Memoirs of the Faculty of Science
Kochi University (Information Science)
Vol. 27 (2006), No. 1

Weil 対を用いた暗号システムに適した CM 曲線の構成

Construction of CM Curves Suitable for Cryptosystem from the Weil Pairing

太田 浩祐[1]　塩田 研一[2]
Kohsuke Ohta[1]　Ken-ichi Shiota[2]

要　旨

楕円曲線上の Weil 対を利用した暗号システムにおいては、数百ビットの m に対して m-等分点の座標を拡大次数の小さな体に納めることが必要であり、supersingular な楕円曲線を用いた場合には定義体の高々 6 次の拡大体での設計が可能である。本研究では CM 曲線の構成法に改良を加えることにより次のような楕円曲線が高速に構成できることを示す：(i) m-等分点の座標が全て素体 $\mathbf{F}_p$ 上有理的であるもの、(ii) 任意の拡大次数 ℓ について、$\mathbf{F}_p$-有理的な m-等分点は m 個のみで、全ての m-等分点の座標を含む体は ℓ-次拡大になるもの。前者は双一次形式を必要とする暗号システムを素体上で設計することを可能にし、後者は、公開鍵は素体上の有理点、セキュリティレベルは拡大体上の Diffie-Hellman 問題と同等、という設計を可能にする。

1. はじめに

$\mathbf{F}_q$ を位数 q の有限体、E を $\mathbf{F}_q$ 上の上の楕円曲線、$\mathcal{O}$ をその無限遠点とし、E の $\mathbf{F}_q$-有理点のなす群を $E(\mathbf{F}_q)$ と表す。$\mathbf{F}_q$ の標数 $p = \mathrm{char}(\mathbf{F}_q)$ と互いに素な自然数 $m > 1$ に対して E の m-等分点の成す群を

$$E[m] = \{P \in E(\overline{\mathbf{F}_q}) \,|\, mP = \mathcal{O}\},$$

また $\overline{\mathbf{F}_q}$ における 1 の m-乗根のなす群を μ_m と表す。Weil 対

$$e_m : E[m] \times E[m] \to \mu_m$$

は非退化な双一次交代形式である。

Weil 対は Miller のアルゴリズムによって高速に計算可能であるが ([1])、この際 $E[m]$ の座標の体 $\mathbf{F}_q(E[m])$ を扱う必要がある。暗号システムへ応用する為には $\mathbf{F}_q(E[m])$ は小さな拡大体であることが望ましく、supersingular な楕円曲線を用いた場合には拡大次数を高々 6 に取る設計が可能である ([4])。

本研究ではまず、素体 $\mathbf{F}_p$ 上の楕円曲線で

$$E[m] \subseteq E(\mathbf{F}_p)$$

を満たすものを構成する。この場合セキュリティレベルは $\mathbf{F}_p$ における Diffie-Hellman 問題と同等であるが、双一次交代形式を必要とするシステム（3 者間での鍵交換システム等）を $\mathbf{F}_p$ 上で実現できるのが利点である。

更に、与えられた $\ell > 1$ に対し $E[m] \subseteq E(\mathbf{F}_{p^\ell})$ を満たす楕円曲線の構成法を述べる。この場合例えば $1 \le f < \ell$ について

$$E[m] \cap E(\mathbf{F}_{p^f}) \cong \mathbf{Z}/m\mathbf{Z}$$

という条件を付けることも可能で、公開鍵は素体上の有理点、セキュリティレベルは $\mathbf{F}_{p^\ell}$ 上の Diffie-Hellman 問題と同等、という設計が可能になる。

2. 有理点の構造

E は supersingular ではないものとし、E の自己準同型環 $\mathrm{End}(E)$ の虚二次の整数環としての判別式を $-D$, 整数底を

$$\omega = \begin{cases} (1+\sqrt{-D})/2 & (-D \equiv 1 \bmod 4) \\ \sqrt{-D}/2 & (-D \equiv 0 \bmod 4) \end{cases}$$

とする。また $\mathbf{F}_q$ 上の Frobenius 写像を φ_q と表す。$E(\mathbf{F}_q)$ の群構造は次のとおりである：

[1]高知大学大学院理学研究科数理情報科学専攻
Department of Mathematics and Information Science, Kochi University
[2]高知大学理学部
Faculty of Science, Kochi University

