the coordinates.

KEY WORDS : Elliptic Curves, Projective Coordinates, Cryptosystem.

INTRODUCTION:

In 1985 Koblitz [1] [2] and Miller [3] independently made use of elliptic curves in cryptography. Later Koyama [4] and Demytko [5] also produced analogue of RSA with elliptic curves to overcome the vulnerabilities like homomorphic nature of RSA, however it was shown that even these non-homomorphic RSA type cryptosystems are not totally free from RSA attacks[6], and it was shown that they are susceptible to chosen message attacks.[7]

In [7] "A New and Optimal Chosen - message Attack on RSA-type Cryptosytems" by Daniel Bleichenbacher, Marc Joye and Jean-Jacques Quisquater, it is show that only one message is needed to mount the attack on Demykto's system.

In this paper we mount the chosen message forgery attack- a signature scheme for cryptosystem with elliptic curves and we impliment the attack with point addition on elliptic curves by formulas for projective coordinates on general Weierstrass equation of elliptic curves, [8][9][10] with these formulas addition requires four additions, six multiplications and two squarings and doubling requires four additions, six multiplications and three squarings with no inversions. For any point P on elliptic curve $E(K)$ and for any integer k to compute the point addition kP it requires only to calculate $2mP$ and $(2m+1)P$ from mP and $(m+1)P$ and we give a fast computation method for kP generalizing the ideas given by P.Smith for Lucas sequences to elliptic curves.

2 POINT ADDITION WITH PROJECTIVE COORDINATES:

Let K be a field with Characteristic $K \neq 2,3$ and consider the elliptic curve $E(K)$ over K in Weierstrass form $E: y^2 = x^3 + Ax + B$ and for any points $P = (x_1, y_1)$ and $Q = (x_2, y_2) \in E \setminus \{O\}$ with $x_1 \neq x_2$ the affine addition $P + Q = (x_3, y_3)$ is given as:[11][12]

$$x_3 = m^2 - x_1 - x_2,$$

$$y_3 = m(x_1 - x_3) - y_1, \text{ where } m = \frac{y_2 - y_1}{x_2 - x_1}.$$

and for $P = (x_1, y_1) \in E$ the affine addition $2P = (x, y)$ is given as:

$$x = m^2 - 2x_1,$$

$$y = m(x_1 - x_3) - y_1, \text{ where } m = \frac{3x_1^2 + A}{2y_1}$$

Now for any point $P = (x, y) \in E$, the projective coordinates are denoted as $P = (X, Y, Z)$ for $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$.

Theorem 1: Let K be a field of characteristic not equal to 2,3 and E be the elliptic curve given by the equation $y^2 = x^3 + Ax + B$. If $P = (x, y)$ then for any positive integer k, the projective coordinates of kP are denoted as $(X_k : Y_k : Z_k)$ and $[X_k : Z_k]$ are given by recursion formulas as follows:

If $k = 2m+1$, $\begin{cases} X_k = -4BZ_m Z_{m+1}(X_m Z_{m+1} + X_{m+1}Z_m) + (X_m X_{m+1} - AZ_m Z_{m+1})^2, \\ Z_k = \dfrac{X}{Z}(X_m Z_{m+1} - X_{m+1}Z_m)^2. \end{cases}$

If $k = 2m$, $\begin{cases} X_k = (X_m^2 - AZ_m^2)^2 - 8BX_m Z_m^3, \\ Z_k = 4Z_m(X_m^3 + AX_m Z_m^2 + BZ_m^3). \end{cases}$

Proof: For any point $M = (x, y)$ on $E : y^2 = x^3 + Ax + B$ we have

$x = \dfrac{X}{Z}, y = \dfrac{Y}{Z}$ for (X, Y, Z) the projective coordinates of M.

Therefore $y^2 = x^3 + Ax + B$.

Which implies that $\left(\dfrac{Y}{Z}\right)^2 = \left(\dfrac{X}{Z}\right)^3 + A\left(\dfrac{X}{Z}\right) + B$.

