KKU Engineering Journal

https://www.tci-thaijo.org/index.php/kkuenj/index

A variant of Pollard's Rho method for the ECDLP over a field of characteristic two

Aekachai Nakhong and Bhichate Chiewthanakul*

Department of Computer Engineering, Faculty of Engineering, Khon Kaen University, Khon Kaen 40002, Thailand.

Received April 2016
Accepted June 2016

Abstract

The security of the elliptic curve cryptography (ECC) depends on the inability to compute the multiplicand given the original and product points. The problem to find this multiplicand is called the elliptic curve discrete logarithm problem (ECDLP). The baby-step giant-step algorithm is a generic algorithm that can be applied for ECDLPs. The running time of this algorithm and the space complexity are $O(\sqrt{Eord})$, where $Eord$ is group order. This paper shows how to apply Pollard's Rho Method to solve the same ECDLPs which has about the same running time as the baby-step giant-step algorithm, but only a small memory requirement.

Keywords: Elliptic curve, Pollard's Rho, ECDLP, Characteristic two

1. Introduction

Public key algorithm is a mechanism for sharing keys among large numbers of participants or entities in a computer information system. The application of elliptic curves in cryptography was suggested independently by Koblitz [1] and Miller [2] as an alternative mechanism for implementing public-key cryptography. It is unlike other popular algorithms such as RSA, ECC (elliptic curve cryptography) is based on a discrete logarithm that is much more difficult to challenge at equivalent key lengths [3]. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications [4] and some small network devices [5].

The security of elliptic curve cryptography rests on the assumption that the elliptic curve discrete logarithm problem (ECDLP) is hard.

Problem 1 [ECDLP]. Let E be an elliptic curve over a finite field $\mathbb{S}$. Suppose there are points P, Q_A in $E(\mathbb{S})$ given such that Q_A in $\langle P\rangle$, where $\langle P\rangle$ is a cyclic group generated by P. Determine the integer n_A such that $Q_A = n_A P$.

In this work, we present how to apply Pollard's Rho method to solve the same ECDLPs which has about the same running time as the baby-step giant-step algorithm, but only a small memory requirement.

2. Background on elliptic curve

In this section, we state the background definitions and the benefits on an elliptic curve over a field of characteristic two called Koblitz curve that is needed for the rest of the paper. For details and examples, see [6].

Let $\mathbb{F}_2$ be a field of characteristic two. And let $\mathbb{S}$ be **GF** (2^k), where **GF** (2^k) is a Galois field of characteristic two and k is a positive integer. Then the most important and advantage of working over $\mathbb{S}$ lies in the suggestion of Koblitz [1] to use an elliptic curve E over $\mathbb{F}_2$, while taking points on E with coordinates in $\mathbb{S}$, because, as Odlyzko [7] explains, discrete logarithms in $\mathbb{S}$ are relatively easy to compute unless k is chosen to be quite large. In particular, this allows the use of the Frobenius map instead of the doubling map and leads to a significant gain in efficiency [6].

Definition 1. [6] A *Koblitz curve* is an elliptic curve defined over $\mathbb{F}_2$ by an equation of the form

$$E_a: Y^2 + XY = X^3 + aX^2 + 1, \qquad (1)$$

with a in $\{0,1\}$. The discriminant of E_a is $\Delta = 1$.

Since $\Delta \neq 0$, we ensure that the curve E is nonsingular, which has no self-intersections.

Let p be a prime and let $\mathbb{F}_{p^k}$ be a finite field of characteristic p. Since **GF** (p^k) is isomorphic to $\mathbb{F}_{p^k}$, therefore **GF** (p^k) can be written as $\mathbb{F}_{p^k}$. Let $\mathcal{O}$ be an identity element of the curve E_a. The elliptic group operation of Koblitz curve is given by [8] as follows Algorithm 1.

```
Algorithm 1. Elliptic group
operation
Input: Points $P_0(x_0, y_0)$ and $P_1(x_1, y_1)$ in $E_a$
Output: The sum $P_2(x_2, y_2) := P_0 + P_1$
    if $P_0 = \mathcal{O}$ then
        output $P_2 \leftarrow P_1$ and stop
    end if
    if $P_1 = \mathcal{O}$ then
        output $P_2 \leftarrow P_0$ and stop
    end if
```

