楕円暗号の数理

小山　謙二[†]　　宮地　充子[††]　　内山　成憲[†††]

Mathematics of Elliptic Curve Cryptography

Kenji KOYAMA[†], Atsuko MIYAJI[††], and Shigenori UCHIYAMA[†††]

あらまし　楕円暗号の数理について，その主要なトピックスについて解説する．

キーワード　楕円曲線，楕円曲線暗号，楕円 RSA 暗号，楕円離散対数問題，素因数分解問題

1. まえがき

本論文では楕円暗号の数理について，その主要なトピックスについて解説する．

2. 楕円曲線上の離散対数問題に基づく暗号

2.1 はじめに

インターネットの普及に伴い，公開鍵暗号の実用化が進み始めた．大型コンピュータでの利用を前提としていた公開鍵暗号が，パーソナルコンピュータや携帯端末で，署名・認証技術あるいは鍵共有技術として要求されるようになってきた．こうして，これまで公開鍵暗号の主流であった RSA 暗号に代わって，楕円曲線上の離散対数問題に基づく暗号，すなわち楕円曲線暗号が脚光を浴びるようになった．楕円曲線暗号は，RSA 暗号に比べ，同じ安全性で鍵サイズが小さいという特徴をもつからだ．また実用化を目指し，高速化の研究が活発になってきた [31], [32], [46], [50], [54].

本論文では，楕円曲線暗号の応用アルゴリズムとして，IEEEP1363 や ISO/IEC 等で取り上げられている ECDSA 及び ECDH を紹介する．また，最近のトピックスである楕円曲線の高速演算アルゴリズムを紹介する．最後に標準化状況を簡単に述べる．

† NTT コミュニケーション科学基礎研究所，京都府
NTT Communication Science Labs, 2–4 Hikaridai, Seika-cho, Soraku-gun, Kyoto-fu, 619–0237 Japan
†† 北陸先端科学技術大学院大学，石川県
Japan Advanced Institute of Science and Technology, 1–1 Asahidai, Tatsunokuchi-cho, Noumi-gun, Ishikawa-ken, 923–1292 Japan
††† NTT 情報流通プラットフォーム研究所，横須賀市
NTT Laboratories, 1–1 Hikarinooka, Yokosuka-shi, 239–0847 Japan

2.2 楕円曲線

まず，楕円曲線について簡単に述べる．楕円曲線とは，$a, b \in K$（体）に対して，

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

で定まる曲線である．ここで $4a^3 + 27b^2 \neq 0$ とし，K の標数は 5 以上とする．標数が 2 または 3 の場合の楕円曲線の標準形については, [47] を参照されたい．楕円曲線は（1）を満たす点の集合であるが，$x \to \infty$ のとき $y \to \infty$ と考えて，無限遠点 $\mathcal{O} = (\infty, \infty)$ も E の点と考える．特に，楕円曲線の K-有理点の集合を，

$$E(K) = \{(x, y) \in K^2 | y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

とする．楕円曲線のパラメータ a, b を含む体 K を楕円曲線の定義体と呼ぶ．楕円曲線には $\mathcal{O}$ が零元になるような加法が定義できる．加算公式については **2.4** で詳しく述べる．

2.3 楕円曲線暗号の応用アルゴリズム

本節では，楕円曲線暗号の応用アルゴリズムとして，署名方式の一つである ECDSA そして鍵共有法の一つである ECDH を紹介する．

2.3.1 初期設定

有限体 $\mathbb{F}_q$ 上の楕円曲線 $E/\mathbb{F}_q$，$E(\mathbb{F}_q)$ の点 G をベースポイントとする．ここで G の位数 n は 160 bits 程度の素数とする（n の大きさは, [36], [37] の攻撃に対する安全性に関与する）．

ユーザ A は正整数 d_A を選びこれを秘密鍵として保持し，

$$P_A = d_A G$$

を計算し，$E(\mathbb{F}_q)$ の元 P_A を公開鍵として公開ファイルに登録する．同様に B の秘密鍵を d_B，公開鍵を P_B とする．

2.3.2 ECDSA

送信者 A が平文 m に署名をして，受信者 B に送信する場合を考える．ハッシュ関数 H は，任意長の平文 m を $\boldsymbol{Z}_n^* = \{\mathbf{1}, \cdots, \boldsymbol{n-1}\}$ に圧縮する関数とする．

署名生成：送信者 A は

1. $e = H(m)$ を計算する．
2. 乱数 $k \in \boldsymbol{Z}_n^*$ を選び，$R_1 = kG$ を計算する．
3. $r_1' = x(R_1) \pmod q$ を計算する．ここで $x(R_1)$ は，R_1 の x-座標である．
4. $sk \equiv e + r_1' x_A \pmod q$ より s を求める．
5. (m, r_1', s) を m の署名文として送る．

署名検証：受信者 B は，

1. $e = H(m)$ を計算する．
2. A の公開鍵 P_A を用いて $r_1' = x(\frac{h}{s}G + \frac{r_1'}{s}P_A) \pmod q$ を検証する．

2.3.3 ECDH（相互通信なし）

A と B が相互通信なしに鍵を共有する場合を考える．

[鍵共有]　A は公開ファイルから B の公開鍵 P_B を入手し，

$$K_{A,B} = d_A P_B = d_A d_B G$$

を計算する．同様に B は公開ファイルから A の公開鍵 P_A を入手し，

$$K_{B,A} = d_B P_A = d_B d_A G$$

を計算する．A と B は $E(\mathbb{F}_q)$ の元 $K_{A,B} = K_{B,A}$ を鍵として共有する．

2.4 楕円曲線の演算アルゴリズム

2.3 からわかるように，楕円曲線暗号の実行時間は楕円曲線のべき演算アルゴリズムに支配される．本章では，楕円曲線のべき演算アルゴリズムについて述べる．

楕円曲線のべき演算アルゴリズムは，図 1 のように三つのレイヤ，定義体上の演算，座標系，加算連鎖からなる．ここでは，第 3 レイヤの加算連鎖と第 2 レイヤの座標系について簡単に述べる．

2.4.1 加算連鎖

本項で述べる加算連鎖とは，楕円曲線 $E/\mathbb{F}_q$ のべき演算 $kP (P \in E(\mathbb{F}_q))$ の計算方法である．べき演算の手法は，G がベースポイントのような固定値の場合と公開鍵のような任意値の場合とで異なる．後者の任意

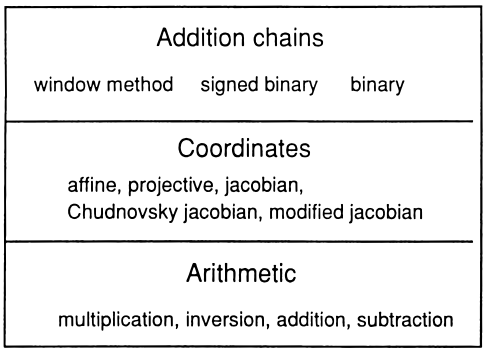

図 1　楕円曲線冪演算の構成レイヤ
Fig. 1　Layer of Elliptic curve exponentiations.

