International Journal of Computer Applications (0975 – 8887)
Volume 124 – No.6, August 2015

Implementation of GCD Attack with Projective Coordinates on Demytko's Cryptosystem

P. Anuradha Kameswari
Department of Mathematics
Andhra University
Visakhapatnam-530003
Andhra Pradesh

L. Praveen Kumar
Department of Mathematics
Andhra University
Visakhapatnam-530003
Andhra Pradesh

ABSTRACT
GCD attack depends on modifying the cipher text and then get an access to the decryption of the modified cipher text that is discarded identifying as due to bad implementation. In this paper we mount a GCD attack on Demytko's cryptosystem on elliptic curves. In this we implement the attack by point addition with projective coordinates using a fast computation method. As this involves working only with X-coordinates. We start with developing the formulas for the projective coordinates $[X:Z]$ generalizing the ideas of Montgomery and propose to use these formulas to generate the polynomials for the GCD attack.

Keywords
Elliptic Curves, Projective Coordinates and Demytko's Cryptosystem.

1. INTRODUCTION
RSA Cryptosystem is the most popular public key cryptosystem with security depending on difficulty of factoring large integers. As RSA is susceptible to homomorphic attacks, systems with non homomorphic nature were developed. In this context, in 1985 Koblitz and Miller made use of elliptic curves in cryptography. Koyama etal and Demykto developed analogues to RSA with elliptic curves. Demytko cryptosystem uses only the first coordinate of a point on elliptic curve making it more resistant to chosen message attack, however in the paper " On the importance of securing your bins: The garbage-man-in-the-middle attack" by Marc Joye and Jean-Jacques Quisquater, it is shown that Demytko cryptosystem is susceptible to gcd attack using division polynomials. In this paper we implemented the gcd attack on Demytko cryptosystem with point addition by projective coordinates. As Demytko cryptosystem involves working only with X-coordinates, we start with developing the formulas for the projective coordinates $[X:Z]$ generalizing the ideas of Montgomery and propose to use these formulas to generate the polynomials for the GCD attack.

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:

$$x_3 = m^2 - x_1 - x_2,$$
$$y_3 = m(x_1 - x_3) - y_1, \text{where} m = \frac{y_2 - y_1}{x_2 - x_1}.$$

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 $k = 2m+1$,

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

If $k = 2m$,

$$\begin{cases} X_k = (X_m^2 - AZ_m^2)^2 - 8BX_mZ_m^3, \\ Z_k = 4Z_m(X_m^3 + AX_mZ_m^2 + BZ_m^3). \end{cases}$$

Proof.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$= \frac{(X_m^2 - AZ_m^2)^2 - 8BX_m Z_m^3}{4Z_m(X_m^3 + AX_m Z_m^2 + BZ_m^3)}$$

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

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 $E(\mathrm{K}): y^2 = x^3 + Ax + B$ and also $P = (x_m, y_m)$ and $Q = (x_{m-1}, y_{m-1}) \in E(\mathrm{K}) \setminus \{O\}$ 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 $y_m = \frac{-\left[2B+(A+x_m x)(x_m+x)-x_{m-1}(x_m-x)^2\right]}{2y}$.

3. 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 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 $e = \sum_{t=0}^{t} x_i 2^{t-i}, x_0 = 1, x_i = 0$ or 1, 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.

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

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

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

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

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

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 $k = 0,1,...,t$ by using recursive formulas for $[X_{2e_k+1} : Z_{2e_k+1}]$ and $[X_{2e_k} : Z_{2e_k}]$.

We give in the following an algorithm for fast computation method for computing the projective coordinates X_e, Z_e of $eP \bmod N$ for a point P on Elliptic curve. Let (X_1, Y_1, Z_1) be the projective coordinates of the initial point P on E we initialize with $[X_1 : Z_1]$ to obtain the result $[X_e : Z_e]$.

