Knapsack Cryptosystem on Elliptic Curves

Koichiro Noro
Graduate School of Science and Engineering,
Yamagata University
4-3-16 Jonan Yonezawa-shi Yamagata, 922-8510 Japan
Email: qq0641q6@cna.ne.jp

Kunikatsu Kobayashi
Graduate School of Science and Engineering,
Yamagata University
4-3-16 Jonan Yonezawa-shi Yamagata, 922-8510 Japan
Email: kobayash@yz.yamagata-u.ac.jp

***Abstract*—The LLL algorithm is strong algorithm that decrypts the additional type Knapsack cryptosystem. However, the LLL algorithm is not applicable in the addition in the group that rational points of elliptic curves on finite fields do. Therefore, we think the Knapsack cryptosystem constructed on elliptic curves. By using the pairing for the decryption, it is shown to be able to make the computational complexity of the decryption a polynomial time by making the decryption function by the pairing value.**

I. Introduction

The additional knapsack cryptosystem can be encrypted at high speed. However, there is a problem in safety because of being often decrypted by the LLL algorithm. The LLL algorithm is an algorithm to which the approximation solution of the shortest vector contained in the lattice is obtained. Ciphertexts of the additional type knapsack cryptosystem are uniting of integers of the public key and the plaintext vector. When we think about the lattice including the ciphertext and compute the short vector in this lattice by the LLL algorithm, the vector corresponding to the plaintext vector appears. As a result ciphertexts is decrypted in the output of the LLL algorithm.

The ciphertext is not uniting of integers of the public key and the plaintext vector if the addition on the knapsack cryptosystem is replaced with the additive group that rational points of elliptic curves on finite fields do.The knapsack cryptosystem on elliptic curve cannot be decrypted by the LLL algorithm because it becomes an output considered the integer uniting the public key with the plaintext vector when the LLL algorithm is applied in this way.

In this paper, we propose the construction of the knapsack cryptosystem on elliptic curves. We describe that by using the pairing for the decryption, it is shown to be able to make the computational complexity of the decryption a polynomial time by making the decryption function by the pairing value. And we show the example of the numerical value.

II. Knapsack cryptosystem by using pairing

A. Pairing on elliptic curves

In this paper the pairing is computed by using the Tate pairing, and the pairing value by rational point P, Q on elliptic curve is shown with $e(P, Q)$. Embedding degree in the pairing is shown by l.

B. Key generation

Let p be a prime number in 1024 bits or more. We think an elliptic curve on $\boldsymbol{F}_p$ as follows:

$$y^2 = x^3 + ax + b \tag{1}$$

We denote this elliptic curve by $E(\boldsymbol{F}_p)$. The prime number p is chosen such that big prime number n in 160 bits or more appear to factorization on prime numbers of order of elliptic curve $\#E(\boldsymbol{F}_p)$. This elliptic curve $E(\boldsymbol{F}_p)$ has torsion group $E(\boldsymbol{F}_p)[n]$ of order n, and we take arbitrary a rational point $P \in E(\boldsymbol{F}_p)[n]$. Here,

$$E(\boldsymbol{F}_p)[n] = \{P \in E(\boldsymbol{F}_p) | nP = O\}, \tag{2}$$

and O is point at infinity. Next we take arbitrary point $Q \in E(\boldsymbol{F}_{p^l})$. By these two points P, Q we compute $e(P, Q)$.

Next, we take constant $k (k \in \boldsymbol{N})$ at random. However, in the following super-increase sequence

$$a_i = k \cdot 2^{i-1} \;\; (i = 1, 2, 3, \cdots, ur), \tag{3}$$

k is chosen to satisfy the following condition

$$\sum_{i=1}^{ur} (k \cdot 2^{i-1}) < \frac{n-1}{2}. \tag{4}$$

Rational point $a_i P (i = 1, 2, 3, \cdots, ur)$ is opened to the public as a vector of knapsack. However, as described later, to decrypt efficiently, u ciphertexts are sent, and each of them is sum of r ratinal points $a_i P$. Hence, the number of a_i is ur. Here, we takes $ur > 100$ so that the ciphertexts may have the tolerance enough in brute force attack.