値の場合，符号付 2 進法と window 法を組み合わせるのが一般的である [21], [31], [32], [34]．ここでは，この 2 手法について簡単に述べる．

［符号付き 2 進法］

符号付き 2 進法とは，k を $\{0, \pm 1\}$ の 3 情報で表すことにより，0 以外（すなわち ± 1）の立つビット数を減らすというアイデアである．

［例 1］　$k = (10\text{進})15 = (2\text{進})1111$ の符号付き 2 進法を考える．通常の 2 進法では，$15G$ の計算に，$15G = 2(2(2G + G) + G) + G$ より 3 回の 2 倍算と 3 回の加算が必要である．k を符号付き 2 進法で表すと，

$$k = (10\text{進})15 = 16 - 1 = (\text{符号付き } 2\text{ 進})1000\overline{1}$$

なる．このとき，$15G$ は

$$15G = 2^4 G - G$$

より，4 回の 2 倍算と 1 回の減算により求められる．このようにして，総計算回数を減らすことができる．符号付き 2 進法の表し方は一意的でないので，いくつかの方法が提案されている [21], [31], [34].

［window 法］[15]

window 法は window の幅を w とするとき，kP の計算を以下の 2 ステップで行う．

（1）　$P_l = lP (l \in \{1, 3, \cdots, 2^w - 1\})$ を計算する（予備計算テーブル作成）．

（2）　kP を 2 倍算と（1）の予備計算テーブル $\{P_l\}$ との加算を繰り返すことにより求める．

［例 2］　$k = (2\text{進})1011111$，$w = 4$ の場合を考える．

（1）　$P_l = lP (l \in \{1, 3, \cdots, 15\})$ を求める．

（2）　$kP = 1011\ 111\, P = 2^3 P_{11} + P_7$ として計算

する．ここで，1011 や 111 を window と呼ぶ．

window の幅は，総計算量（予備計算テーブル作成の計算量も含む）が最小になるように設定する．

楕円曲線のべき演算は，符号付き 2 進法と window 法を組み合わせる．この組合せ方には，以下の二つの案が提案されている．

（1） k を符号付 2 進法で表し，次に window に分割する方法 [21].

（2） window の幅 w により，符号付 2 進法を決定する方法 [32].

計算量は後者の方が少なくなる．

2.4.2 座 標 系

楕円曲線の表し方には，大きくアファイン座標系（1）と射影座標系がある．アファイン座標系では，加算及び 2 倍算が定義体上の除算を必要とする．除算は乗算に比べ時間がかかるので，除算演算が不要な射影座標系を利用する場合が多い．

射影座標系には，$(x, y) = (X/Z, Y/Z)$ の変換を行う座標系（projective 座標系）と $(x, y) = (X/Z^2, Y/Z^3)$ の変換を行う座標系（jacobian 座標系）がある [6], [31]. 二つの座標系を比べると，加算は projective 座標系が早く，2 倍算は jacobian 座標系が早い．楕円曲線のべき演算は加算より 2 倍算を多く要求するので，jacobian 座標系がべき演算には適している．また jacobian 座標系は，保持するパラメータを変えると，更に 2 倍算の計算量を減らすことができる．ここでは jacobian 座標系及び 2 倍算の計算量を減らした modified jacobian 座標系を紹介する．

jacobian 座標系の楕円曲線は，（1）を $(x, y) = (X/Z^2, Y/Z^3)$ とおくことにより与えられる．

$$E_J : Y^2 = X^3 + aXZ^4 + bZ^6. \qquad (2)$$

加算公式は以下のようになる．$P = (X_1, Y_1, Z_1)$, $Q = (X_2, Y_2, Z_2)$, $P + Q = R = (X_3, Y_3, Z_3)$ とおく．

- 加算公式 $(P \neq \pm Q)$

$$\begin{aligned} X_3 &= -H^3 - 2U_1H^2 + r^2, \\ Y_3 &= -S_1H^3 + r(U_1H^2 - X_3), \\ Z_3 &= Z_1Z_2H, \end{aligned}$$

ここで $U_1 = X_1Z_2^2, U_2 = X_2Z_1^2, S_1 = Y_1Z_2^3, S_2 = Y_2Z_1^3, H = U_2 - U_1, r = S_2 - S_1$ である．

- 2 倍算公式（$R = 2P$）

$$X_3 = T, Y_3 = -8{Y_1}^4 + m(s - T), Z_3 = 2Y_1Z_1,$$

ここで $s = 4X_1Y_1^2, m = 3X_1^2 + aZ_1^4, T = -2s + m^2$ である．

加算及び 2 倍算の計算量 $t(\mathcal{J}, \mathcal{J})$, $t(2\mathcal{J})$ は，$t(\mathcal{J}, \mathcal{J}) = 12M + 4S$, $t(2\mathcal{J}) = 4M + 6S$ となる．ここで，M 及び S はそれぞれ定義体上の乗算と 2 乗算の計算量を表す．

jacobian 座標系を (X, Y, Z, aZ^4) とする modified jacobian 座標系では，加算及び 2 倍算の計算量 $t(\mathcal{J}^m, \mathcal{J}^m)$, $t(2\mathcal{J}^m)$ は，$t(\mathcal{J}^m, \mathcal{J}^m) = 13M + 6S$, $t(2\mathcal{J}^m) = 4M + 4S$ となる．加算では aZ_3^4 を求める余分な計算量が必要になるが，2 倍算では

$$aZ_3^4 = 2^4(Y_1^4)(aZ_1^4)$$

となることから，aZ^4 をもつことで計算量が削減できる．楕円曲線のべき演算の総計算量は，2 倍算の計算量が少ないので，modified jacobian 座標系を用いた方が jacobian 座標系より小さくなる．更に，いくつかの座標系を組み合わせる混合座標系も提案されている [32].

2.5 楕円曲線暗号の標準化

IEEE（Institute of Electrical and Electronics Engineers）はアメリカの学会であるが，アメリカの国内標準を規定する ANSI（American National Standards Institute）から信任されたアメリカの国内標準化組織の一つでもある．この IEEE の P1363 グループで，'94 年から楕円曲線暗号を含む公開鍵暗号の標準化が始まっている．また ANSI ASC A9.62, A9.63 においても，本節でも述べた楕円曲線を用いた署名方式 ECDSA や鍵共有方式 ECDH の標準化が進められている．更に'98 年から，ISO/IEC JTC 1/SC27（ISO は International Organization for Standardization［国際標準化機構］，IEC は International Electrotechnical Commision［国際電気標準会議］，JTC1 は ISO と IEC が共同で設置した情報処理関連技術の国際規格の作成委員会，SC27 はその下部組織）において楕円曲線暗号の標準化が始まった．楕円曲線暗号全般，署名方式，鍵共有方式の標準化が N2034, N2056, N2057 において議論されている．

3. 楕円暗号への攻撃法と安全な曲線の選択

3.1 はじめに

1976 年の Diffie と Hellman による公開鍵暗号の提

案以来，数多くの暗号方式が提案され，その中でも，最近特に注目されているものに楕円曲線を利用した楕円暗号（ここでは，楕円 ElGamal 暗号をこう呼ぶことにする）と呼ばれるものがある．ここでは，現在までに提案されている楕円暗号への攻撃法と，それらを考慮した上で，安全な楕円曲線の生成方法について述べる．ただし，紙数の関係上，楕円暗号への攻撃法について詳しく記述し，安全な楕円曲線の生成方法については最小限の記述にとどめた．また，数学用語については，本特集号の桂氏の解説論文及び標準的な教科書 [27], [47] を参照して頂きたい．