2.1 定理 ([3])

$\varphi_q \in \mathrm{End}(E)$ を $\varphi_q = a + b\omega \quad (a, b \in \mathbf{Z})$ と表したとき $d = \gcd(a-1, b)$, $d' = \sharp E(\mathbf{F}_q)/d$ とおくと、

$$E(\mathbf{F}_q) \cong (\mathbf{Z}/d\mathbf{Z}) \times (\mathbf{Z}/d'\mathbf{Z}).$$

2.2 系

定理 **2.1** の記号のもと、

$$a - 1 \equiv b \equiv 0 \mod m$$

が成り立てば $E[m] \subseteq E(\mathbf{F}_q)$.

証明 $\varphi_q - 1 = m(a' + b'\omega)$ (a', $b' \in \mathbf{Z}$) とおけ、

$$\begin{aligned} E(\mathbf{F}_q) &= \mathrm{Ker}(\varphi_q - 1) \\ &= \mathrm{Ker}(m(a' + b'\omega)) \supseteq E[m]. \quad \square \end{aligned}$$

2.3 系

m は奇数とする。$\varphi_q = (U + V\sqrt{-D})/2 \ \ (U, V \in \mathbf{Z})$ と表したとき

$$U \equiv 2,\ V \equiv 0 \mod m$$

が成り立てば $E[m] \subseteq E(\mathbf{F}_q)$.

証明 $a = (U - V)/2$ または $U/2$, $b = V$ ゆえ。 $\square$

2.4 注

このとき

$$q = N_{\mathbf{Q}(\sqrt{-D})/\mathbf{Q}}(\varphi_q) = (U^2 + DV^2)/4,$$

$$\sharp E(\mathbf{F}_q) = 1 + q - U = \left(\frac{U}{2} - 1\right)^2 + \frac{D}{4}V^2$$

が成り立つ。

3. $E[m] \subseteq E(\mathbf{F}_p)$ を満たす CM 曲線

本節では素体 $\mathbf{F}_p$ 上の楕円曲線で $E[m] \subseteq E(\mathbf{F}_p)$ を満たすものを構成する。

3.1 従来の CM 曲線生成アルゴリズム

判別式 $-D$ の虚二次の整数環を $\mathrm{End}(E)$ にもつ素体 $\mathbf{F}_p$ 上の楕円曲線 E は、通常次のアルゴリズムによって生成される：

(1) 判別式 D を設定する。
(2) ランダムな素数 p を求める。
(3) $4p = u^2 + Dv^2$ の整数解 u, v を Cornacchia のアルゴリズムを用いて求める。整数解が無ければ (2) へ戻る。
(4) Hilbert 類多項式 $H_D(X)$ の根 $j \in \mathbf{F}_p$ を求める。根を持たなければ (2) へ戻る。
(5) j-不変量が j となる $E/\mathbf{F}_p$ を (同型の意味で) 全て求める。($j \neq 0, 1728$ ならツイストの関係にある 2 個。)
(6) $\sharp E(\mathbf{F}_p) = 1 + p \pm u$ である E を乱数点を用いて判定し、出力する。

3.2 群構造の条件

3.1 によって求まった $E/\mathbf{F}_p$ が

$$\sharp E(\mathbf{F}_p) = 1 + p - u$$

を満たすとする。このとき $\mathrm{End}(E)$ において

$$\varphi_p = (u + v\sqrt{-D})/2$$

となり、系 **2.3** より、m が奇数のとき

$$u \equiv 2,\ v \equiv 0 \bmod m \qquad \cdots \ (*)$$

が満たされれば $E[m] \subseteq E(\mathbf{F}_p)$ が成り立つ。従って **3.1** のステップ (3) の次に

条件 $(*)$ を満たさなければ (2) へ戻る

というステップを付加すれば我々の目的が叶うかのように見える。しかし m が 30 ビット程度でもこれには膨大な時間が掛かる。ランダムな p に由来する u, v にとって条件 $(*)$ が強過ぎるのが原因である。

3.3 改良アルゴリズム

改良のアイデアは単純である。始めから u, v を条件 $(*)$ のもとで与えれば良い。すなわち

(1) 判別式 D と、奇数 $m > 1$ を設定する。

(2) $u \equiv 2,\ v \equiv 0 \bmod m$ を満たす u, v を与える。(偶奇にも条件が付く。)

