**IMPACT: International Journal of Research in
Engineering and Technology
ISSN (P): 2347–4599; ISSN (E): 2321–8843
Vol. 12, Issue 10, Oct 2024, 1–10
© Impact Journals**

EKR CRYPTOSYSTEM RESISTANCE AGAINST TO SIMPLE POWER ANALYSIS ATTACKS

Dr. E. Kesavulu Reddy

Professor, Department of Computer Science, S.V. University, Tirupati-Andhra Pradesh, India

Received: 09 Oct 2024 **Accepted:** 15 Oct 2024 **Published:** 20 Oct 2024

ABSTRACT

Elliptic curve cryptosystems are more efficient and secure than the conventional cryptosystems like RSA cryptosystems. We developed a Secret Key in the EKR Modified Montgomery Inversion Algorithm to eliminate the number of Iterations of the main loop directly leaks the value of f and also the attacker can not guess the Secret key (t) to retrieve the valuable information in smart cards and mobile devices. We want to develop the new cryptosystem based on EKR Modified Montgomery Inversion Algorithm to resistance against Simple Power Analysis Attacks in Side- channel Attacks in Elliptic Curve Cryptosystems like RSA Cryptosystems

KEYWORDS: *EKR modified Montgomery Inversion, E. Kesavulu Reddy Cryptosystems, RSA Cryptosystems*

INTRODUCTION

Applications of healthcare, financial services and government depend on the underlying security already available in the wired computing environment. Both for secure (authenticated, private) Web transactions and for secure (signed, encrypted) messaging, a full and efficient public key infrastructure is needed. Three basic choices for public key systems are available for these applications:

- RSA
- Diffe-Hellman (DH) or Digital Signature
- Algorithm (DSA) modulo a prime *p*
- Elliptic Curve Diffie-Hellman (ECDH) or Elliptic Curve Digital

Signature Algorithm (ECDSA)

The RSA is a system that was published in 1978 by Rivest, Shamir, and Adleman, based on the difficulty of factoring large integers.

ELLIPTIC CURVE CRYPTOSYSTEMS

Let K be a finite field and E be an elliptic curve (EC) over K defined by the following Weierstrass form equation

$$E:\ y^2+a_1xy+a^{3}y= x^3+ a_2 x^2+a_4 x + a_6 \qquad (1)$$

Where $a^{i} \in K$ and $\Delta \neq 0$, where Δ is the discriminant of E

Let L be an extension field of K. Then E (L) denotes the set of L-rational points (x, y) on E, where (x, y) $\in$ L × L and satisfy (3.1), together with the point at infinity ∂. The addition of two points on the curve is performed using a chord-and-tangent rule the set E (L) with the addition operation form an abelian group, where ∂ is the identity.

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.

A. Elliptic curves over prime fields

If K = F^p, where p > 3 is a prime, (1) can be simplified to

$$E: y^2 = x^3 + ax + b \qquad (2)\ (3.2)$$

Where a and b$\in$ F^p, The discriminant of this curve is $\Delta = -16\,(4a^3+27b^2)$. The negative of a point P = (x, y) is −P = (x, −y) such that P + (−P) = ∂.This simplification is generally applicable when the characteristic of K is not 2 or 3.

- Standard (homogeneous) projective coordinates (P); the projective point (X Y: Z), Z $\neq$ 0, corresponds to the affine point (X/Z, Y/Z), ∂ corresponds to (0 : 1 : 0) and the negative of (X : Y : Z) is (X : −Y : Z).
- Jacobian projective coordinates (J); the projective point (X : Y : Z), $Z^6 = 0$, corresponds to the affine point (X/Z^2, Y/Z^3), O corresponds to (0: 1 : 0) and the negative of (X: Y: Z) is (X: −Y : Z).
- Chudnovsky coordinates (C); the Jacobian point (X: Y: Z) is represented as(X: Y: Z: Z^2 : Z^3).

B. Elliptic Curves over Binary Fields

If K = F^{2^m} , (3.1) can be simplified to

$$E: y^2 = x^3 + ax + b, \qquad (3)$$

Where a and b $\in$ $F\ 2^m$. The discriminant of this curve is Δ = b and the negative of a point P = (x, y) is −P = (x, x + y). Such a curve is known as non-supersingular.