*Corresponding author. Tel.: +66 4336 2160
Email address: bhichi@kku.ac.th

doi: 10.14456/kkuenj.2016.143

```
if $x_0 = x_1$ then
    if $y_0 + y_1 = x_1$ then
        output $P_2 \leftarrow \mathcal{O}$
    else
        set $\lambda \leftarrow x_1$+$y_1/x_1$; $x_2 \leftarrow \lambda^2$+ $\lambda$ +$a$; $y_2 \leftarrow$
        $x_1^2$+($\lambda$+1)$x_2$
    end if
else
    set $\lambda \leftarrow (y_0 + y_1)/(x_0 + x_1)$; $x_2 \leftarrow \lambda^2$+ $\lambda$
    +$x_0$+$x_1$+$a$; $y_2 \leftarrow (x_1 + x_2)\ \lambda$+$x_2$+$y_1$
end if
output $P_2 \leftarrow (x_2, y_2)$.
```

We apply Algorithm 1 with $P(x,y)$ in E_a to get $-P = (x, x-y)$.

Next theorem provides a bound on the number of points on a curve over a finite field $\mathbb{F}_{p^k}$.

Theorem 1 (Hasse). [6, 9] *Let E be an elliptic curve over $\mathbb{F}_{p^k}$. Let $\#E$ denote the number of points on E. Then*

$$\#E(\mathbb{F}_{p^k}) = p^k + 1 - t_{p^k} \textit{ with } t_{p^k} \textit{ satisfying } |t_{p^k}| \leq 2p^{k/2}\ .$$

Theorem 2. [6] *Let E be an elliptic curve over $\mathbb{F}_p$ and let*

$$t = p + 1 - \#E(\mathbb{F}_p). \tag{2}$$

If α and β be the complex roots of the quadratic polynomial $Z^2 - tZ + p$. Then

$$\#E\,(\mathbb{F}_{p^k}) \ = \ p^k + 1 - \alpha^k - \beta^k\ . \tag{3}$$

3. Elliptic curve with coordinates in $\mathbb{S}$

We use (1) to obtain the following proposition.

Proposition 1. *For $E = E_1$ we have*

$$\#E = 2.$$

Proof. From (1) we have

$$E: Y^2 + XY \ = \ X^3 + X^2 + 1. \tag{4}$$

Taking $X = 0$ in (4) we obtain $Y = 1$. Taking $X = 1$ in (4) we have no solution. Since every elliptic curve has an extra point denote by $\mathcal{O}$, this serves as the identity element. Then $E = \{(0,1), \mathcal{O}\}$, and we have $\#E = 2$. ■

The first important result about the number of points on E over $\mathbb{F}_2$ is as follows.

Proposition 2. *If $\mathbb{S} = \mathbb{F}_{2^k}$ then*

$$\#E\,(\mathbb{S}) = 2^k + 1 - \left((1+\sqrt{-7})/2\right)^k - \left((1-\sqrt{-7})/2\right)^k. \tag{5}$$

Proof. Taking $p = 2$ and $\#E(F\_2) = 2$ in (2) we have $t = 1$. Using Theorem 2 we have, $\alpha = (1 + i\sqrt{7})/2$, $\beta = (1 - i\sqrt{7})/2$ be the complex roots of the quadratic polynomial $Z\text{^}2 - Z + 2$. Taking values of α and β in (3) we obtain $\#E\ (\ \mathbb{S}\ ) = 2^k + 1 - \left((1+\sqrt{-7})/2\right)^k - \left((1-\sqrt{-7})/2\right)^k$. ■

One sees from this proposition that we can find the exact number of points on the elliptic curve over a field of characteristic two, which is necessary input parameter for the Pollard's Rho method.

The SageMath [10] scripts for finding the exact order of $E(\mathbb{S})$ are given by Example 1. We used Sage-6.9-x86_64-Linux for Ubuntu 14.04 LTS 64 bits to run the scripts on Dell Inspiron 1420, CPU Intel core 2 duo 2.1 GHz with 4 GBytes of memory.