3.2 一般的な攻撃法（baby-step-giant-step 等）

楕円暗号の安全性は，有限体上の楕円曲線の有理点のなす群における離散対数問題（ECDLP）の困難さに基づく．したがって，ECDLP の解法アルゴリズムの研究は，RSA に対する素因数分解アルゴリズムの研究と同じ意味で重要となる．ECDLP の解法アルゴリズムは，いくつかの特殊な性質をもつ楕円曲線については，効果的なアルゴリズムが発見されている．しかし，それらを除く一般の楕円曲線上の ECDLP に対しては，任意の有限群上の離散対数問題に対して適用可能なアルゴリズムである Pohlig-Hellman-Silver アルゴリズム [36]，Shanks による BSGS（baby-step-giant-step）アルゴリズム [4] や，Pollard による ρ 法 [37] と呼ばれるものなどが最も有効である．最近，ρ 法の高速化 [51], [53] もいくつか提案されているが，これらはどれも，入力サイズの指数時間のアルゴリズムである．一方，有限体の乗法群上の離散対数問題（DLP）や，素因数分解問題に対しては，実行時間が，その入力サイズの準指数時間となる，指数計算法（Index-Calculus method）と呼ばれるアルゴリズムが存在することが知られている [45]．しかし，一般の楕円曲線上の ECDLP に対して，指数計算法が適用できるかどうかは，現在のところ未解決である [29], [48].

このように，一般の楕円曲線上の ECDLP に対しては，準指数時間アルゴリズムが発見されておらず，RSA 等の素因数分解問題に基づく公開鍵暗号などと比較して，その安全性のパラメータとなる鍵のサイズが短くできる利点がある．このとにより，IC カードのようなメモリサイズや処理能力の限定された装置上にも適した方式とも考えられ，昨今注目され，実用化も進んでいる．

次に，現在までに知られている，特殊な性質を満たす楕円曲線に基づく楕円暗号に対する攻撃法について解説する．これらは，大きく分けると 2 種類あって，一つは，楕円曲線の定義体の拡大体の乗法群への埋込みによるもの，もう一つは楕円曲線に付随した Fermat 商等を用いる方法である．

前者で最初に発見されたものは，1991 年の Menezes-岡本-Vanstone による，Weil 対を用いて，その楕円曲線の定義体の拡大体の乗法群上の離散対数問題に帰着させるアルゴリズムで，いわゆる，MOV 帰着と呼ばれる．この攻撃法は，その楕円曲線上の離散対数問題を埋め込む拡大体の拡大次数が小さい場合に有効であることが知られている．特に，超特異（supersingular）と呼ばれるクラスの楕円曲線に対して有効であることが [28] で示されている．その後，Frey-Rück によって，Tate 対と呼ばれるものを用いて，楕円曲線に限らず一般の曲線の Jacobi 多様体上の離散対数問題を，その定義体の拡大体の乗法群上の離散対数問題に帰着させる方法が提案されている [10]．これをここでは，FR 帰着と呼ぶことにする．これらの手法は，ECDLP に対する一つの指数計算法の実現例ともいえる．また，Balasubramanian-Koblitz [3] は，有限素体 $\mathbb{F}_p$ 上の楕円曲線で $\#E(\mathbb{F}_p)$ が素数となるものを任意に選んだとき，MOV 帰着が準指数時間アルゴリズムとなる確率は無視できるほど小さいことを示している．更に, [52] では，MOV 帰着と FR 帰着の比較によって，トレース 2 の楕円曲線上の ECDLP に対して，MOV 帰着は指数時間アルゴリズム，FR 帰着は準指数時間アルゴリズムとなり，それ以外では準指数時間アルゴリズムとなる条件は等価であることが示されている．更に，トレースが 2 の場合に詳しい帰着のアルゴリズムが与えられているが，これは, [10] を単純に実現したもの（例えば, [11]）とは異なっている．

次に，後者のアルゴリズムは，Semaev [44]，Smart [49]，佐藤–荒木 [41] によってそれぞれ独立に提案され，anomalous と呼ばれる楕円曲線に対して有効であることが知られている．anomalous 楕円曲線とは，有限素体 $\mathbb{F}_p$ 上定義された楕円曲線 E が，$\#E(\mathbb{F}_p) = p$ となるものをいう．ここでは，このアルゴリズムを SSSA アルゴリズムと呼ぶことにする．Semaev，Rück の手法は代数幾何学的であり，Smart，佐藤–荒木の手法は代数的整数論的であるが，これらのアルゴリズムが提案されるまで，離散対数問題は，概して “難しい問題 ” であろうと思われていたが，驚くべきことにこれらのアルゴリズムは多項式時間アルゴリズムである．また，Semaev の結果は，Rück [39] によって，一般の曲線

の Jacobi 多様体上の離散対数問題に対して一般化もされている．

以下で，上記の攻撃法について解説するが，その前に，若干の言葉の準備と ECDLP の定義を与えておく．

［ECDLP の定義］

E を有限体 $\mathbb{F}_q$ 上定義された楕円曲線，位数 l の点 $P \in E(\mathbb{F}_q)$ と，点 $Q \in \langle P \rangle$ が与えられたとき，$Q = [m](P)$ なる整数 m $(0 \leqq m < l)$ を求めよ，という問題を ECDLP とする．ただし，Pohlig-Hellman-Silver アルゴリズムなどが効率的に適用できない場合を考えれば十分なので，ここでは l は十分大きな素数（l と q のサイズは，ほとんど同じ）としておく．

［Tate 対］

E を有限体 $\mathbb{F}_q$ 上定義された楕円曲線，n は $\mathbb{F}_q$ の標数と互いに素な自然数とし，更に，$\mathbf{F}_{q^k}$ が 1 の原始 n 乗根を含む最小の拡大体とする．このとき，$E[n] \cap E(\mathbb{F}_{q^k}) \times E(\mathbb{F}_{q^k})/nE(\mathbb{F}_{q^k})$ から μ_n（1 の n 乗根全体のなす群）$(\subset \mathbb{F}_{q^k})$ への写像 $\langle\ ,\ \rangle_n$ で，双線形性，非退化性などをもつものが存在する．

この写像 $\langle\ ,\ \rangle_n$ を，Tate 対と呼ぶ(注1)．

3.3 Weil 対，Tate 対による乗法群への帰着

E を有限体 $\mathbb{F}_q$ 上定義された楕円曲線，素数位数 l の点 $P \in E(\mathbb{F}_q)$ と，点 $Q \in \langle P \rangle$ が与えられているものとする．

このとき，l が $\mathbb{F}_q$ の標数 p と異なるとき，Weil 対 e_l（Weil 対については [27] を参照）を用いて，$\langle P \rangle$ は，$\mathbb{F}_q$ のある拡大体の乗法群に埋め込まれることが知られている．すなわち，

［定理 3.1］[28]

$$f : \langle P \rangle \ni R \mapsto e_l(R, S) \in \mu_l \subset \mathbb{F}_{q^k}^{\times}$$