C. Elliptic Curve Scalar Multiplication (ECSM)

Scalar multiplication in the group of points of an elliptic curve is analogous to exponentiation in the multiplicative group of integers modulo a fixed integer. Thus, it is the fundamental operation in EC-based cryptographic systems. The scalar multiplication,[9] denoted kP, is the result of adding the point P to itself k times, where k is a positive integer, that is

kP = P + P + · · · + P | {z} k copies and −kP = k (−P). u is said to be the order of P if u is the smallest integer.

Let (k^{n-1}, k^{n-2}, . . . , k^1, k^0)$_2$ be the binary representation of k, i.e., $k^i \in \{0, 1\}$ for $0 \leq i < n - 1$. Thus,

$$kP = (\sum_{i=0}^{n-1} k_i 2^i)P = 2(2(\cdot\cdot\cdot 2(2(k_{n-1}P) + k_{n-2}P) + \cdot\cdot\cdot) + k_1P) + k_0P$$

$$= (k_{n-1}2^{n-1}P) + k_1 2P) + (k_0P) \qquad (.4)$$

Hence, kP can be computed using the straightforward double-and-add approach in n iterations. These algorithms are analogous to the square-and-multiply algorithms employed in exponentiation-based cryptosystems.

WINDOW METHODS

This method is sometimes referred to as m-ary method. 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 such, it has to contribute to the overall goal of knowledge discovery.

This method is sometimes referred to as m-ary method. 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 radix2^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.

POWER AND ELECTROMAGNETIC ANALYSIS ATTACKS ON ECCS

The attacks are those that monitor the power consumption and [2], or the electromagnetic emanations of a device, e.g., a smart card or a handheld device, and can infer important information about the instructions being executed or the operands being manipulated at a specific instant of interest.

These attacks are broadly divided into two categories; simple and differential analysis attacks. We will refer to the former category as SPA attacks and the latter as DPA attacks. Though SPA and DPA are the acronyms for simple power analysis and differential power analysis.

Power analysis attacks use the fact that the instantaneous power consumption of a hardware device is related to the instantaneous computed instructions and the manipulated data. The attacker could measure the power consumption during the execution of a cryptographic algorithm, store the waveform using a digital oscilloscope and process the information to learn the secret key. Kocher et al., in [4], first introduced this type of attack on smart cards performing the DES operation. Then Messerges et al. [10] augmented Kocher’s work by providing further analysis and detailed examples of actual attacks they mounted on smart cards.

In general, SPA attacks are those based on retrieving valuable information about the secret key from a single leaked information power consumption or electromagnetic emanation trace. On the other hand, DPA attacks generally include all attacks that require more than one such trace along with some statistical analysis tools to extract the implicit information from those traces.

A. 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. Window methods process the key on a digit (window) level. The basic version of this method, that is where $\xi = 0$ in Section 3.1, 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 [12], [11] and [10] in order to recode the digits of the key such that the digit set does not include 0.

B. DPA Attack on ECCs and its Countermeasures

When the relation between the instructions executed by a cryptographic algorithm and the key bits is not directly observable from the power signal, an attacker can apply differential power analysis (DPA). DPA attacks are in general more threatening and more powerful than SPA attacks because the attacker does not need to know as many details about how the algorithm was implemented. The technique also gains strength by using statistical analysis and digital signal processing techniques on a large number of power consumption signals to reduce noise and to amplify the differential signal. The latter is indicated by a peak, if any, in the plot of the processed data. This peak appears only if the attacker's guess of a bit or a digit of the secret key is correct. The attacker's goal is to retrieve partial or full information about a long-term key that is employed in several ECSM executions.

