



Scan to know paper details and
author's profile

Security Through Elliptic Curves for Wireless Network in Mobile Devices

Dr. E. Kesavulu Reddy

Sri Venkateswara University

ABSTRACT

The basic principle is “A function is easy to evaluate but its invert is infeasible unless a secret key is known”.

It is mathematically proved that security of cryptographic algorithms does not imply its implementation of security of the system against Side-channel Attacks. The security of the system lies in the difficulty of extracting k from P and Q . It is essential to secure the implementation of cryptosystems in embedded devices against side-channel attacks. These attacks monitor the power consumption or the Electromagnetic emanations of a device Ex smart cards or mobile devices. The attacker’s goal is to retrieve partial or full information about a long-term key that is employed in several ECSV executions.

We are implementing a secret key to avoid retrieving the valuable information by the attacker through Simple Power Analysis Attacks.

Keywords: elliptic curve cryptography, simple power analysis, differential power analysis.

Classification: ACM Code: C.2.0

Language: English



Great Britain
Journals Press

LJP Copyright ID: 975825

Print ISSN: 2514-863X

Online ISSN: 2514-8648

London Journal of Research in Computer Science & Technology

Volume 24 | Issue 2 | Compilation 1.0



Security Through Elliptic Curves for Wireless Network in Mobile Devices

Dr. E. Kesavulu Reddy

Professor _Department of Computer Science Sri Venkateswara University Tirupati, Andhra Pradesh India.

ABSTRACT

The basic principle is “A function is easy to evaluate but its invert is infeasible unless a secret key is known”.

It is mathematically proved that security of cryptographic algorithms does not imply its implementation of security of the system against Side-channel Attacks. The security of the system lies in the difficulty of extracting k from P and Q . It is essential to secure the implementation of cryptosystems in embedded devices against side-channel attacks. These attacks monitor the power consumption or the Electromagnetic emanations of a device Ex smart cards or mobile devices. The attacker’s goal is to retrieve partial or full information about a long-term key that is employed in several ECSV executions.

We are implementing a secret key to avoid retrieving the valuable information by the attacker through Simple Power Analysis Attacks.

Keywords: elliptic curve cryptography, simple power analysis, differential power analysis.

I. INTRODUCTION

Elliptic curve cryptosystems (ECCs) are suitable for implementation on devices with limited memory and computational capability such as smart cards and also with limited power such as wireless handheld devices. This is due to the fact that elliptic curves over large finite fields provide the same security level as other cryptosystems such as RSA for much smaller key sizes.

Considering power analysis attacks, there are two main types that were presented by Kocher et al. These are simple and differential power analysis attacks (referred to as SPA and DPA respectively).

Both of them are based on monitoring the power consumption of a cryptographic token while executing an algorithm that manipulates the secret key.

The traces of the measured power are then analyzed to Hence, DPA attacks are, in general, more powerful than the SPA attack. Randomization of the data processed at some instant is essential in resisting this type of attack. Electromagnetic emanations present another powerful side channel since the information is leaked from the device via more than one channel and is a function of space as well as of time. In [2], Agrawal et al. presented both simple and differential electromagnetic analysis attacks on smart cards and on a Palm pilot. In these attacks they conclude that software countermeasures rely on signal information reduction, which is achieved by “randomization and/or frequent key refreshing within the computation”, which agrees with the concept of resisting DPA attacks.

The point addition operation consists of finite field operations carried in the underlying field K . We denote the field inversion by I , the multiplication by M , the squaring by S . The point addition is denoted by A . When the two operands of the addition are the same point, the operation is referred to as point doubling and is denoted by D .

II. WINDOW METHODS

This method is sometimes referred to as the m -ary method. There are different versions of window methods. What is common among them is that, if the window width is w , some multiples

of the point P up to $(2^w - 1)P$ are precomputed and stored and k is processed w bits at a time. k is recoded to the radix 2^w . k can be recoded in a way so that the average density of the nonzero digits in the recoding is $1/(w + \xi)$, where $0 \leq \xi \leq 2$ depends on the algorithm. Let the number of precomputed points be t , in the Precomputation stage, each point requires either a doubling or an addition to be computed also depending on the algorithm.

