Resisting Side Channel Attack on Elliptic Curve Cryptosystem

Jayaprakash Kar
Department of Information Technology
Al Musanna College of Technology
Sultanate of Oman
jayaprakashkar@yahoo.com

***Abstract*—In this paper several elliptic curve multiplication algorithms which are secure against Side Channel Attacks (SCA) have been described. Also countermeasure against Differential Power Analysis have been specified. Subsequently uses Here Coron's dummy algorithm for scalar multiplication which is the countermeasure against Simple Power Analysis and discuss about the efficiency of the algorithm in term of addition, subtraction, multiplication and inverse operations.**
Keywords: Side Channel Attack, ECC, DPA.

I. INTRODUCTION

The Internet has become the most convenient, affordable, widely connected and accepted medium for data communication now. While billions of users worldwide are sharing the same network, sensitive information must be adequately protected from 'prying eyes'. The search for newer and newer PKC's and their cryptanalysis has become a part of the mainstream of computer scientific research. The reason for search of newer cryptosystems is twofold: firstly,to increase the ease at which the task of encryption and decryption can be carried out and secondly, to reduce the computational overhead involved. In PKC's the breaking of the cryptosystem is the getting hold of one's secret private key with feasible amount of computations. Naturally, the larger the private key, the more secure is the cryptosystem. However the length of the private key is a computational overhead and a smaller key length means more efficiency.

These are perticularly suitable for implementation of on handheld devices such as smart cards, PDA etc. Due to physical characteristics of such devices the power consumption and time consumption using the secret key can be clearly observed.Thus Side Channel Attack(SCA)are a serious threat against these devices.

The main target for Side Channel Attack(SCA) against ECC implementation is the algorithm used for scalar multiplication on the elliptic curve.

II. BACKGROUND

This section describes about Elliptic Curve Arithmetics, elementary concepts of Elliptic Curves and Elliptic Curve Discrete Logarithm Problem.

A. Elementary concepts of Elliptic Curve

An elliptic curve E over a field K is defined by an equation of the form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (1)$$

where $a_1, a_2, a_3, a_4, a_6 \in K$ and $\Delta \neq 0$

Δ is called discriminant of E and is defined as follows

$$\Delta = -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6$$

$$d_2 = a_1^2 + 4a_2$$

$$d_4 = 2a_4 + a_1a_3$$

$$d_6 = a_3^2 + 4a_6$$

$$d_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$$

If L is any extension field of K , then the set of L rational points on E is

$$E(L) = \{(x, y) \in L\times L : y^2+a_1xy+a_3y-x^3-a_2x^2-a_4x-a_6\}\cup\{\mathcal{O}\}$$

where $\mathcal{O}$ is a special point, called the point at infinity . The equation is called Weierstrass equation [4]. If characteristics of $K \neq 2$ or 3 then the admissible change of variables

$$(x, y) \rightarrow (\frac{x - 3a_1^2 - 12a_2}{36}, \frac{y - 3a_1x}{216} - \frac{a_1^3 + 4a_1a_2 - 12a_3}{24})$$

transform E to the curve $y^2 = x^3 + ax + b$ where $a, b \in K$ and $\Delta = -16(4a^3 + 27b^2)$
We will consider the elliptic curve E of the above simplified equation and have no multiple roots i,e $4a^3 + 27b^2 \neq 0$

B. Group Law

Let E be an elliptic curve defined over the field $K0$. There is a chord and tangent rule for adding two point in $E(K)$,if $P_1, P_2 \in E(K)$ then $P_1 + P_2 \in E(K)$ denoted as a third point R which is the reflection of the point of intersection of the chord P_1P_2 to the curve for $P_1 \neq P_2$. If $P_1 = P_2$ then the tangent of $E(K)$ at P_1 gives rise to the point $P_1 + P_2$. The double R of P is defined as follows
First draw a tangent line intersect the elliptic curve at a second point.Then R is the reflection of this point about X-axis. $E(K)$ form an abelian group with addition operation .

