■1 群（信号・システム）- 3 編（暗号理論）

7 章 楕円曲線暗号とペアリング

（執筆者：高木　剛）［2008 年 11 月 受領］

■概要■

楕円曲線暗号は，1985 年に Miller と Koblitz により独立に発表された．楕円曲線暗号の安全性は，楕円曲線上の離散対数問題の困難性をもとにしている．素因数分解問題の困難性をもとにした RSA 暗号とは異なり，鍵長に対する準指数時間の解読アルゴリズムが知られていない．そのため，楕円曲線暗号は，RSA 暗号より短い鍵長で，RSA 暗号と同等のセキュリティレベルを達成できることを特徴とする．

一方，楕円曲線上の一方向双線形性写像を利用した暗号方式として，2001 年に境隆一らによって ID ベース暗号が提案された．その後，ペアリング写像を利用することにより，従来の公開鍵暗号では実現が難しいとされていた暗号プロトコル（暗号文キーワード検索，効率的なブロードキャスト暗号など）が提案された．

【本章の構成】

本章では，楕円曲線暗号及びペアリングの基本な性質について説明を行う．

■1 群 - 3 編 - 7 章

7-1 楕円曲線暗号

（執筆者：高木　剛）[2008 年 11 月 受領]

7-1-1 楕円曲線の加法公式

素数 p の位数をもつ有限体 $GF(p)$ を，$GF(p) = \{0, 1, 2, ..., p-1\}$ により表現する．$p > 3$ の有限体 $GF(p)$ 上の楕円曲線曲線 $E(p)$ は，

$$E(p) := \{(x,y) \in GF(p) \times GF(p) | y^2 = x^3 + ax + b\} \cup \{\infty\} \tag{7･1}$$

により定義される．ここで，$a, b \in GF(p)$ は $4a^3 + 27b^2 \neq 0$ を満たし，∞ は無限遠点といわれる $E(p)$ の元である．式 (7･1) の定義式をワイヤストラスの標準形と呼ぶ．楕円曲線 $E(p)$ は ∞ を零元として加法群をなし，点 $P = (x,y)$ の逆元は $-P = (x,-y)$ となる．Hasse-Weil の定理から $\#E(p) = p + 1 - t$, $|t| \leq 2\sqrt{p}$ を満たし，楕円曲線 $E(p)$ の位数 $\#E(p)$ は p と同じビット長となる．ここで，t は，$E(p)$ のトレースといわれる不変量である．

楕円曲線 $E(p)$ 上の無限遠点とは異なる 2 点 $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ に対して，加法 $P_1 + P_2 = (x', y')$ は次により計算される．

$$x' = \lambda^2 - x_1 - x_2, \quad y' = \lambda(x_1 - x') - y_1,$$

$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1) \text{ for } P_1 & \neq \pm P_2 \\ (3x_1^2 + a)/(2y_1) \text{ for } P_1 & = P_2 \end{cases} \tag{7･2}$$

この楕円曲線の加算 $P_1 + P_2$, $(P_1 \neq \pm P_2)$ を ECADD，2 倍算 $2P_1$ を ECDBL と記述する．

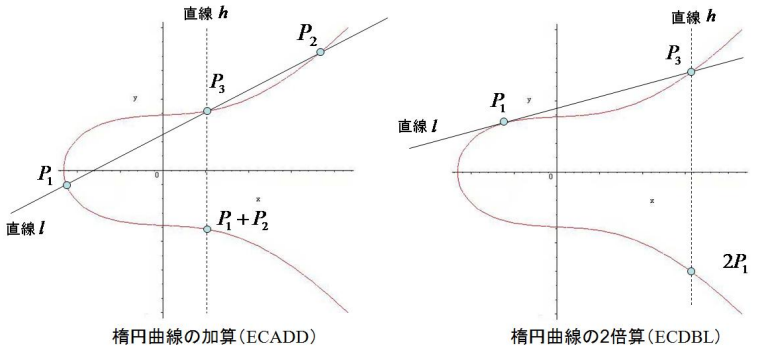

図 7･1　楕円曲線の加算及び 2 倍算

図 7･1 に，実数体上の楕円曲線 $y^2 = x^3 + 1$ を用いて，ECADD 及び ECDBL の説明をする．ECADD では，2 点 P_1, P_2 を通る直線 l に対して，P_1, P_2 とは異なる楕円曲線 $E(p)$ との交点 P_3 が存在する．この P_3 と無限遠点 ∞ を通る直線（P_3 から x 軸への垂線）h に対して，P_3 とは異なる楕円曲線 $E(p)$ との交点が加算の結果 $P_1 + P_2$ となる．同様に，ECDBL