This ECSM method is suitable for unknown or fixed-point P . The cost is Storage: t points, where $2^{w-2} \leq t \leq 2^{w-1}$ depending on the algorithm. Precomputation: t point operations (A or D). Expected running time:

$$(n-1)D + n \frac{n}{w+\xi} A,$$

where $0 \leq \xi \leq 2$ depending on the algorithm. Note that the number of doublings is between $n - w$ and $n - 1$.

2.1. Simultaneous multiple point multiplication

This method is used to compute $kP + lS$ where P may be a known point. This algorithm was referred to as Shamir's trick in [10]. If k and l are n -bit integers, then their binary representations are written in a $2 \times n$ matrix called the exponent array. Given width w , the values $iP + jS$ are calculated for $0 \leq i, j < 2^w$. Now the algorithm

performs $d = \lceil n/w \rceil$ iterations. In every iteration, the accumulator point is doubled w times and the current $2 \times w$ window over the exponent array determines the precomputed point that is to be added to the accumulator.

Algorithm 2.1. Simultaneous multiple point multiplication (*Shamir-Strauss method*)

Input: Window width w , $d = \lceil n/w \rceil$,

$$k = (K^{d-1}, \dots, K^1, K^0) 2^w \quad l = (L^{d-1}, \dots, L^1, L^0)$$

2^w , and $P, S \in E(F^q)$. 3 Also according to [Bero1], it is originally due to Straus [Str64].

Output: $kP + lS$.

1. Precomputation. Compute $iP + jS$ for all $i, j \in [0, 2^w - 1]$.
2. $Q \leftarrow K_{d-1}P + L_{d-1}S$.
3. for i from $d - 2$ down to 0 do
 - 3.1 $Q \leftarrow 2^w Q$.
 - 3.2 $Q \leftarrow Q + (K_i P + L_i S)$.
4. Return(Q).

Storage: $2^{2w} - 2$ points. For $w = 1, 3$ points.

For $w = 2, 15$ points.

Precomputation:

$$(2^{2(w-1)} - 2^{w-1})D + (3 \cdot 2^{2(w-1)} - 2^{w-1} - 1)A.$$

For $w = 1, 1A$.

For $w = 2, 1D + 11A$.

$$\frac{(2^{2w} - 1)}{2^{2w}}$$

Expected running time: $(d - 1)wD + \frac{(2^{2w} - 1)}{2^{2w}}d - 1A$.

$$\text{For } w = 1, (n-1)D + \left(\frac{3}{4}n-1\right)A.$$

$$\text{For } w = 2, (n-1)D + \left(\frac{15}{32}n-1\right)A.$$

Using sliding windows can save about $1/4$ of the precomputed points and decrease the number of

additions to $\frac{n}{w+(1/3)}$, which is about 9% saving for $w \in \{2, 3\}$.

2.2. Interleaving method

This method is also a multiple point multiplication method, that is we want to compute $\sum k^j P_j$ for points P_j and integers k^j . In the comb and simultaneous multiplication methods, each of the precomputed values is a sum of the multiples of the input points. In the interleaving method, each precomputed value is simply a multiple of one of the input points. Hence, the required storage and the number of point additions at the precomputation phase is decreased at the expense of the number of point additions in the main loop. This method is flexible

in that each k^j can have a different representation, e.g., different window size, as if a separate execution of a window method is

performed for each $k^j P^j$ with the doubling step performed jointly on a common accumulator, as shown in [12]. As an illustration, we provide the following algorithm that computes $kP + lS$ where both k and l are represented to the same base 2^w .

Algorithm 2.2. Interleaving method

Input: width w , $d = \lceil n/w \rceil$,
 $k = (K^{d-1}, \dots, K^1, K^0) 2^w$ $l = (L^{d-1}, \dots, L^1, L^0) 2^w$, and $P, S \in E(F^q)$.

Output: $kP + lS$.

1. Precomputation. Compute iP and iS for all $i \in [0, 2^w - 1]$.

2. $Q \leftarrow K_{d-1}P$.

3. $Q \leftarrow Q L_{d-1}S$.

4. for i from $d - 2$ down to 0 do

4.1 $Q \leftarrow 2^w Q$.