978-1-4244-8767-7 /11/$26.00 ©2011 IEEE

Group Law for $E/K : y^2 = x^3 + ax + b$

1) Identity : $P + \mathcal{O} = \mathcal{O} + \mathcal{P} = \mathcal{P}$, for all $P \in E(K)$
2) Negative : if $P(x, y) \in E(K)$ then $(x, y)+(x, -y) = \mathcal{O}$, The point (x,-y) is dented as -P called negative of P.
3) Point addition: Let $P((x_1, y_1), Q(x_2, y_2) \in E(K)$,then $P + Q = R \in E(K)$ and coordinate $(x_3, y_3)$of R is given by $x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = \lambda(x_1 - x_3) - y_1$ where $\lambda = \frac{y_2-y_1}{x_2-x_1}$
4) Point doubling : Let $P(x_1, y_1) \in E(K)$ where $P \neq -P$ then $2P = (x_3, y_3)$ where $x_3 = (\frac{3x_1^2+a}{2y_1})^2 - 2x_1$ and $y_3 = (\frac{3x_1^2+a}{2y_1})(x_1 - x_3)$- y_1

Group Order

Let E be the elliptic curve defined over the field F_q. The no. of points in $E(F_q)$ denoted as $\#E(F_q)$ is called the order of E over F_q.

Theorem 1. Hasse's Theorem

It states that number of points $\#E(F_q) = q + 1 - t$,where $t \leq 2\sqrt{q}$ or we can write $(q + 1 - 2\sqrt{q}) \leq t \leq (q + 1 + 2\sqrt{q})$,$[q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]$ is called Hasse interval.

Group Structure

Ler E be the elliptic curve defined over F_q, then E_q is isomerphic to $Z_{n_1} \oplus Z_{n_2}$. Where n_1 and n_2 are uniquely determined positive integer such that n_2/n_1 and $n_2/q - 1$. $\#E(F_q) = n_1 n_2$, If $n_2 = 1$ then $E(F_q)$ is a cyclic group. If $n_2 > 1$ then $E(F_q)$ is said to have rank 2.

C. Point representation and the group law

Since inversion in K is significantly more expensive than other field operations during the computation of doubling and adding of points, several other co-ordinate system have been proposed in litrature. Projective and jacobian co-ordinate are described below.

Projective Co-ordinate

Let K be a field and c and d be positive integers. It can be defined an equivalence relation $\sim$ on the set $K^3\backslash\{(0, 0, 0)\}$ of nonzero triples over K by
$(X_1, Y_1, Z_1) \sim (X_2, Y_2, Z_2)$ if $X_1 = \lambda^c X_2, Y_1 = \lambda^d Y_2, Z_1 = \lambda Z_2$ for some $\lambda \in K_*$
The equivalence class containing $(X, Y, Z) \in K^3\backslash\{(0, 0, 0)\}$ is
(X:Y:Z) = $(\lambda^c X, \lambda^d, \lambda Z) : \lambda \in K^*$
(X:Y:Z) is called projective point and (X,Y,Z) is called a representative of (X:Y:Z)
Negaive of the point P i.e $-P$ = (X:-Y:Z) and point at infinity is (0:1:0).

Jacobian Coordinade

The is a perticular of Projective co-ordinate. Here $c = 2$ and $d = 3$. The projective point (X:Y:Z), $Z \neq 0$,corresponds to the affine point $(X/Z^2, Y/Z^3)$
The point at infinity corresponds to $(1 : 1 : 0)$ and negative of $(X : Y : Z)$ is $(X : -Y : Z)$

Definition 1. Elliptic Curve Discrete Logarithm Problem

The elliptic curve discrete logarithm problem(ECDLP) is :given an elliptic curve E defined over a finite field F_q,a point $P \in E(F_q)$ of order n, and a point $Q \in< P >$,find the integer $l \in [0, n-1]$ such that $Q = lP$.The integer l is called discrete logarithm of Q to base P, denoted $l = log_p Q$.