As for the SPA attack, Kocher et al. were the first to introduce the DPA attack on a smart card implementation of DES [43]. Techniques to strengthen the attack and a theoretical basis for it were presented by Messerges et al. in [10]. Coron applied the DPA attack to ECCs [3]. It is based on randomly splitting the key into two parts such that each part is different in every ECSM execution. An additive splitting using subtraction is attributed to [7]. It is based on computing

$$kP=(k-r)P + rP, \qquad (5)$$

The authors mention that the idea of splitting the data was abstracted in [13]. Where r is a n-bit random integer, that is, of the same bit length as k. alternatively, Ciet and Joy [16] suggest the following additive splitting using division, that is, k is written as

$$k = \lfloor k/r \rfloor + (k \bmod r). \qquad (6)$$

Hence, if we let $k^1 = (k \bmod r)$, $k^2 2 = \lfloor k/r \rfloor$ and $S = rP$, we can compute $kP = k^1 p + k^2 P$ (7)

Where the bit length of r is n/2. They also suggest that (3.6) should be evaluated with Shamir-Strauss method as in Algorithm 3.2.1. However, they did not mention whether the same algorithm should be used to evaluate (3.5).

The following multiplicative splitting was proposed by Trichina and Bellezza [9] where r is a random integer invertible modulo u, the order of P. The scalar multiplication kP is then evaluated $P = [kr^{-1}(\mathrm{modu})](rP)$ (8)

To evaluate (3.8), two scalar multiplications are needed; first R = rP is computed, and then $kr^{-1}R$ is computed.

E.K.R MODIFIED MONTGOMERY INVERSION

A. Linear Congruence's

A congruence of the form $ax \equiv b \pmod m$ where m is a positive integer, a and b are integers, and x is a variable, is called Linear congruence. Such congruence's arise throughout number theory and its applications.

B. Definition: If a and b are integers, then a is said to be congruent to b modulo n, write $a \equiv b \pmod n$, if n divides

(a – b). The integer n is called the modulus of the congruence.

C. Definition: The equivalence class modulo n of an integer b is the set of all integers congruent to b modulo n.

D Definition: The ring of integers modulo n, denoted by Zn, is the set of (equivalence classes of) is the integers {0, 1, 2, n–1}. Addition, subtraction, and multiplication in Zn are performed modulo n.

We [1] modified the Nevine Maurice Ebied's Almost Montgomery inverse and A SECRET KEY of Savas and Koc to be resistant to SPA attacks as in the following algorithm.

Algorithm .E. EKR Modified Montgomery Inversion [1]

```
Input: u: a n-bit prime, d = $\lceil n/w \rceil$ ,
m = dw, $R^2$ (mod u) = $(2^m)^2$(mod u), $u^1 = u^{-1}$ mod $2^w$ 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   $2^{w-z} \leq t \leq 2^{w-1}$   Output: $b^{-1}$ R (mod u).
1. Select a number b such that (b, $2^m$)
                        = 1
  2. Compute b such that
         $bb^{-1} \equiv 1$(mod  $2^m$)
3. If f > m then x = $b^{-1} 2^f$ (mod u)
              $\because$  x = $b^{-1} 2^f$ (mod u)
                          4. If (f $\leq$ m) then
                          5. x $\leftarrow$ $R^2 R^{-1}$(mod u)   $\because$ R = $2^m$
                          6. x= $b^{-1} 2^{m+f}$ (mod u) f $\leftarrow$ m+f
                          7. Return(x)
```

E KESAVULU REDDY CRYPTOSYSTEM TO RESISTANCE AGAINST TO SPA ATTACKS

We develop a new cryptosystem i.e EKR Cryptosystem to resistance against Simple Power Analysis Attacks with one Public key and one Private Key to resistance against to Simple power Analysis Attacks in Side-Channel Attacks in elliptic curve cryptosystems based on EKR Modified Montgomery inversion algorithm

Algorithm A EKR Cryptosystem to Resistance against to SPA Attacks

Step (1). Select u as an n-bit prime.

Step (2). Choose t as Secret key as a prime integer and

$t \in [1, n]$.

Step (3). Compute w if $2^{w-2} \leq t \leq 2^{w} - 1$

and $1 \leq w \leq n$.

Step (4). Compute m = dw

Step (5). Select a number b such that $(b, 2^{m}) =1$

Step (6). Compute b^{-1} such that $bb^{-1} \equiv 1(\text{mod } 2^{m})$.