なる同型写像が存在する．ただし，$S \in E[l]$ は $e_l(P, S) = \zeta_l$（1 のある原始 l 乗根）を満たす．

この埋込みを用いて ECDLP を DLP に帰着させて解くアルゴリズムが MOV 帰着と呼ばれる．これについての詳しいアルゴリズムについては，[27] を参照．この Weil 対を計算するためには，$E[l] \subset E(\mathbb{F}_{q^k})$ となる拡大次数 k を求める必要がある．E が超特異楕円曲線の場合は，一般に $k \leqq 6$ であることが証明でき，すなわち，この場合には，$\mathbb{F}_{q^k}$ 上の離散対数問題に帰着させたとき，実行時間が，入力サイズ $|q|$ の準指数時間アルゴリズムとなって効果的となる．現在までに知られている有限体の乗法群の離散対数問題の解法アルゴリズムを使えば，$k < \log q$ であれば，$|q|$ の準指数時間アルゴリズムとなることが証明できる [52]．ここで，$E[l] \subset E(\mathbb{F}_{q^k})$ ならば $q^k \equiv 1 \pmod{l}$ であることに注意しておく．

次に，Frey-Rück による Tate 対を用いた場合も，MOV 帰着と同様にして次を得る．

［定理 3.2］[10] 各 $R \in \langle P \rangle$ に対して，ある $S_R \in E(\mathbb{F}_{q^k})$ が存在し

$$g : \langle P \rangle \ni R \mapsto \langle R, \overline{S_R} \rangle_l \in \mathbb{F}_{q^k}^{\times}/(\mathbb{F}_{q^k}^{\times})^l$$

なる同型写像が得られる．

ECDLP から DLP への変換の手間の計算量だけに着目すれば，Tate 対を用いた方が Weil 対を用いるよりも，2 倍程度高速であることが [40] で注意されている．

3.4 SSSA アルゴリズム

ここでは，anomalous 楕円曲線を用いた楕円暗号への攻撃法である，SSSA アルゴリズムについて簡単に解説するが，[42] に，非常にわかりやすい解説があるので，ここでは，概略のみを記す（詳しくは [1], [39], [41], [44], [49] を参照）．

[41], [49] で用いられている手法を簡単に述べると以下のようになる：$\tilde{E}$ を anomalous 楕円曲線，すなわち，$\tilde{E}$ は素体 $\mathbb{F}_p$ 上定義された楕円曲線で，$\#\tilde{E}(\mathbb{F}_p) = p$ となるものとする．p 進数体と呼ばれる体 $\mathbf{Q}_p$ 上に，anomalous 楕円曲線 $\tilde{E}$ をもち上げたものを E とする．このとき，E に付随した形式群の対数関数を用いて，$\mathbb{Z}/p\mathbb{Z}$ への同型写像 λ_E を構成し，この対数関数 λ_E を用いて $\tilde{E}$ 上の ECDLP を解く手法がとられている．

また，このアルゴリズムは，E が素体上定義されていない場合，すなわち，$\mathbb{F}_{p^r}$ 上定義されている場合でも，$E(\mathbb{F}_{p^r})$ の p-part に対して有効であることが [41] で注意されている．

3.5 安全な楕円曲線の選択

ここでは，楕円暗号に安全な楕円曲線の生成方法について簡単に述べる．上で見たように，現在のところは，楕円曲線の有理点の位数のみにその安全性が依存していると考えられるので，上で見た攻撃を避けるために，いかにして有理点の位数をコントロールして楕円曲線を生成するかが問題となる．

楕円曲線の生成方法は大きく虚数乗法に基づく方法，

(注1)：[10] では，一般の曲線上のものが定義されているが，本論文では，楕円曲線の場合のみ定義しておく．

Schoof-Atkin-Elkies に基づく方法，Weil 予想に基づく方法の 3 種類に分類される．

虚数乗法に基づく方法（CM 法）とは，代数体上定義された楕円曲線で虚数乗法をもつものを用いて，有限体上の楕円曲線のパラメータを生成する方法である [5], [30], [33].

次に，Weil 予想に基づく方法であるが，これは，比較的サイズの小さな有限体上定義された楕円曲線を選び，その拡大体有理点の位数を Weil 予想を用いて求めるというものである [16].

最後に，Schoof-Atkin-Elkies に基づく方法であるが，これは，ランダムに楕円曲線を選び，その有理点の個数を数える SEA アルゴリズムを使う方法である．オリジナルの Schoof [43] の方法は，当初あまり実用的ではないと考えられていたが，Elkies [9]，Atkin [2] らによる理論的な改良と最近の高速実装の研究の進展 [7], [14], [26] により，現在では，十分実用的だと考えられる．

これらを比較すれば，虚数乗法に基づく方法や Weil 予想に基づく方法は，SEA アルゴリズムを用いたものと比べれば，ある意味で，制限された楕円曲線しか生成できないが，高速である．

3.6 まとめ

楕円暗号への攻撃法と安全なパラメータ生成について述べたが，これからの最も大きな課題はその安全性についての研究であると思われる．安全性についての研究が活発になったのは，1990 年代になってからであり，今後の研究が期待される．例えば，有限体上の離散対数問題に対して有効な指数計算法が, [29], [48] の意味では適用できないとしても，楕円離散対数問題に対していかなる方法を用いても使えないかどうかを明らかにすることは大きな問題であると思われる．

4. RSA 型楕円暗号方式

4.1 はじめに

楕円曲線（特異でない 3 次曲線）又は特異な 3 次曲線上で構成した 4 種の RSA 型暗号方式を紹介する．楕円曲線上の方式（方式 1 と方式 2）は，原理的に世界で初めて明らかにしたものである．特異な 3 次曲線上の方式（特に方式 4）は，RSA 暗号と同等の安全性を保ちながら，復号化速度が RSA 暗号の 2 倍以上となっている．

ここで，3 次曲線とは，$f(x,y)$ の次数が 3 であるような代数方程式 $f(x,y)=0$ の解の集合である． 中でも特異点（$\partial f/\partial x = 0$ かつ $\partial f/\partial y = 0$ なる点）のない 3 次曲線は楕円曲線と呼ばれる．

本論文では，まず楕円曲線及び特異な 3 次曲線の新たな応用として，素因数分解問題に基づく公開鍵暗号について述べる．本章では，

$$y^2 \equiv x^3 + ax + b \pmod{p}$$

なる方程式に基づく楕円曲線と

$$y^2 + uxy \equiv x^3 + vx^2 \pmod{p}$$

なる方程式に基づく特異な 3 次曲線のみを扱うので，楕円曲線を $E_p(a,b)$，特異な 3 次曲線を $S_p(u,v)$ で表す．

一方，法が合成数 n である楕円曲線や特異な 3 次曲線では加算が定義できない場合もあるが，ここでは単に上の定義で素数 p を合成数 n に置き換えたものとする．

4.2 楕円曲線上の RSA 型暗号方式

楕円曲線上の RSA 型暗号方式は楕円曲線が超特異か否かによって方式 1 [20] と方式 2 [22] に分類される．各々の構成法と留意点について述べる．

4.2.1 超特異な楕円曲線上の RSA 型暗号方式：方式 1

［鍵生成］ $p \equiv q \equiv 2 \pmod 3$ を満たす二つの素数 p,q $(\geqq 5)$ を選び，その積を n とする．また $\ell_n = \mathrm{lcm}(p+1, q+1)$ とおく．ここで，$\mathrm{lcm}(x,y)$ は x と y の最小公倍数を表す．整数 e を $\gcd(e,\ell_n)=1$ を満たすように選び，$d_p = e^{-1} \bmod (p+1)$，$d_q = e^{-1} \bmod (q+1)$ とする．公開鍵（暗号化鍵）は n と e，秘密鍵（復号化鍵）は p,q,d_p,d_q である． □