Algorithm:

Write the binary expression of e as $e = \sum_{i=0}^{t} x_i 2^{t-i}, x_0 = 1$. Initialize the values for A, B, X_1, Z_1 and $\frac{X_1}{Z_1}$.

$$[X_c : Z_c] = [X_1 : Z_1]$$
$$[X_{c_+} : Z_{c_+}] =$$
$$[(X_1 - AZ_1^2)^2 - 8BX_1Z_1^3 : 4Z_1(X_1^3 + AX_1Z_1^2 + BZ_1^3)]$$

For i from 0 to t do

$$c \leftarrow 2c$$

$$c_+ \leftarrow 2c + 1$$

$$X_{2c} \leftarrow (X_c^2 - AZ_c^2)^2 - 8X_cZ_c^3$$

$$Z_{2c} \leftarrow 4Z_c(X_c^3 + AX_cZ_c^3 + BZ_c^3)$$

$$X_{2c+1} \leftarrow -4BZ_cZ_{c_+}(X_cZ_{c_+} + X_{c_+}Z_m) + (X_cX_{c_+} - AZ_cZ_{c_+})^2$$

$$Z_{2c+1} \leftarrow \frac{X_1}{Z_1}(X_cZ_{c_+} - X_{c_+}Z_c)^2$$

$$X_c \leftarrow X_{2c}$$

$$Z_c \leftarrow Z_{2c}$$

$$X_{c_+} \leftarrow X_{2c+1}$$

$$Z_{c_+} \leftarrow Z_{2c+1}$$

if $x_i = 1$

then $c \leftarrow 2c+1$

$c_+ \leftarrow 2(c+1)$

$$X_{2c+1} \leftarrow -4BZ_cZ_{c_+}(X_cZ_{c_+} + X_{c_+}Z_m) + (X_cX_{c_+} - AZ_cZ_{c_+})^2$$
$$X_{2(c+1)} \leftarrow (X_{c_+}^2 - AZ_{c_+}^3 + AX_{e_+}Z_{c_+}^2 + BZ_{c_+}^3)$$

$X_c \leftarrow X_{2c+1}$

$Z_c \leftarrow Z_{2c+1}$

$X_{c_+} \leftarrow X_{2(c+1)}$

$Z_{c_+} \leftarrow Z_{2(c+1)}$

else $c \leftarrow 2c$

$c_+ \leftarrow 2c+1$

Remark 4: For any point $M \in E(Z_n)$ where $n = pq$, the point $M = (M \bmod p, M \bmod q)$ as $E(Z_{pq});\ E(Z_p) \oplus E(Z_q)$ and therefore the formulas in Theorems 1, 2 and 3 are valid for M on $E(Z_{pq})$.

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. THE GCD ATTACK ON DEMYTKO'S CRYPTOSYSTEM WITH PROJECTIVE COORDINATES

Demytko's System:

In this paper we impliment the gcd attack on Demytko's system using point addition with projective coordinated given as in above theorems. We first describe Demytko's system.

In this system sender chooses two large primes p, q and makes $n = pq$ public. If m is the message to be sent sender takes $m = M_x$, for $M = (M_x, M_y)$ a point on an elliptic curve $E_{A,B} : y^2 = x^3 + Ax + B \bmod n$ with $(\Delta, n) = 1$.

Encryption: For $N_n = \# E_n$, sender chooses $(e, N_n) = 1$ and d be such that

$ed \equiv 1 \bmod N_n$ then e is made public.

The sender encrypts the m as $C = x(Me) = \dfrac{X_e}{Z_e}$ and $[X_e : Z_e]$ computed by using the point addition with projective coordinates.

Decryption:

Receiver recover s$m$by $x(M) = x(M_{ed}) \bmod n$as

$$x(dC) = x(edM)$$

$$= \frac{X_{ed}}{Z_{ed}} \bmod n$$

$$= x(M) \text{in} E(Z_n) \text{as } ed \equiv 1 \bmod N_n.$$

Let m be the message such that $m = x(M)$ for M a point on elliptic curve mod N for $N = pq$ and for $(e, \# E(Z_N)) = 1$ let (e, N) be the public key and if $C_x = x(C)$ for $C = eM$ is the cipher text.

In gcd attack the cryptanalyst chooses a random integer k, such that $(k, e) = 1$ and computes $\tilde{C}_x = x(kC)$ and sends $\tilde{C}_x$ to the receiver, the receiver computes $C_x^{'} = x(d\tilde{C})$ finds $C_x^{'}$ irrelevant and discards, then cryptanalyst gets hold of $C_x^{'}$ and recovers $x(M)$ as follows.

The projective co-ordinates of a point M on E are given as $M = (X, Y, Z)$ then for point addition eM of M the projective coordinates are denoted as (X_e, Z_e, M_e) as we have formulas for $[X_e : Z_e]$ as in the Theorem 1 and $x(eM) = \dfrac{X_e}{Z_e}$ and for $\dfrac{X}{Z} = x, X_e = X_e(x)$ and $Z_e = Z_e(x)$, we implement the point addition on projective coordinates as in Theorem 1 and find $[X_e : Z_e]$.