Step (7). Choose Public key = (u, b).

Choose Private Key = (u, b^{-1})

Step (8). Encrypt the message M = 8 then

$$C \equiv M^{E} (\text{mod } N)$$

$$C \equiv M^{b} b^{-1} 2^{m} \ (\text{mod } u)$$

$$C \equiv 8^{7} * 55 * 64 \ (\text{mod } 17).$$

C = 16. Cipher Text = 15.

Step (9). To decrypt the cipher text as follows

$$M = C^{D} \ (\text{mod } N)$$

$$M = C^{b^{-1}} b^{-1} 2^{m} \ (\text{mod } u),$$

$$M = 15^{55} * 55 * 64(\text{mod } 17)$$

M = 8 , Plain Text = 8.

B. Case Study I. Performance Analysis of RSA Cryptosystems with one Public Key and one Private Key

Step (1). Select two prime integers p = 17. q = 5

Step (2). Compute n = pq = 85, Φ (n) = (p-1)(q-1) = 64

Step (3). Choose e=5, Check gcd (5, p-1) = gcd (5, 16) = 1

Check gcd (5, q-1) = gcd (5, 4) =1

Check gcd (e, (p-1) (q-1)) = gcd(5, 64) = 1

e = 5.

Step (4). Compute d such that ed =1(mod Φ (n))

Step (5). Compute d = e^{-1} (mod Φ (n))

$d = 5^{-1}$ (mod 64)

Find a unique value d such that 64 divides 5d-1 value ---- pi

d = 13

Step (6). Public Key = (n, e) = (85, 5).

Private Key = (n, d). = (85, 9).

Step (7). Encrypt the message M = 8 then

$C \equiv M^{E}$ (mod N)

$C \equiv 8^{5\,(}$mod 85) = 43, Cipher Text = 43

Step (8). To decrypt the cipher text we have $M = C^{d}$ (mod n)

$M = 43^{13}$ (mod 85)

M = 8, Plain Text = 8

4.2. Case Study I1. Performance Analysis of EKR Cryptosystem with one Public Key and one Private Key to Resistance against to Simple Power Analysis Attacks.

Step.(1). Select u as a prime integer = 13.

Step.(2). Select t is secret key as a prime integer = 5.

Step (3). Compute w if $2^{w-2} \leq t \leq 2^{w} - 1$ and $1 \leq w \leq n$.

Step (4). Compute m = dw; m=6.

Step (5). Select a number b such that $(b, 2^{m}{}^{)}{}^{=1} \Rightarrow b = 7$.

Step (6). Compute b^{-1} such that $bb^{-1} \equiv 1(\text{mod } 2^{m}) \Rightarrow b^{-1} = 55$.

Step (7). Public Key = (u, b)

= (13, 7).

Private Key = (u, b^{-1}).

= (13, 55).

Step (8). Encrypt the message M = 8 then

$C \equiv M^{E}(\text{mod N})$

$C \equiv M^{b} b^{-1}2^{m}$ (mod u)

$C \equiv 8^{7} * 55 * 64$ (mod 13).

C = 2097152 X 55 X 64(mod 13) = 11, Cipher Text = 11.

Step (9). To decrypt the cipher text as follows

$M = C^{D\,(}$mod N)

$M = C^{b\ -1}\ b^{-1}2^{m}$ (mod u),

$M = 11^{55} * 55 * 64$(mod 13)

$=6.654881814988989267387731337\text{ X }10^{30}$

M = 8 , Plain Text = 8.

C. Case Study II. Performance Analysis of RSA Cryptosystems with one Public Key and one Private Key.

Step (1). Select two prime integers p = 13. q = 5

Step (2). Compute n = pq = 65, Φ (n) = (p-1)(q-1) = 48

Step (3). Choose e=5, Check gcd (5, p-1) = gcd (5, 12) = 1

Check gcd (5, q-1) = gcd (5, 4) =1

Check gcd (e, (p-1) (q-1)) = gcd(5, 48) = 1

e = 5.