Example 1. Let $\mathbb{S}$ be $\mathbf{GF}\ (2^{50})$ in indeterminate variable V, and let $E(\mathbb{S})$: $Y^2 + XY = X^3 + (V^{43} + V + 1)X^2 + 1$ be an elliptic curve over $\mathbb{S}$. Then we can use Proposition 2 to find the exact order of $E(\mathbb{S})$ as follows.

```
k=50;Eord=expand(2^k+1-( (1+sqrt(-7))/2 )
^k-( (1-sqrt(-7))/2 )^k )
pretty_print(html("</h0>The exact value
of $\#E(S)=%s$</h0>"%latex(Eord))
   The exact value of #E(S)=1125899954494568.
```

We obtain $E(\mathbb{S}) = 1125899954494568$. But the function called *E.order()* from SageMath given us the weaker estimate as follows.

```
k=50;S.<V>=GF(2^k);E=EllipticCurve(S,[1,V^
43+V+1,0,0,1]);Eord=E.order()
pretty_print(html("</h0>$E:%s$</h0>"%latex
(E)))
pretty_print(html("</h0>The estimate value
of $\#E(S):%s$</h0>"%latex(Eord)))
$E(\mathbb{S})$: $Y^2 + XY = X^3 + (V^{43} + V + 1)X^2 + 1$
estimate value of #E(S)=1125899859190682,
```

which is the weaker estimate. #

4. Group homomorphism

In this section, we applied a mathematical structure to find an homomorphism relation between the group of units and the elliptic group. For a general theory of this structure can be found in [11-12].

We now introduce an homomorphism mapping from one algebraic system to other algebraic system which preserves the structure. Let $\mathbb{F}_p$ be a prime field and let $\mathbb{F}_p^*$ be the group of units of $\mathbb{F}_p$.

Definition 2. [12] A mapping ϕ from a group G into a group H is called an *homomorphism* if for all a, b in G we have

$$\phi(ab) = \ \phi(a)\,\phi(b).$$

Proposition 3. *Let ϕ: $\mathbb{F}_p^* \rightarrow E(\mathbb{S})$. If g in $\mathbb{F}_p^*$ and P in $E(\mathbb{S})$ we have*

$$\phi(g^n) = \ nP \textit{ for all integers } n$$

is a group homomorphism.

Proof. First we prove $\langle g \rangle$ is subgroup of $\mathbb{F}_p^*$ Let g in $\mathbb{F}_p^*$ then $\langle g \rangle$ is a subset of $\mathbb{F}_p^*$. If elements a, b in $\langle g \rangle$ we have $a = g^{n_1}$ and $b = g^{n_2}$ for some integers n_1, n_2. Since $ab = g^{n_1}g^{n_2} = g^{n_1+n_2}$ we obtain ab in $\langle g \rangle$. Let m be order of $\langle g \rangle$. It follows that $g^n g^{m-n} = 1$ from which we obtain $g^{-n} = g^{m-n}$ in $\langle g \rangle$. Therefore, $\langle g \rangle$ is a subgroup of $\mathbb{F}_p^*$.

Next we prove $\langle P \rangle$ is subgroup of $E(\mathbb{S})$. Let P in $E(\mathbb{S})$ then $\langle P \rangle$ is a subset of $E(\mathbb{S})$. If elements C, D in $\langle P \rangle$ we have $C = n_3P$ and $D = n_4P$ for some integers n_3, n_4. Since $C + D = n_3P + n_4P = (n_3 + n_4)P$ we obtain $C + D$ in $\langle P \rangle$. Let $\widehat{m}$ be order of $\langle P \rangle$. It follows that $nP + (\widehat{m} - n)P = \mathcal{O}$ from which we obtain $-nP = (\ \widehat{m} - n)P$ in $\langle P \rangle$. Therefore, $\langle P \rangle$ is a subgroup of $E(\mathbb{S})$.

Finally, we prove ϕ is an homomorphism. Since $\phi\,(\,g^{n_1}g^{n_2}\,) = \phi(\,g^{n_1+n_2}) = (n_1 + n_2)P = n_1P + n_2P$ this implies $\phi(ab) = \ \phi(a) + \phi(b)$, so this completes the proof. ■

The Proposition 3 shows that ϕ is an homomorphism mapping from a group of units to the elliptic group which preserves structure. Hence, the algorithm that uses multiplicative operation on a group of units can be replaced by additive operation on the elliptic group to solve the ECDLPs. For $1 \in \mathbb{F}_p^*$, an identity of $\mathbb{F}_p^*$ we have $\phi(1) = \mathcal{O}$.

