Non Adjacent Form Based Scalar Multiplication Technique for Increasing Speed of ECC

[1]A.Vithya Vijayalakshmi, [2]Dr. L. Arockiam
[1]Ph.D. Scholar, [2]Associate Professor,
Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli, Tamilnadu, India

Abstract

Internet of Things connects anything, anyplace and any device. Every 'thing' is connected to the global Internet and 'things' are communicating each other, which results in data security. Data security is one of the most critical challenges in the IoT Environment. Elliptic curve based cryptosystem is an efficient public key cryptosystem suitable for IoT environments. The most expensive and time-consuming operation in Elliptic curve cryptosystem is scalar multiplication operation. This paper proposes a method for performing scalar multiplication based on Non-Adjacent Form. This optimization of scalar multiplication will substantially enhance the Elliptic Curve Cryptography performance.

Keywords— **Internet of Things, Data Security, Elliptic Curve Cryptography, Scalar Multiplication, Non-Adjacent Form**

1. INTRODUCTION

Internet of Things (IoT) is a world-wide network that offers a huge number of interconnected heterogeneous things such as Sensors, Bluetooth devices, Radio-Frequency Identification (RFID) tags, Zigbee and mobile phones which are able to interact and provide a smart environment to improve our daily life [1]. It can be defined as "a network of uniquely identifiable, accessible, and manageable smart things that are capable of performing communication, computation and ultimate decision making" [2]. The concept of IoT has become popular in many areas such as smart electric meter reading, telemedicine monitoring, intelligent transportation and greenhouse monitoring. But still there exists several challenges in IoT that need to be interpreted and addressed.

Security is one of the most fundamental issues in many such areas. In IoT, providing security to the sensed data is a major issue. There are several security challenges in the IoT such as counterfeit attacks, malicious code attacks, security risks in information transmission etc. Encryption is considered as the most effective technique to protect IoT data. Different encryption schemes for protection of data have been in use for many decades. But, elliptic curve based cryptosystem is an efficient public key cryptosystem, which is more suitable for IoT environments. The performance of elliptic curve cryptosystem depends on an operation called point multiplication. It is the multiplication of a scalar with the given point on the elliptic curve [6]. This paper deals with the scalar multiplication using Non- Adjacent Form.

The rest of the paper is organized as follows. Section 2 describes related works. Section 3 presents the basic concepts of Elliptic Curve Cryptography. Section 4 gives the problem definition. Section 5 presents the proposed methodology. Finally, Section 6 concludes the proposed work and references at the end.

2. RELATED WORKS

Zhe Liu et al. [3] discussed the security system of Internet of Things (IoT). An emerging family of lightweight elliptic curves (MoTE Curves) was defined. The design of a scalable, regular, and highly-optimized ECC library was defined for both MICAz and Tmote Sky nodes, which supports both widely-used key exchange and signature schemes. Two different parameters namely speed and memory efficiency were used to measure the performance at different curves in ECC. The emerging twisted Edwards models of elliptic curves were proved to be more suitable for IoT with high performance and reasonable memory and power consumption.

Mohammad Rasmi et al. [4] discussed the use of elliptic curve cryptography in detail. The research parameters of ECC such as power, computation and storage were presented. The point multiplication operation in ECC is the time-consuming operation. The two factors that affect the efficiency of EC scalar multiplication were stated. A survey was done to find which composite EC operation is suitable for ECC to improve the computational efficiency and also presented which new recoding method is optimum to accelerate the EC computations for efficient composite scalar multiplication operation.

Debabrat Boruah et al. [5] compared two different algorithms such as RSA and ECC and stated that ECC offers equal security with smaller key size when compared to RSA. They discussed ElGamal based Elliptic Curve Encryption. ElGamal Elliptic Curve Cryptography is a public key cryptography analogue to ElGamal encryption schemes which uses Elliptic Curve Discrete Logarithm. Here, the whole cryptosystem was divided into seven phases and implemented to perform various mathematical manipulations.

Harsandeep Brar et al. [6] reviewed elliptic curve cryptography and highlighted the importance of point multiplication. An efficient block method was proposed

for computing NAF in scalar multiplication, whose operational efficiency directly determines the performance of ECC. A comparative study of both standard and block methods for computing NAF was presented and the proposed method was proved to be more effective than standard methods. Finally the proposed algorithm was implemented and proved. It was found that the proposed algorithm improved the speed of computing NAF than other methods.