Then, rational points

$$a_1 P, \cdots, a_{ur} P, \tag{5}$$

the elliptic curve $E(\boldsymbol{F}_p)$, arbitrary point

$$R (\neq a_1 P, \cdots, a_{ur} P) \in E(\boldsymbol{F}_p)[n], \tag{6}$$

and

$$S = dR \tag{7}$$

where $d \in \boldsymbol{Z_n}$ taken at random are opened to the public.

Next, for each $C_i (i = 1, \cdots, u)$ which are transmitted as ciphertext, the decryption functions are made as follows. First, we compute

$$b_{11} = e(P, Q)^k, \tag{8}$$

and compute

$$b_{1j} = (e(P,Q)^k)^j \quad (j = 1, 2, 3, \cdots, 2^{r-1}). \tag{9}$$

Hereafter, b_{ij} are made as follows:

$$\begin{aligned} b_{2j} &= (b_{1j})^{2^r} \\ &= ((e(P,Q)^k)^j)^{2^r} \\ &= ((e(P,Q)^k)^{2^r})^j \quad (10) \\ b_{3j} &= (b_{2j})^{2^r} \\ &= (((e(P,Q)^k)^{2^r})^j)^{2^r} \\ &= ((e(P,Q)^k)^{2^{2r}})^j \quad (11) \\ &\cdots\cdots\cdots \\ b_{uj} &= (b_{u-1,j})^{2^r} \\ &= ((e(P,Q)^k)^{2^{(u-1)r}})^j. \quad (12) \end{aligned}$$

These are computed as follows: first we compute

$$b_{i1} = b_{i-1,1}^{2^r} \qquad (i = 2, 3, \cdots, u), \tag{13}$$

and next we compute

$$b_{ij} = b_{i,j-1} b_{i1} \quad (i = 1, \cdots, u, j = 2, 3, \cdots, 2^{r-1}). \tag{14}$$

Finally, we make the polynomial as follows:

$$f_i(x) = (x - b_{i1}) \cdots (x - b_{i2^{r-1}})(x-1) \quad (i = 1, \cdots, u). \tag{15}$$

The public key and the secret key are as follows:

$$\begin{aligned} PublicKey &: a_1P, \cdots, a_{ur}P, E(\boldsymbol{F}_p), R, S, r \quad (16) \\ SecretKey &: d, f_i(x), e(P,Q), a_1, \cdots, a_{ur} \quad (17) \end{aligned}$$

C. Encryption

The plaintext is assumed to be binary vector $M = (m_1, m_2, \cdots, m_{ur})$,
$m_i \in \{0, 1\}, (i = 1, 2, \cdots, ur)$, and ciphertext C is provided as follows:

$$C = m_1(a_1P) + m_2(a_2P) + \cdots + m_{ur}(a_{ur}P). \tag{18}$$

Next, $C_1, \cdots, C_{u-1}$ that is the sum of r pieces are made as follows:

$$\begin{aligned} C_1 &= m_1(a_1P) + \cdots + m_r(a_rP) \quad (19) \\ C_2 &= m_{r+1}(a_{r+1}P) + \cdots + m_{2r}(a_{2r}P) \quad (20) \\ &\cdots\cdots\cdots \\ C_{u-1} &= m_{(u-2)r+1}(a_{(u-2)r+1}P) + \cdots \\ &\quad + m_{(u-1)r}(a_{(u-1)r}P). \quad (21) \end{aligned}$$

Next, $t_1, t_2, \cdots, t_{u-1}$ are generated at random, and

$$\begin{aligned} C_{11} &= t_1R, \ C_{12} = C_1 + t_1S \quad (22) \\ C_{21} &= t_2R, \ C_{22} = C_2 + t_2S \quad (23) \\ &\cdots\cdots\cdots \\ C_{u-1,1} &= t_{u-1}R, \ C_{u-1,2} = C_{u-1} + t_{u-1}S \quad (24) \end{aligned}$$

are computed. And, $C, C_{11}, C_{12}, \cdots, C_{u-1,1}, C_{u-1,2}$ are transmitted.