5. The Pollard's Rho discrete logarithm algorithm

For an overview of this algorithm, see [13]. Let $\mathbb{F}_p^*$ be a group of units and let $\in \mathbb{F}_p^*$, which have multiplicative order m. Let h be an element in the cyclic group $\langle g \rangle$. Then we can treat the discrete logarithm problem $\log_g h$ as an element of $\mathbb{Z}_m$.

The idea behind this method is the following. We define a sequence by taking any initial x_0, and setting $x_i = f(x_{i-1})$ mod m, which is a random-looking function. Once we obtain two elements x_i and x_j in the sequence such that $x_i = x_j$ and $i < j$, we can compute $\log_g h$ by seeking a collision of the form $x_i = x_{2i}$, in order to save time and memory.

Let $\mathbb{F}_p^* = G_1 \cup G_2 \cup G_3$, where G_1, G_2, G_3 are partitions of $\mathbb{F}_p^*$. These partitions are defined as follows:

$G_1 = \{x \in \mathbb{F}_p^* : x \equiv 1 \ (\text{mod } 3)\}$
$G_2 = \{x \in \mathbb{F}_p^* : x \equiv 0 \ (\text{mod } 3)\}$
$G_3 = \{x \in \mathbb{F}_p^* : x \equiv 2 \ (\text{mod } 3)\}$.

Let f: $\langle g \rangle \times \mathbb{Z}_m \times \mathbb{Z}_m$ as follows:

$$f(x,\alpha,\beta) = \begin{cases} (hx, \alpha, \beta+1) & \text{if } x \in G_1 \\ (x^2, 2\alpha, 2\beta) & \text{if } x \in G_2 \\ (gx, \alpha+1, \beta) & \text{if } x \in G_3, \end{cases}$$

and we define

$$(x_i,\alpha_i,\beta_i) = \begin{cases} (1,0,0) & \text{if } i = 0 \\ f(x_{i-1},\alpha_{i-1},\beta_{i-1}) & \text{if } i \geq 1. \end{cases}$$

Then, a pseudocode of the Pollard’s Rho discrete logarithm algorithm over a prime field is given by Stinson [13].

6. A variant of Pollard’s Rho method for the ECDLP

We now consider a variant of Pollard's Rho method for the ECDLP over a field of characteristic two. The basic propositions, which we have discussed in the previous sections for finding the additive group order and mapping from multiplicative group operation to additive group operation of $E(\mathbb{S})$ give us an excellent algorithm method to solve the ECDLP over a field of characteristic two.

Let $E(\mathbb{S})$ be an elliptic curve over field of characteristic two and let $P \in E(\mathbb{S})$ be a generator of $E(\mathbb{S})$, which has additive order $Eord$ or $\#E$. Let Q_A be an element in the cyclic group $\langle P \rangle$. Similarly, we can treat the ECDLP $\log_P Q_A$ as an element of $\mathbb{Z}_{\#E}$.

Let $(E[i])$ be an increasing sequence of the elements of $E(\mathbb{S})$, and let $E(\mathbb{S}) = E_1 \cup E_2 \cup E_3$, where E_1, E_2, E_3 are partitions of $E(\mathbb{S})$. If we consider E as an array, then the partitions are defined as follows:

$E_1 = \{x \in E(\mathbb{S}) : x < E[\lfloor \#E/3 \rfloor]\}$
$E_2 = \{x \in E(\mathbb{S}) : E[\lfloor \#E/3 \rfloor] \leq x < E[\lfloor \#E \cdot 2/3 \rfloor]\}$
$E_3 = \{x \in E(\mathbb{S}) : x \geq E[\lfloor \#E \cdot 2/3 \rfloor]\}$.

Let f: $\langle P \rangle \times \mathbb{Z}_{\#E} \times \mathbb{Z}_{\#E}$ as follows:

$$f(x,\alpha,\beta) = \begin{cases} \left(Q_A + x, \alpha, \beta + \mathbb{Z}_{\#E}(1)\right) & \text{if } x \in E_1 \\ (2x, \mathbb{Z}_{\#E}(2) \cdot \alpha, \mathbb{Z}_{\#E}(2) \cdot \beta) & \text{if } x \in E_2 \\ (P + x, \alpha + \mathbb{Z}_{\#E}(1), \beta) & \text{if } x \in E_3 \end{cases}$$

and we define

$$(x_i,\alpha_i,\beta_i) = \begin{cases} (E(\mathcal{O}), \mathbb{Z}_{\#E}(0), \mathbb{Z}_{\#E}(0)) & \text{if } i = 0 \\ f(x_{i-1},\alpha_{i-1},\beta_{i-1}) & \text{if } i \geq 1. \end{cases}$$

where $E(\mathcal{O})$ is an additive identity of a group $E(\mathbb{S})$, and $\mathbb{Z}_{\#E}(0)$ is an additive identity of a ring $\mathbb{Z}_{\#E}$.