III. ELGAMAL CRYPTOSYSTEM

There are numerous cryptosystem based their security on the difficuly of solving the Discrete Logarithm Problem.One such public key cryptosystem is the **ElGamal Cryptosystem** in F_p.Which is .
Let p be a prime number such that the DLP in F_p is intracible,and let $\alpha \in F_p$ be a primitive element and α is publicly known. User X chooses a secret key a_X and publishes β where $\beta \equiv \alpha^{a_X} (\mathrm{mod} p)$.
Let Alice send her message $x \in F_p$, she will choose a random number $k \in Z_p^*$ and send

$$(y_1, y_2) = (\alpha^k \bmod p, x\beta^k \bmod p)$$

To decrypt, the recipient Bob computes

$$y_2(y_1^{a_B})^{-1} \bmod p.$$

Where a_B is the secret key.
The decryption is done as

$$y_2(y_1^{a_B})^{-1} \equiv x\beta^k(\alpha^{ka_B})^{-1} \equiv x\alpha^{a_B k} \equiv x \bmod p$$

An attacker could decrypt Alice's message is Bob's secret key $a_B$could be computed from $\beta \equiv \alpha^{a_B} (\mathrm{mod} p)$ and α which is publicly known. This is the DLP.
Since the ElGamal protocol can be generalized to work in an arbitary finite cyclic group,in 1987 Kobliz proposed that it is implemented on an elliptic curve over the field. This is described as below.

Let F be a finite field,an elliptic curve is defined over F and a base point $P \in E(F)$.
All of these are fixed and publicly known.User X of this system chooses,a random integer a_X which is the own secret key, then computes and publishes the point $a_X P$.
Suppose Alice wishes to send a message M to Bob.First she imbeds the value m on to the elliptic curve E i.e she represent the plaintext M as a point $P_m \in E$.Now she encrypt P_m.
Let a_B be the bob's secret key,so $Q = a_B P$ will be publicly known. Alice first chooses a random number k and sends Bob a pair of points on E:

$$(C_1, C_2) = (kP, P_m + kQ)$$

To decrypt the cyphertext,Bob computes
$C_2 - a_B(C_1) = P_m + k(a_B P) - a_B(kP) = P_m$

Algorithm 1 (Elliptic curve encryption)

INPUT : Elliptic curve domain parameters (p, E, P, n),public key Q,plain text m

OUTPUT: Cipher text (C_1, C_2)

1) Represent the message m as a point $M \in E(F_p)$
2) Select $k \in [1, n-1]$
3) Compute $C_1 = kP$
4) Compute $C_2 = M + kQ$
5) return (C_1, C_2)

Algorithm 2 (Elliptic curve decryption)
INPUT : Elliptic curve domain parameters (p, E, P, n),private key a_B,cipher text (C_1, C_2)
OUTPUT: Plain text m

1) Compute $M = C_2 - a_B C_1$ and extract m from M
2) return (m)

A. Cryptanalytic attack on ECC

1) General Attack against ECDLP : The discrete logarithm problem (DLP) became important to cryptographers with the invention of public-key cryptography by Diffie and Hellman in 1976 [3]. The best algorithm known for solving DLP in prime fields is the number field sieve which has a subexponential expected running time:
$exp((1.923 + o(1))\ (log\ p)^{1/3}(log\ log\ p)^{2/3})$. To circumvent this attack, the prime p should be chosen to be sufficiently large. As of today's computer technology, a prime p of length 1024 bits is recommended for medium-term security. For long-term security, even a larger modulus is recommended. As a consequence of this, the implementation of discrete log cryptosystems using the group Z_p is infeasible or impractical in some resource constrained computational devices like smart cards and hand-held wireless devices, such as cellphones and pagers. Since the discovery of Public Key Cryptography in 1976, a variety of groups have been proposed for use in discrete log cryptosystems. These include:

1) the multiplicative group of a finite field of characteristic 2 or a proper subgroup of it,
2) the group of units of Z_n , n being a composite integer.
3) the group of points on an elliptic curve defined over a finite field.
4) the Jacobian of a hyperelliptic curve defined over a finite field.
5) the class group of an imaginary quadratic number field.
6) the Jacobian of a superelliptic curve defined over a finite field .