では，楕円曲線上の点 P_1 における接線 l が，楕円曲線 $E(p)$ と交わる別の点を P_3 とし，P_3 と無限遠点 ∞ を通る直線 h と交わる別の点が 2 倍算の結果 $2P_1$ となる．

7-1-2 楕円曲線暗号

楕円曲線 $E(p)$ を利用した公開鍵暗号方式では，小さな位数の部分群に対する攻撃を避けるために，曲線の位数が素数となる楕円曲線を利用する．式 (7･1) のランダムな曲線係数 $a, b \in GF(p)$ に対して楕円曲線の位数 $\#E(p)$ を求める方法として，Schoof のアルゴリズムとその改良が知られている [1, Chapter VII]．与えられた曲線位数 $\#E(p)$ 及び定義体の標数 p に対して，曲線係数 $a, b \in GF(p)$ を求める方法として虚数乗法がある [1, Chapter VIII]．一方，楕円曲線暗号では，a, b, p を固定した 1 本の楕円曲線を多くユーザが利用できるため，今までに報告された攻撃を考慮した上で安全となる暗号用の推奨曲線が公開されている（http://www.secg.org/）．

以下，楕円曲線を利用したエルガマル暗号について説明する．

［システムパラメータ生成］ 素数位数 ℓ の楕円曲線 $E(p)$ を生成して，その生成元を G とする．システムパラメータとして $E(p), G, \ell$ をユーザ全体で共有する．

［公開鍵及び秘密鍵生成］ 秘密鍵 $s \in \{1, 2..., \ell - 1\}$ に対して，$Q = sG$ を公開鍵とする．

［暗号化］ 平文 m を位数 ℓ のビット長以下となるビット列とする．乱数 $r \in \{1, 2..., \ell - 1\}$ を発生して，システムパラメータ G 及び公開鍵 Q に対して，$C_1 = rG$，$C_2 = rQ \in E(p)$ を計算する．C_2 の x 座標である $x(C_2)$ に対して，ビットごとの排他的論理和 $c_2 = x(C_2) \oplus m$ を計算する．(C_1, c_2) を暗号文とする．

［復号化］ 暗号文 (C_1, c_2) に対して，秘密鍵 s を利用して，$D = sC_1 \in E(p)$ を計算する．関係式 $D = sC_1 = s(rG) = r(sG) = rQ = C_2$ より，平文が $m = c_2 \oplus x(D)$ により復号化できる．

楕円曲線 $E(p)$ の生成元 G 及び公開鍵 Q から秘密鍵 s を求める問題は，楕円曲線 $E(p)$ の離散対数問題といわれる．エルガマル暗号の安全性は，楕円曲線 $E(p)$ の離散対数問題の困難性をもとにしている．楕円曲線上の離散対数問題を解くアルゴリズムで，現在最も高速なアルゴリズムは Pollard の ρ 法である [1, 7 章]．その計算量は基礎体の位数 p のビット長に対して漸近的に指数時間 $O(\sqrt{p})$ である．一方，素因数分解問題の解法は，漸近的により高速な準指数時間のアルゴリズムが知られている．RSA 暗号で利用されている 1024 ビットの素因数分解問題は，160 ビットの楕円曲線上の離散対数問題と同等の困難性があると見積もられている．このように RSA 暗号と比較して鍵長が短くなっているため，楕円曲線暗号はメモリの制限された組み込みシステム用ディバイスでの実装に向いているといわれている．

■1 群 - 3 編 - 7 章

7-2 楕円曲線暗号の実装方法

（執筆者：高木　剛）[2008 年 11 月 受領]

本章では，楕円線暗号の実装に関して，最も計算量の多いスカラー倍算に関して説明を行う．スカラー倍算は，整数 d 及び楕円曲線上の点 P に対して dP を計算する演算のことである．スカラー倍算を効率的に計算する多くの方法が提案されている [7]．ここでは，楕円曲線を表現する座標系を選ぶ方法，整数 d をハミング重みが少ない符号付き 2 進展開として表現する方法を説明する．