We can now give the Algorithm 2 of a variant of Pollard's Rho method for finding the solution of the ECDLP over field of characteristic two.

Example 2. Let $\mathbb{S}$ be $\mathbf{GF}\ (2^{17})$ in an indeterminate variable V, and let $E(\mathbb{S})$ is defined as follow:

$E(\mathbb{S})$: $Y^2 + XY = X^3 + AX^2 + 1$,

Where $A = V^{16} + V^{12} + V^{11} + V^{10} + V^9 + V^5 + V^3 + V^2 + 1$. If we have $P = (V^{16} + V^{15} + V^{10} + V^8 + V^7 + V^4 + V^3, V^{16} + V^{15} + V^{14} + V^{12} + V^7 + V^5 + V^4 + V^3 + V^2 + V)$ and $Q_A = (V^{14} + V^{13} + V^{12} + V^{11} + V^9 + V^8 + V^6 + V^4 + V^3 + V^2 + V + 1, V^{12} + V^{11} + V^6 + V^5 + V^3 + 1)$.
We can find $t = \log_P Q_A$ as follows.

We take $k = 17$ in Proposition 2 we have $\#E = 131174$. Then, the Algorithm 2 can be used to find $t = \log_P Q_A$. We obtain, $t = 50190$. #

7. The complexities of proposed algorithm

Proposition 4. *For* $Eord = \#E(\mathbb{S})$. *Let ECDLP be* $t = \log_P Q_A$, *then the Algorithm 2 computes in time of* $O(\sqrt{Eord})$ *additive group operation and in space of* $O(1)$ *group elements.*

Proof. Let $\phi: \mathbb{F}_p^* \to E(\mathbb{S}), g^n \mapsto nP$ which implies that the number of multiplicative operation of g in $\mathbb{F}_p^*$ is equal to the number of additive operation of P in $E(\mathbb{S})$. For m be the multiplicative order of g, the Pollard's Rho computes DLP over $\mathbb{F}_p^*$ in time of $O(\sqrt{m})$ multiplicative group operation and in space of $O(1)$ group elements. Hence the running time of the Algorithm 2 is $O(\sqrt{Eord})$ additive group operation. Similarly, the space usage of this algorithm is $O(1)$ group elements. ■

Algorithm 2. A variant of Pollard's Rho ECDLP
Input: $(E(\mathbb{S}), \#E, P, Q_A)$
Output: $t \in \mathbb{Z}_{\#E}$

```
procedure $f(x,\alpha,\beta)$
    if $x < E[\lfloor \#E/3 \rfloor]$ then
        $(x,\alpha,\beta) \leftarrow (Q_A + x, \alpha, \beta + \mathbb{Z}_{\#E}(1))$
    Else
        if $x \geq E[\lfloor \#E/3 \rfloor]$ and $x < E[\lfloor \#E \cdot 2/3 \rfloor]$ then
            $f \leftarrow (2x, \mathbb{Z}_{\#E}(2) \cdot \alpha, \mathbb{Z}_{\#E}(2) \cdot \beta)$
        else
            $f \leftarrow (P + x, \alpha + \mathbb{Z}_{\#E}(1), \beta)$
        end if
    end if
    return $(x,\alpha,\beta)$
main
    $(x,\alpha,\beta) \leftarrow (E(\mathcal{O}), \mathbb{Z}_{\#E}(0), \mathbb{Z}_{\#E}(0))$ ; $(x',\alpha',\beta')$
                                  $\leftarrow f(x,\alpha,\beta)$
    while $x \neq x'$do
        $(x,\alpha,\beta) \leftarrow f(x,\alpha,\beta)$; $(x',\alpha',\beta') \leftarrow f(x',\alpha',\beta')$;
        $(x',\alpha',\beta') \leftarrow f(x',\alpha',\beta')$
    end while
    if $gcd(\beta' - \beta, \#E) \neq 1$ then
        return (“failure”)
    else
        $c \leftarrow (\alpha - \alpha')(\beta' - \beta)^{-1} \bmod \#E$
        return $(t)$
    end if
```

Remark 1.

