International Research Journal of Computer Science (IRJCS)
Volume 1 Issue 4 (December 2014)
ISSN: 2393-9842
www.irjcs.com

RANDOMIZED SCALAR MULTIPLICATION FOR CANONICAL RECORDING OF ECC

Thangarasu.N[1],
[1]*Research Scholar in Department of Computer Science*
Bharathiyar University
Coimbatore

Dr.A.Arul Lawrence Selvakumar[2]
[2]*Rajiv Gandhi Institute of Technology-Bangalore*
Dean & Professor, Department of CSE
Bangalore ,INDIA

Abstract: Elliptic curve cryptography (ECC) is the most efficient public key encryption scheme based on elliptic curve concept of equations in binary scalar multiplication. The canonical bit recording technique can be used to reduce the average number of multiplications require to compute x^E provide that x^{-1} is supplied along with x. We model the generation of the digits of the canonical recording D of an n-bit long exponent E. Randomization on ECC scalar multiplication is one of the fundamental concepts together with the NAF recording algorithm.

Keywords: Elliptic curve cryptosystem, binary scalar multiplication, canonical recording, Non- adjacent recording Algorithm.

INTRODUCTION:

Elliptic curve system is applied for cryptography were first proposed in 1986 independently by Neal Koblitz[7] and victor Miller[8]. ECC can use much smaller sizes of keys bits, typically around 160 bits which provides the same security level as a 1024 bit RSA. The problem can be using the equation of weirestrass in elliptic curve groups is believed to be more difficult than the corresponding problem for Binary scalar multiplication, canonical recording and Non-Adjacent Form(NAF) underlying the finite field. The elliptic curves are a curve that also forms groups. Group's laws are constructed geometrically. In the method is a tool of mathematical problem typically used to establish the elliptic curve over a finite field for elliptic curve computations the binary method [9] Computes $Y = X^E$ using n-1 squaring and as many multiplication as one les than the number of nonzero bits in the binary expansion of the exponent, where $n= 1 +[\log_2 E]$. It is well known than n-1 is a lower bound for the number of squaring operations required. However, it is possible to reduce the number of subsequent multiplications using recording of the exponent[10,11,12,13]. More recently Oswald and Aigner[14] randomized the binary algorithm. they inserted a random decision in the process of building the addition- subtraction chain which had been originally utilized for speeding up the ordinary binary scalar multiplication of an elliptic curve point[1]. it uses the randomization concept together with non- adjacent form(NAF) algorithm[3][4]to change an ordinary binary multiplication representation to a form of signed scalar.

ELLIPTIC CURVE CRYPTOSYSTEM:

An elliptic curve is a set of points(x,y) which solutions of a bivariate cubic equation over a field K. An equation of the form

$$Y^2 + a_1xy+a_3y = x^3+a_2x^2+a_6$$

Where $a_i \varepsilon k$, defines an elliptic curve over k. As an example, if char K $\neq$ 2 and char k$\neq$3, the above equation can be transformed to wirestar equation:

$$Y^2 = x^3 + ax = b$$

With a, b ε K. This curve has one point 0 at infinity, which is the identify element of the group.
Let $P = (x_1,y_1) \neq 0$ be a point, inverse of P is $-P = (x_1,-y_1)$. Let $Q = (x_2, y_2) \neq 0$ be a second point with $Q \neq - P$, the sum $P + Q = (x_3, y_3)$ can be calculated as

$$x_3 =\lambda^2 - x_1 - x_2$$
$$y_3= \lambda(x_1 - x_3) - y_1$$

ELLIPTIC CURVE COMPUTATIONS

View the graph and an elliptic curve Graph the elliptic curve $y^2 = x^3 - x$ over the real number field R.
Determine the elements in an elliptic curve over a finite field:
When F = Zp (or more generally, when F is a finite field), the elliptic curves over Zp will be a finite set. Here we take a= 1 and b=0 with $F = Z_{19}$ and consider

$$E = \{(x,y): Y^2 = x^3 + x \pmod{19} \} \cup \{0\}.$$

Now we want to know what points are on E
To do that, we first compute the square table over F, which tells us what element in F can have a square root. This can be done by using power mod in mat lab.