(3) $p = (u^2 + Dv^2)/4$ を素数判定し、素数でなければ (2) へ戻る。

(4) Hilbert 類多項式 $H_D(X)$ の根 $j \in \mathbf{F}_p$ を求める。根を持たなければ (2) へ戻る。

(5) j-不変量が j となる $E/\mathbf{F}_p$ を全て求める。

(6) $\sharp E(\mathbf{F}_p) = 1 + p - u$ である E を乱数点を用いて判定し、出力する。

3.4 計算量

このアルゴリズムの計算量は m の 2 倍程度のサイズの p に対する CM 曲線生成と同程度である。

3.5 数値例

D = 479 (類数 25)

m = 116636286176240004724910111162260075957264836412237861657711 3 (200 ビット)

p = 165207258384259011422434356545320889105041282309936686045736314226038371409481498674649662687391395267211962272835166059497 99

E : $y^2 = x^3 + Ax + B$

A = 125385083781134306472065033954349021943949707023663833033218396298834405208945772999030836961500682368324076815900382212635 44

B = 285209697260032005072319037877923849276193772457969933402334927905434796694700157744706704118699898231453971196551994552576 3

$\sharp E(\mathbf{F}_p) = m^2 \times 12144$

4. $E[m] \subseteq E(\mathbf{F}_{p^2})$ を満たす CM 曲線

アルゴリズム **3.3** における u, v についての合同条件を取り替えると次のような定理が成り立つ :

4.1 定理

$m > 1$ を奇数とする。**3.3** (2) の合同条件を

$$u \equiv -2,\ v \equiv 0 \bmod m$$

に置き換えたとき、得られた $E/\mathbf{F}_p$ について

$$E[m] \subseteq E(\mathbf{F}_{p^2}), \quad E[m] \cap E(\mathbf{F}_p) = \{\mathcal{O}\}$$

が成り立つ。

証明 系 **2.3** を $q = p^2$ として用いると、$\varphi_{p^2} = (\varphi_p)^2$ ゆえ $U = (u^2 - Dv^2)/2,\ V = uv.$ 従って

$$U \equiv (-2)^2/2 = 2,\ V \equiv 0 \mod m.$$

また

$$\begin{aligned} \sharp E(\mathbf{F}_p) &= \left(\frac{u}{2} - 1\right)^2 + \frac{D}{4}v^2 \\ &\equiv 4 \not\equiv 0 \mod m. \end{aligned}$$

□

4.2 数値例

D = 551 (類数 26)

m = 116079907419677564320628593647559342276369161101802984088829 3 (200 ビット)

p = 185625330632783157446385409198039983202182578932530574301306727432151341700197510094361359906973967465594678333649383800041 1

E : $y^2 = x^3 + Ax + B$

A = 107661921889934301175417821597870400469059753618512821391898548155809582376384247218370323198662097327654180155947793991860 18

B = 197990087647236299363001559984672017452674995625150569024442823789360203884991622848696736044178652724992616523537664024775 0

$\sharp E(\mathbf{F}_p) = 185625330632783157446385409198039998320218257893253057430130672766431115653955263873561854720209265201833300053725535197770 00 \equiv 4 \bmod m$

$$\sharp E(\mathbf{F}_{p^2}) = m^2 \times 255717455479722077698140539$$
$$711219901685932672073745411915748014803035504924888771512218811062560283742045554154012297288447952000$$

4.3 定理

m を D と互いに素な奇素数、$-D$ は mod m の平方剰余であるとし、$\alpha^2 \equiv -4/D \mod m$ を満たす $\alpha \in \mathbf{Z}$ を取る。**3.3** (2) の合同条件を

$$u \equiv 0,\ v \equiv \alpha \bmod m$$

に置き換えたとき、得られた $E/\mathbf{F}_p$ について

$$E[m] \subseteq E(\mathbf{F}_{p^2}), \quad E[m] \cap E(\mathbf{F}_p) \cong \mathbf{Z}/m\mathbf{Z}$$

が成り立つ。

証明 今度は

$$U \equiv -D\alpha^2/2 \equiv 2,\ V \equiv 0 \mod m.$$

となる。また

$$\begin{aligned}\sharp E(\mathbf{F}_p) &= \left(\frac{u}{2}-1\right)^2 + \frac{D}{4}v^2 \\ &\equiv 1 + \frac{D}{4}\left(-\frac{4}{D}\right) \equiv 0 \mod m\end{aligned}$$