1. The proposed algorithm works in any case of ECDLP over field of characteristic two likes Pollard's Rho a method for the DLP (Discrete Logarithm Problem). Both algorithms have the same complexities in group units.

2. Wang [14] shown that the algorithm of Baby-Step Giant-Step over prime field computes the DLP in time of $O(\sqrt{m})$ and in space of $O(\sqrt{m})$ group unit. The analysis of algorithm by Bhichate [15] also shown that the space complexity of the Baby-step Giant-step for computing the ECDLP over field characteristic two is $O(\sqrt{Eord}),$ which is lower efficiency than the proposed algorithm.

8. Conclusions

The security of the elliptic curve cryptography (ECC) depends on the inability to compute the multiplicand given the original and product points. The problem to find this multiplicand is called the elliptic curve discrete logarithm problem (ECDLP). Elliptic curves studied here are elliptic curves defined over fields of characteristic two. The baby-step giant-step algorithm is a generic algorithm that can be applied for ECDLPs. The running time of this algorithm and the space complexity are $O(\sqrt{Eord})$, where $Eord$ is group order. However, the disadvantage of this algorithm is that it requires a considerable amount of storage $O(\sqrt{Eord})$. This paper shows how to apply Pollard's Rho Method to solve the same ECDLPs which has about the same running time as the baby-step giant-step algorithm, but only a small memory requirement.

The results of this study shown that the proposed algorithm can be used to compute any ECDLP. This algorithm has the running time of $O(\sqrt{Eord})$ and the space usage of $O(1)$. It has higher efficiency than the naive exhaustive search calculation, which need the running time of $O(Eord)$. Furthermore, it has higher efficiency in space usage than the baby-step giant-step for computing the ECDLP over field characteristic two. Hence, the proposed algorithm can be implemented on small memory devices.

9. References

[1] Koblitz N. Elliptic curve cryptosystems. Mathematics of computation 1987;48(177):203-209.

[2] Miller V. Use of elliptic curves in cryptography. In: Williams HC, editor. Advances in cryptology–crypto’85 proceedings. New York: Springer; 1986. p. 417–426.

[3] Sravani SL. Survey on elliptical curve cryptography. International Journal of Recent Advances in Multidisciplinary Research 2015;2(5):431-435.

[4] Sharad KV, Ojha D. A Discussion on Elliptic Curve Cryptography and Its Applications. International Journal of Computer Science Issues. 2012;9(1):74-77.

[5] Titinan T, Pornchai P, Wannarat S, Kanadit C. Analysis of power loss in sensor node (unode). KKU Engineering Journal 2012;39(2):147-153. [InThai].

[6] Hoffstein J, Pipher J, Silverman JH. An introduction to mathematical cryptography. New York: Springer; 2008.

[7] Odlyzko AM. Discrete logarithms in finite fields and their cryptographic significance. In: Beth T, Cot N, Ingemarsson I, editors. Advances in cryptology: Proceedings of EUROCRYPT 84 A Workshop on the Theory and Application of Cryptographic Techniques; 1984 April 9-11; Paris, France. New York: Springer; 1985. p. 224-314.

[8] Solinas JA. Efficient arithmetic on Koblitz curves. Designs, Codes and Cryptography 2000;19(2-3):195-249.

[9] Silverman JH, Cornell G. Arithmetic geometry. New York: Springer; 1986.

[10] Stein W. SageMath mathematics software (Version 6.9); 2015.

[11] Dummit DS, Foote RM. Abstract algebra. 3rd ed. USA: John Wiley & Sons; 2004.

[12] Herstein IN. Topics in algebra. 2nd ed. USA: John Wiley & Sons; 2006.

[13] Stinson DR. Cryptography: theory and practice. 3rd ed. USA: CRC press; 2005.

[14] Wang P, Zhang F. Computing elliptic curve discrete logarithms with the negation map. Information Sciences 2012;195:277-286.

[15] Bhichate C. A variant of the baby-step giant-step for computing the elliptic curve discrete logarithm over field characteristic two. International conference on internet studies; 2015 July 18-19; Tokyo, Japan.