D. Decryption

First, we decrypt $C_1, \cdots, C_{u-1}$ from $C_{11}, C_{12}, \cdots, C_{u-1,1}$, $C_{u-1,2}$ by secret key d as follows:

$$\begin{aligned} C_{i2} - dC_{i1} &= C_i + t_iS - dt_iR \\ &= C_i + t_idR - dt_iR \\ &= C_i. \quad (25) \end{aligned}$$

Next, we compute pairing value $e(C, Q)$ with the rational point C.

Next, we compute pairing value $e(c_1, Q)$. From this value, $m_1, \cdots, m_r$ are decrypted as follows:
First of all, let

$$X = e(C_1, Q), \tag{26}$$

and we compute

$$f_1(X/e(P,Q)^{a_r}). \tag{27}$$

If this value is 0, $m_r = 1$, and let

$$X = X/e(P,Q)^{a_r}. \tag{28}$$

Otherwise, $m_r = 0$, and we compute

$$f_1(X/e(P,Q)^{a_{r-1}}). \tag{29}$$

In the same way, if

$$f_1(X/e(P,Q)^{a_i}) = 0, \tag{30}$$

$m_i = 1$, and let

$$X = X/e(P,Q)^{a_i}. \tag{31}$$

Otherwise, $m_i = 0$, and we compute

$$f_1(X/e(P,Q)^{a_{i-1}}). \tag{32}$$

By repeating until $r = 1$ in the same way, we can decrypt C_1. And in the same way, we can decrypt $C_2, \cdots, C_{u-1}$.

Finally, C_u is decrypted as follows. Let

$$X_u = e(C,Q)/(e(C_1,Q) \cdots e(C_{u-1},Q)), \tag{33}$$

and we compute

$$f_u(X_u/e(P,Q)^{a_{ur}}). \tag{34}$$

If this value is 0, $m_{ur} = 1$, and let

$$X_u = X_u/e(P,Q)^{a_{ur}}. \tag{35}$$

Otherwise, $m_{ur} = 0$, and we compute

$$f_u(X_u/e(P,Q)^{a_{ur-1}}). \tag{36}$$

By repeating until $u(r-1)+1$ in the same way, we can decrypt C_u. Then decryption of M is completed.

E. Validity of decryption

First, we explains the decryption of C_1. Let

$$\begin{aligned} Y &= e(C_1, Q)/e(P, Q)^{a_r} \\ &= e(m_1(a_1P) + \cdots + m_r(a_rP), Q)/e(a_rP, Q) \\ &= e(m_1(a_1P) + \cdots + m_r(a_rP) - a_rP, Q) \\ &= e((m_1a_1 + \cdots + m_ra_r - a_r)P, Q) \\ &= e(k(m_1 + \cdots + m_r2^{r-1} - 2^{r-1})P, Q) \\ &= (e(P, Q)^k)^{(m_1+\cdots+m_r2^{r-1}-2^{r-1})}. \end{aligned} \tag{37}$$

If

$$m_1 + \cdots + m_r2^{r-1} - 2^{r-1} \geq 0, \tag{38}$$

we call it positive pairing value. Otherwise we call it negative pairing value. In equation

$$b_{1j} = (e(P, Q)^k)^j \quad (j = 1, 2, 3, \cdots, 2^{r-1}), \tag{39}$$

b_{1j} are all distinct values because

$$k \cdot 2^{r-1} < \frac{n-1}{2} < n \tag{40}$$

and pairing values are primitive root of unity. Since $1, 2, \cdots, 2^{r-1}$ has super increasing, so

$$1 + 2 + \cdots + 2^{r-2} < 2^{r-1}. \tag{41}$$

Hence, since

$$m_1 + \cdots + m_r2^{r-1} - 2^{r-1} < 2^{r-1}, \tag{42}$$

if $m_r = 1$, then $f_1(Y) = 0$, because Y is positive pairing value and is equal to one of b_{1j}. Otherwise $f_1(Y) \neq 0$, because Y is negative pairing value and is not equal to any of b_{1j}. By repeating this process, we can decrypt C_1 from m_r to m_1.