4.2 $Q \leftarrow Q + K_i P$.

4.3 $Q \leftarrow Q + L_i S$.

5. Return(Q).

Storage: $2^{w+1} - 2$ points.

Precomputation: $2(w-1)D + 2(2^w - w - 1)A$.

Expected running time: $w(d-1)D + (2d-1)A$.

$$\frac{(2^{2w} - 1)}{2^{2w} A}$$

In general, if different basis and/or representations are used for k and l , we have

Storage: $2t$ points, where $2^{w-2} \leq t \leq 2^{w-1}$ depending on the particular window algorithm used as discussed in Section 2.1.3.

Precomputation: $2t$ point operations (A or D).

Expected running time: $(n-1)D + 2 \frac{n}{w+i} A$, where $1 \leq i \leq 2$ depending on the algorithm

2.3. SPA Attack on ECCs and its Countermeasures

Coron [3] has transferred the power analysis attacks to ECCs and has shown that an unaware implementation of EC operations can easily be exploited to mount an SPA attack. Moreover, it may also enable it to recognize the exact instruction that has been executed. For example, if the difference in power consumption between point doubling (D) and point addition (A) is obvious in their respective power traces, then, by investigating one power trace of a complete execution of a double-and-add algorithm, the bits of the scalar k are revealed. That is, whenever a D

is followed by A, the corresponding bit is $k^i = 1$, otherwise if D is followed by another D, then $k^i = 0$. This sequence of point operations is referred to as the DA sequence.

Window methods process the key on a digit (window) level. The basic version of this method, that is where $_ = 0$ in Section 2.1.3, is inherently uniform since in most iterations, w D operations are followed by 1 A, except for possibly when the digit is 0. Therefore, fixed-sequence window methods were proposed in order to recode the digits of the key such that the digit set does not include 0.

2.4. DPA Attack on ECCs and its Countermeasures

As for the SPA attack, Kocher et al. were the first to introduce the DPA attack on a smart card implementation of DES. Techniques to strengthen the attack and a theoretical basis for it were presented by Messerges et al. in [3]. Coron applied the DPA attack to ECCs [3].

In order to resist DPA attacks, it is important to randomize the value of the long-term key involved in the ECSV across the different executions. Some of the countermeasures that were based on randomizing the key representation were proven to be inadequate since the intermediate point computed in the accumulator Q at certain

iteration remained one of two possible values. The constancy of the value of this intermediate point is an integral part in the success of first-order DPA attacks.

A potential DPA countermeasure is known as key splitting. It is based on randomly splitting the key into two parts such that each part is different in every ECSV execution. An additive splitting using subtraction is attributed to Clavier and Joye. It is based on computing

$$kP = (k - r)P + rP, \quad (I)$$

The authors mention that the idea of splitting the data was abstracted in [5], where r is a n -bit random integer, that is, of the same bit length as k . Alternatively, Ciet and Joye [8] suggest the following additive splitting using division, that is, k is written as

$$k = \lfloor k/r \rfloor + (k \bmod r). \quad (1)$$

Hence, if we let $k^1 = (k \bmod r)$, $k^2 = \lfloor k/r \rfloor$ and $S = rP$, we can compute

$$kP = k^1 P + k^2 P \quad (II)$$

where the bit length of r is $n/2$. They also suggest that (II) should be evaluated with the Shamir-Strauss method as in Algorithm 2.3. However, they did not mention whether the same algorithm should be used to evaluate (I). The following multiplicative splitting was proposed by Trichina and Bellezza [6] where r is a random integer invertible modulo u , the order of P . The scalar multiplication kP is then evaluated as

$$kP = [kr^{-1} \pmod{u}] (rp) \quad (III)$$

To evaluate (III), two scalar multiplications are needed; first $R = rP$ is computed, then $kr^{-1} R$ is computed.

III. KEY SPLITTING METHODS

3.1. Introduction

We discuss different forms of key splitting along with their strengths and weaknesses. We also discuss the candidate SPA-resistant algorithms and compare the resulting performance when combined with each form of key splitting. At the

end of the chapter, we present countermeasures to DPA attacks on the ECDSA and the ECMQV algorithms.