素数 p $(\equiv 2 \pmod 3)$ と任意の整数 b $(\neq 0)$ に対して，楕円曲線 $E_p(0,b)$ は超特異な楕円曲線である．

［暗号化］ 平文を $M=(m_x,m_y)$ $(0 \leqq m_x, m_y \leqq n-1)$ とする．平文 $M \in E_n(0,b)$ を楕円曲線 $E_n(0,b)$ 上で e 倍した点 $C=(c_x,c_y) \in E_n(0,b)$ が暗号文である． □

平文 M が一様に分布していると仮定すると，楕円曲線 $E_n(0,b)$ 上で加算が定義できない確率は $O(1/p+1/q-1/n)$ である．p,q を大きな素数に選べば，その確率は無視できるほど小さい．また，$m_y^2 \equiv m_x^3 \pmod n$ ならば，$b=0$ となり，楕円曲線ではない．しかし，p,q を大きな素数に選べば，その確率も無視できるほど小さい．係数 b は $b = m_y^2 - m_x^3 \bmod n = c_y^2 - c_x^3 \bmod n$ であるが，暗号

化の計算には必要ない．$b_p = b \bmod p$, $b_q = b \bmod q$ とする．平文 M は，$M_p = (m_{xp}, m_{yp}) = (m_x \bmod p, m_y \bmod p) \in E_p(0, b_p)$ と $M_q = (m_{xq}, m_{yq}) = (m_x \bmod q, m_y \bmod q) \in E_q(0, b_q)$ を中国人剰余定理で合成した点とみなせる．よって，暗号文 C は，M_p を e 倍した点 C_p と M_q を e 倍した点 C_q を中国人剰余定理で合成した点とみなせる．

［復号化］ $c_{xp} = c_x \bmod p$, $c_{yp} = c_y \bmod p$ とする．$C_p = (c_{xp}, c_{yp})$ を楕円曲線 $E_p(0, b_p)$ 上で d_p 倍した点を (m_{xp}, m_{yp}) とする．素数 q に対しても同様の計算を行って (m_{xq}, m_{yq}) を得る．中国人剰余定理を用いて (m_{xp}, m_{yp}) と (m_{xq}, m_{yq}) から平文 (m_x, m_y) を得る． □

係数 b_p は，$b_p = c_{yp}^2 - c_{xp}^3 \bmod p$ であるが，復号化の計算には必要ない．素数 p に対して，$(m_{xp}, m_{yp}) \in E_p(0, b_p)$ を e 倍した点 (c_{xp}, c_{yp}) を更に d_p 倍すると，もとの点 (m_{xp}, y_{yp}) になることが巡回性から導ける．また，復号化のときは素数 p と素数 q に分けて計算しているので，常に加算が定義されている．

一方，素数 p ($\equiv 3 \pmod 4$) と任意の整数 a ($\neq 0$) に対して，楕円曲線 $E_p(a, 0)$ は超特異な楕円曲線である．したがって，素数 p, q ($\equiv 3 \pmod 4$) を用いて，楕円曲線 $E_n(a, 0)$ 上でも同様の暗号方式を構成できる [20].

4.2.2 超特異でない楕円曲線上の RSA 型暗号方式：方式 2

［鍵生成］ $p \equiv q \equiv 1 \pmod 3$ を満たす二つの素数 p, q ($\geqq 5$) を選び，その積を n とする．素数 p に対して，

$$\begin{cases} p = \alpha_p^2 - \alpha_p\beta_p + \beta_p^2, \\ \alpha_p \equiv 2 \pmod 3, \\ \beta_p \equiv 0 \pmod 3 \end{cases} \tag{3}$$

を満たす α_p, β_p を求め，$\chi_p = 4^{(p-1)/3} \bmod (\alpha_p + \beta_p\omega)$ を計算する．ただし，$\omega = (-1+\sqrt{-3})/2$ である．

$$\tau_{p1} = \chi_p,\ \ell_{p1} = p + 1 + (2\alpha_p - \beta_p),$$
$$\tau_{p2} = -\chi_p,\ \ell_{p2} = p + 1 - (2\alpha_p - \beta_p),$$
$$\tau_{p3} = \omega^2\chi_p,\ \ell_{p3} = p + 1 + (-\alpha_p - \beta_p),$$
$$\tau_{p4} = -\omega^2\chi_p,\ \ell_{p4} = p + 1 - (-\alpha_p - \beta_p),$$
$$\tau_{p5} = \omega\chi_p,\ \ell_{p5} = p + 1 + (-\alpha_p + 2\beta_p),$$
$$\tau_{p6} = -\omega\chi_p,\ \ell_{p6} = p + 1 - (-\alpha_p + 2\beta_p)$$

とおく．素数 q に対しても同様に $\alpha_q, \beta_q, \chi_q, \tau_{qi}, \ell_{qi}$ $(i = 1, \cdots, 6)$ を求める．整数 e を ℓ_{pi}, ℓ_{qi} $(i = 1, \cdots, 6)$ すべてに対して互いに素な整数に選ぶ．$d_{pi} = e^{-1} \bmod \ell_{pi}$, $d_{qi} = e^{-1} \bmod \ell_{qi}$ $(i = 1, \cdots, 6)$ を計算する．公開鍵は n と e，秘密鍵は $p, q, \tau_{pi}, \tau_{qi}, \alpha_p, \alpha_q, \beta_p, \beta_q, d_{pi}, d_{qi}$ である． □

素数 p ($\equiv 1 \pmod 3$) に対して，式 (3) を満たす α_p, β_p は必ず存在し，$O((\log_2 p)^3)$ の演算量で計算する方法が知られている．素数 p ($\equiv 1 \pmod 3$) と任意の整数 b ($\neq 0$) に対して，楕円曲線 $E_p(0, b)$ の位数は $\ell_{p1}, \cdots, \ell_{p6}$ のいずれかであり，楕円曲線 $E_p(0, b)$ は超特異でない楕円曲線である．

［暗号化］ 方式 1 の暗号化と同じ． □

［復号化］ 素数 p に対して，$c_{xp} = c_x \bmod p$, $c_{yp} = c_y \bmod p$, $b_p = c_{yp}^2 - c_{xp}^3 \bmod p$ を計算し，$\tau_{pj} = b_p^{(p-1)/6} \bmod (\alpha_p + \beta_p\omega)$ となる j をみつけ，$d_p = d_{pj}$ とおく．(c_{xp}, c_{yp}) を $E_p(0, b_p)$ 上で d_p 倍した点を (m_{xp}, m_{yp}) とする．素数 q に対しても同様にして (m_{xq}, m_{yq}) を求める．中国人剰余定理を用いて，(m_{xp}, m_{yp}) と (m_{xq}, m_{yq}) から平文 (m_x, m_y) を得る． □

一方，素数 p ($\equiv 1 \pmod 4$) と任意の整数 a ($\neq 0$) に対して，楕円曲線 $E_p(a, 0)$ は超特異でない楕円曲線であり，その位数は $p + 1 \pm \gamma$, $p + 1 \pm \delta$ のいずれかである．ただし，γ, δ は $p = \gamma^2 + \delta^2$ を満たす整数である．したがって，素数 p, q ($\equiv 1 \pmod 4$) を用いて，楕円曲線 $E_n(a, 0)$ 上でも同様の暗号方式 [22] を構成できる．