Mohsen Bafandehkar et al. [7] reviewed the use of elliptic curve cryptography and point multiplication in ECC. The existing methods used for scalar multiplication were presented and found that the optimization of scalar multiplication enhanced the speed of ECC. An efficient {0,1,3}-NAF scalar recoding algorithm by applying block method technique was presented. A fixed lookup table which requires less computation for recoding, was created. The Big-O notation was used to measure the complexity and (μs) to evaluate the running time of the existing and proposed method. The results were compared and finally it was proved that the complexity of the existing algorithm was reduced and performance time has also been improved.

3. PROBLEM STATEMENT

The security of IoT data is one of the main issues. To provide an efficient data security, a mechanism that provides secure data encryption is needed. There are many security mechanisms available. Elliptic Curve Cryptography is more suitable for IoT environments. Here, scalar multiplication is one of the major research areas. Different researches have focused on that, because the complexity of the algorithm directly affects the speed of data encryption and decryption. So, algorithm that will help to increase the speed of scalar multiplication in ECC is needed.

4. BACKGROUND STUDY

4.1 ELLIPTIC CURVE CRYPTOGRAPHY

Cryptography is used to secure data. There are many cryptographic techniques such as RSA, DES, AES, ECC etc. are already available in literature. The use of Elliptic Curve Cryptography (ECC) in encrypting data gives the same level of security with smaller key size (i.e.) the security level given by RSA with 1024 bit key can be achieved with 160 bit key by ECC. Table 1 shows the key size for both ECC and RSA. Elliptic Curve Cryptography is a public key cryptosystem developed by Neil Kobiltz and Victor Miller in 19th century [8] which offers a new way to perform mathematical operations. The security strength of ECC depends on the difficulty of Elliptic Curve Discrete Logarithm Problem (ECDLP) [9].

Elliptic Curve operations are performed over a finite field. Thus, its efficiency affects the implementation or design of ECC algorithm. Three types of fields are commonly used in ECC: prime, binary and extension fields. Prime fields are considered better than binary fields for software implementation, while binary fields are the best for hardware implementation [4].

Table 1. Key Size for ECC and RSA [10]

ECC Key Size	RSA Key Size
112	512
160	1024
224	2048
256	3072

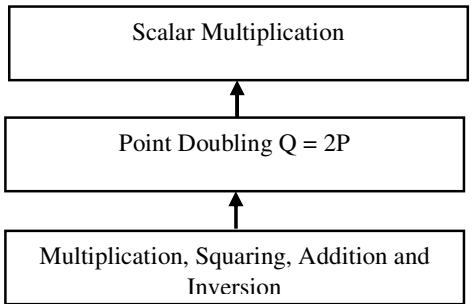
4.2 POINT GENERATION

The mathematical operations of ECC is defined over the elliptic curve $y^2=x^3+ax+b$ where $4a^3+27b^2 \neq 0$. The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the generator point G in the curve. The generator point G, the curve parameters "a" and "b" together with few more constants constitutes the domain parameter of ECC [6]. Table 2 shows the point generation for the curve $y^2=x^3+x+1$ mod 11.

Table 2. Point generation for the curve $y^2=x^3+x+1$ mod 11 [11]

x	$a = (x^3 + x + 1)$	a power 1 mod 11	Curve	Points
1	3	1	Y	(1,10) (1,1)
2	0	0	N	-
3	9	1	Y	(3,5) (3,6)
4	3	1	Y	(4,2) (4,9)
5	10	10	N	-
6	3	1	Y	(3,4) (3,7)
7	10	10	N	-
8	1	1	Y	(8,3) (8,8)
9	10	10	N	-
10	10	10	N	-

ECC involves various mathematical operations as shown in figure1. Thus, the complexity of ECC will not allow the intruder to understand the ECC and to break the security of key. Hence, it is well suited for IoT devices which are resource constraint devices.



4.3 SCALAR MULTIPLICATION

Scalar multiplication is the essential operation of elliptic curve cryptosystem. It involves the computation of kP where k is the secret key (scalar) and P is a point on the elliptic curve [6]. For any k, the calculation of kP involves number of point additions and point doublings. Each value of
"a" and "b" gives a different elliptic curve. There are two methods of scalar multiplication: single-scalar and multi-scalar multiplication. Computing kP, where $k \in Z$ and $P \in (Fp)$, is called single-scalar multiplication while computing $kP + lQ$ is called multi-scalar multiplication [4]. Figure 2 shows various scalar multiplication methods for ECC.