This approach was suggested by Clavier and Joye in [CJ01] and revisited by Ciet [Cie03] as follows. In order to compute the point kP , the n -bit key k is written as

$$k = k^1 + k^2,$$

such that $k^1 = k - r$ and $k^2 = r$, where r is a random integer of length n bits. Then kP is computed as

$$kP = k^1 P + k^2 P. \quad (4.1)$$

It is important to note that each of the terms should be evaluated separately and their results combined at the end using point addition. That is the multiple-point multiplication methods that use a common *accumulator* to save doubling operations. Whether at the bit level ($w \equiv 1$) or window level ($w > 1$)—should not be used, even when a countermeasure against SPA is employed. This observation is based on the following lemma.

Let $b \rightarrow a$ denote $\lfloor k(\bmod 2^{b+1})2^a \rfloor$ or, simply, the bits of k from bit position b down to bit position a , with $b \geq a$.

Lemma 3.2 Let splitting scheme I at the end of some iteration j , $0 < j \leq n - 1$, there are only two possible values for Q , those are $[k^{n-1-j}] P$ or $[k^{n-1-j} - 1] P$.

Proof. Algorithm 2.3—and similarly Algorithm 2.4—computes the required point by scanning

$$k^1 = (k^{1n-1}, \dots, k^{10})_2 \text{ and}$$

$k^2 = (k^{2n-1}, \dots, k^{20})_2$ from the most significant end down to the least significant end. Hence, at the end of iteration j , the accumulator Q contains the value

$$Q = k^{1n-1-j} P + k^{2n-1-j} P \quad (4.2)$$

$$= [k^{1n-1-j} + k^{2n-1-j}] P.$$

We can write k , k^1 and k^2 as

$$k = k^{n-I-j^j} 2^j + k^{j-1-0}$$

$$k^i = k^{i-n-I-j^j} 2^j + k^{i-j-1-0} \quad (4.3)$$

Since $k = k^1 + k^2$ we have

$$k^{1-j-1-0} + k^{2-j-1-0} j = k^{j-1-0} + b 2^j \text{ where } b \in \{0, 1\} \quad (4.5)$$

and

$$k^{1-n-I-j} + k^{2-n-I-j} = k^{n-I-j} - b$$

The DPA attack would proceed in the same way, whether the algorithm processes a single bit or a digit per iteration, though it would be more involved in the latter case depending on the digit size. The attacker can double the number of traces gathered and compute the necessary intermediate points as if there was no countermeasure in place.

3.2 Modular Division:

In the following algorithm, a and b are integers internally represented each by an array of w -bit digits. The length of each array is $d = \lceil n/w \rceil$ digits. Note that for the modular inversion, as mentioned by Savas and Ko, c [25], b needs not be less than the modulus u , but be in $[1, 2^m - 1]$, where $m = dw$. Also note that the values $R^2 \bmod u$, where $R = 2^m$, and u' are computed once per modulus, i.e., per curve.

Algorithm 3.4. Modular division

Input: u : a n -bit prime, $d = \lceil n/w \rceil$, $m = dw$, $R^2 \bmod u = (2m)^2 \bmod u$, $u' = u^{-1} \bmod 2^w$, $a \in [1, p-1]$ and $b \in [1, 2^m - 1]$.

Output: $ab^{-1} \bmod u$.

1. Compute $b^{-1} R \bmod u$ using Algorithm 6.6.
2. Compute $x = a(b^{-1} R)R^{-1} \bmod u$ using Algorithm 6.5.
3. Return(x).

The following algorithm is Algorithm 14.36 in [21]. We include it here for the sake of completeness.

Algorithm 3.5 Montgomery multiplication

Input: u : a n -bit prime, $d = \lceil n/w \rceil$, $m = dw$, $u' = u^{-1} \bmod 2^w$, $x = (x^{d-1}, \dots, x_0)2^w$ and $y = (y^{d-1}, \dots, y_0)2^w$.

Output: $xy2^{-m} \pmod{u}$.