Step (4). Compute d such that ed =1(mod Φ (n))

Step (5). Compute $d = e^{-1}$ (mod Φ (n))

$d = 5^{-1}$ (mod 48)

Find a unique value d such that 64 divides 5d-1 value ---- pi

d = 10

Step (6). Public Key = (n, e) = (65, 5).

Private Key = (n, d). = (65, 10).

Step (7). Encrypt the message M = 8 then

$C \equiv M^{E}(\text{mod N})$

$C \equiv 8^{5\,(}$mod 65) = 43, Cipher Text = 43

Step (8). To decrypt the cipher text we have $M = C^{d}$ (mod n)

$M = 43^{10}$ (mod 65)

M = 64, Plain Text = 64. ** Wrong **

PERFORMANCE COMPARISONS

In the existing system experiments were performed on both PCs and mobile devices. Data was collected from various studies conducted by research institutes and individual experiments. Elliptic curve cryptosystems provides more security and efficiency for mobile devices and PC's but also it is alternative to conventional cryptosystems like RSA and DSA.

In the proposed EKR Cryptosystem to resistant against to Simple Power Analysis Attacks was most suitable for side-channel attacks in elliptic curve cryptosystems. Because secret key "t" was infeasible in cryptosystem and also the generation of public Key and Private Key are infeasible, so the attacker unable to guess the secret key in the cryptographic operation. The attacker could not measure the power consumption using the execution of a cryptographic algorithm store the wave form using oscilloscope and process the information to learn the secret key.

The generation of secret key and Private Key was not easy to guess to retrieve the valuable information from single leaked information in a power consumption electromagnetic emanation trace in Simple Power Analysis Attacks. Finally the proposed application i.e. EKR cryptosystem to resistance against to Simple power Analysis attacks most suitable for mobile devices than the conventional cryptosystems like RSA.

CONCLUSIONS

ECC is the most for suitable PKC schemes use in a constrained environment. Its efficiency and security makes it an attractive alternative to conventional cryptosystems, like RSA and DSA, not just in constrained devices, but also on powerful computers.

It is no doubt about ECC was being recognized as a fast powerful cryptographic scheme. We provided a new cryptosystem i.e EKR Cryptosystem to resistance against to Simple Power Analysis Attacks and more efficient to conventional cryptosystems like RSA. Wireless devices are rapidly becoming more dependent on more security features such as the ability to do secure email, web browsing and virtual private networking to corporate networks and ECC allows more efficient implementation of all of these features.

REFERENCES

1. *E.Kesavulu Reddy "Security through Elliptic Curves for Wireless Networks in Mobile Devices "published in Lecture Notes in Computer Science in vol.1 pp 208-213, World Congress On Engineering and Computer Science 2010, San Francisco, USA*
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's. 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.*

4. *Kocher. P, J. Jaffe & B. Jun. "Differential power analysis". In Advances in Cryptology – CRYPTO '99, LNCS, vol. 1666, pp 2, 22, 24, 172, 194. Springer-Verlag, 1999. .*

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.*

7. *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.*

8. *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.*

9. *B. Moller. "Securing elliptic curve point multiplication against side channel attacks". In International Security Conference – ISC '01, LNCS, vol. 2200, pp. 324–334. Springer-Verlag, 2001.*

10. *Okeya, K., and Sakurai, K. Power analysis breaks elliptic curve cryptosystems even secure against the timing attack. In Progress in Cryptology{ INDOCRYPT2000 (2000), B. K. Roy and E. Okamoto, Eds., vol. 1977 pp. 178-190*

11. *Mangard. Stefan, Elisabeth Oswald, and Thomas Popp. Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security). Springer, 2007.*

12. *Kirtane. Varad, C.Pandu Rangan "Side Channel Attack Resistant Implementation of Multi-Power RSA using Hensel Lifting" Dept.of Computer Science IIT-Madras.*

13. *Brown et al .M., "Software Implementation of the NIST Elliptic Curves over Prime Fields," D. Naccache, Ed., Topics in Cryptology — CT-RSA 2001, LNCS, vol.2020, pp 250–65 .Springer-Verlag, 2001.*