ゆえ $E(\mathbf{F}_p) \supseteq \mathbf{Z}/m\mathbf{Z}$ であるが、定理 **2.1** より $E(\mathbf{F}_p) \not\supseteq E[m]$. □

4.4 注

この定理を用いると、Weil 対を用いた暗号システムにおいて、公開鍵は $\mathbf{F}_p$-有理点、セキュリティレベルは $\mathbf{F}_{p^2}$ 上の Diffie-Hellman 問題と同等、という設計が可能である。

4.5 数値例

D = 671 (類数 30)

m = 10144399409280990155176707943076206958293801820576532652958 21 (200 ビット)

p = 232217587330751562259318579250999947486239333559988312325523413458222429532412623729731928929835841837981126902783838586220607

E : $y^2 = x^3 + Ax + B$

A = 104338856446940240749709119681328859755067238538436843221127839874351855295269906563731698312482115282893488340647201912036722

B = 69559237631293493833139413120885906503378159025624562147418559916234570196846604375821132208321410188595658893764801274691148

$\sharp E(\mathbf{F}_p) = m \times 228912109984843911353009391953787856001305135652168896217025917240$

$\sharp E(\mathbf{F}_{p^2}) = m^2 \times 524007540977132755371703765469926388193104882541815090047622681547115711621387695383836348828593660099488587171312851733335743893440$

5. $E[m] \subseteq E(\mathbf{F}_{p^3})$ を満たす CM 曲線

3 次拡大についても **4** 節と同様の定理が作れる。

5.1 定理

m を $m \equiv 1 \mod 3$ を満たす奇素数とし、$\alpha^3 \equiv 1,\ \alpha \not\equiv 1 \mod m$ を満たす $\alpha \in \mathbf{Z}$ を取る。**3.3** (2) の合同条件を

$$u \equiv 2\alpha,\ v \equiv 0 \bmod m$$

に置き換えたとき、得られた $E/\mathbf{F}_p$ について

$$E[m] \subseteq E(\mathbf{F}_{p^3}), \quad E[m] \cap E(\mathbf{F}_p) = \{\mathcal{O}\}$$

が成り立つ。

証明 系 **2.3** を $q = p^3$ として用いる。$\varphi_{p^2} = (\varphi_p)^3$ ゆえ $U = (u^3 - 3Duv^2)/4,\ V = (3u^2v - Dv^3)/4$. 従って

$$U \equiv 2\alpha^3 = 2,\ V \equiv 0 \mod m.$$

であり

$$\begin{aligned}\sharp E(\mathbf{F}_p) &= \left(\frac{u}{2}-1\right)^2 + \frac{D}{4}v^2 \\ &\equiv (\alpha-1)^2 \not\equiv 0 \mod m.\end{aligned}$$ □

5.2 定理

$m \neq 19$ を $3D$ と互いに素な奇素数、$3D$ は mod m の平方剰余であるとし、$\alpha^2 \equiv 3/D \mod m$ を満たす $\alpha \in \mathbf{Z}$ を取る。**3.3** (2) の合同条件を

$$u \equiv -1,\ v \equiv \alpha \bmod m$$

に置き換えたとき、得られた $E/\mathbf{F}_p$ について

$$E[m] \subseteq E(\mathbf{F}_{p^3}), \quad E[m] \cap E(\mathbf{F}_p) = \{\mathcal{O}\}$$

が成り立つ。

証明は同様である。

6. $E[m] \subseteq E(\mathbf{F}_{p^\ell})$ を満たす CM 曲線

一般の拡大次数については

6.1 定理

m を D と互いに素な奇素数、$\ell > 1$ を $m-1$ の約数とし、mod m での 1 の原始 ℓ-乗根 $\beta \in \mathbf{Z}$ を取る。**3.3** (2) の合同条件を

$$u \equiv 2\beta,\ v \equiv 0 \bmod m$$

に置き換えたとき、得られた $E/\mathbf{F}_p$ について

$$E[m] \subseteq E(\mathbf{F}_{p^\ell}),$$
$$E[m] \cap E(\mathbf{F}_{p^f}) = \{\mathcal{O}\} \quad (1 \leq f < \ell)$$