また，$p \equiv -q \equiv 2 \pmod 3$ や $p \equiv -q \equiv 3 \pmod 4$ なる素数 p, q を用いると，それぞれ $E_n(0, b)$, $E_n(a, 0)$ 上で超特異な楕円曲線上の方式と超特異でない楕円曲線上の方式を組み合わせた方式 [22] も構成できる．

4.3 特異な 3 次曲線上の RSA 型暗号方式

特異な 3 次曲線上の RSA 型暗号方式は，結節点付き 3 次曲線上で構成される．その主要な二つの構成法である方式 3 [24] と方式 4 [19] について述べる．

4.3.1 結節点付き 3 次曲線上の RSA 型暗号方式

$u^2 + 4v$ が素数 p ($\geqq 5$) の平方剰余ならば，結節点付き 3 次曲線 $S_p(u, v)$ は乗法群 F_p^* と同型であり，その同型写像 ϕ_p は，

$$\phi_p :\ \mathcal{O} \mapsto 1,\ (x, y) \mapsto \frac{y - sx}{y - tx} \bmod p$$

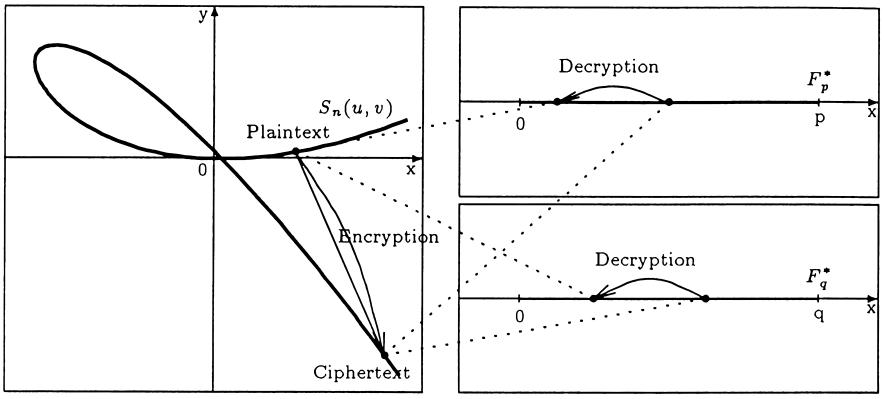

図 2　結節点付き 3 次曲線上の RSA 型暗号方式の概念
Fig. 2　Concept of RSA-type cryptosystem over cubic curves with a node.

である．ただし，$s,t=(-u\pm\sqrt{u^2+4v})/2 \bmod p$ である．その同型逆写像 ϕ_p^{-1} は，

$$\phi_p^{-1}:1\mapsto\mathcal{O},$$
$$z\mapsto\left(\frac{(t-s)^2z}{(z-1)^2} \bmod p, \frac{(t-s)^2z(tz-s)}{(z-1)^3} \bmod p\right)$$

である．したがって，u^2+4v が素数 p の平方剰余ならば，結節点付き 3 次曲線 $S_p(u,v)$ の位数は $p-1$ である．

方式 3 と方式 4 では，復号化を結節点付き 3 次曲線上で行う代わりに，同型写像を利用して結節点付き 3 次曲線上の暗号文を乗法群上の暗号文に変換し，復号化を乗法群上で行うことにより復号化速度を向上させている（図 2）．

a）　方式 3

［鍵生成］　二つの素数 p,q $(\geqq 5)$ を選び，その積を n とする．また $\ell_n=\mathrm{lcm}(p-1,q-1)$ とおく．整数 e を $\gcd(e,\ell_n)=1$ を満たすように選び，$d_p=e^{-1} \bmod (p-1)$，$d_q=e^{-1} \bmod (q-1)$ とする．公開鍵は n と e，秘密鍵は p，q，d_p，d_q である．□

［暗号化］　平文を $M=(m_x,m_y)$ $(1\leqq m_x,m_y\leqq n-1)$ とする．乱数 s を発生させ，$t=(m_x^3-m_y^2+sm_xm_y)/(m_x(sm_x-m_y)) \bmod n$ を計算する．$u=-s-t \bmod n$，$v=-st \bmod n$ とする．平文 $M\in S_n(u,v)$ を e 倍した点 $C=(c_x,c_y)\in S_n(u,v)$ が暗号文である．受信者には，暗号文 C と u を送る．□

$u^2+4v=(s-t)^2$ であるから，素数 p，q に対して平方剰余である．よって，結節点付き 3 次曲線 $S_p(u \bmod p, v \bmod p)$ と $S_q(u \bmod q, v \bmod q)$ の位数は各々 $p-1$，$q-1$ である．方式 3 では送信データ量は平文の 1.5 倍である．また，乱数 s を用いているので，同じ平文 M を複数回送信してもその都度暗号文 C が変化する．

［復号化］　素数 p に対して，$c_{xp}=c_x \bmod p$，$c_{yp}=c_y \bmod p$，$u_p=u \bmod p$，$v_p=(c_{yp}^2+u_pc_{xp}c_{yp}-c_{xp}^3)/c_{xp}^2 \bmod p$ とする．$\chi^2+u_p\chi-v_p\equiv 0 \pmod p$ の解を s_p，t_p とする．同型写像 ϕ_p を用いて，$c_p=(c_{yp}-s_pc_{xp})/(c_{yp}-t_pc_{xp}) \bmod p$ を計算する．$m_p=c_p^{d_p} \bmod p$ を計算する．同型逆写像 ϕ_p^{-1} を用いて，m_p から (m_{xp},m_{yp}) を計算する．素数 q に対しても同様にして (m_{xq},m_{yq}) を得る．(m_{xp},m_{yp}) と (m_{xq},m_{yq}) から中国人剰余定理を用いて，平文 (m_x,m_y) を得る．□

法が素数 p のときの 2 次方程式は，$O((\log_2 p)^3)$ の演算量で解く方法が知られている．

b）　方式 4

［鍵生成］　方式 3 の鍵生成と同じ．□

［暗号化］　平文を $M=(m_x,m_y)$ $(1\leqq m_x,m_y\leqq n-1)$ とする．平文 $M\in S_n(u,0)$ を e 倍した点 $C=(c_x,c_y)\in S_n(u,0)$ が暗号文である．ただし，$u=(m_x^3-m_y^2)/(m_xm_y) \bmod n$ である．□

$u^2+4v=u^2$ なので，素数 p,q $(\geqq 5)$ に対して平方剰余である．よって，素数 p,q $(\geqq 5)$ と任意の整数 u $(\neq 0)$ に対して，結節点付き 3 次曲線 $S_p(u \bmod p,0)$ と $S_q(u \bmod q,0)$ の位数は各々 $p-1$，$q-1$ である．

［復号化］　素数 p に対して，$c_{xp}=c_x \bmod p$，$c_{yp}=c_y \bmod p$，$u_p=-s_p=(c_{xp}^3-c_{yp}^2)/(c_{xp}c_{yp}) \bmod p$，$v_p=t_p=0$ とし，同型写像 ϕ_p を用いて，$c_p=c_{xp}^3/c_{xp}^2 \bmod p$ を計算する．$m_p=c_p^{d_p} \bmod p$ を計算