In a similar way, we can decrypt C_i as follows, let

$$\begin{aligned} Y &= e(C_i, Q)/e(P, Q)^{a_{ir}} \\ &= e(m_{(i-1)r+1}(a_{(i-1)r+1}P) + \\ &\qquad \cdots + m_{ir}(a_{ir}P), Q)/e(a_{ir}P, Q) \\ &= e(m_{(i-1)r+1}(a_{(i-1)r+1}P) + \\ &\qquad \cdots + m_{ir}(a_{ir}P) - a_{ir}P, Q) \\ &= e((m_{(i-1)r+1}a_{(i-1)r+1} + \\ &\qquad \cdots + m_{ir}a_{ir} - a_{ir})P, Q) \\ &= e(k(m_{(i-1)r+1}2^{(i-1)r} + \\ &\qquad \cdots + m_{ir}2^{ir-1} - 2^{ir-1})P, Q) \\ &= (e(P, Q)^k)^{m_{(i-1)r+1}2^{(i-1)r}+\cdots+m_{ir}2^{ir-1}-2^{ir-1}} \\ &= (e(P, Q)^k)^{2^{(i-1)r}(m_{(i-1)r+1}+\cdots+m_{ir}2^{r-1}-2^{r-1})}. \end{aligned} \tag{43}$$

Since

$$b_{ij} = ((e(P, Q)^k)^{2^{(i-1)r}})^j \quad (j = 1, 2, 3, \cdots, 2^{r-1}), \tag{44}$$

if $m_{ir} = 1$, $f_i(Y) = 0$, because Y is positive pairing value and is equal to one of b_{ij}. Otherwise $f_i(Y) \neq 0$, because Y is negative pairing value and is not equal to any of b_{ij}. By repeating this process, we can decrypt C_i from m_{ir} to $m_{(i-1)r+1}$.

Finally, Since

$$\begin{aligned} X_u &= e(C, Q)/(e(C_1, Q) \cdots e(C_{u-1}, Q)) \\ &= e(C - C_1 - \cdots - C_{u-1}, Q) \\ &= e(C_u, Q), \end{aligned} \tag{45}$$

we can decrypt C_u in a similar way with decryption of C_i.

F. Computational Complexity

Computational complexity of pairing is polynomial time in $\log p$[4]. In encryption, computational complexity of addition on elliptic curves is also polynomial time in $\log p$. In decryption, computational complexity of quotient pairing values is also polynomial time since they are computed in $\mathrm{mod} p$. Although we judge whether the pairing value is positive or negative by decryption functions, it computed in polynomial time since it is computed in finite times of subtractions and multiplications in $\mathrm{mod} p$.

G. Security consideration

Chipertexts $C_{11}, C_{12}, \cdots, C_{u-1,1}, C_{u-1,2}$ are encrypted by ElGamal encryption on elliptic curve. Hence, since to decrypt $C_i (i = 1, \cdots, u-1)$ from them is to solve the elliptic curve discrete logarithm problem, it is secured by taking p in 1024 bits or more, and n which is order of torsion group in 160 bits or more. And since C is consisted of 100 or more dimensions knapsack vector, it is difficult to decrypt C by brute force attack.

H. Example of the numerical value

We show the example of the numerical value. Consider the supersingular elliptic curve

$$E(\boldsymbol{F}_p) : y^2 = x^3 - x \tag{46}$$

and $p = 10202130657668293802865103277946942060930683196983(163bits)$.
$\#E(\boldsymbol{F}_p) = p + 1 = 2^3 \times 3^3 \times 59 \times 113 \times 708445873377740404845389902584519528254884 7$, so we can take $n = 7084458733777404048453899025845195282548847(143bits)$.
And embedding degree in the pairing on supersingular elliptic curves is 2[1].

1) Key generation: We choose $P \in E(\boldsymbol{F}_p)[n]$ at random as follows:
$P = (x_0, y_0)$,
$x_0 = 501220034641261684772702387415524122053584516405 3$,
$y_0 = 101930771766616765090981713067971713005370639898 81$.

Let $\boldsymbol{F}_{p^2} \cong \boldsymbol{F}_p[\alpha]/(\alpha^2+1)$. By Distortion map, we compute $Q \in E(\boldsymbol{F}_{p^2})$ as follows:
$Q = (x_1, y_1)$,
$x_1 = -1766812744814253651192235073902080733833549100228$,
$y_1 = 72476494929351057531681257939559472341769609702 78\alpha$.