が成り立つ。

証明 $\mathbf{F}_{p^f}$ に対する系 **2.3** の U, V を U_f, V_f と表すこととし、$\mathrm{End}(E)$ における共役を $\overline{\ }$ で表すと

$$U_f = (\varphi_p)^f + (\overline{\varphi_p})^f,$$
$$V_f = \frac{1}{\sqrt{-D}}\left((\varphi_p)^f - (\overline{\varphi_p})^f\right)$$

である。今の場合 $\varphi_p \equiv \overline{\varphi_p} \equiv \beta \bmod m$ ゆえ

$$U_f \equiv 2\beta^f,\ V_f \equiv 0 \mod m.$$

特に

$$U_\ell \equiv 2,\ V_\ell \equiv 0 \mod m.$$

また $1 \leq f < \ell$ のときは

$$\begin{aligned} \sharp E(\mathbf{F}_{p^f}) &\equiv \left(\frac{U_f}{2} - 1\right)^2 + \frac{D}{4}(V_f)^2 \\ &\equiv (\beta^f - 1)^2 \not\equiv 0 \mod m. \end{aligned}$$

($-D$ が mod m の平方剰余でない場合は合同式は二次体で考える。) □

6.2 定理

m を D と互いに素な奇素数、$-D$ は mod m の平方剰余であるとし、$\alpha^2 \equiv -D \mod m$ を満たす $\alpha \in \mathbf{Z}$ を取る。また $\ell > 1$ を $m-1$ の約数とし、mod m での 1 の原始 ℓ-乗根 $\beta \in \mathbf{Z}$ を取る。**3.3** (2) の合同条件を

$$u \equiv 1 + \beta,\ v \equiv (1-\beta)/\alpha \bmod m$$

に置き換えたとき、得られた $E/\mathbf{F}_p$ について

$$E[m] \subseteq E(\mathbf{F}_{p^\ell}),$$
$$E[m] \cap E(\mathbf{F}_{p^f}) \cong \mathbf{Z}/m\mathbf{Z} \quad (1 \leq f < \ell)$$

が成り立つ。

証明 今度は $\varphi_p \equiv 1,\ \overline{\varphi_p} \equiv \beta \bmod m$ となるように u, v を設定してある。従って

$$U_f = 1 + \beta^f,\ V_f = \frac{1}{\alpha}\left(1 - \beta^f\right) \mod m.$$

特に

$$U_\ell \equiv 2,\ V_\ell \equiv 0 \mod m.$$

また $1 \leq f < \ell$ のときは

$$\begin{aligned} \sharp E(\mathbf{F}_p) &= 1 + p - u \\ &= 1 + (\varphi_p\overline{\varphi_p}) - (\varphi_p + \overline{\varphi_p}) \\ &\equiv 1 + (1 \times \beta) - (1 + \beta) \\ &\equiv 0 \qquad \bmod m \end{aligned}$$

より $E(\mathbf{F}_{p^f}) \supseteq E(\mathbf{F}_p) \supseteq \mathbf{Z}/m\mathbf{Z}$ であるが、定理 **2.1** より $E(\mathbf{F}_{p^f}) \not\supseteq E[m]$. □

6.3 注

この場合も定理 **4.3** と同様、公開鍵は $\mathbf{F}_p$-有理点、セキュリティレベルは $\mathbf{F}_{p^\ell}$ 上の Diffie-Hellman 問題と同等、という設計が可能である。(ℓ を先に決めて、m は $m \equiv 1 \bmod \ell$ を満たすものを取る。)

なお、定理 **6.1** は定理 **4.1**, **5.1** の、定理 **6.2** は定理 **4.3** の拡張になっている。

6.4 数値例

$$\begin{aligned} D &= 951 \text{ (類数 26)} \\ m &= 1153117463639648382753578275381 \\ &\quad (100 \text{ ビット}) \end{aligned}$$

$$
\begin{aligned}
\ell &= 30 \\
p &= 542825042183572124183193359026128546870861187322080105133410406407 \\
E &: y^2 = x^3 + Ax + B \\
A &= 378466830468546341357514386666020069481881920115936524818257645 89 \\
B &= 252311220312364227571676257777346712987921280077291016545505097 26 \\
\sharp E(\mathbf{F}_p) &= m \times 4707456606113859743748026879620840
\end{aligned}
$$

