社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2008－CSEC－42（4）
2008/7/24

楕円曲線上のナップザック暗号

野呂耕一郎† 小林邦勝†

† 山形大学工学部
〒992-8510 山形県米沢市城南 4-3-16
E-mail: †qq0641q6@cna.ne.jp, ††kobayash@yz.yamagata-u.ac.jp

あらまし 加算型ナップザック暗号を解読する強力なアルゴリズムとして LLL アルゴリズムがあるが，これは有限体上の楕円曲線の有理点がなす群における加法演算には適用できない．これにより，楕円曲線上でナップザック暗号を構築することを考える．復号化にペアリングを用いてペアリング値による復号化関数を作ることにより，復号化の計算量を多項式時間にすることが可能である．

キーワード ナップザック暗号，楕円曲線，ペアリング，復号化関数

Knapsack Cryptosystem on Elliptic Curves of Trace Tow

Koichiro NORO† and Kunikatsu KOBAYASHI†

† Faculty of Engineering, Yamagata University 4-3-16 Jonan Yonezawa-shi Yamagata, 922-8510 Japan
E-mail: †qq0641q6@cna.ne.jp, ††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 .

Key words Knapsack cryptosystem, elliptic curves,pairing, decryption function

1. はじめに

加算型ナップザック暗号は高速暗号処理が可能であるが，LLL アルゴリズムで解読されることが多く，安全性の点で問題がある．LLL アルゴリズムは，格子に含まれる最短ベクトルの近似解を求めるアルゴリズムである．加算型ナップザック暗号の暗号文は，公開鍵と平文ベクトルの整数結合であり，暗号文を含む格子を考え，この格子の短いベクトルを LLL アルゴリズムを適用して求めると，LLL アルゴリズムの出力に平文ベクトルに対応するベクトルが現れ，解読されてしまう．

ここで加算型ナップザック暗号における加法を有限体上の楕円曲線の有理点がなす群における加法演算に置き換えると，暗号文は，公開鍵と平文ベクトルの整数結合ではなくなる．これに LLL アルゴリズムを適用すると公開鍵と平文ベクトルの整数結合と見なしたときの出力となるので，楕円曲線上のナップザック暗号は LLL アルゴリズムでは解読できない．

本文では，supersingular 楕円曲線を利用した楕円曲線上でのナップザック暗号の構築を提案する．また，復号化にペアリングを用い，ペアリング値による復号化関数を作ることで復号化の計算量が多項式時間にすることが可能であることを示す．

2. ペアリングを用いた楕円曲線上のナップザック暗号

2.1 supersingular 楕円曲線におけるペアリング

supersingular 楕円曲線においては，埋め込み次数を 2 にすることが可能である [5]．本文では埋め込み次数が 2 の supersingular 楕円曲線を考え，曲線上の有理点 P,Q によるペアリング値を $e(P,Q)$ の形で表す．本文では，Tate ペアリングを用いてペアリング計算を行う．

2.2 鍵 生 成

1024 ビット以上の素数 p に対して，F_p 上の supersingular 楕円曲線

$$E(F_p) : y^2 = x^3 + ax + b \tag{1}$$

を考える．$\#E(F_p) = p+1$ であり，$p+1$ の素因数分解に 160 ビット以上の大きな素数 n が現れるように p を選ぶ．

この楕円曲線 $E(F_p)$ は位数 n のねじれ群 $E(F_p)[n]$ を持ち，このねじれ群の任意の点 $P \in E(F_p)[n]$ をとる．ここで

$$E(F_p)[n] = \{P \in E(F_p) | nP = O\} \text{ (O は無限遠点)} \quad (2)$$

である．次に点 $Q \in F_p^2$ をとる．これは Distortion 写像により求められる [5]．この 2 点 P, Q により，ペアリング値 $e(P, Q)$ を求める．