By Tate pairing, we compute $e(P, Q)$ as follows:
$e(P, Q) = 8475497648993092975335009347858163770$

$014603729939\alpha + 9913604526190110896292215516390$
$296267756985968335.$

Next, let $r = 16$ and $u = 7$, we take $k = 495540812$ at random, and compute

$$a_i = k \cdot 2^{i-1} \ (i = 1, 2, 3, \cdots, 112). \tag{47}$$

From a_i, we compute rational points on E as follows:
$a_1P = (5491083210437081599569515825667616852633005560207, 4025572442589594681926119686744008800428809714792)$,
$a_2P = (1802092574501091217699025151592855938055099246 77, 6704058657406005714026569948683588326450019877997)$,
$\cdots\cdots$
$a_{112}P = (502503665807135226384344846230916746911495788 6607, 1015638517891985839541416952620464054321779774 4294)$.

Next, we choose $R \in E(\boldsymbol{F}_p)[n]$ and $d \in \boldsymbol{Z_n}$ as follows:
$R = (x_2, y_2)$,
$x_2 = 1597786150412263930474643845572603589715914691929$,
$y_2 = 3515967848299199929642824171328829834564198507251$,
$d = 1542457417324392617238920679364826279643599.$
Then we compute $S = dR = (x_3, y_3)$ as follows:
$x_3 = 3089284737822503233707830715353083734212244071544$,
$y_3 = 7606713931728309350571261148422467231166511389087.$
Therefor, we open

$$a_1P, \cdots, a_{112}P, E(\boldsymbol{F}_p), R, S, r = 16 \tag{48}$$

to public.

Next, we make the decryption functions. First,we compute
$b_{11} = e(P, Q)^{495540812}$
$= 20464477392502020231859674942000004855582062699506\alpha + 18933905927853420313908286942906368691612696 58646.$
From b_{11}, we compute

$$b_{i1} = b_{i-1,1}^{2^{16}} \qquad (i = 2, 3, \cdots, 7) \tag{49}$$

as follows:
$b_{21} = b_{11}^{2^{16}}$
$= 24929588269659052671706349764500492605069664974 45\alpha + 30964067944284859162530647068228945882356343 10596$,
$b_{31} = b_{21}^{2^{16}}$
$= 41944145746340633232549477906606080438649140198 10\alpha + 16683017503914571731554013487859869385874649 21959$,
$b_{41} = b_{31}^{2^{16}}$
$= 57964885121530669172676645617919817946908954059 71\alpha + 47620547636682708701251196718084429423441630 62911$,
$b_{51} = b_{41}^{2^{16}}$
$= 98385108030417840297449750089850507391766038527 14\alpha + 70818510396910600233073044388754061455433663 18557$,
$b_{61} = b_{51}^{2^{16}}$
$= 38434529363258719164700338897415344188518645542 52\alpha 51238865732823992044723984312711016086970754 66005$,
$b_{71} = b_{61}^{2^{16}}$
$= 86462514574945456904759106367817540780362421390 36\alpha + 63273438163858565009354165403429041358888575 59210.$
Furthermore from these values, we compute

$$b_{ij} = b_{i,j-1}b_{i1} \quad (i = 1, \cdots, 7, j = 2, 3, \cdots, 2^{15}). \tag{50}$$

For example, we compute as follws:
$b_{12} = b_{11}b_{11}$
$= 24929588269659052671706349764500492605069664974 45\alpha + 30964067944284859162530647068228945882356343 10596$,
$b_{13} = b_{12}b_{11}$
$= 41944145746340633232549477906606080438649140198 10\alpha + 16683017503914571731554013487859869385874649 21959$,
$b_{14} = b_{13}b_{11}$
$= 57964885121530669172676645617919817946908954059 71\alpha + 47620547636682708701251196718084429423441630 62911$,
$\cdots\cdots$
Finally, we make the functions such that

$$f_i(x) = (x - b_{i1}) \cdots (x - b_{i2^{15}})(x - 1) \ (i = 1, \cdots, 7). \tag{51}$$