Inparticular for a fixed $P = (x, y)$ on E and any integer $m \geq 0$, we have for $(2m+1)P$

$$\frac{X_{2m+1}}{Z_{2m+1}} = \left(\frac{\dfrac{Y_{m+1}}{Z_{m+1}} - \dfrac{Y_m}{Z_m}}{\dfrac{X_{m+1}}{Z_{m+1}} - \dfrac{X_m}{Z_m}}\right)^2 - \frac{X_m}{Z_m} - \frac{X_{m+1}}{Z_{m+1}}$$

$$\frac{X_{2m+1}}{Z_{2m+1}}\left(\frac{X_{m+1}}{Z_{m+1}} - \frac{X_m}{Z_m}\right)^2 = \left(\frac{Y_{m+1}}{Z_{m+1}} - \frac{Y_m}{Z_m}\right)^2 - \left(\frac{X_m}{Z_m} + \frac{X_{m+1}}{Z_{m+1}}\right)\left(\frac{X_{m+1}}{Z_{m+1}} - \frac{X_m}{Z_m}\right)^2$$

$$= \left[\left(\frac{Y_{m+1}}{Z_{m+1}} \right)^2 + \left(\frac{Y_m}{Z_m} \right)^2 - 2 \frac{Y_{m+1}}{Z_{m+1}} \frac{Y_m}{Z_m} \right] -$$

$$\left[\left(\frac{X_{m+1}}{Z_{m+1}} \right)^3 + \left(\frac{X_m}{Z_m} \right)^3 - \left(\frac{X_{m+1}}{Z_{m+1}} \right)^2 \frac{X_m}{Z_m} - \left(\frac{X_m}{Z_m} \right)^2 \frac{X_{m+1}}{Z_{m+1}} \right]$$

$$= A \left(\frac{X_{m+1}}{Z_{m+1}} \right) + B + A \left(\frac{X_m}{Y_m} \right) + B$$

$$- 2 \frac{Y_{m+1}}{Z_{m+1}} \frac{Y_m}{Z_m} + \left(\frac{X_{m+1}}{Z_{m+1}} \right)^2 \frac{X_m}{Z_m} + \left(\frac{X_m}{Z_m} \right)^2 \frac{X_{m+1}}{Z_{m+1}}$$

$$= -2 \frac{Y_{m+1}}{Z_{m+1}} \frac{Y_m}{Z_m} + 2B + \left(A + \frac{X_m}{Z_m} \frac{X_{m+1}}{Z_{m+1}} \right) \left(\frac{X_m}{Z_m} + \frac{X_{m+1}}{Z_{m+1}} \right)$$

$$\frac{X}{Z} \left(\frac{X_{m+1}}{Z_{m+1}} - \frac{X_m}{Z_m} \right)^2 = 2 \frac{Y_{m+1}}{Z_{m+1}} \frac{Y_m}{Z_m} + 2B + \left(A + \frac{X_m}{Z_m} \frac{X_{m+1}}{Z_{m+1}} \right) \left(\frac{X_m}{Y_m} + \frac{X_{m+1}}{Z_{m+1}} \right).$$

$$\left(\frac{X_{2m+1}}{Z_{2m+1}} \right) \left(\frac{X}{Z} \right) \left(\frac{X_{m+1}}{Z_{m+1}} - \frac{X_m}{Z_m} \right)^4 = \left[2B + \left(A + \frac{X_{m+1}}{Z_{m+1}} \frac{X_m}{Z_m} \right) \left(\frac{X_{m+1}}{Z_{m+1}} + \frac{X_m}{Z_m} \right) \right]^2$$

$$- 4 \left(\frac{Y_{m+1}}{Z_{m+1}} \right)^2 \left(\frac{Y_m}{Z_m} \right)^2$$

$$= -4 \left[\left(\frac{X_{m+1}}{Z_{m+1}} \right)^3 + A \left(\frac{X_{m+1}}{Z_{m+1}} \right) + B \right] \left[\left(\frac{X_m}{Z_m} \right)^3 + A \left(\frac{X_m}{Z_m} \right) + B \right]$$

$$+ \left[2B + \left(A + \frac{X_{m+1}}{Z_{m+1}} \frac{X_m}{Z_m} \right) \left(\frac{X_{m+1}}{Z_{m+1}} + \frac{X_m}{Z_m} \right) \right]^2$$

$$= -4B\left[\left(\frac{X_m}{Z_m}\right)^3 + \left(\frac{X_{m+1}}{Z_{m+1}}\right)^3 - \left(\frac{X_m}{Z_m}\right)\left(\frac{X_{m+1}}{Z_{m+1}}\right)^2 - \left(\frac{X_{m+1}}{Z_{m+1}}\right)\left(\frac{X_m}{Z_m}\right)^2\right]$$