する．同型逆写像 ϕ_p^{-1} を用いて，m_p から (m_{xp}, m_{yp}) を計算する．素数 q に対しても同様にして (m_{xq}, m_{yq}) を得る．(m_{xp}, m_{yp}) と (m_{xq}, m_{yq}) から中国人剰余定理を用いて，平文 (m_x, m_y) を得る． □

一方，素数 p $(\geqq 5)$ と任意の整数 v $(\neq 0)$ に対して，結節点付き 3 次曲線 $S_p(0, v)$ の位数は $p-1$ または $p+1$ である．したがって，素数 p, q $(\geqq 5))$ を用いて，結節点付き 3 次曲線 $S_n(0, v)$ 上で RSA 型暗号方式 [25] も構成できる．しかし，この方式は方式 3 と方式 4 と比較して，復号化速度が遅く，安全性の証明が部分的にしかできていない．なお，尖点付き 3 次曲線 $S_p(u, v)$ は加法群 F_p^+ と同型であり，尖点付き 3 次曲線上の RSA 型暗号方式は安全でない．

4.4 安全性と効率

4.4.1 素因数分解の難しさ

RSA 型 3 次曲線暗号の安全性は，RSA 暗号と同様，合成数 n の素因数分解の難しさに根拠をおいている．現在，n のサイズは 1024 ビット（10 進 310 けた程度）が標準的に使われている．素因数分解の難しさは現在知られている最良の解法でその計算量が見積もられ，準指数関数的な時間を要することがわかっている [35]．最高速の素因数分解アルゴリズムは数体ふるい法 [35] である．その計算量は

$$\exp(b'(\ln n)^{1/3}(\ln\ln n)^{2/3})$$

であり $(1 < b' < 2)$，理論的に従来手法よりも優れている．

4.4.2 1 対 1 通信の安全性

合成数 n が素因数分解されると，RSA 暗号と RSA 型暗号は解読される．しかし，これらの暗号を解読する手間と素因数分解の手間の間の等価性は証明されていない．つまり，素因数分解以外の手法で RSA（型）暗号が破られるかもしれない．1 対 1 通信において，方式 4 の RSA 型暗号の解読の難しさと RSA 暗号の解読の難しさの等価性を我々は証明した [19]．つまり方式 4 が何らかの方法で破られると RSA 暗号も破られ，RSA 暗号が何らかの方法で破られると方式 4 も破られる．更に，方式 3 が何らかの方法で破られると RSA 暗号も破られることを我々は証明した [24]．RSA 暗号が破られると方式 3 が破られることは証明できないので，方式 3 は RSA 暗号よりも強いか，同等の安全性をもつことになる．なお，方式 1 及び方式 2 の解読の難しさと RSA 暗号の解読の難しさの等価性はまだ証明されていない．

4.5 効　　率

楕円曲線上の演算を高速化するアルゴリズムを使っても，方式 1 の復号化速度は RSA 暗号の復号化速度よりも約 4.6 倍遅かった．しかし，特異な 3 次曲線上の RSA 型暗号を考案することによって大幅な速度向上が達成できた．これは，特異な 3 次曲線上の加法群と RSA 本来の演算を行う乗法群の間の写像を利用することによって可能となった．方式 3 の復号化速度は RSA 暗号の復号化速度と同等であり，方式 4 の復号化速度は RSA 暗号よりも約 2 倍高速である．その理由は RSA 暗号のブロック長の 2 倍の長さのデータをほぼ一度に処理できるからである．データ長が長ければ長いほど速度向上が図ることができる．

5. むすび

整数論の長年の研究テーマであった楕円曲線が，暗号理論においても重要な位置を占めるようになった．本論文で解説した楕円曲線暗号や RSA 型楕円暗号は，その主要なものといえよう．楕円曲線暗号は提案から 10 年が過ぎ，実用化及び標準化という新たな局面を迎え，RSA 型楕円暗号は楕円曲線の新たな魅力を引き出している．楕円曲線は，今後ますます，理論面においても実用面においても重要になっていくと思われる．

文　　献

[1] K. Araki, T. Satoh, and S. Miura, "Overview of elliptic curve cryptography," Proc. of PKC'98, LNCS 1431, pp.29–49, Springer-Verlag, 1998.

[2] A.O.L. Atkin, "The number of points on an elliptic curve modulo a prime," preprint, 1998.

[3] R. Balasubramanian and N. Koblitz, "Improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm," Journal of Cryptology, vol.2, no.11, pp.141–145, 1998.

[4] D. Shanks, "Class number, A theory of factorization, and genera," Proc. Symposium Pure Mathematics, AMS, 1985.

[5] J. Chao, K. Tanada, and S. Tsujii, "Design of elliptic curves with controllable lower boundary of extension degree for reduction attacks," Proc. of Crypto'94, LNCS 839, pp.50–55, Springer-Verlag, 1994.

[6] D.V. Chudnovsky and G.V. Chudnovsky, "Sequences of numbers generated by addition in formal group and new primality and factorization tests," Advances in Applied Math., vol.7, pp.385–434, 1986.

[7] J.M. Couveignes and F. Morain, "Schoof's algorithm and isogeny cycles," Proc. of ANTS-I, LNCS 877, pp.43–58, Springer-Verlag, 1994.