Y=[ ]; for y= [0:18], Z=[Y; powermod(Y^2,19)]; y=[Y,Z]; end , Y,

This generates the following square root table mod p(p=19here)

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
0	1	4	9	16	6	17	11	7	5	5	7	11	17	9	16	9	4	1

Then, we compute x=0,1,2,-------18 to solve the equation $Y^2 = x^3 + x$ in Z_{19}. Thus (0,0) ε E. For X=1, Y^2= 1 +1 and so the square root table gives y= ± , Hence (1 ±) ε E. For x=2, we have Y^2 =8 + 2 =10. The square root table tell us that there is no solution, and so we move onto the case x=3 the following matlab comment computes all the needed information.
X= [ ]; for x=[0:18], z=[x; mod(x^3 + x, 19)]; x=[x,z]; end, x,

X=

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
0	2	10	11	11	16	13	8	7	16	3	12	11	6	5	8	3	9	17

BINARY SCALAR MULTIPLICATION

The operation of adding a point P to itself K items is called scalar multiplication by K and denoted Q = KP. We usually make use of the binary algorithm for the computation of scalar multiplication Q= KP. The binary algorithm is described in the following figure 1. The binary algorithm is the analogue of the square- and multiply method for exponential for validity and explanation see[1]

Binary Algorithm:
Input: A point P, an n-bit integer $K = \sum_{i=0}^{n-1} k_i 2^i$, $k_i \varepsilon \{0,1\}$
Output: Q = KP
Q = 0
for i = n – 1 to 0 by -1 do
{
Q = 2Q
if(k_i = = 1)_then Q = Q + P
}
return Q

CANONICAL RECORDING:

A signed- digit vector D of E is a sparse recording of E using digits from the set $\{\bar{1},0,1\}$. The recording is canonical if D contains no adjacent nonzero digits[3,8,13].Thus, a canonical signed-digit vector of E is of the form D=($D_{n-1}D_{n-2}$ ----D0) with $D_i \varepsilon \{\bar{1},0,1\}$ and

$D_i.D_{i-1} = 0$ for $1 \leq i \leq n-1$.

It can be shown that the canonical signed-digit vector for E is unique if the binary expansion of E is viewed as padded with in initial zero. This canonical signed-digit vector can be constructed by the canonical recording algorithm of Reitwiesner[3]. Reitwiesner's algorithm computes D starting from the least significant digit and proceeding to the left. First the auxiliary carry variable C_0mis set to 0 and subsequently the binary expansion of E is scanned two bits at a time. The canonically recorded digit D_i and the next value of the auxiliary binary variable C_{i+1} for i=0,1,2,----,n are generated. As an example, when E 3038, we compute the canonical signed-digit vector D as

E=(0101111011110)= $2^{11}+2^9+2^8+2^7+2^6+2^4+2^3+2^2+2^1$
D=($10\bar{1}0000\bar{1}00\bar{1}0$)=$2^{12}- 2^{10} – 2^5- 2^1$.

NON-ADJACENT FORM (NAF) RECORDING ALGORITHM

The Non-adjacent Form (NAF) representation in the form of addition – subtraction chain can reduce the number of point operations in ECCs compared to the ordinary binary representation. A minimum discussion about NAF to details[1,3,4,5,6]. Consider an integer representation of the form d= $\sum_{i=0}^{n} d_i 2^i$, $d_i \varepsilon \{\bar{1},0\ 1\}$

Where $\bar{1}$= -1`. We call it a binary signed representation. A non adjacent from (NAF) has the lowest weight among all signed-digit representations of a given k. Notice that every integer k has each unique NAF. The NAF recording number d of scalar k can be constructed by the Non-adjacent Form.