$$-4\left[\left(\frac{X_m}{Z_m}\right)^3\left(\frac{X_{m+1}}{Z_{m+1}}\right)^3 + A\left(\frac{X_m}{Z_m}\right)^3\frac{X_{m+1}}{Z_{m+1}} + A\left(\frac{X_m}{Z_m}\right)\left(\frac{X_{m+1}}{Z_{m+1}}\right)^3 + A^2\left(\frac{X_m}{Z_m}\right)\left(\frac{X_{m+1}}{Z_{m+1}}\right)\right]$$

$$+\left[A^2 + \left(\frac{X_m}{Z_m}\right)^2\left(\frac{X_{m+1}}{Z_{m+1}}\right)^2 + 2A\frac{X_m}{Z_m}\frac{X_{m+1}}{Z_{m+1}}\right]\left[\left(\frac{X_m}{Z_m}\right)^2 + \left(\frac{X_{m+1}}{Z_{m+1}}\right)^2 + 2\frac{X_m}{Z_m}\frac{X_{m+1}}{Z_{m+1}}\right]$$

$$= -4B\left(\frac{X_m}{Z_m} + \frac{X_{m+1}}{Z_{m+1}}\right)\left(\frac{X_m}{Z_m} - \frac{X_{m+1}}{Z_{m+1}}\right)^2 + \left(\frac{X_m}{Z_m}\frac{X_{m+1}}{Z_{m+1}} - A\right)^2\left(\frac{X_m}{Z_m} - \frac{X_{m+1}}{Z_{m+1}}\right)^2$$

$$\frac{X_{2m+1}}{Z_{2m+1}} = \frac{\left[-4B\left(\frac{X_m}{Z_m} + \frac{X_{m+1}}{Z_{m+1}}\right) + \left(\frac{X_m}{Z_m}\frac{X_{m+1}}{Z_{m+1}} - A\right)^2\right]\left(\frac{X_m}{Z_m} - \frac{X_{m+1}}{Z_{m+1}}\right)^2}{\frac{X}{Z}\left(\frac{X_m}{Z_m} - \frac{X_{m+1}}{Z_{m+1}}\right)^4}$$

$$= \frac{-4B\left(\frac{X_m Z_{m+1} + X_{m+1}Z_m}{Z_m Z_{m+1}}\right) + \left(\frac{X_m X_{m+1} - AZ_m Z_{m+1}}{Z_m Z_{m+1}}\right)^2}{\frac{X}{Z}\left(\frac{X_m Z_{m+1} - X_{m+1}Z_m}{Z_m Z_{m+1}}\right)^2}$$

$$= \frac{-4BZ_m Z_{m+1}(X_m Z_{m+1} + X_{m+1}Z_m) + (X_m X_{m+1} - AZ_m Z_{m+1})^2}{\frac{X}{Z}(X_m Z_{m+1} - X_{m+1}Z_m)^2}$$

$$[X_{2m+1}; Z_{2m+1}] = [-4BZ_m Z_{m+1}(X_m Z_{m+1} + X_{m+1}Z_m) + (X_m X_{m+1} - AZ_m Z_{m+1})^2;$$

$$\frac{X}{Z}(X_m Z_{m+1} - X_{m+1}Z_m)^2]$$

$$\text{For } k = 2m, \frac{X_k}{Z_k} = \frac{\left[3\left(\frac{X_m}{Z_m}\right)^2 + A\right]^2}{4\left(\frac{Y_m}{Z_m}\right)^2} - 2\left(\frac{X_m}{Z_m}\right)$$

$$= \frac{\left(\frac{X_m}{Z_m}\right)^4 + A^2 - 2A\left(\frac{X_m}{Z_m}\right)^2 - 8B\left(\frac{X_m}{Z_m}\right)}{4\left[\left(\frac{X_m}{Z_m}\right)^3 + A\left(\frac{X_m}{Z_m}\right) + B\right]}$$

$$= \frac{\left[\left(\frac{X_m}{Z_m}\right)^2 - A\right]^2 - 8B\left(\frac{X_m}{Z_m}\right)}{4\left[\left(\frac{X_m}{Z_m}\right)^3 + A\left(\frac{X_m}{Z_m}\right) + B\right]}$$