7-2-1 座標系

楕円曲線の点を表現する基本的な座標系としては，アフィン座標 $\mathcal{A}$，射影座標 $\mathcal{P}$，ヤコビアン座標 $\mathcal{J}$ などが知られている．アフィン座標 $\mathcal{A}$ において，無限遠点 ∞ を除いた楕円曲線の点は，式 (7･1) の定義方程式 $y^2 = x^3 + ax + b$ を満たす $x, y \in GF(p)$ に対して $P = (x, y)$ と表現される．アフィン座標の点 (x, y) に対して，射影座標 $\mathcal{P}$ 及びヤコビアン座標 $\mathcal{J}$ の点 $(X : Y : Z)$ は，それぞれ $(x, y) = (X/Z, Y/Z)$ 及び $(x, y) = (X/Z^2, Y/Z^3)$ と対応する．

これらの座標系を使って，前節の加法項式である ECADD 及び ECDBL を実装した場合，計算時間に大きな差が生ずる．これらの計算時間は，有限体 $GF(p)$ での乗算 M，平方算 S，逆元の計算 I の回数によって見積もられる．実装環境にもより変化するが，平方算は乗算より若干高速であり，逆元の計算は乗算より大幅に遅い．そのため，乗算や平方算の計算を増やしても逆元の計算を避ける座標系の実装方法が提案されている [6]．また，曲線の係数を $a = -3$ とした場合，射影座標及びヤコビアン座標において片方の点の Z 座標を $Z = 1$ とした実装も高速化が実現できる．これらの高速化アルゴリズムの計算量を表 7･1 に示した．

表 7･1　ECADD 及び ECDBL の計算量

Coordinate System	ECADD		ECDBL	
	$Z \neq 1$	$Z = 1$	$a \neq -3$	$a = -3$
A	$2M + 1S + 1I$	—	$2M + 2S + 1I$	
P	$12M + 2S$	$9M + 2S$	$7M + 5S$	$7M + 3S$
J	$12M + 4S$	$8M + 3S$	$4M + 6S$	$4M + 4S$

7-2-2 符号付き 2 進展開を用いたスカラー倍算

楕円曲線のスカラー倍算を高速に計算する方法として，幅 w の非隣接形式（wNAF）が知られている．wNAF は，n ビット整数を

$$d = \sum_{i=0}^{n} d_w[i]2^i, \quad d_w[i] \in \{0, \pm 1, \pm 3, ..., \pm(2^{w-1} - 1)\} \tag{7･3}$$

と表現した場合に，隣接する w 個の桁がたかだか 1 個の非零桁をもつ表現のことをいう．n ビットの各整数に対して一意的な wNAF が存在する．wNAF の $n \to \infty$ に対する漸近的な非零桁の平均濃度は $1/(1 + w)$ である．幅 $w = 2, 3$ の場合，wNAF の 1 例を次に示す ($\overline{1} = -1, \overline{3} = -3$ とする).

バイナリ	1001110111100111000101101111000110101011111001
wNAF (w=2)	$10100\bar{0}10\bar{0}0\bar{1}0\bar{1}00\bar{1}0\bar{1}0\bar{1}00\bar{1}0\bar{0}0\bar{1}00\bar{1}0\bar{1}0\bar{1}0\bar{0}0\bar{0}0\bar{1}001$
wNAF (w=3)	$100\bar{3}000\bar{1}0000\bar{3}00\bar{1}0000\bar{3}00\bar{1}000\bar{1}00\bar{1}000\bar{3}00\bar{3}000\bar{0}\bar{1}001$

以下，wNAF の生成アルゴリズム及び wNAF を利用したスカラー倍算を計算するアルゴリズムを示す．

wNAF の生成アルゴリズム

Input: An n-bit d，a width w
Ooutput: $d_w[n]$, $d_w[n-1]$, ..., $d_w[0]$

1. $i \leftarrow 0$
2. **while** $d > 0$ **do**
   2.1. **if** d is odd **then do**
      2.1.1. $d_w[i] \leftarrow d$ mods 2^w
      2.1.2. $d \leftarrow d - d_w[i]$
   2.2. **else** $d_w[i] \leftarrow 0$
   2.3. $d \leftarrow d/2$, $i \leftarrow i+1$
3: **return** $d_w[n], d_w[n-1], ..., d_w[0]$

wNAF を利用したスカラー倍算

Input: $d_w[i]$, P, $(|d_w[i]|)P$
Output: dP

1. $Q \leftarrow d_w[c]P$
   for the largest c with $d_w[c] \neq 0$
2. **for** $i = c-1$ **to** 0 **do**
   2.1. $Q \leftarrow$ ECDBL(Q)
   2.2. $Q \leftarrow$ ECADD($Q, d_w[i]P$)
3. **return** Q