Now the cryptanalyst consider the polynomials $X_e(x), Z_e(x), X_k(x)$ and $Z_k(x)$ as in Remark 1 for a variable x and takes

$$P(x) = X_e(x) - C_x Z_e(x) \bmod N,$$

$$Q(x) = X_k(x) - C_{x'} Z_k(x) \bmod N.$$

Now note for $x = x(M)$ solves the polynomials $P(x)$ and $Q(x)$, there fore as $x - m$ is a common factor of $P(x), Q(x)$, the cryptanalysis recovers the message $m = x(M)$ from the $\gcd(P(x), Q(x))$, further note $P(x), Q(x)$ is of high probability that gcd is a linear polynomial, for $x = \tilde{m}$ is any other common solution for $P(x)$ and $Q(x)$ then we have

$$\begin{cases} X_e(\tilde{m}) - C_x(Z_e(\tilde{m})) = 0 \\ X_k(\tilde{m}) - C'_x(Z_k(\tilde{m})) = 0. \end{cases}$$

Suppose $\begin{cases} Z_e(\tilde{m}) \neq 0 \bmod N \text{and} \\ Z_k(\tilde{m}) \neq 0 \bmod N, \end{cases}$ then

$$\begin{cases} \dfrac{X_e(\tilde{m})}{Z_e(\tilde{m})} - C_x = 0 \\ \dfrac{X_k(\tilde{m})}{Z_k(\tilde{m})} - C_{x'} = 0. \end{cases}$$

That is for $\tilde{M} = (\tilde{M}_x, \tilde{M}_y)$ with $\tilde{M}_x = \tilde{m}$, we have

$$\begin{cases} x(e\tilde{M}) - C_x = 0 \\ x(k\tilde{M}) - C_{x'} = 0. \end{cases}$$

Therefore we have $\begin{cases} x(e\tilde{M}) - x(eM) = 0 \\ x(k\tilde{M}) - x(kM) = 0. \end{cases}$

Now as $(e,k) = 1$ there exist r, s such that $er + ks = 1$.
Then $x(r(e\tilde{P})) - x(r(eP)) = 0$ and $x(s(k\tilde{P})) - x(s(kP)) = 0$.
Which implies that $x((er+ks)\tilde{P}) - x((er+sk)P) = 0$.
This gives that $x(\tilde{P}) - x(P) = 0$.

Then $\tilde{m} - m = 0$.

Therefore $m = \tilde{m}$.

Example: Take $M = (1,122)$ a point on elliptic curve $E : y^2 = x^3 + 3x + 8$ over $E(Z_{143})$ then as $\# E(Z_{143}) = 144$. Choose $e = 5$ and take $k = 2$.

Computations of C_x:

$C_x = x(C) = x(eM) = \dfrac{X_e}{Z_e}$. Now Using the fast computation method we find $[X_e : Z_e]$ as follows:

For $e = 5 = 1\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0$ with $e_0 = 1$ and as $M = (X_1, Y_1, Z_1) = (1,122,1)$,
we have $[X_{e_0} : Z_{e_0}] = [X_1 : Z_1] = [1:1]$.
Now for $X_{e_0} = 1, Z_{e_0} = 1$, we have

$$X_{e_1} = X_{2e_0} = (X_{e_0}^2 - AZ_{e_0}^2)^2 - 8BX_{e_0}Z_{e_0}^3 = 83,$$

$$Z_{e_1} = Z_{2e_0} = 4Z_{e_0}(X_{e_0}^3 + AX_{e_0}Z_{e_0}^2 + BZ_{e_0}^3) = 48;$$

$$X_{e_1+1} = -4BZ_{e_0}Z_{e_0+1}\left(X_{e_0}Z_{e_0+1} + X_{e_0+1}Z_{e_0}\right) + \left(X_{e_0}X_{e_0+1} - AZ_{e_0}Z_{e_0+1}\right)^2 = 131,$$