1. $A \leftarrow 0$. // $A = (ad, a_{d-1}, \dots, a_0)2^w$
2. for i from 0 to $d-1$ do
 - 2.1 $ui \leftarrow (a_0 + x_i y_0) \bmod 2^w$
 - 2.2 $A \leftarrow (A + x_i y_0 + u_i m) / 2^w$
3. if ($A > u$) then
 $A \leftarrow u$.
4. Return(A).

The following algorithm was presented by Savas and Ko, c as the modified Kaliski-Montgomery Inverse.

Algorithm 3.6. Montgomery inversion

Input: u : a n -bit prime, $d = \lceil n/w \rceil$, $m = dw$, $R^2 \bmod u = (2^m)^2 \bmod u$, $u' = u^{-1} \bmod 2^w$ and $b \in [1, 2^m - 1]$.

Output: $b^{-1} R \bmod u$.

1. Compute f and $x = b^{-1} 2f \bmod u$ using Algorithm 6.7,
Where $n \leq f \leq m+n$.
2. if ($f \leq m$) then
 - 2.1 $x \leftarrow xR^2 R^{-1} \bmod u$ using Algorithm 6.5. // $x = b^{-1} 2^{m+f} \bmod u$
 - 2.2 $f \leftarrow f + m$. // $f > m$, $x = b^{-1} 2^{m+f} \bmod u$
3. $x \leftarrow x2^{2m-f} R^{-1} \bmod u$ using Algorithm 6.5.
// $x = b^{-1} 2^f 2^{2m-f} 2^{-m} = b^{-1} 2^m \bmod u$
4. Return(x).

IV. EXISTING SYSTEM

Nevine Maurice Ebied modified the almost Montgomery inverse algorithm of [ScKKoo] to be resistant to SPA attacks as in the following algorithm. Swap Address(c, d) denotes

interchanging the memory addresses of the integer's c and d. This is an inexpensive operation, hence its usage as a dummy operation to balance the branches of the main loop. We implemented the "if" statement in steps 3.4 and 3.5 such that the number of conditions checked per loop iteration is always three. In assembly language, this can be easily ensured. Written in Java, step 3.4 is implemented as

If ((xLSb == 0) && (xLSb == 0) && (xLSb == 0)).

If the condition is false, due to short-circuit evaluation, the flow control will move to the following "if" after the first check, otherwise, it will perform the check three times. The following "if"—step 3.5—is similar but with the condition checked only two times if((yLSb == 0) && (yLSb == 0)).

Algorithm 3.7. Almost Montgomery inverse
:Input: u: a n-bit prime,

$d = \lceil n/w \rceil$, m = dw and $b \in [1, 2^m - 1]$.

Output: f and $b^{-1} 2^f \pmod{u}$, where $n \leq f \leq m + n$.

```

1. x  $\leftarrow$  u; y  $\leftarrow$  b; r  $\leftarrow$  0; s  $\leftarrow$  1.
2. f  $\leftarrow$  0.
3. while (v > o) do
3.1 U  $\leftarrow$  x - y; V  $\leftarrow$  -U.
3.2 T  $\leftarrow$  r + s.
3.3 f  $\leftarrow$  f + 1.
3.4 if (((lsb(x) == 0))) then
// This "if" is special SwapAddress(x, U);
SwapAddress(x, U) // dummy
SHR(x); SHL(s).
3.5 else if ((lsb(y) == 0)) then
// This "if" is special SwapAddress(y, V);
SwapAddress
(y, V) // dummy
SHR(y); SHL(r).
3.6 else if (V >= o) then
SwapAddress(y, V);
SwapAddress(s, T)
SHR(y); SHL(r).
3.7 else
SwapAddress(x, U);

```

SwapAddress(r, T)

SHR(x); SHL(s).

4. T \leftarrow u - r; V \leftarrow u + T.
5. if (T > o) then
- Return(f, T)
- else

Return(f, V).

The drawback of this algorithm is that an SPA of the number of iterations of the main loop directly leaks the value of f. If f is uniformly distributed, the search space of b is reduced from 2^w to $2^{m - \log_2 m}$, which is not a significant reduction. It is interesting to study how f is actually distributed.

4.1. PROPOSED SYSTEM

We modified the Nevine Maurice Ebied's Almost Montgomery inverse and A SECRET KEY of [ScKKOO] to be resistant to SPA attacks as in the following algorithm.