wNAF の生成アルゴリズムは，整数 d から対応する wNAF を生成するアルゴリズムである [7]．ここで，ステップ 2.1.1 の mods 2^w は，mod2^w の符号付き剰余類 $\{\pm 1, \pm 3, .., \pm(2^{w-1}-1)\}$ を表す．wNAF を利用したスカラー倍算では，整数 d の wNAF を上位ビットから走査することにより計算する．ステップ 2.1 では wNAF の各ビットで ECDBL を計算し，ステップ 2.2 では桁 $d_w[i]$ が非零の場合に ECADD を計算する．以上より，ECDBL がたかだか n 回，ECADD が $n/(1+w)$ 回必要になる．スカラー倍算は w が大きくなると高速になるが，より多くのメモリが必要となる．また，楕円曲線では点 $P=(x,y)$ の逆元 $-P=(x,-y)$ は y 座標の符号変換のみで計算できる．そのため，wNAF を利用したスカラー倍算は，点 $\{-P, -3P, ..., -(2^{w-1}-1)P\}$ を予備計算する必要はなく，符号なし 2 進展開を利用した場合よりメモリが削減できる特徴をもつ．

■1 群 - 3 編 - 7 章

7-3 ペアリング

（執筆者：高木　剛）[2008 年 11 月 受領]

7-3-1 ペアリング写像

本章では標数 $p > 3$ の有限体上の超特異曲線を利用した Tate ペアリングについて取り扱う．有限体 $GF(p)$ 上の超特異曲線は，$b = 0, 1$ に対して

$$E^b(p) = \{(x, y) \in GF(p) \times GF(p) | y^2 = x^3 + (1 - b)x + b\} \cup \{\infty\},$$

により定義される．超特異曲線 $E^b(p)$ のトレースは 0 であり，$E^b(p)$ の位数は $\#E^b(p) = p + 1$ となる．ℓ を標数 p と互いに素数であり，$\ell | \#E^b(p)$ を満たすとする．$\ell | (p^2 - 1)$ より，拡大体 $GF(p^2)$ は 1 の原始 ℓ 乗根を含む．$E^b(p)[\ell]$ を位数 ℓ の $E^b(p)$ の部分群とする．また，乗法群 $GF(p^2)^\times$ の 2 元 a, b に対して，ある $c \in GF(p^2)^\times$ が存在して $a = bc^\ell$ と表現できるとき a, b は同値であると定義する．乗法群 $GF(p^2)^\times$ において，この同値関係による商群 $GF(p^2)^\times/(GF(p^2)^\times)^\ell$ は，位数 ℓ の部分群となる．同様に，拡大体 $GF(p^2)$ 上の位数 ℓ の商群を $E^b(p^2)/\ell E^b(p^2)$ とする．ここで，Tate ペアリングは，

$$e : E^b(p)[\ell] \times E^b(p^2)/\ell E^b(p^2) \to GF(p^2)^\times/(GF(p^2)^\times)^\ell$$

により定義される双線形写像 e である．点 $P \in E^b(p)$ に対して，関数 $f_P^{(\ell)}(x, y)$ を，その因子 $(f_P^{(\ell)})$ が $\ell(P) - \ell(\infty)$ に同値なものとする．ここで，点 $R = (x, y) \in E^b(p^2)/\ell E^b(p^2)$ に対して，$e(P, R) = f_P^{(\ell)}(R)$ により Tate ペアリングは計算される．

次に，$i^2 = -1$ を満たす $i \in GF(p^2)$ に対して，拡大体 $GF(p^2)$ の $GF(p)$ 基底として $\{1, i\}$ を選ぶ．以下，この基底に対して曲線 $E^0(p)$ を考える（曲線 $E^1(p)$ も別の基底により同様に議論できる）．点 $Q = (x, y) \in E^0(p)$ に対して，distortion 写像を $\psi(x, y) = (-x, iy) \in E^0(p^2)$ により定義する．剰余群 $E^0(p^2)/\ell E^0(p^2)$ の点 R に対して $R = \psi(Q)$ となる点 $Q \in E^0(p)[\ell]$ が存在するため，Tate ペアリング $e(P, \psi(Q))$ は点 $P, Q \in E^0(p)[\ell]$ に対して定義できる．ここで，Tate ペアリングを剰余群 $GF(p^2)^\times/(GF(p^2)^\times)^\ell$ において一意的な値とするために，点 $P, Q \in E^0(p)$ に対して簡約 Tate ペアリングを $\hat{e}(P, Q) = e(P, \psi(Q))^{(p^2-1)/\ell}$ により定義する．簡約 Tate ペアリングは，非零整数値 a に対して双線形性