2) Encryotion: The plaintext is assumed to be binary vector $M = (m_1, m_2, \cdots, m_{112})$ as follows:
$M = (1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1,$
$1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1,$
$0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 0, 1, 0,$
$1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0,$
$1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0).$
And ciphertext C is computed as follows:
$C = m_1(a_1P) + m_2(a_2P) + \cdots + m_{112}(a_{112}P)$
$= (43281542142933565184532813596845620137214377142 21, 15296105157319061133938229904232078164680852 14837).$
Next, $C_1, \cdots, C_6$ which are sums of every 16 of m_i is computed, and $t_1, \cdots, t_6$ are generated at random.
By $C_1, \cdots, C_6, t_1, \cdots, t_6$,
$C_{11} = (1782223046749329996264170617398956684041646577761, 6782616410816676715253759049367467811067149115502)$,
$C_{12} = (8547627102158170877981243302710968176964571821002, 7443442984383728260844880699187021412941961387365)$,
$C_{21} = (2882414812235430289245970779131977269528925717 87, 8301255646856521999203638966892825577913729867808)$,
$C_{22} = (3910715007140132234088440855519194 5215$

$96600570488, 75620241436522889585781134393494$
$86570343195706173)$,
$C_{31} = (98435789479500059274879828208427433116$
$27191091089, 22162205160985094296355426769093$
$30122074972818978)$,
$C_{32} = (15517492452279509074207406614349816913$
$23087232174, 48056188893927851787720808887470$
$15402732808675863)$,
$C_{41} = (13932425920449395062198868138506476670$
$87688107336, 16179628659902359763909366455075$
$02503501339833535)$,
$C_{42} = (73408528010378380949334563136247988294$
$34090499261, 65884394786484204231938410927098$
$49980979498739062)$,
$C_{51} = (11195349987381019384588104470465987850$
$86306752817, 36761666041709818906186833553065$
$37530939027662534)$,
$C_{52} = (34362962511590730097211482441834861350$
$41652820542, 16781515151061422020057957239916$
$88234601957501385)$,
$C_{61} = (10083856998953238764023285654124841812$
$86140016712, 26725922581055779624672990233688$
$55518445847788876)$,
$C_{62} = (93166021473708513048434271480163984618$
$17145422991, 62832463037745179647524820158753$
$0335736133590164)$
are computed.
Finally, $C, C_{11}, C_{12}, \cdots, C_{61}, C_{62}$ is transmited.

3) Decryption: First, $C_1, C_2, \cdots, C_6$ are decrypted from $C_{11}, C_{12}, \cdots, C_{61}, C_{62}$ by secret key d. Next, we compute the pairing values as follows:
$e(C_1, Q) = 13070032223281325525625089972550 16$
$302134270352159\alpha + 8337579406038302479848920$
$0278425079787184537779660$,
$e(C_2, Q) = 127146485095556363322093637841075 8$
$100644076617498\alpha + 8756622456927197875457246$
$3001553768210999896 80714$,
$e(C_3, Q) = 846287992521990114212577594855759 8$
$095221183575760\alpha + 2986234543325439708373224$
$2681734183392455557335 77$,
$e(C_4, Q) = 571854970546433195355441343654182 9$
$87212276166770\alpha + 9823725177689186941509811 7$
$4226476926894222460004 5$,
$e(C_5, Q) = 448504414737233761082042103626547 5$
$518821131014810\alpha + 6938936904028993630666509$
$9132175678830662982069 75$,
$e(C_6, Q) = 368379903014042322313017850317839 8$
$870547579645278\alpha + 8414894691892071411638941$
$6831031396826083681779 3$.
Let