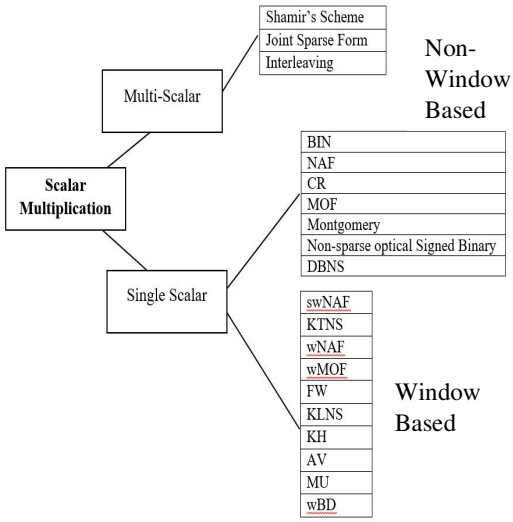


Figure 2. Scalar Multiplication Methods for ECC [4]

4.4 RECOD MULTIPL

Th
depends o
additions. E
this depend
decides the
integer *K* d
in scalar r
weight. Th
will get aff
binary form
addition wh
field multip
where *I* de
cost of mu
requires 1*I*
recoding the value k in scalar m
Non-Adjacent Form (NAF) decrea
and increases the computation speed of Elliptic Curve Cryptography.

Algorithm: Standard method for computing NAF of an integer [6]

Input: Positive integer k
Output: NAF (k)
1. i ← 0
2. While $k \geq 1$ do
   2.1 If k is odd then: $ki \leftarrow 2 - (k \bmod 4)$,
   $k \leftarrow k - ki$
   2.2 Else: $ki \leftarrow 0$
   2.3 $k \leftarrow k/2$, i← i +1
3. Return (ki-1, ki-2,….., k1, k0)

Algo
Point
Inpu
Outp
1. R
2. Fo
3. Re

Figure 3. Existing Standard Algor

5. EXISTING METHOD OF NON- ADJACENT FORM (NAF)

Non Adjacent Form (NAF) is a method for scalar multiplication proposed by Booth [6], called signed binary method. In this method, among the two consecutive digits, atmost one digit is non-zero. The unique representation of integer k will be obtained by $l-1$, $k = \Sigma k_j 2^j$, $J=0$. Where, each kj € {-1, 0, 1} such that no two consecutive digits are non-zeros. This is known as Non-Adjacent Form (NAF) [6]. The expected weight of a NAF of length n is n/3. A procedure for computing NAF for a positive integer k and left-to-right NAF method for point multiplication (addition-subtraction method) is described in the following algorithm given below [4].

The Hamming weight of the signed binary representation is lower than the Hamming weight of binary representation. The revised version is addition-subtraction method which performs from left to right. This algorithm performs (n-1) doublings and (n-1)/3 additions in an average [4]. Then a block method is introduced by Pathak

and Shanghi (2010) to improve the scalar multiplication using NAF. A lookup table contains NAF value for each index. By using NAF lookup table, the process of calculating NAF in point multiplication operation were done efficiently.

6. PROPOSED METHOD

In this paper, an algorithm to secure IoT data is proposed. Here, ElGamal based ECC encryption is used to secure the data. In ECC encryption, scalar multiplication plays a major role. To increase the computation speed of scalar multiplication in ECC, a block method for computing NAF is used which improves the speed of data encryption and decryption method. The block method for computing NAF includes two parts for performing point multiplication operations. First, calculating NAF for a given input. Second, computing point multiplication operation using NAF.

In the existing method, computing point multiplication is done easily by using lookup table. Because, a lookup table contains 256 values of NAF. For example, 8 bits block size as 2^8 = 256. Some NAF values are shown in the above table 3. In the proposed method, a look up tree is introduced. The value of NAF for each index will be assigned to the tree nodes. To reduce the search time of NAF value from the lookup table, a lookup tree is introduced. By using lookup tree, the NAF value for a particular index can be obtain quickly when compare with the lookup table. The number of steps in finding the NAF value will get reduced tremendously. The use of lookup tree will helps to reduce the computational time and increases the speed of scalar multiplication. The below figure 3 shows the lookup tree for NAF values form 0 to 255 with a block size of 8 bits.