$$\hat{e}(aP, Q) = \hat{e}(P, aQ) = \hat{e}(P, Q)^a$$

を満たす．

以下に，Tate ペアリングを効率的に計算する方法である Miller アルゴリズム [11]を説明する．点 P_1, P_2 を通る直線を l，直線 l と楕円曲線の交点 P_3 と無限遠点を通る直線を h とする．これらの直線 l, h は，前節の楕円曲線上の加法公式（図 7･1）で用いた．関数 $f_P^{(\ell)}$ は，点 $P_1, P_2 \in E^b(p)$ に対して

$$f_{P_1+P_2}^{(\ell)} = f_{P_1}^{(\ell)} f_{P_2}^{(\ell)} \frac{g_l}{g_h} \tag{7･4}$$

を満たす [2, Chapter IX]．関数 g_l, g_h は以下を因子にもつ．

$$(l) = (P_1) + (P_2) + (P_3) - 3(\infty), \quad (h) = (P_3) + (P_1 + P_2) - 2(\infty)$$

関係式 (7･4) により，位数 ℓ を 2 進展開することにより，$O(\log p)$ 回の関数の計算によりペアリング $\hat{e}(P,Q) = (f_P^{(\ell)}(\psi(Q)))^{(p^2-1)/\ell}$ を計算することができる．Algorithm 1 に具体的な計算方法を記述する．

Algorithm 1 : Computation of Tate Pairing for $E^0(p)$

Input: $P = (x_p, y_p)$, $Q = (x_q, y_q) \in E^0(p)[\ell]$, $\ell = \sum_{i=0}^{t-1} \ell[i]2^i$, $\ell[t-1] = 1$
Output: $\hat{e}(P,Q)^{(p^2-1)/\ell} \in GF(p^2)^{\times}/(GF(p^2)^{\times})^{\ell}$

1. $f \leftarrow 1$ **and** $V \leftarrow P$
2. **for** $i \leftarrow n-1$ **to** 0 **do**
2.1. **Set the lines** l **and** h **for ECDBL**(T)
2.2. $f \leftarrow f^2, \frac{g_l(\psi(Q))}{g_h(\psi(Q))}$ **in** $GF(p^2)$
2.3. $T \leftarrow$ **ECDBL**(T) **in** $E^0(p)$
2.4. **if** $\ell[i] = 1$ **do**
2.5. **Set the lines** l **and** h **for ECADD**(T,P)
2.6. $f \leftarrow f, \frac{g_l(\psi(Q))}{g_h(\psi(Q))}$ **in** $GF(p^2)$
2.7. $T \leftarrow$ **ECADD**(T,P) **in** $E^0(p)$
3. **return** $T^{(p^2-1)/\ell}$

Algorithm 1 の各ループは，有限体 $GF(p)$ の演算（加算，乗算，逆元）を定数回行うことにより実装できるため，$O((\log p)^2)$ 回のビット演算で計算できる．そのため，Miller アルゴリズムは，p のビット長に対する多項式 $O((\log p)^3)$ で計算可能である．また，Miller アルゴリズムを高速化する方法として，分母 $g_h(\psi(Q))$ の計算を省略する方法，ℓ の 2 進展開におけるハミング重みを下げる方法，ヤコビアン座標を用いる方法などが知られている[8]．最近の実装結果では，ペアリング写像は同じセキュリティレベルの RSA 暗号と同じ程度の速度で実装できることが報告されている [14]．

7-3-2 ID ベース暗号

簡約 Tate ペアリング $\hat{e}$ の双線形性により，個人の公開鍵を自由なビット列をして選ぶことができる ID ベース暗号が実現できる [12, 13]．

[システムパラメータ生成] 標数 p に対して，大きな素数位数 ℓ をもつ楕円曲線 $E^b(p)$ を生成して，部分群 $E^b(p)[\ell]$ の生成元を P とする．マスター鍵 $s \in \{0, 1, ..., \ell-1\}$ を生成して，$Q = sP$ とする．システムパラメータとして ℓ, P, Q をユーザ全体で共有する．

[公開鍵及び秘密鍵] ユーザの ID に対応する点 $Q_{ID} \in E^b(p)$ を生成して，ユーザの秘密鍵を $S_{ID} = sQ_{ID}$ とする．