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

$$X_{e_2} = -4BZ_{e_1}Z_{e_1+1}\left(X_{e_1}Z_{e_1+1} + X_{e_1+1}Z_{e_1}\right) + \left(X_{e_1}X_{e_1+1} - AZ_{e_1}Z_{e_1+1}\right)^2 = 68,$$

$$Z_{e_2} = \frac{X}{Z}\left(X_{e_1}Z_{e_1+1} - X_{e_1+1}Z_{e_1}\right)^2 = 36;$$

$$\text{Therefore } C_x = \frac{X_e}{Z_e} = \frac{X_{e_2}}{Z_{e_2}} = \frac{68}{36} = 129 \bmod 143.$$

Computation of $C_{x'}$:

As
$C_{x'} = X(d\tilde{C}) = x(d(kC_x)) = x(k(d(eM))) = x(kM)$, we have for $k = 2$ and $M = (1,122) \in E(Z_{143})$,

$$C'_x = x(C') = x(kM) = \frac{X_k}{Z_k}.$$

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

$$X_{e_1} = X_{2e_0} = (X_{e_0}^2 - AZ_{e_0}^2)^2 - 8BX_{e_0}Z_{e_0}^3 = 83,$$

$$Z_{e_1} = Z_{2e_0} = 4Z_{e_0}(X_{e_0}^3 + AX_{e_0}Z_{e_0}^2 + BZ_{e_0}^3) = 48;$$

Therefore $C'_x = \dfrac{X_k}{Z_k} = \dfrac{83}{48} = 106 \bmod 143$, the cryptanalyst gets hold of $C_{x'}$ computed by the receiver.

Then for $e = 5, k = 2$ and $N = 143$ the cryptanalyst consider the polynomials $X_5(x), Z_5(x)$ and $X_2(x), Z_2(x)$ as follows:

$$P(x) = X_e(x) - C_x Z_e(x) \bmod N,$$

$$Q(x) = X_k(x) - C_{x'} Z_k(x) \bmod N.$$

Taking $[X_{e_0} : Z_{e_0}] = [x:1]$

we have for $e = 5 = 1\cdot 2^2 + 0\cdot 2^1 + 1$;

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

$$= X_{e_1} = X_{2e_0} = x^4 - 6x^2 - 64x + 9 \text{and} Z_{e_1}$$
$$= 4x^3 + 12x + 32.$$

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

$$= x^{10} - 36x^8 - 53x^7 + 127x^6 + 139x^5 + 40x^4 + 24x^3 - x^2 + 33x.$$

$$Z_{e_1+1} = x(x_{e_0}Z_{e_0+1} - X_{e_0+1}Z_{e_0})^2$$
$$= 9x^9 + 108x^7 + 4x^6 + 127x^5 + 24x^4 + 26x^3 + 131x^2 + 81x.$$

$$X_{e_2} = -32(4x^3 + 12x + 32)(9x^9 + 108x^7 + 4x^6 + 127x^5 + 24x^4 + 26x^3 + 131x^2 + 81x)$$
$$[(x^4 - 6x^2 - 64x + 9)(9x^9 + 108x^7 + 4x^6 + 127x^5 + 24x^4 + 26x^3 + 131x^2 + 81x) + (x^{10} - 36x^8 - 53x^7 + 127x^6 + 139x^5 + 40x^4 + 24x^3 - x^2 + 33x)(4x^3 + 12x + 32)] +$$
$$[(x^4 - 6x^2 - 64x + 9)(x^{10} - 36x^8 - 53x^7 + 127x^6 + 139x^5 + 40x^4 + 24x^3 - x^2 + 33x) - 3(4x^3 + 12x + 32)(9x^9 + 108x^7 + 4x^6 + 127x^5 + 24x^4 + 26x^3 + 131x^2 + 81x)]^2.$$

$$= x^{28} + 129x^{26} + 91x^{25} + 87x^{24} + 110x^{23} + 99x^{22} + 140x^{21} + 98x^{20} - x^{19} + 14x^{18} + 6x^{17} + 136x^{16} + 64y^{15} + 84x^{14} + 60x^{13} + 135x^{12} + 108x^{11} + 135x^{10} + 108x^9 + 18x^8 + 121x^7 + 13x^6 + 49x^5 + 89x^4 + 33x^3.$$

$$Z_{e_2} = x[(x^4 - 6x^2 - 64x + 9)(9x^9 + 108x^7 + 4x^6 + 127x^5 + 24x^4 + 26x^3 + 131x^2 + 81x) - (x^{10} - 36x^8 - 53x^7 + 127x^6 + 139x^5 + 40x^4 + 24x^3 - x^2 + 33x)(4x^3 + 12x + 32)]^2.$$

$$= 25x^{27} + x^{25} + 84x^{24} + 121x^{23} + 7x^{22} + 99x^{21} + 100x^{20} + 108x^{19} + 114x^{18} + 45x^{17} + 39x^{16} + 97x^{15} + 79x^{14} + 119x^{13} + 56x^{12} + 26x^{11} + 19x^{10} + 54x^9 + 26x^8 + 53x^7 + 5x^6 + 38x^5 + 43x^4 + 108x^3.$$