Table 3. Look up Table for NAF [4]

INDEX	NAF VALUE {1,0,-1}
0	000000000
1	000000001
2	000000010
3	00000010-1
4	000000100
5	000000101
8	000001000
.	.
.	.
255	10000000-1

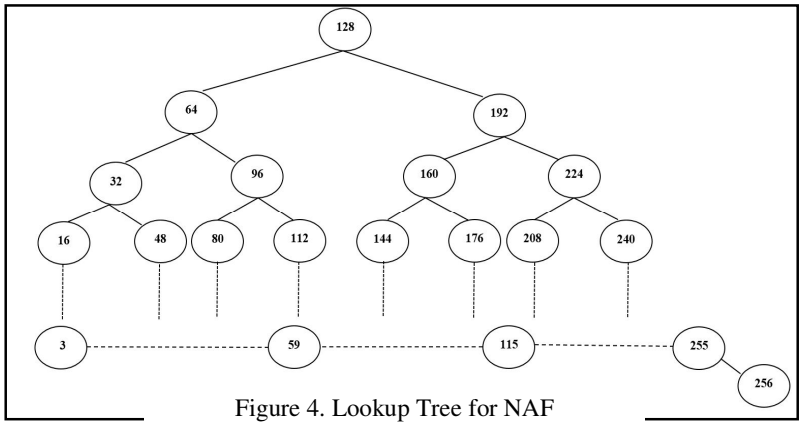


Figure 4. Lookup Tree for NAF

The above lookup tree will holds the NAF value for the index 0 to 255. In lookup table, the NAF value for a given input n has to search from 1 to n values. But, in lookup tree it can be done in few steps. By using this block method for computing NAF, the below algorithm can works faster.

Algorithm: ElGamal based ECC encryption using Non-Adjacent Form (NAF)

Input: text, point
Output: Cipher text in points
Step1: Message Embedding
- 1.1 Let the individual character of M is considered as $m_i \in M$
- 1.2 Message M should satisfy (m+1)k < P, where mi∈M, then xi=mi(30)+j, 0≤ j< 30, for j=0,1,…,29.
- 1.3 Pm is represented as Pmi = xi k + j

Step2: Key Generation
- 1.1 Generate Private Key $P_A = n_A G \bmod P$
- 1.2 Generate Public Key $P_B = n_B G \bmod P$

Step3: Block method for computing NAF for point multiplication
- 3.1 Define the input in bits and convert it into binary values
- 3.2 Divide the input into n blocks. Each block must contain equal number of bits
- 3.3 Choose lower block which has least significant and obtain NAF for each block from look up tree
- 3.4 Combine the blocks starting from right to left
- 3.5 Make boundary addition with LSB of upper block and MSB of lower block
- 3.6 Return $(k_m, k_{m-1},\ldots, k_1, k_0)$ NAF

Step4: Encryption
- 4.1 Pc = $[kG, Pm + kP_B]$

7. WORKING PROCEDURE OF THIS ALGORITHM IS EXPLAINED USING THE FOLLOWING EXAMPLE:

Let E is selected as E7777769 (2512, 2007) where a=2512, b=2007 and p= 7777769. The points generated from E7777769 (2512, 2007) are used.

Step 1: Message Embedding

Let the Message M be 'SIR'

Step1: Message 'SIR' Embedding

m_1 = 'S'

m_1=ASC(S) = 83

To find, x_1= mk + j

When j=0, x_1= (83 * 30)+0.

There is no point in the curve

When j=1, x_1= (83 * 30)+1 =

The points are (2490, 1477104)

m_1="S" is embedded as Pm= (2490, 1477104)

m_2 = 'I'

m_1=ASC(I) = 73

To find, x_1= mk + j

When j=0, x_1= (73 * 30)+0.

There is no point in the curve

When j=1, x_1= (73 * 30)+1 =

The points are (2191, 1004762)

m_2="I" is embedded as Pm= (2191, 1004762)

m_3 = 'R'

m_1=ASC(R) = 82

To find, x_1= mk + j

When j=0, x_1= (82 * 30) + 0.

The points are (2460, 878080)

m_3="R" is embedded as Pm= (2460, 878080)

Step 2: Key Generation

- Let G = (12735, 131827), now n = 7777768 nA= 8096 < 7777768, nB= 4570 < 7777768
- Let K= 8096
- Generate P_B and P_A

Step3: Block method for computing NAF for point multiplication

To compute P_B= 4570 (12735, 131827)

The binary representation of 4570 is $(1000111011010)_2$

There are two blocks of 8bits as

Block 1=11011010

Block 2=00010001

Above blocks after making to NAF are

Block 1=100-10-1010

Block 2=000010001

Now combining the blocks:

000010001

100-10-1010

= 00001001000-10-1010

$=2^{12}+2^9-2^5-2^3+2^1$

=4096 +512 -32 -8 +2

Then find P_B. Follow the same procedure to find out kG and kP_B.

Step 4: Encryption

Pc = [kG, Pm + kP_B]

Encrypt the message using ElGamal based ECC.