Algorithm:4.2. E.KESAVULU REDDY (EKR)
Modified Montgomery Inversion

Input: u: a n-bit prime, $d = \lceil n/w \rceil$,
m = dw, $R^2 \pmod{u} = (2^m)^2 \pmod{u}$, $u = u^{-1} \pmod{2^w}$ and $b \in [1, 2^m - 1]$, t is Secret key.
t: No of precomputed points $1 \leq t \leq n$
W: Window width least significant of bit

$$2^{w-z} \quad t \leq 2^w - 1$$

Output: $b^{-1} R \pmod{u}$.

Select a number b such that $(b, 2^m) = 1$

Compute b^{-1} such that $bb^{-1} \equiv 1 \pmod{2^m}$

3. If $f > m$ then $x = b^{-1} 2^f \pmod{u}$
 $\otimes x = b^{-1} 2^f \pmod{u}$
4. If $f \leq m$ then
5. $x \leftarrow R^2 R^{-1} \pmod{u}$ $\otimes R = 2^m$
6. $x = b^{-1} 2^{m+f} \pmod{u}$
7. $f \leftarrow m+f$
8. Return(x)

In the EKR modified Montgomery Inverse Algorithm of Savas and Koc , we select f such that

gcd $(b, 2^m) = 1$, $m \leq f \leq m+n$. So b is not reduced from 2^m to $2^{m-\log 2^m}$. Therefore, this is significant reduction and hence f is not uniformly distributed and it can't leak the value package javaapplication1;

```

import java.util.ArrayList;
import java.util.Scanner;
public class Main {
    public static void main(String[] args)
    {
        Scanner s=new Scanner(System.in);
        System.out.println("Enter a Prime Integer(U):");
        int u=s.nextInt();
        String binU=Integer.toBinaryString(u);
        int n=binU.length();
        System.out.println("Enter a secrete Key(t):");
        int t=s.nextInt();
        double w=0;
        for(int wi=1;wi<=t;wi++)
        {
            int i1=(int)Math.pow(2,wi-2);
            int i2=(int)Math.pow(2,wi)-1;
            if(i1<=t && t<=i2)
            {
                w=wi;
                break;
            }
        }
        System.out.println("Window width (W): "+w);
        int d=(int)Math.ceil(n/w);
        System.out.println("Length of Each Array (d) :" +d);
        int m=(int)(d*w);
        System.out.println("....(m) :" +m);
        int on1=(int)Math.floor(Math.pow(2,m-1));
        int n2=(int)Math.pow(2,m);
        for(int i=m;i<on1;i++)
        {
            int n1=i;
            while(n1!=n2)
            {
                if(n1>n2)
                    n1=n1-n2;
                else
                    n2=n2-n1;
            }
        }
        //System.out.println("GCD of two number is "+n1+"and i is "+i);
        if(n1==1){on1=i;break;}
    }
}
```

```

    }
    System.out.println("B=" +on1);
    int b=on1;
    int b_inverse=0;
    for(int i=1;i<b;i++)
    {
        int t2m=(int)Math.pow(2,m);
        int temp=t2m*i;
        temp=temp+1;
        b_inverse=temp/b;
        if((temp%b)==0)
        {
            break;
        }
    }
    System.out.println("B inverse: " +b_inverse);
    ArrayList<Integer> af=new ArrayList<Integer>();
    for(int i=n;i<=(m+n);i++)
    {
        af.add(i);
    }
    int x=0;
    for(int f=n;f<=(n+m);f++)
    {
        if(f>m)
        {
            x=(int)(b_inverse*Math.pow(2, f))/u;
            System.out.println("f=" +f +"\nx=" +x);
        }
        else if (f<m)
        {
            x=(int)(b_inverse*(Math.pow(2,m+f)))/u;
            System.out.println("f=" +af.get(f) +"\nx=" +x);
        }
    }
}

INPUT AND OUTPUT
Enter a Prime Integer(U):
111
Enter a secrete Key(t):
117
Window width (W): 7.0
Length of Each Array (d) :1
....(m) :7
B=7
B inverse: 55
f=8
x=126
f=9