次に，定数 $k(k \in N)$ をランダムにとる．ただしこの k は超増加列

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

において，

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

となるように選ぶ．有理点 a_iP $(i = 1, 2, 3, \cdots, ur)$ をナップザックベクトルとして公開するが，後述のように効率的に復号するために暗号文を r の倍数ごとに u 個送信してもらう．これにより a_i は ur 個となる．ここで暗号文が総当り攻撃に十分に耐性を持つように $ur > 100$ とする．

これらより E 上の有理点

$$a_1P, \cdots, a_{ur}P \quad (5)$$

と楕円曲線 $E(F_p)$，任意の点

$$R(\neq a_1P, \cdots, a_{ur}P) \in E(F_p)[n] \quad (6)$$

と

$$d \in Z_n \quad (7)$$

をランダムにとり，

$$S = dR \quad (8)$$

を公開する．

次に送信される暗号文 $C_i, (i = 1, \cdots, u)$ ごとに復号化関数を次のように作る．まず $e(P, Q)^k$ を求め，この値より

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

を求める．以下，

$$b_{2j} = (b_{1j})^{2^r}, b_{3j} = (b_{2j})^{2^r}, \cdots, d_{uj} = (b_{u-1,j})^{2^r} \quad (10)$$

のように b_{ij} を作る．つぎに関数

$$f_i(x) = (x - b_{i1}) \cdots (x - b_{ic}^{r-1}) \quad (11)$$

を作る．

以上をまとめると，

公開鍵：$a_1P, \cdots, a_{ur}P, E(F_p), R, S, r$ (12)

秘密鍵：$d, f_i(x), e(P, Q)$ (13)

である．

2.3 暗 号 化

平文を 2 進ベクトル $M = (m_1, m_2, \cdots, m_{ur})$，$m_i \in \{0, 1\}, (i = 1, 2, \cdots, ur)$ とし，暗号文 C を

$$C = m_1(a_1P) + m_2(a_2P) + \cdots + m_{ur}(a_{ur}P) \quad (14)$$

で定める．次に以下のように m_1 から r 個ごとの和 $C_1, \cdots, C_{u-1}$ をつくる．

$$C_1 = m_1(a_1P) + \cdots + m_r(a_rP)$$

$$\cdots\cdots\cdots$$

$$C_{u-1} = m_{(u-2)r+1}(a_{(u-2)r+1}P) + \cdots + m_{(u-1)r}(a_{(u-1)\,r}P).$$

さらにランダムに $t_1, t_2, \cdots, t_{u-1}$ を生成し，

$$C_{11} = t_1R,\ C_{12} = C_1 + t_1S$$

$$C_{21} = t_2R,\ C_{22} = C_2 + t_2S$$

$$\cdots\cdots\cdots$$

$$C_{u-1,1} = t_{u-1}R,\ C_{u-1,2} = Cu - 1 + t_{u-1}S.$$

そして $C, C_{11}, C_{12}, \cdots, C_{u-1,1}, C_{u-1,2}$ を送信する．

2.4 復 号 化

まず，$C_{11}, C_{12}, \cdots, C_{u-1,1}, C_{u-1,2}$ から暗号文 $C_i, (i = 1, \cdots, u-1)$ を復号する．秘密鍵 d を用いて

$$C_{i2} - dC_{i1} = C_i + t_iS - dt_iR = C_i + t_idR - dt_iR = C_i$$

を計算する．

次に受信した有理点 C のペアリング値 $e(C, Q)$ を求める．

次に C_1 のペアリング値 $e(C_1, Q)$ を用いて $m_1, \cdots, m_r$ の復号化を行う．

$$X = e(C_1, Q)/e(P, Q)^{a_r} \quad (15)$$

とおき，$f_1(X)$ を計算し，この値が 0 であれば，$m_r = 1$ であり

$$X/e(P, Q)^{a_{r-1}} \quad (16)$$

を X とおく．0 でなければ $m_r = 0$ となり，

$$X = e(C_1, Q)/e(P, Q)^{a_{r-1}} \quad (17)$$

とおく．以下同様にして $r = 1$ まで繰り返すことによって，C_1 を復号することができる．同様にして $C_1, \cdots, C_{u-1}$ までの復号をする．