$$X = e(C_1, Q) \tag{52}$$

and since

$$f_1(X/e(P,Q)^{a_{16}}) = 0, \tag{53}$$

$m_{16} = 1$, and let $X = X/e(P,Q)^{a_{16}}$.
Since

$$f_1(X/e(P,Q)^{a_{15}}) = 0, \tag{54}$$

$m_{15} = 1$, and let $X = X/e(P,Q)^{a_{15}}$.
Since

$$f_1(X/e(P,Q)^{a_{14}}) = 0, \tag{55}$$

$m_{14} = 1$, and let $X = X/e(P,Q)^{a_{14}}$.
Since

$$f_1(X/e(P,Q)^{a_{13}}) = 0, \tag{56}$$

$m_{13} = 1$, and let $X = X/e(P,Q)^{a_{13}}$.
Since

$$f_1(X/e(P,Q)^{a_{12}}) \neq 0 \tag{57}$$

$m_{12} = 0$, then we compute

$$f_1(X/e(P,Q)^{a_{11}}). \tag{58}$$

In the same way, if

$$f_1(X/e(P,Q)^{a_i}) = 0, \tag{59}$$

$m_i = 1$, and let

$$X = X/e(P,Q)^{a_i}. \tag{60}$$

Otherwise, $m_i = 0$, and we compute

$$f_1(X/e(P,Q)^{a_{i-1}}). \tag{61}$$

By repeating until $r = 1$ in the same way, we can decrypt C_1. Furthermore, by using $f_2, \cdots, f_6$, m_i are decrypted until m_{96} in the same way. Finally, let

$$X_7 = e(C,Q)/(e(C_1,Q)\cdots e(C_{u-1},Q)), \tag{62}$$

by using f_7 we compute in the same way with C_i, decrypt $m_{97}, \cdots, m_{112}$. Then decryption of M is completed.

III. Conclusion

We proposed the knapsack cryptosystem on elliptic curves which the computational complexity of the decryption is a polynomial time by using the decryption function. This cryptosystem is not decrypted by LLL algorithm because we replace the addition on Knapsack cryptosystem with the addition on elliptic curves. Although ciphertexts are rational points on elliptic curves, they are not decrypted by difficulty of elliptic curve discreat logarithm probrem since they are consisted by ElGamal cryptosystem on ellptic curves. Although ciphertexts are rational points on elliptic curves, since they are constructed by ElGamal cryptosystem on elliptic curves, they are not decrypted by difficulty of elliptic curve discrete logarithm problem.

In this time, we used Tate pairing. But since in the study of pairing more fast speed pairings have been being studied, it is able to compute more fast by other pairing methods. The more greatly we takes r, the more security increases. But then the computational complexity and amount of needed memories increase. In fact, in our present experiments, the max value of r is 16, which is used in the section 2.8. This fact depends on the environment that uses this cryptosystem. Hoever, the way of the key generation such that even if r is enlarged as much as possible the computational complexity doesn't increase is an examination problem. In addition, though we used elliptic curve Elgamal cryptosystem for the encryption, whether another method of no dependence on the difficulty of the elliptic curve discrete logarithm problem can be used is an examination problem.

ACKNOWLEDGMENT

I am deeply grateful to Department of Computer and Information Sciences of Faculty of Engineering of Nagasaki University Dr.Ryuichi Harasawa for his advice of the elliptic curve discrete logarithm problem and the security for the pairing.

REFERENCES

[1] R.Harasawa, J.Shikata, J. Suzuki and H. Imai, *Compairing the MOV and FR reductions in ellipric curve cryptography*, The Transactions of the Institute of Electronics, Information and Communication Engineers. A Vol.J82-A, No.8(19990825) pp. 1278-1290

[2] S.Uchiyama and T.Saitoh, *A Note on the Discrete Logarithm Problem on Elliptic Curves of Trace Tow*, IEICE Technical Report, ISEC98, July 1998.

[3] A.Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishes, 1994.

[4] N.Kanayama, E.Okamoto, *Ellipic Curve and Cryptography*, http://www.math.kyushu-u.ac.jp/˜trkomatu/fukuokaNT/repo/kanayama.pdf.

[5] E.Okamoto, K.Okamoto, N.Kanayama, *Recent research trend concerning pairing*, http://w2.gakkai-web.net/gakkai/ieice/vol1pdf/vol1_051.pdf.

[6] I.F.Blake, G.Seroussi, N.P.Smart, *Elliptic curves in Cryptography*, Peason Education Japan, 2001.

[7] M. Kasahara, R.Sakai, *Mathematics series of days of the Internet, Cryptography-Key that defends security of networked society*, Kyoritsu Shuppan, 2002.