We have $X_{e_x} = X_5(x) = X_{e_2}(x)$

$$Z_{e_x} = Z_5(x) = Z_{e_2}(x).$$

and for $k = 2, X_k(x) = X_2(x)$

$$= X_{2e_0}(x) = x^4 - 6x^2 - 64x + 9.$$
$$Z_k(x) = Z_2(x) = Z_{2e_0}(x) = 4x^3 + 12x + 32.$$

Then cryptanalyst takes the polynomials

$$P(x) = X_5(x) - C_x Z_5(x) \bmod 143,$$
$$Q(x) = X_2(x) - C'_x Z_2(x) \bmod 143.$$

Now note $x = 1$, solves $P(1)$ and $Q(1)$, i.e.,

$$P(1) = X_5(1) - 129Z_5(1)$$
$$= 1927 - 129(1466) = 0 \bmod 143,$$

$$Q(1) = X_2(1) - 106Z_2(1) = 83 - 106(48) = 0 \bmod 143.$$

Therefore $x-1$ is a common factor of $P(x)$ and $Q(x)$ and also note $x-1$ is the only common factor.

Hence the cryptanalyst recovers the message $m = 1$ from the $\gcd(P(x), Q(x))$, note the computation of gcd is easy by an appropriate choice of k.

5. CONCLUSION

In the gcd attack on Demytko's system by Marc Joye and Jean-Jacques Quisquater in the paper " On the importance of securing your bins: The garbage-man-in-the-middle attack" division polynomials are used. In this paper we mounted the attack by replacing the division polynomials with polynomials generated by the recursive formulas for $[X_k : Z_k]$ of the projective coordinates $[X_k, Y_k, Z_k]$ and in the evaluation of polynomials $P(x)$ and $Q(x)$ fast computation method plays a vital role in the computation of $[X_k : Z_k]$, $[X_e : Z_e]$ and these polynomials are easy to handle than the division polynomials.

6. REFERENCES

[1] R. Balasubramanian "Elliptic Curves and Cryptography" proceedings of the advanced instructional workshop on Algebraic number theory, *HBA (2003)325-345*

[2] I.F.Blake, G. Seroussi and N. P. Smart "Elliptic Curves in Cryptography", volume 265 of London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 2000.

[3] J. Buchmann"Introduction to cryptography" , Springer-Verlag 2001.

[4] 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.

[5] Jeffery Hoftstein, Jill Pipher, Joseph H. Silverman, " An Introduction to Mathematical Cryptography", Springer.

[6] D. Husemoller. Elliptic Curves, 2nd edition, volume 111 of Graduate Texts in Mathematics. Springer-Verlag, New York, 2004. With appendices by O. Forster, R. Lawrence, and S. Theisen.

[7] Marc Joye and Jean - Jacques Quisquater, " On the importance of securing your bins: The garbage-man-in-the-middle attack", ACM Press, 1997.

[8] 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.

[9] 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.

[10] Neal Koblitz " Algebraic Aspects of Cryptography", volume 3 of Algorithms and Computation in Mathematics. Springer-Verlag, Berlin, 1998.

[11] Neal Koblitz " Elliptic Curve Cryptosystems" Mathematics of Computation, 48: 203-209, 1987.

[12] Neal Koblitz "A course in number theory and cryptography ISBN 3-578071-8,SPIN 10893308 "

[13] H.W. Lenstra, JR. Elliptic Curves and Number-Theoretic Algorithms .Proceedings of the International Congress of Mathematicians, Berkeley, California, USA, 1986.

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

[15] 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.

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

[17] Lawrence C. Washington "Elliptic Curves Number Theory and Cryptography" 2nd edition, CRC press.

[18] Lawrence C. Washington, Wade Trappe "Introduction to Cryptography with Coding Theory" 2nd edition, Pearson

.