Why so many alternative groups are being consided for the purpose? There are two primary reasons. First one is, the operation in some groups may be easier to implement in software or in hardware than the operation in other groups. Secondly, the DLP in the group may be harder than the DLP in other groups. Consequently, one could use a group G that is smaller than Z_p while maintaining the same level of security. This potentially gives rise to smaller key sizes, bandwidth savings, and faster implementations.

Among these groups, $E(F_q)$, the group of F_q-rational points of an elliptic curve E, defined over a finite field F_q , is an attractive choice. By Hasse's Theorem, the order of the group is almost equal to q. If the largest prime factor of this order is n, then the best algorithm known for the DLP in $E(F_q)$ (Pollard's rho attack) takes $O(\sqrt{n})$ steps; i.e., the algorithm take fully exponential time. As a result, E(F_q) where q is a 160 bit integer, can achieve the same level of security as when a group Z_p is used with a 1024 bit integer. That is almost a 84 percent saving of bandwidth.

One disadvantage of using curves of higher genus instead of elliptic curves is that the group operation in the former may be computationally more expensive and more complex, even though the underlying field size is much smaller. In fact, in cryptography there is still much scope for research in that direction. Also, this disadvantage can be overcome by designing specific hardware, to be used in resource constrained systems.

The elliptic curve parameter for cryptographic shemes should be carefully choosen in order to resist all known attacks on ECDLP.The most naive algotithm for solving the ECDLP is exhaustive search whereby one computes the sequece of points until Q is encountered.

The running time is aproximatelyn steps in worst case and $n/2$ steps in average.Therefore exhausive search can be circumvented by selecting elliptic curve parameters with sufficiently large to represent an infeasible amount of computation.

To resist this attack,the elliptic curve parameter should be choosen so that n is divisible by a prime number p sufficiently large so that $\sqrt{(p)}$ steps is an infeasible amount of coumputation.(e.g $p > 2^{160}$)
If in addition,the elliptic curve parameters are choosen to defeat all other known attacks, then ECDLP is believed to be insfeasible given the state of todays computer technology. The best general algorithm are given below

1) **Naive Exhaustive Search:**
2) **Pohlig Hellman Algorithm:** [12]Exploits factorization of $n = \ O(P)$.The algorithm reduces the problem of recovering λ to the problem of recovering λ modulo each prime factor of λ, λ is then recovered by Chinese remainder theorem.
3) **Baby-step Giant-step Algorithm :**
4) **Pollard's Rho Algorithm:**
5) **Parallelised Pollard's rho algorithm:** executes Pollard's rho algorithm parallelly in r processors. Runs in $O(m)/(2r)$ steps.
6) **Pollard's Lambda Algorithm :** another randomised algorithm due to Pollard. It can also be parallelised with a linear speedup. Slightly slower than parallelised rho method. Faster if λ is known to be in a subinterval $[0, b]$ of $[0, n-1]$ where $b < 0.39n$.