PERFORMANCE FOR ELLIPTIC CURVE CRYPTOGRAPHY IMPLEMENTATION

Although Scalar Multiplication for computations in ECC, Canonical recording and NAF are using the binary scalar multiplication for randomization. The binary algorithm is the analogue of the square- and multiply method for exponential for weirestrass equation.

- *Suitability of methods available for optimizing finite field arithmetic like addition, multiplication, squaring, and inversion.*
- *Suitability of methods available for optimizing elliptic curve cryptosystem for elliptic curve Graph for finite field.*
- *Application plat form like software, hardware, or firmware.*
- *The randomization of canonical signed-digit vector can be constructed by the canonical fields.*

CONCLUSION:

Randomized scalar multiplication can be using the elliptic curve point for the graph using the equation for finite field. Problem can be solving the matlab components. The canonical signed-digit vector for E is unique if the binary expansion of E is viewed as padded with in initial zero. The Non-adjacent Form (NAF) representation in the form of addition – subtraction chain can reduce the number of point operations in ECCs compared to the ordinary binary representation. Also mathematical calculations required by the elliptic curve cryptosystem.

ACKNOWLEDGEMENT:

We would like to thank to Mathematics faculties C.T.Nagarajan , Rajesh Kannan and B. Sakthivel for discussion of the problem matlab. We are also grateful to the anonymous referees for their comments and suggestions.

REFERENCE:

1. D.E. Knuth, the art of the computer programming,vol2: Seminumerical Algorithms,reading, MA":Addision-Wesely, 2nd Edition, 1981.
2. F.Morain and J.Olivos, " Speeding up the computation on an elliptic curve using addition- subtraction chains", Inform Theory Appl., vol.24,pp.531-543,1990.
3. G.W.Reitwiesner, Binary arithmetic, Advances in Computers, 1:231-308,1960.
4. O.Egecioglu and C.K.Koc,"Exponentiation using canonical recording," Theoretical Computer Science, vol.129, no.2, pp.407-417,1994.
5. O.Egecioglu and C.K.Koc, "fast modular exponential," In E.arikan, editor, communication, control, and Singnal Processing: Proceedings of 1990 Bilkent International Conference on New Trends in Communication, Control, and Signal Processing, PP.188-194, Bilkent Univ, Ankara, Turkey, july 1990.
6. C.N.Zhang, "An improved binary algorithm for RSAS," Computer Math. Application., vol.25,no.6, pp.15-24,1993.
7. N. Koblitz, Elliptic Curve cryptosystems, In Mathematics of Computation, vol48,pp.203-209,1987.
8. V.S.Miller, "Use of elliptic curve in cryptography," In advances in Cryptography – Crypto'85', LNCS 218, pp,,417-426,Springer-Verlag,1986.
9. D.E.Knuth, The Art of Computer Programming , vol. 2: Seminumerical Algorithms(Addison-Wesley, reading, Ma,2nd ed., 1981.
10. J. Jedwab and C.J.Mitchell, Minimum weight modified signed-digit representations and fast exponentiation, electron, let,25(1989) 1171-1172.
11. N. Koblitz,, CM-curves with good cryptographyic properties, in: J.Feignbaum, ed., Advance in Cryptography – proc Cryptolog- Proc CRYPTO '91, LectureNotes in Computer Science, vol.576(springer, Newyork, 1991)279-287.
12. C.K.Koc High-radix and bit recording techniques for modular exponential, Internal.J.computer.Math.40(19991)139-156.
13. N.Takagi.A.radix-4 modular multiplication hardware algorithm for modular exponentiation, IEE trans, Comput.41(1992).
14. 14. E.Oswald and M.Aigner,"Randomized addition- subtraction chains as a counter measure against power attacks," In Cryptographic Hardware and Embedded Systems CHES' 01, LNCS 2162.