$$= \frac{\left[\left(X_m^2 - AZ_m^2\right)^2 - 8BX_mZ_m^3\right]}{4Z_m^4\left[\left(\frac{X_m}{Z_m}\right)^3 + A\left(\frac{X_m}{Z_m}\right) + B\right]}$$

$$= \frac{\left(X_m^2 - AZ_m^2\right)^2 - 8BX_mZ_m^3}{4Z_m\left(X_m^3 + AX_mZ_m^2 + BZ_m^3\right)}$$

$$[X_{2m}; Z_{2m}] = \left[\left(X_m^2 - AZ_m^2\right)^2 - 8BX_mZ_m^3 ; 4Z_m\left(X_m^3 + AX_mZ_m^2 + BZ_m^3\right)\right]$$

Remark 1: The formulas for computation of $[X_k : Z_k]$ in kP depend only on $[X_1 : Z_1]$ for $P = (x, y)$ and $X_1 = x, Z_1 = 1$; i.e., the formulas are polynomials in $x(P)$ and $\begin{cases} X_k = X_k(x) \\ Z_k = Z_k(x). \end{cases}$

Theorem 2: Let K be a field of characteristic not equal to 2, 3 and let E be the elliptic curve given by the equation $E(K): y^2 = x^3 + Ax + B$ and also $P = (x_m, y_m)$ and $Q = (x_{m-1}, y_{m-1}) \in E(K) \setminus \{O\}$ with $P \neq Q$. Given the point $P - Q = (x, y)$, if $y \neq 0$ then the y-coordinate of P satisfies

$$y(P) = y_m = \frac{-\left[2B + (A + x_m x)(x + x_m) - x_{m-1}(x - x_m)^2\right]}{2y}.$$

Proof: Define $D = P - Q = (x, y)$.

Since $Q = P - D = (x_{m-1}, y_{m-1})$, we have $x_{m-1} = \left(\frac{y_m + y}{x_m - x}\right)^2 - x_m - x.$

Then $x_{m-1}(x_m - x)^2 = (y_m + y)^2 - (x_m + x)(x_m - x)^2$

$= y_m^2 + y^2 + 2y_m y - (x_m^3 + x^3 - x_m^2 x - x^2 x_m)$

$= 2y_m y + (A + x_m x)(x_m + x) + 2B$

$2y_m y = x_{m-1}(x_m - x)^2 - (A + x_m x)(x_m + x) - 2B$

$$y_m = \frac{-2B - (A + x_m x)(x_m + x) + x_{m-1}(x_m - x)^2}{2y}$$

Therefore $$y_m = \frac{-\left[2B + (A + x_m x)(x_m + x) - x_{m-1}(x_m - x)^2\right]}{2y}.$$

FAST COMPUTATION METHOD FOR X_e AND Z_e:

We describe the fast computation method to compute X_e and Z_e suggested by P. Smith for Lucas sequences [13] and this method directly leads to the computation of $[X_e : Z_e]$ with no ambiguity of adding or doubling at each stage right from $[X_1 : Z_1]$ by using the above recursive formulas.

For any integer e, we have the binary expression given as

$$e = \sum_{t=0}^{t} x_i 2^{t-i}, x_0 = 1, \; x_i = 0 \text{ or } 1, \text{ for } i \geq 0.$$

Let $e_k = \sum_{i=0}^{k} x_i 2^{k-i}$, for $0 \leq k \leq t$, then $e_t = e, e_0 = 1$.

Theorem 3: $e_{k+1} = \begin{cases} 2e_k & \text{if } x_{k+1} = 0 \\ 2e_k + 1 & \text{if } x_{k+1} = 1. \end{cases}$

Proof: We have $e_{k+1} = \sum_{i=0}^{k+1} x_i 2^{k+1-i}$

$$= 2\sum_{i=0}^{k} x_i 2^{k-i} + x_{k+1} 2^{k+1-k-1}$$

$$= 2\sum_{i=0}^{k} x_i 2^{k-i} + x_{k+1}$$

$$= 2e_k + x_{k+1}.$$

Therefore $e_{k+1} = \begin{cases} 2e_k & \text{if } x_{k+1} = 0 \\ 2e_k + 1 & \text{if } x_{k+1} = 1. \end{cases}$