7) **Index-Calculus Method:** First of all we attempt to find the logarithms of elements of a fixed subset $S = \{\sigma_1, \sigma_2, \ldots, \sigma_\tau\}$ of G, called the factor base. We pick a random integer s and try to express α^s as

$$\sigma_1^{a_1}\sigma_2^{a_2}\ldots\sigma_\tau^{a_\tau}$$

. If we are successful, then taking logarithms we get,

$$s = a_1 log_\alpha \sigma_1 + a_2 log_\alpha \sigma_2 + \ldots + a_\tau log_\alpha \sigma_\tau \pmod n$$

After collecting a sufficient number of such relations, we can hopefully solve for the indeterminates $log_\alpha \sigma_i$. Next, we repeatedly pick random integers until $\alpha^s\beta$ can be written as a product of elements in S, i.e.

$$\alpha^s\beta = \sigma_1^{b_1}\sigma_2^{b_2}\ldots\sigma_\tau^{b_\tau}$$

Taking logarithms in both the sides we get

$$log_\alpha\ \beta = b_1 log_\alpha \sigma_1 + b_2 log_\alpha \sigma_2 + \ldots + b_\tau log_\alpha \sigma_\tau - s \pmod n$$

The running time for this algorithm is $O(exp((2 + o(1))(lnp)^{1/2}(lnlnp)^{1/2}))$ for F_p.

8) **MOV attack:**

IV. Side Channel Attack against ECC

Side Channel Attack (SCA) allowed adversaries to obtain the secret key in the cryptographic device, or partial information on it by observing information such as computing time and power consumption. This is the idea of simple and differential power analysis was first introduce by Kocher [8]. This is a serious threat espesially to mobile device such as smart cards.Thus implimenters need algorithm that are not only efficent but also SCA registant.

Simple power analysis is a technique that involves directly interpreting power consumption measurement collected during cryptographic operations.SPA can yield information about device's operation as well as key material.

Differential power analysis is the technique that involve in large scale power variation due to the instruction sequence. There are effect correlated to data values being manipulated. These variations tend to be smaller and are some times overshadowed by measurement errors and other noise. In such cases,it is still often possible to breake the system using statistical fuctions tailored to the target algorithm.

In scalar multipliation algorithm two function *elliptic curve adding* (ECADD) and *elliptic curve doubling* (ECDBL) havae to be executed.

A. Addition and Doubling Algorithms and their Efficiency

The curve in the simplified form of *Weierstress Equation* is given by

$$E : y^2 = x^3 + ax + b \tag{2}$$

The coefficient a is arbitary field element.However many curve recomended by specification such as [NIST,ANSI,SEC2] use $a = -3$ for more efficent ECDBL implementation. The general algorithm ECDBL requires time $4M + 6S + 11A$, where M,S and A denote time needed for multiplication,squaring and adding respectively. This uses 6 auxiliary variables.The optimized algorithm ECDBL for $a = -3$ requires $4M + 4S + 3A$ using 5 auxiliary variables

Algorithm (ECDBL)

Input:(X_1, Y_1, Z_1, a)
Output:(X_2, Y_2, Z_2)
$R_4 \leftarrow X_1, R_5 \leftarrow Y_1, R_6 \leftarrow Z_1$
$R_1 \leftarrow R_4^2$
$R_2 \leftarrow R_5^2$
$R_2 \leftarrow R_2 + R_2$
$R_4 \leftarrow R_4 * R_2$
$R_4 \leftarrow R_4 + R_4$
$R_2 \leftarrow R_2^2$
$R_2 \leftarrow R_2 + R_2$
$R_3 \leftarrow R_6^2$
$R_3 \leftarrow R_3^2$
$R_6 \leftarrow R_5 * R_6$
$R_6 \leftarrow R_6 + R_6$
$R_5 \leftarrow R_1 + R_1$
$R_1 \leftarrow R_1 + R_5$
$R_3 \leftarrow a * R_4$
$R_1 \leftarrow R_1 + R_3$
$R_1 \leftarrow R_1^2$
$R_1 \leftarrow R_4 + R_4$
$R_3 \leftarrow R_3 - R_5$
$R_5 \leftarrow R_4 - R_5$
$R_5 \leftarrow R_1 * R_4$
$R_4 \leftarrow R_1 - R_2$
$X_2 \leftarrow R_5, Y_2 \leftarrow R_4, Z_2 \leftarrow R_6$