最後に C_u の復号についてであるが，

$$X_u = e(C, Q)/e(C_1, Q)/\cdots/e(C_{u-1}, Q) \quad (18)$$

とおき，さらに

$$X = X_u/e(P, Q)^{a_{ur}} \quad (19)$$

とおいて $f_u(X)$ を計算し，この値が 0 であれば，$m_{ur} = 1$ で

あり

$$X/e(P,Q)^{a_{ur-1}} \tag{20}$$

を X とおく．0 でなければ $m_{ur}=0$ となり，

$$X=X_u/e(P,Q)^{a_{ur-1}} \tag{21}$$

とおく．以下同様にして $u(r-1)+1$ まで繰り返すことによって，C_u を復号することができ，平文ベクトル $M=(m_1,m_2,\cdots,m_{ur})$ の復号化が完了する．

2.5 復号化の正当性

まず C_1 の復号化について説明する．

$$\begin{aligned}Y &= e(C_1,Q)/e(P,Q)^{a_r}\\ &= e(m_1(a_1P)+\cdots+m_r(a_rP),Q)/e(a_rP,Q)\\ &= e(m_1(a_1P)+\cdots+m_r(a_rP))-a_rP,Q)\\ &= e(m_1a_1+\cdots+m_ra_r-a_r)P,Q)\\ &= e(k(m_1+\cdots+m_r2^{r-1}-2^{r-1})P,Q)\\ &= (e(P,Q)^k)^{(m_1+\cdots+m_r2^{r-1}-2^{r-1})}\end{aligned} \tag{22}$$

において

$$m_1+\cdots+m_r2^{r-1}-2^{r-1}\geqq 0 \tag{23}$$

であれば Y は正のペアリング値，

$$m_1+\cdots+m_r2^{r-1}-2^{r-1}<0 \tag{24}$$

であれば Y は負のペアリング値と呼ぶことにする．

$$b_1,\ j=(e(P,Q)^k)^j\ \ (j=1,2,3,\cdots,2^{r-1}) \tag{25}$$

において $k\cdot 2^{r-1}<\frac{n-1}{2}<n$ であり，ペアリング値は 1 の原始 n 乗根であることから b_{1j} はすべて異なる値である．$1,2,\cdots,2^{r-1}$ は超増加性を持つので

$$1+2+\cdots+2^{r-2}<2^{r-1} \tag{26}$$

であり，

$$m_1+\cdots+m_r2^{r-1}-2^{r-1}<2^{r-1} \tag{27}$$

となるから Y が正のペアリング値であれば，d_{1j} のどれかと一致するので $f_1(Y)=0$ となり，Y が負のペアリング値であれば，d_{1j} のどれとも一致しないので $f_1(Y)\neq 0$ となる．同様にして C_i の復号化は

$$\begin{aligned}Y &= e(C_i,Q)/e(P,Q)^{a_{ir}}\\ &= e(m_{(i-1)r+1}(a_{(i-1)r+1}P)+\\ &\quad \cdots+m_{ir}(a_{ir}P),Q)/e(a_{ir}P,Q)\\ &= e(m_{(i-1)r+1}(a_{(i-1)r+1}P)+\\ &\quad \cdots+m_{ir}(a_{ir}P))-a_{ir}P,Q)\\ &= e(m_{(i-1)r+1}a_{(i-1)r+1}+\\ &\quad \cdots+m_{ir}a_{ir}-a_{ir})P,Q)\\ &= e(k(m_{(i-1)r+1}2^{(i-1)r}+\\ &\quad \cdots+m_{ir}2^{ir-1}-2^{ir-1})P,Q)\\ &= (e(P,Q)^k)^{m_{(i-1)r+1}2^{(i-1)r}+\cdots+m_{ir}2^{ir-1}-2^{ir-1}}\\ &= (e(P,Q)^k)^{2^{(i-1)r}(m_{(i-1)r+1}+\cdots+m_{ir}2^{r-1}-2^{r-1})}\end{aligned} \tag{28}$$