Remark 2: $e_{k+1} + 1 = \begin{cases} 2e_k + 1 & \text{if } x_{k+1} = 0 \\ 2(e_k + 1) & \text{if } x_{k+1} = 1. \end{cases}$

$$e_{k+1} - 1 = \begin{cases} 2e_k - 1 & \text{if } x_{k+1} = 0 \\ 2e_k & \text{if } x_{k+1} = 1. \end{cases}$$

Remark 3: $[X_e : Z_e]$ are computed by evaluating $[X_{e_k} : Z_{e_k}]$ for $k = 0,1,\ldots, t$ by using recursive formulas for $[X_{2e_k+1} : Z_{2e_k+1}]$ and $[X_{2e_k} : Z_{2e_k}]$.

Remark 4: For any point $M \in E(Z_n)$ where $n = pq$, we have the point $M = (M \bmod p, M \bmod q)$ as $E(Z_{pq})$; $E(Z_p) \oplus E(Z_q)$ and we have the formulas in Theorems 1 and 3 are valid for M on $E(Z_{pq})$. [1][4][11]

Notation: For any point $M \in E(Z_n)$ we write as $M = (M_x, M_y)$ and for any integer k, X_k the point kM is written as $kM = (M_{k,x}, M_{k,y})$.

4 SIGNATURE SCHEME ON CRYPTOSYSTEM WITH ELLIPTIC CURVES:

Let message be a point $M = (M_x, M_y)$ on an elliptic curve $E(Z_n) : y^2 = x^3 + Ax + B \bmod n$, where $n = pq$ and let $\# E(Z_n) = N_n$, $(e, N_n) = 1$ with d such that $ed \equiv 1 \bmod N_n$ and (M, n, e) is public.

The aim of cryptanalyst is to obtain signature $dM = (M_{d,x}, M_{d,y})$.

The cryptanalyst adapts the following steps in the signature scheme:

Let k be an integer such that $(k, e) = 1$ and $(k, N_n) = 1$, then there exist r, s such that $kr + es = 1$.

Let $M' = kM = k(M_x, M_y) = (M_{k,x}, M_{k,y})$ and M' may be evaluated using point addition with projective coordinates.

Obtain the signature on M' as follows:

$dM' = (M'_{d,x}, M'_{d,y}) \bmod n$ and let $C' = dM' \bmod n$;

Evaluate the point rC' and sM using the point addition with projective coordinates.

The cryptanalyst obtains dM as follows:

We have

$$kr + es = 1$$

$$krd + eds = d$$

$$krd + s \equiv d \bmod N_n$$

$$d = (krd + s) + N_n t \text{ for some integer } t.$$

Therefore the point addition $dM = [(krd + s) + N_n t]M$

$$= (krd + s)M$$

$$= krdM + sM$$

$$= r(dM') + sM.$$

$$= rC' + sM.$$

Using step 4 point dM is obtained by affine addition of $rC' + sM$.

Example: Let $n = pq = 143$ and $M = (1,122)$ be a point on Elliptic curve $E(Z_{143}) : y^2 = x^3 + 3x + 8 \bmod 143$ and for $N_n = \# E(Z_{143}) = 144$, take $e = 5$, as $(5,144) = 1$.

Then we have (M, n, e), the public key and d the secrete exponent such that $ed \equiv 1 \bmod N_n$.

The cryptanalyst obtain the signature dM as follows:

Let $k = 7$ be an integer such that $(k, e) = (7,5) = 1$, then there exist integers $r = -2, s = 3$ such that $kr + es = 1$.

Consider $M' = kM = 7M$ and M' is evaluated by using point addition with projective coordinates as follows:

$$7 = 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$$

$$X_{e_0} = 1, Z_{e_0} = 1;$$

$$X_{2e_0} = (X_{e_0}^2 - AZ_{e_0}^2)^2 - 8BX_{e_0}Z_{e_0}^3 = 83,$$

$$Z_{2e_0} = 4Z_{e_0}(X_{e_0}^3 + AX_{e_0}Z_{e_0}^2 + BZ_{e_0}^3) = 48;$$

$$X_{e_1} = X_{2e_0+1} = -4BZ_{e_0}Z_{e_0+1}\left(X_{e_0}Z_{e_0+1} + X_{e_0+1}Z_{e_0}\right) + \left(X_{e_0}X_{e_0+1} - AZ_{e_0}Z_{e_0+1}\right)^2$$