Algorithm ECDBL for $a = -3$

Input:(X_1, Y_1, Z_1)
Output:(X_2, Y_2, Z_2)
$R_4 \leftarrow X_1, R_5 \leftarrow Y_1, R_6 \leftarrow Z_1$
$R_2 \leftarrow R_5^2$
$R_2 \leftarrow R_2 + R_2$
$R_3 \leftarrow R_4 * R_2$
$R_3 \leftarrow R_3 + R_3$
$R_2 \leftarrow R_2^2$
$R_2 \leftarrow R_2 + R_2$
$R_5 \leftarrow R_5 * R_6$
$R_5 \leftarrow R_5 + R_5$
$R_6 \leftarrow R_6^2$
$R_4 \leftarrow R_4 + R_6$
$R_6 \leftarrow R_6 + R_6$
$R_6 \leftarrow R_4 - R_6$
$R_4 \leftarrow R_4 * R_6$
$R_6 \leftarrow R_4 + R_4$
$R_4 \leftarrow R_4 + R_6$
$R_6 \leftarrow R_4^2$
$R_6 \leftarrow R_6 - R_3$
$R_6 \leftarrow R_6 - R_3$
$R_3 \leftarrow R_3 - R_6$

$R_4 \leftarrow R_4 * R_3$
$R_4 \leftarrow R_4 - R_2$
$X_2 \leftarrow R_5, Y_2 \leftarrow R_4, Z_2 \leftarrow R_5$

For ECADD,we consider two cases : The general case of addition of point given in Jacobian co-ordinates and the special case where one of the input point has Z co-ordinate of 1 i.e represented in affine co-ordinates.The general case requires time $12M + 4S + 7A$ using 7 auxiliary variables and the other case $(Z = 1)$ requires $8M + 3S + 7A$ using 7 auxiliary variables.

The algorithm are given below

Algorithm (ECADD using Jacobian Co-ordinate)

Input:$(X_1, Y_1, Z_1, (X_2, Y_2, Z_2)$
Output:(X_3, Y_3, Z_3)

$R_2 \leftarrow X_1, R_3 \leftarrow Y_1, R_4 \leftarrow Z_1$
$R_5 \leftarrow X_2, R_6 \leftarrow Y_2, R_7 \leftarrow Z_2$
$R_1 \leftarrow R_7^2$
$R_2 \leftarrow R_2^1$
$R_3 \leftarrow R_3 * R_7$
$R_3 \leftarrow R_3 * R_1$
$R_1 \leftarrow R_4^2$
$R_5 \leftarrow R_5 * R_1$
$R_6 \leftarrow R_6 * R_4$
$R_6 \leftarrow R_6 * R_1$
$R_5 \leftarrow R_5 - R_2$
$R_7 \leftarrow R_4 * R_7$
$R_7 \leftarrow R_5 + R_7$
$R_1 \leftarrow R_5^2$
$R_4 \leftarrow R_6^2$
$R_2 \leftarrow R_2 * R_1$
$R_5 \leftarrow R_1 * R_5$
$R_4 \leftarrow R_4 - R_5$
$R_1 \leftarrow R_2 + R_2$
$R_4 \leftarrow R_4 - R_1$
$R_2 \leftarrow R_2 - R_4$
$R_6 \leftarrow R_6 * R_2$
$R_1 \leftarrow R_3 * R_5$
$X_1 \leftarrow R_6 - R_1$
$X_3 \leftarrow R_4, Y_3 \leftarrow R_1, Z_3 \leftarrow R_7$

Algorithm ECADD for $Z_1 = 1$

Input:$(X_1, Y_1, X_2, Y_2, Z_2$
Output:(X_3, Y_3, Z_3)