[8] N. Demytko, "A new elliptic curves based anologue of

RSA," Proc. of Eurocrypto'93, LNCS 765, pp.40–49, Springer-Verlag, 1993.
[9] N.D. Elkies, "Explicit isogeny," preprint, 1991.
[10] G. Frey and H.G. Rück, "A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves," Math. Comp., vol.62, no.206, pp.865–874, 1994.
[11] 原澤隆一，杉山佳子，四方順司，鈴木 譲，"Frey-Rück Attack に関する一考察，" Technical Report of IEICE, ISEC98-23, pp.25–30, 1998.
[12] J. Hastad, "On using RSA with low exponent in a public key network," Proc. of Crypto'85, LNCS 218, pp.403–408, Springer-Verlag, 1985.
[13] 池野信一，小山謙二，現代暗号理論，電子情報通信学会，1986.
[14] T. Izu, J. Kogure, M. Noro, and K. Yokoyama, "Efficient implementation of schoof's algorithm," Proc. of Asiacrypto'98, LNCS 1514, pp.66–79, Springer-Verlag, 1998.
[15] D.E. Knuth, "Seminumerical algorithm (arithmetic)," The Art of Computer Programming, vol.2, Addison Wesley, 1969.
[16] N. Koblitz, "A course in number theory and cryptography," GTM 114, Springer-Verlag, 1987.
[17] N. Koblitz, "Elliptic curve cryptosystems," Math. Comp., vol.48, no.177, pp.203–209, 1987.
[18] 小山謙二，"楕円曲線に基づく暗号理論の最近の発展，" システム/制御/情報，vol.38, no.2, pp.87–94, 1994.
[19] K. Koyama, "Fast RSA-type schemes based on singular cubic curves $y^2 + axy \equiv x^3 \pmod{n}$," Proc. of Eurocrypto'95, LNCS 921, pp.329–340, Springer-Verlag, 1995.
[20] K. Koyama, U. Maurer, T. Okamoto, and S.A. Vanstone, "New public-key schemes based on elliptic curves over the ring $\mathbf{Z}_n$," Proc. of Crypto'91, LNCS 576, pp.252–266, Springer-Verlag, 1991.
[21] K. Koyama and Y. Tsuruoka, "Speeding up elliptic cryptosystems using a signed binary window method," Proc. of Crypto'92, LNCS 740, pp.345–357, Springer-Verlag, 1992.
[22] H. Kuwakado and K. Koyama, "Efficient cryptosystems over elliptic curves based on a product of form–free primes," IEICE Trans. Fundamentals, vol.E77-A, no.8, pp.1309–1318, Aug. 1994.
[23] H. Kuwakado and K. Koyama, "Security of RSA-type cryptosystems over elliptic curves against Hastad attack," Electronics Letters, vol.30, no.22, pp.1843–1844, 1994.
[24] K. Kuwakado and K. Koyama, "A new RSA-type scheme based on singular cubic curves $(y - \alpha x)(y - \beta x) \equiv x^3 \pmod{n}$," Proc. of JW-ISC'95, pp.144–151, 1995.
[25] H. Kuwakado, K. Koyama, and Y. Tsuruoka, "A new RSA–type scheme based on singular cubic curves $y^2 \equiv x^3 + bx^2 \pmod{n}$," IEICE Trans. Fundamentals, vol.E78-A, no.1, pp.27–33, Jan. 1995.
[26] R. Lercier, "Finding good random elliptic curves for cryptosystems defined over $\mathbf{F}_{2^n}$," Proc. of Eurocrypto'97, LNCS 1233, pp.379–392, Springer-Verlag, 1997.
[27] A. Menezes, Elliptic Curve Public Key Cryptosystem, Kluwer Academic Publishers, 1993.
[28] A. Menezes, T. Okamoto, and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," IEEE Trans. on Information Theory, vol.IT-39, no.5, pp.1639–1646, 1993.
[29] V.S. Miller, "Use of elliptic curves in cryptography," Proc. of Crypto'85, LNCS 218, pp.417–426, Springer-Verlag, 1985.
[30] A. Miyaji, "Elliptic curve suitable for cryptosystems," IEICE Trans. Fundamentals, vol.E77-A, no.1, pp.98–105, Jan. 1994.
[31] A. Miyaji, T. Ono, and H. Cohen, "Efficient elliptic curve exponentiation," Proc. of ICICS'97, LNCS 1334, pp.282–290, Springer-Verlag, 1997.
[32] A. Miyaji, T. Ono, and H. Cohen, "Efficient elliptic curve exponentiation using mixed coordinates," Proc. of Asiacrypto'98, LNCS 1514, pp.51–65, Springer-Verlag, 1998.
[33] F. Morain, "Building cyclic elliptic curves modulo large primes," Proc. of Eurocrypto'85, LNCS 547, pp.328–336, Springer-Verlag, 1991.
[34] F. Morain and J. Olivos, "Speeding up the computations on an elliptic curve using addition-subtraction chains," Theoretical Informatics and Applications, vol.24, no.6, pp.531–544, 1990.
[35] 岡本龍明，太田和夫編，暗号・ゼロ知識証明・数論，共立出版，1995.
[36] S. Pohlig and M. Hellman, "An improved algorithm for computing logarithms over $GF(p)$ and its cryptographical significance," IEEE Trans. Information Theory, vol.24, pp.106–110, 1978.
[37] J.M. Pollard, "Monte Carlo methods for index computation mod p," Math. Comp., vol.32, pp.918–924, 1978.
[38] R.L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol.21, no.2, pp.120–126, 1978.
[39] H.G. Rück, "On the discrete logarithm in the divisor class group of curves," to appear in Math. Comp.
[40] H.G. Rück, "The Tate Pairing on Elliptic Curves," ECC'98 (Waterloo), 1998.
[41] T. Satoh and K. Araki, "Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves," Commentarii Math. Univ. Sancti Pauli, vol.47, no.1, pp.81–92, 1998.
[42] 佐藤孝和，荒木純道，"Fermat Quotients と Anomalous 楕円曲線の離散対数の多項式時間解法アルゴリズムについて（II），" 「代数幾何・数論及び符合・暗号」研究集会報

告集，pp.139–145, 東大数理，1998.
[43] R. Schoof, "Elliptic curves over finite fields and the computation of square roots mod p," Math. Comp., vol.44, pp.483–494, 1985.
[44] T.A. Semaev, "Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p," Math. Comp., vol.67, no.221, pp.353–356, 1998.
[45] O. Schirokauer, D. Weber, and T. Denny, "Discrete logarithms: The effectiveness of the index calculus method," Proc. of ANTS-II, LNCS 1122, pp.337–361, Springer-Verlag, 1996.
[46] R. Schroeppel, H. Orman, S. O'Malley, and O. Spatscheck, "Fast key exchange with elliptic curve systems," Proc. of Crypto'95, LNCS 963, pp.43–56, Springer-Verlag, 1995.
[47] J.H. Silverman, "The arithmetic of elliptic curves," GTM 106, Springer-Verlag, 1986.
[48] J.H. Silverman and J. Suzuki, "Elliptic curve discrete logarithms and the index calculus," Proc. of Asiacrypto'98, LNCS 1514, pp.110–125, Springer-Verlag, 1998.
[49] N.P. Smart, "The discrete logarithm problem on elliptic curves of trace one," to appear in Journal of Cryptology.
[50] J.A. Solinas, "An improved algorithm for arithmetic on a family of elliptic curves," Proc. of Crypto'97, LNCS 1294, pp.357–371, Springer-Verlag, 1997.
[51] E. Teske, "Speeding up Pollard's Rho Method for Computing Discrete Logarithms," Proc. of ANTS-III, LNCS 1423, pp.541–554, Springer-Verlag, 1998.
[52] S. Uchiyama and T. Saitoh, "A note on the discrete logarithm problem on elliptic curves of trace two," Technical Report of IEICE, ISEC98-27, pp.51–57, 1998.
[53] M.J. Wiener and R.J. Zuccherato, "Faster attacks on elliptic curve cryptosystems," Proc. of SAC'98, pp.196–207, 1998.
[54] E.D. Win, A. Bosselaers, and S. Vandenberghe, "A fast software implementation for arithmetic operations in GF(2^n)," Proc. of Asiacrypt'96, LNCS 1163, pp.65–76, Springer-Verlag, 1996.

（平成 11 年 3 月 10 日受付）

小山　謙二　（正員）

コミュニケーション科学基礎研究所小山特別研究室長．昭 49 入社．分散処理計算機，情報セキュリティ，暗号理論の研究に従事．昭 47 京都大・工・電気卒．昭 49 同大大学院工学研究科修士課程了．昭 58 工博（京都大学）．情報処理学会，IACR, 感情心理学会各会員．本会論文賞，米澤ファウンダーズメダル受賞記念賞，著述賞；情報処理学会・Best Author 賞；科学技術庁長官賞（研究功績者賞），コンピュータ将棋協会研究賞を各受賞．

宮地　充子　（正員）

1988 阪大・理・数学卒．1990 同大大学院修士課程了．同年，松下電器産業（株）入社．1998 北陸先端科学技術大学院大学・情報科学研究科助教授，現在に至る．情報セキュリティの研究に従事．理博．IACR 会員．

内山　成憲　（正員）

平 3 九大・理・数学卒．平 8 同大大学院博士課程了．博士（数理学）．同年日本電信電話（株）入社．以来，情報セキュリティの研究に従事．現在，NTT 情報流通プラットフォーム研究所研究主任．日本数学会会員．