```

```

x=253
f=10
x=507
f=11
x=1014
f=12
x=2029
f=13
x=4059
f=14
x=8118

```

BUILD SUCCESSFUL (total time: 29 seconds)

V. CONCLUSION

We modified the Nevine Maurice Ebied's Almost Montgomery inverse and A New variant of [ScKKoo] of Montgomery Inversion i.e is the EKR Modified Montgomery Algorithm to be resistant to SPA attacks . The EKR Modified Montgomery Inverse Algorithm eliminate the number of Iterations of the main loop directly leaks the value of f and also it is mathematically proved that f is uniformly distributed with a significant reduction

A function that is easy to evaluate but infeasible to invert unless the secret trapdoor t is known. So, the attacker cannot guess the key (t) to retrieve the valuable information in smart cards and mobile devices .

REFERENCES

1. Nevine Maurice Ebied's Key Randomization Counter Measures To Power Analysis Attacks On Elliptic Curve Cryptosystems Ph.D. thesis, University of Waterloo, Ontario, Canada, 2007
2. D. Agrawal, B. Archambeault, J. R. Rao & P. Rohatgi. The EM Side- Channel(s): Attacks and Assessment Methodologies. Internet Security Group, IBM Watson Research Center.ps. 2, 3
3. J.-S. Coron. "Resistance against differential power analysis for elliptic curve cryptosystems". In Cryptographic Hardware and Embedded Systems –CHES '99, LNCS, vol. 1717, pp. 292–302. Springer-Verlag, 1999. 2, 22, 24, 158, 170, 180, 181, 186
4. S. Chari, C. S. Jutla, J. R. Rao & P. Rohatgi. "Towards sound approaches to counteract power-analysis attacks." In Advances in Cryptology – CRYPTO '99, LNCS, vol. 1666, pp. 398–412. Springer-Verlag, 1999. 24
5. C. Clavier & M. Joye. "Universal exponentiation algorithm a first step towards provable SPA-resistance". In Cryptographic Hardware and Embedded Systems – CHES '01, LNCS, vol. 2162, pp. 300–308. Springer-Verlag, 2001. 4, 24, 120
6. M. Ciet, J.-J. Quisquater & F. Sica. "Preventing differential analysis in GLV elliptic curve scalar multiplication". In Cryptographic Hardware and Embedded Systems – CHES '02, LNCS, vol. 2523, pp. 540–550. Springer- Verlag, 2003. 4, 25, 126, 173, 179
7. T. ElGamal. "A public key cryptosystem and a signature scheme based on discrete logarithms". IEEE Transactions on Information Theory, 31(4):469– 472, 1985.
8. J. Ha & S. Moon. "Randomized signed-scalar multiplication of ECC to resist power attacks". In Cryptographic Hardware and Embedded Systems – CHES '02, LNCS, vol. 2523, pp. 551–563. Springer-Verlag, 2002. 3, 24, 27, 31, 40, 58, 70, 75, 93, 101, 173
9. T. S. Messerges, E. A. Dabbish & R. H. Sloan. "Investigations of power analysis attacks on smart cards". In USENIX Workshop on Smart- card Technology, pp. 151–161. May 1999. 2, 24, 172
10. B. M"oller. "Securing elliptic curve point multiplication against side channel attacks". In International Security Conference – ISC '01, LNCS, vol. 2200, pp. 324–334. Springer-Verlag, 2001. Extended version.pdf. 23, 164,196,19:195–249, 2000. 4, 14, 15, 20, 37, 46, 50, 58, 70, 89, 90, 91, 92, 95, 110, 112.
11. N. Thériault. "SPA resistant left-to-right integer recodings". In Selected Areas in Cryptography – SAC '05, LNCS, vol. 3897, pp. 345–358. Springer- Verlag, 2006. 23,128, 133, 164).



Dr.E.Kesavulu Reddy working as a Professor in the department of Computer Science, S.V.University,

Tirupati. He Published research papers in various National and International Journals and presented papers in national and International Conferences. He was awarded National and International awards with different prestigious organizations in India. He was honored Fellow of Computer Science Research Council (**FCSR**C) from Open association of Research society (U.S.A), Global Journals, U.S.A on 31-01-2019.