$R_2 \leftarrow X_1, R_3 \leftarrow Y_1, R_5 \leftarrow X_2, R_6 \leftarrow Y_2, R_7 \leftarrow Z_2$
$R_1 \leftarrow R_7^2$
$R_2 \leftarrow R_2 * R_1$
$R_3 \leftarrow R_3 + R_7$
$R_3 \leftarrow R_3 * R_1$
$R_5 \leftarrow R_5 - R_2$
$R_7 \leftarrow R_5 * R_7$
$R_6 \leftarrow R_6 - R_3$
$R_1 \leftarrow R_5^2$
$R_4 \leftarrow R_6^2$
$R_2 \leftarrow R_2 * R_1$
$R_5 \leftarrow R_1 * R_5$
$R_4 \leftarrow R_4 - R_5$
$R_1 \leftarrow R_2 + R_2$
$R_4 \leftarrow R_4 - R_1$
$R_2 \leftarrow R_2 - R_4$
$R_6 \leftarrow R_6 * R_2$
$R_1 \leftarrow R_3 * R_5$
$R_1 \leftarrow R_6 - R_1$
$X_3 \leftarrow R_4, Y_3 \leftarrow R_4, Z_3 \leftarrow R_7$

V. Scalar Multiplication and Side Channel Attacks

Let d be a positive integer and P be a point on an elliptic curve E(K).

Scalar multiplication is defined as sum of point P with itself d times i.e $dP = \sum_{1 \le i \le d} P$

The sclar multiplication is used for Encryption and Decryption and varification of elliptic curve cryptosystem

. There are two type of standard method.These are

1) left-to-right binary method
2) right-to-left binary method

These two method are describe below

Let the binary representation of positive integer d is $d = d[k-1]2^{k-1} + \ldots + d[0]2^0$

So given $d[0], d[1], \ldots d[k-1]$ and P,we can compute dP.

Algorithm (left-to-right binary method)

INPUT : d, P,$(d[0], d[1], \ldots, d[k-1])$
OUTPUT: $d * P$

1) Q = P
2) for $i = \ k-2$ down to 0
   - Q = ECDBL(Q)
   - if $d[i] == \ 1$
   - Q = ECADD(Q,P)
3) return Q

Algorithm(right- to- left binary method)

INPUT : d,P,$(d[0], d[1], \ldots, d[k-1])$
OUTPUT: d*P

1) Q = P
2) for i = 0 down to k-2
   - if d[i] = 1
   - Q = ECADD(Q,P)
   - P = ECDBL(P)
3) return Q

ECADD and ECDBL are two different operations. They differ in computational complexity. Their computation takes different amount of power and time.Hence an attacker sample the side channel information. In the above algorithm as addition is carried out only if the corresponding bit is 1. Hence if an attacker can detect the sequence of ECDBL and ECADD operations carried one can compute scalar multiplication i.e dP,and can know which bit are 1. Hence he can know the

entire d. So computing dP by the above algorithm is not secure.

A. SPA-Resistance Scalar Multiplication Method

Now we will describe Coron's dummy addition method which is also known as double and always add is one of a special countermeasures against SPA [6].

Algorithm(Coron's dummy addtion method)

INPUT : d,P,$(d[0], d[1], \ldots, d[k-1])$
OUTPUT: $d * P$

1) Q[0] = P
2) for i = 0 down to k-2
   - Q[0] = ECDBL(Q[0])
   - Q[1] = ECADD(Q[0],P)
   - Q[0] = Q[d[i]]
3) return Q[0]

We note that there is a potential security problem with this method.If $d[i] = 0$,the point that is one of the inputs to ECADD in current iteration will be input to ECDBL in the next iteration.When using projective coordinates,both ECDBL and ECADD involves squaring the Z coordinate.So the same Z value will be squared again if $d[i] = 0$. Side channel may provide hints that the same squaring is performed again.Thus liking information on $d[i]$. Coron's dummy addition method requares $(k-1)$ ECDBL operation,it is slower than standard binary method.When we use algorithms ECADD and ECDBL or ECDBL for $a = -3$,Coron's dummy addition method require $12(k-1)M + 9(k-1)S + 18(k-1)A$ for $a \neq -3$ and $12(k-1)M + 7(k-1)S + 20(k-1)A$ for $a = -3$ There are three basis approachs are known to SPA resistance.