7. 拡大体上の CM 曲線

拡大体上の CM 曲線については次のようにアルゴリズムをアレンジする。

7.1 アルゴリズム

(1) 判別式 D と奇数 $m > 1$、拡大次数 k を設定する。

(2) mod m での適切な合同条件を満たす u, v を与える。

(3) $p = (u^2 + Dv^2)/4$ を素数判定し、素数でなければ (2) へ戻る。

(4) $\varphi_p = (u+v\sqrt{-D})/2$, $U_k = (\varphi_p)^k + (\overline{\varphi_p})^k$ とおく。

(5) Hilbert 類多項式 $H_D(X)$ の根 $j \in \mathbf{F}_{p^k}$ を求める。根を持たなければ (2) へ戻る。

(6) j-不変量が j となる $E/\mathbf{F}_{p^k}$ を全て求める。

(7) $\sharp E(\mathbf{F}_{p^k}) = 1 + p^k - U_k$ である E を乱数点を用いて判定し、出力する。

7.2 定理

m, ℓ, α, β は定理 **6.2** のとおりとし、更に k は ℓ の約数であるとする。$h = \ell/k$ とおいて、**7.1** (2) の合同条件を

$$u \equiv \beta^h + \beta,\ v \equiv (\beta^h - \beta)/\alpha \bmod m$$

としたとき、得られた $E/\mathbf{F}_{p^k}$ について

$$E[m] \subseteq E(\mathbf{F}_{p^\ell}),$$

$$E[m] \cap E(\mathbf{F}_{p^{kf}}) \cong \mathbf{Z}/m\mathbf{Z} \quad (1 \le f < h)$$

が成り立つ。

証明 $\varphi_p \equiv \beta^h$, $\overline{\varphi_p} \equiv \beta \bmod m$ ゆえ

$$U_f = \beta^{hf} + \beta^f,\ V_f = \frac{1}{\alpha}\left(\beta^{hf} - \beta^f\right) \bmod m.$$

特に

$$U_\ell \equiv 2,\ V_\ell \equiv 0 \bmod m.$$

また $1 \le f < h$ のときは

$$
\begin{aligned}
\sharp E(\mathbf{F}_{p^k}) &= 1 + p^k - U_k \\
&= 1 + (\varphi_p\overline{\varphi_p})^k - ((\varphi_p)^k + (\overline{\varphi_p})^k) \\
&\equiv (1-\beta^\ell)(1-\beta^k) \\
&\equiv 0 \qquad \bmod m
\end{aligned}
$$

より $E(\mathbf{F}_{p^{kf}}) \supseteq E(\mathbf{F}_{p^k}) \supseteq \mathbf{Z}/m\mathbf{Z}$ であるが、定理 **2.1** より $E(\mathbf{F}_{p^{kf}}) \not\supseteq E[m]$. □

7.3 注

$k > 1$ のとき φ_p には Frobenius 写像としての意味は無いが、φ_{p^ℓ} を制御するための道具として働くのである。

文　献

[1] I.Blake, K.Murty and G.Xu, Refinements of Miller's algorithm for computing Weil/Tate pairing, IACR Cryptology ePrint Archive, Report 2004/065.

[2] I.Blake, G.Seroussi and N.Smart, Elliptic Curves in Cryptography, LMS Lecture Note Series, 265, Cambridge University Press, 1999.

[3] N.Ishii, Trace of Frobenius endomorphism of an elliptic curve with complex multiplication, Bulletin of Australian Math. Soc. 70, 125-142, 2004.

[4] A.J.Menezes, T.Okamoto and S.A.Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, Proc. of STOC, 80-89, 1991.

[5] F.Morain and J.-L.Nicolas, On Cornacchia's algorithm for solving the diophantine equation $u^2 + dv^2 = m$, Courbes elliptiques et tests de primalite, Universite de Lyon I, 1990.

[6] R.Schoof, Nonsingular plane cubic finite fields, J. of Combinatorial Theory, Ser. A, 46, 183-211, 1987.

[7] F. Zhang, R. Safavii-Naine and W. Susilo, Efficient verifiably encrypted signature and partially blind signature from bilinear pairings, INDOCRYPT 2003, LNCS 2904, 191-204.

[8] 岡本龍明, 太田和夫編, 暗号・ゼロ知識証明・数論, 共立出版, 1995.