$$= 131$$

$$Z_{e_1} = Z_{2e_0+1} = \frac{X}{Z}\left(X_{e_0}Z_{e_0+1} - X_{e_0+1}Z_{e_0}\right)^2 = 81.$$

$$X_{e_1+1} = X_{2(e_0+1)} = \left(X_{e_0+1}^2 - AZ_{e_0+1}^2\right)^2 - 8BX_{e_0+1}Z_{e_0+1}^3 = 131.$$

$$Z_{e_1+1} = Z_{2(e_0+1)} = 4Z_{e_0+1}\left(X_{e_0+1}^3 + AX_{e_0+1}Z_{e_0+1}^2 + BZ_{e_0+1}^3\right) = 64.$$

$$X_{e_2} = X_{2e_1+1} = -4BZ_{e_1}Z_{e_1+1}\left(X_{e_1}Z_{e_1+1} + X_{e_1+1}Z_{e_1}\right) + \left(X_{e_1}X_{e_1+1} - AZ_{e_1}Z_{e_1+1}\right)^2$$

$$= 58.$$

$$Z_{e_2} = Z_{2e_1+1} = \frac{X}{Z}\left(X_{e_1}Z_{e_1+1} - X_{e_1+1}Z_{e_1}\right)^2 = 3.$$

Therefore $x(7M) = \dfrac{X_{e_2}}{Z_{e_2}} = \dfrac{58}{3} = 67 \mod 143.$

Torecover $y(7M)$ as follows :

$$X_{e_2-1} = X_{2e_1} = \left(X_{e_1}^2 - AZ_{e_1}^2\right)^2 - 8BX_{e_1}Z_{e_1}^3 = 79.$$

$$Z_{e_2-1} = Z_{2e_1} = 4Z_{e_1}\left(X_{e_1}^3 + AX_{e_1}Z_{e_1}^2 + BZ_{e_1}^3\right) = 16.$$

$$x(6M) = \frac{X_{e_2-1}}{Z_{e_2-1}} = \frac{79}{16} = 139 \mod 143.$$

For $x = x(M) = 1$, $x_m = x(7M) = 67$ and $x_{m-1} = x(6M) = 139.$

$$y_1 = y(7M) = \frac{-\left[2B + (A + x_m x)(x_m + x) - x_{m-1}(x_m - x)^2\right]}{2y} = -23.$$

Therefore $M' = 7M = (67,-23) = (67,120)$

Cryptanalyst obtain the signature on M' as

$$C' = dM' = (M'_{d,x}, M'_{d,y}) = (129,37).$$

Now the cryptanalyst computes rC', sM' as follows:

$rC' = -2(129,37).$

$X_{e_0} = 129$ and $Z_{e_0} = 1.$

$X_{e_1} = X_{2e_0} = \left(X_{e_0}^2 - aZ_{e_0}^2\right)^2 - 8bX_{e_0}Z_{e_0}^3 = 107.$

$Z_{e_1} = Z_{2e_0} = 4Z_{e_0}\left(X_{e_0}^3 + aX_{e_0}Z_{e_0}^2 + bZ_{e_0}^3\right) = 42.$

$x = \frac{X_{e_1}}{Z_{e_1}} = \frac{107}{42} = 40.$

For $x_m = 40$, $x = 1$ and $x_{m-1} = 1$, we have

$$y_m = \frac{-\left[2B + (A + x_m x)(x_m + x) - x_{m-1}(x_m - x)^2\right]}{2y} = 47.$$

Therefore $rC' = (40,47).$

$sM = 3M = 3(1,122).$

$X_{e_0} = 1,\ Z_{e_0} = 1.$

$X_{e_0+1} = X_{2e_0} = \left(X_{e_0}^2 - aZ_{e_0}^2\right)^2 - 8bX_{e_0}Z_{e_0}^3 = 83.$

$Z_{e_0+1} = Z_{2e_0} = 4Z_{e_0}\left(X_{e_0}^3 + aX_{e_0}Z_{e_0}^2 + bZ_{e_0}^3\right) = 48.$

$X_{e_1} = X_{2e_0+1} = -4bZ_{e_0}Z_{e_0+1}\left(X_{e_0+1}Z_{e_0} + X_{e_0}Z_{e_0+1}\right) + \left(X_{e_0+1}X_{e_0} - aZ_{e_0+1}Z_{e_0}\right)^2$