1) The first one is use to indistinguishable addition and doubling algorithms in scalar multiplication.Jacobi form and Hesse form elliptic curve achieve this as they allow using the same algorithm for both addition and doublings.

2) The second one is the so called double and always add approach.Coron's dummy addition method is of this type.Okeya and Sakuari proposed to use Montogomery form of elliptic curves to achieve such algorithm.

3) The third approach is to use a special addition chain with a squence of addtions and doublings that does not depend on the bit information of the secret key.

B. Countermeasures against DPA

Even if a scalar multiplecation is secure against SPA ,it may be possible to break it using Differential Power Analysis(DPA).By using stastical tools such as finding the expectation of power of the points one can analyse the information observed in many execution of the algorithm.We describe two countermeasure below.

1) This countermeasure describe by Coron is called projective randomization.
   Let $P = (X : Y : Z)$ be a base point given in Jacobian co-ordinates then for all $r \in K \backslash 0$,$(r^2X : r^3Y : rZ)$ represent the same point.If we transform a base point $(X : Y : Z)$ into $(r^2X : r^3Y : rZ)$ with a random r before starting the scalar multiplication, the side channel information available to the statistic analysis will be randomized.The addition computational cost is only $4M + 1S$.
2) Joye and Tymen proposed another countermeasure.It is based on randomly selected isomerphisms between elliptic curves.This is described below
   Let $P(x, y)$ be the base point and the defining coefficents a,b of elliptic curve can be randomized into $P' = (r^2x, r^3Y)$ and $a' = r^4a, b' = r^6b$, yields corresponding point on curve isomerphic to given one defined by the coefficent a', b'. dP' is computed and again tranform back the result into the first curve to get dP.

VI. Conclusion

Due to physical characteristics of handheld devices the power consumption and time consumption using the secret key can be clearly observed. Thus Side Channel Attack(SCA)are a serious threat against these devices. The main target for Side Channel Attack(SCA) against ECC implementation is the algorithm used for scalar multiplication on elliptic curve .Therefore various elliptic curve multiplication algorithms designed to resist Side Channel Attack and Differential Power Analysis Attack have been proposed. Also computed the time complexity in term of operation multiplication, squaring and addtion.

References

[1] N. Koblitz *Elliptic Curves in Cryptography* In Journal of Cryptology,
[2] D. Henkerson, A. Menezes, S. Vanstone *Guide to Elliptic Curve Cryptography*, Springer-Verlag, 2004.
[3] W. Diffie and M. Hellman. *New direction in cryptography,IEEE Transaction on Information Theory,Vol 22,1976*
[4] E. Brier and M. Joye *Weierstrass Elliptic Curves and Side-Channel Attacks*
[5] B. Moller *Securing Elliptic curve point against side channel attack*
[6] A. Menezes,P.C. van Oorschot, and S.A. Vanstone. *Hand book of applied cryptography*,C.R.C press,1997
[7] N. Koblitz. *A course in Number Theory and Cryptography ,2nd edition* Springer-Verlag-1994
[8] C. Kocher, J. Jaffe and B. June . *Differential Power Analysis*,CRYPTO99
[9] K. Okeya, K. Miyazaki and K. Sakuari . *A first scalar method with randomized projective coordinates on a Montgomery form Elliptic curve secure against side channel attacks*
[10] E. Brier and M.Joye . *Weierstrass elliptic curves and side channel attacks*,Springer-2002
[11] K. Koc, David Naccache, and Christof Paar . *Cryptograhic Hardware and Embbeded Systems*,Springer -Verlag-2001
[12] D. R. Stinson . *Cryptograhic :theory and practice*,CRC Press, Ibc, 1995
[13] V. S. Miller . *Use of Elliptic Curves in Cryptography.Advances in Cryptology CRYPT '85*