From the above example, it is evident that the proposed Non- Adjacent Based Scalar Multiplication technique using lookup tree will reduces the steps involved in the scalar multiplication and also improves the performance time in ECC.

8. CONCLUSION

The objective of the proposed method is to improve the security of the IoT data by optimizing the scalar multiplication in Elliptic Curve Cryptography. The proposed block method for scalar multiplication for computing NAF of an integer is more efficient. It improves the speed of computing NAF as compared to standard method and also the hamming weight of k is reduced, which improves the speed of the scalar multiplication. This method helps to improve the operational speed of Elliptic Curve Cryptography.

ACKNOWLEDGEMENT

This research was supported by the funds provided by University Grants Commission (UGC) under Junior Research Fellowship (JRF) to A. Vithya Vijayalakshmi.

REFERENCES

1. Raja Benabdessalem, Mohamed Hamdi and Tai-Hoon Kim, "A Survey on Security Models, Techniques, and Tools for the Internet of Things", IEEE International Conference on Advanced Software Engineering & Its Applications, 2014, DOI 10.1109/ASEA.2014.15, pp. 44 – 48.
2. A.Vithya Vijayalakshmi and Dr. L. Arockiam, "Enhancing the Security of IoT Data using Multilevel Encryption", of International Journal of Advanced Research in Computer Science, 2017, ISSN: 0976-5697, Vol.8, Iss.9, pp. 1 – 6.
3. Zhe Liu, Xinyi Huang, Zhi Hu, Muhammad Khurram Khan, and Lu Zhou. "On Emerging Family of Elliptic Curves to Secure Internet of Things: ECC Comes of Age", IEEE Transactions on Dependable and Secure Computing, 2016, pp. 1-5.
4. Mohammad Rasmi, Ahmad Abu Sokhon, Mohammad Sh. Daoud and Hani Al-Mimi, "A Survey on Single Scalar Point Multiplication Algorithms for Elliptic Curves over Prime Fields", IOSR Journal of Computer Engineering, 2017, ISSN: 2278-0661, Vol. 18, Iss.2, pp. 31 – 47.

5. Debabrat Boruah and Monjul Saikia, "Implementation of ElGamal Elliptic Curve Cryptography Over Prime Field Using C", IEEE ICICES, 2014, pp. 1 – 8.
6. Harsandeep Brar and Rajpreet Kaur, "Design and Implementation of Block Method for Computing NAF", International Journal of Computer Applications, 2011, ISSN No. 0975 – 8887, Vol. 20, No.1, pp. 37 – 41.
7. Mohsen Bafandehkar, Sharifah Md Yasin and Ramlan Mahmod, "Optimizing {0, 1, 3}-NAF Recoding Algorithm Using Block-Method Technique in Elliptic Curve Cryptosystem", Journal of Computer Science, 2016, Vol. 12, Iss. 11, pp. 534 - 544.
8. Koblitz. N, "Elliptic Curve Cryptosystems", Mathematics of Computation, 1987, Vol. 48, Iss. 177, pp. 203-209.
9. Shruti.P and Chandraleka.R, "Elliptic Curve Cryptography Security in the Context of Internet of Things", International Journal of Scientific & Engineering Research, 2017, ISSN 2229-5518, Vol. 8, Iss. 5, pp. 90 – 93.
10. R. Harkanson and Y. Kim, "Applications of Elliptic Curve Cryptography", ACM, 12th Annual Cyber and Information Security, (CISRC'17), 2017, pp. 1 – 7.
11. A.Vithya Vijayalakshmi, A. Dalvin Vinoth Kumar, Karthigai Priya Govindrajan and Dr. L. Arockiam, "A Secured Public key Exchange Technique for Elliptic Curve Cryptography", International Journal of Engineering Research in Computer Science and Engineering, 2017, ISSN No. 2394-2320, Vol. 4, Iss. 9, pp. 72 – 77.
12. Anusha K.P and Dr. Pritam Gajkumar Shah, "Enhanced Security Model for Cloud Using Ones compliment Re-coding for Fast Scalar multiplication in ECC", IOSR Journal of Computer Engineering, 2014, ISSN No. 2278-0661, Vol. 16, Iss. 3, pp. 107-112.
13. Christina Thomas, Gnana Sheela and Saranya P Krishnan, "A Survey on Various Algorithms Used for Elliptic Curve Cryptography", International Journal of Computer Science and Information Technologies, 2014, ISSN. No. 0975 – 9646, Vol. 5, Iss. 6, pp. 7296 – 7301.