において

$$b_{ij}=((e(P,Q)^k)^{2(i-1)r})^j\ \ (j=1,2,3,\cdots,2^{r-1}) \tag{29}$$

であるから Y が正のペアリング値であれば，d_{ij} のどれかと一致するので $f_i(Y)=0$ となり，Y が負のペアリング値であれば，d_{ij} のどれとも一致しないので $f_i(Y)\neq 0$ となる．

最後に C_u の復号については，

$$\begin{aligned}Xu &= e(C,Q)/e(C_1,Q)/\cdots/e(C_{u-1},Q)\\ &= e(C-C_1-\cdots-C_{u-1},Q)\\ &= e(C_u,Q)\end{aligned} \tag{30}$$

であるから，上のように C_i のときと同様に C_u の復号ができる．

2.6 計 算 量

ペアリング値の計算量は $\log p$ の多項式時間である [4]．暗号化における楕円加算，2 倍計算も $\log p$ の多項式時間である．復号化関数の作成において法 p でのべき乗計算を繰り返すが，2^{r-1} までと制限するので，r によって計算量の増大を制御することができる．復号化においてペアリング値同士の除算をするがこれは法 p での除算であるので計算量は多項式時間である．

2.7 安 全 性

暗号文 $C_{11},C_{12},\cdots,C_{u-1,1},C_{u-1,2}$ は楕円エルガマル暗号により暗号化されるので，これらから $C_i,(i=1,\cdots,u-1)$ を解読することは楕円曲線離散対数問題を解くことであるから，1024 ビット以上の素数 p と有理点 $R\in E(F_p)[n]$ を 160 ビット以上にとることで安全性は確保される．また，C は 100 次より大きいナップザックベクトルから構成されるので，総当り攻撃による解読は困難である．

3. む す び

supersingular 楕円曲線上でペアリングと復号化関数を利用して復号化の計算量を多項式時間にする楕円曲線上のナップザック暗号を提案した．これは加算型ナップザック暗号における加法を楕円曲線における加法演算に置き換えているため，LLL アルゴリズムにより解読はできない．また，暗号文は楕円曲線上の有理点であるが，楕円エルガマル暗号により構成されるので，楕円曲線離散対数問題の困難性により解読はできないし，C は 100 次より大きいナップザックベクトルから構成されることより，総当り攻撃による解読も困難である．

今回は supersingular 楕円曲線上で Tate ペアリングを利用したが，ペアリングについてはより高速なペアリングが研究されているので，他の楕円曲線，ペアリング方法でさらに高速に処理することは可能である．また，r をできるだけ大きくとることでナップザックベクトルとしての次数が高くなり，安全性も高くなるが計算量も大きくなってしまう．これはこの暗号システムを使用する環境にも依存するが，r をできるだけ大きくして計算量を増大させないようにする鍵生成方法についての検

討も課題である．さらに暗号化に楕円エルガマル暗号を利用したが，楕円曲線離散対数問題の困難性に拠らない別の方法が利用できないかということも検討課題である．

謝辞　楕円曲線離散対数問題とペアリングの安全性についてご助言をいただきました長崎大学工学部情報システム工学科原澤隆一先生に感謝申し上げます．

文　献

[1] 原澤隆一，四方順司，鈴木誠，今井秀樹，楕円曲線における MOV 帰着と FR 帰着の比較について，電気情報通信学会論文誌　A,Vol.J82 − A,No.8 pp.1278-1290,Aug 1999.

[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] 金山直樹，岡本栄司，楕円曲線と暗号，http://www.math.kyushu-u.ac.jp/~trkomatu/fukuokaNT/repo/kanayama.pdf.

[5] 岡本栄司，岡本健，金山直樹，ペアリングに関する最近の研究動向，http://w2.gakkai-web.net/gakkai/ieice/vol1pdf/vol1_051.pdf.

[6] イアン・F・ブラケ，ガディエル・セロッシ，ナイジェル・P・スマート，楕円曲線暗号，ピアソン・エデュケーション，2001.

[7] 笠原正雄，境隆一，インターネット時代の数学シリーズ　暗号－ネットワーク社会の安全を守る鍵，共立出版，2002.