$= 131.$

$$Z_{e_1} = Z_{2e_0+1} = \frac{X}{Z}\left(X_{e_0+1}Z_{e_0} - X_{e_0}Z_{e_0+1}\right)^2 = 81.$$

$$x = \frac{X_{e_1}}{Z_{e_1}} = \frac{131}{81} = 74 \mod 143.$$

For $x_m = 74,\ x = 1$ and $x_{m-1} = \frac{83}{48} = 106,$ we have

$$y_m = \frac{-\left[2B + (A + x_m x)(x_m + x) - x_{m-1}(x_m - x)^2\right]}{2y} = 59.$$

Therefore $sM = (74,59).$

The cryptanalyst obtain $dM = rC' + sM$ as follows:

By using point addition with affine coordinates,

$$rC' + sM = (40,47) + (74,59) = (41,62).$$

Therefore the cryptanalyst retrieve the signature as $(41,62)$.

CONCLUSION:

In the signature scheme on Cryptosystem with elliptic curves implemented by point addition with projective coordinates for $P = (x, y)$ with projective coordinates (X_1, Y_1, Z_1) it requires only four additions, six multiplications and two squarings with no inversions in the computations of $[X_k : Z_k]$ at each consecutive addition leading to the projective coordinates $(X_k : Y_k : Z_k)$ and the $x(kP) = \frac{X_k}{Z_k}$ is obtained with one inversion and the corresponding y -coordinate is recovered with five additions, four multiplications and one inversion. Also the fast computation method directly leads to the computation of $[X_k : Z_k]$ with no ambiguity of adding or doubling at each stage right from $[X_1 : Z_1]$ by using the recursive formulas.

REFERENCES:

Journal Papers:

1. Neal Koblitz *"Elliptic Curve Cryptosystems" Mathematics of Computation, 48:* 203-209, 1987.

Books:

2. Neal Koblitz *"A course in number theory and cryptography ISBN 3-578071-8,SPIN 10893308 ".*

Chapters in Books:

3. V.S. Miller *" Use of Elliptic Curves in Cryptography".* In H.C. Williams, editor *Advances in Cryptology - CRYPTO 85, Volume 218* of Lecture notes in Computer Science, 417-426, Springer-Verlag, 1986.
4. K. Koyama, U.M. Maurer, T. Okamoto and S.A. Vanstone *"New public-key Schemes based on elliptic curves over the ring* Z_n." In J. Feigenbaum, editor *Advances in Cryptology - CRYPTO 91, Volume 576* of Lecture notes in Computer Science, 252-266, Springer-Verlag, 1991.

5. N. Demytko *"A new elliptic curve based analogue of RSA".* In T. Helleseth, editor *Advances in Cryptology - EUROCRYPTO 93, Volume 765* of Lecture notes in Computer Science, 40-49, Springer-Verlag, 1994.

Books:

6. J. Buchmann *"Introduction to cryptography" ,* Springer-Verlag 2001.

Chapters in Books:

7. Daniel Bleichenbacher, Marc Joye and Jean-Jacques Quisquater *"A New and Optimal Chosen-message Attack on RSA-type Cryptosystems".* In Y. Han, T. Okamoto and S. Qing, editors, Information and Communications Security

(ICICS'97), *vol.1334* of Lecture Notes in Computer Science, pp.302-313, Springer-Verlag, 1997.

Books:

8. J. H. Silverman. *The Arithmetic of Elliptic Curves*, *volume 106* of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

Journals:

9. J. H. Silverman. Elliptic curves and cryptography. In *Public-Key Cryptography*, *volume 62* of *Proc. Sympos. Appl. Math.,* pages 91-112. Amer. Math. Soc., Providence, RI, 2005.

Books:

10. J. H. Silverman and J. Tate. *Rational Points on Elliptic Curves*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

11. Lawrence C. Washington *"Elliptic Curves Number Theory and Cryptography"* 2nd edition, CRC press.

12. Jeffery Hoftstein, Jill Pipher, Joseph H. Silverman, *" An Introduction to Mathematical Cryptography",* Springer.

Jornals:

13. P.Smith, *"LUC Public-key encryption"*, Dr. Dobb's Journal(Jan 1993), 44-49.