[暗号化] 平文 m を $GF(p^2)$ の元とする．乱数 $r \in \{0, 1, 2..., \ell-1\}$ を発生し

て，システムパラメータ P, Q 及び公開鍵 Q_{ID} に対して，$C_1 = rP \in E^b(p)$，$c_2 = m\hat{e}(Q_{ID}, Q)^r \in GF(p^2)$ を計算する．(C_1, c_2) を暗号文とする．

[復号化] 暗号文 (C_1, c_2) に対して，秘密鍵 $S_{ID} \in E^b(p)$ を利用して，復号化 $m = c_2\hat{e}(S_{ID}, C_1)^{-1} \in GF(p^2)$ を行う．

ここで，

$$c_2\hat{e}(S_{ID}, C_1)^{-1} = m\hat{e}(Q_{ID}, Q)^r\hat{e}(S_{ID}, C_1)^{-1} = m\hat{e}(Q_{ID}, P)^{rs}\hat{e}(Q_{ID}, P)^{-rs} = m$$

が成り立つため，平文 m は一意的に復号可能である．

ID ベース暗号では各ユーザの ID の点 Q_{ID} に対して秘密鍵 S_{ID} を生成するため，RSA 暗号や楕円曲線暗号と異なり，公開鍵 Q_{ID} の x 座標を自由なビット列（例えば

```
abcdef@fun.ac.jp
```

など）として選ぶことが可能となる．一方，ID ベース暗号と同様の構成を楕円曲線暗号で行う場合は，ユーザ ID の点 Q_{ID} に対して生成元 G から $Q_{ID} = sG$ を満たす秘密鍵 s を求める必要があり，離散対数問題を解く程度の困難性があるため実現することは難しい．

最後に，ペアリング写像 $\hat{e}$ の双線形性を利用して，従来の公開鍵暗号では構成が難しいとされていた暗号プロトコル（暗号文キーワード検索方式 [4]，効率的なブロードキャスト暗号 [5] など）が提案されている．

■参考文献

1) I. Blake, G. Seroussi, N. Smart, “Elliptic Curves in Cryptography,” London Mathematical Society, Lecture Note Series 265, 1999.
2) I. Blake, G. Seroussi, N. Smart (eds), “Advances in Elliptic Curve Cryptography,” London Mathematical Society, Lecture Note Series 317, 2005.
3) D. Boneh and M. Franklin, “Identity Based Encryption from the Weil Pairing,” SIAM Journal of Computing, Vol.32, No.3, pp.586-615, 2003.
4) D. Boneh, G. Di Crescenzo, R. Ostrovsky and G. Persiano, “Public Key Encryption with Keyword Search,” Springer-Verlag, EUROCRYPT 2004, LNCS 3027, pp.506-522, 2004.
5) D. Boneh, C. Gentry and B. Waters, “Collusion Resistant Broadcast Encryption With Short Ciphertexts and Private Keys,” Springer-Verlag, CRYPTO 2005, LNCS 3621, pp.258-275, 2005.
6) H. Cohen, A. Miyaji, T. Ono, “Efficient Elliptic Curve Exponentiation Using Mixed Coordinates,” Springer-Verlag, ASIACRYPT 1998, LNCS 1514, pp.51-65, 1998.
7) D. Hanerson, A. Menezes and S. Vanstone, “Guide to Elliptic Curve Cryptography,” Springer, 2003.
8) T. Izu, T. Takagi, “Efficient Computations of the Tate Pairingfor the Large MOV Degrees,” ICISC 2002, LNCS 2513, pp.283-297, 2002.
9) N. Koblitz, “Elliptic Curve Cryptosystems,” Mathematics of Computation, Vol.48, pp.203-209, 1987.
10) V. Miller, “Use of Elliptic Curves in Cryptography,” Springer-Verlag, CRYPTO 1985, LNCS 218, pp.417-426, 1985.
11) V. Miller, “The Weil Pairing, and Its Efficient Calculation,” Journal of Cryptology, vol.17, no.4, pp.235-261, 2004.

12) 境隆一, 大岸聖史, 笠原正雄, “楕円曲線上のペアリングを用いた暗号方式,” 暗号と情報セキュリティシンポジウム, SCIS2001, vol.7B-2, 2001. SCIS2000-C20, 2000.
13) 辻井重男, 笠原正雄 (篇), “暗号理論と楕円曲線,” 森北出版, 2008.
14) M. Yoshitomi, T. Takagi, S. Kiyomoto, and T. Tanaka, “Efficient Implementation of the Pairing on Mobilephones using BREW,” IEICE Transaction, vol.E91-D, no.5, pp.1330-1337, 2008.