楕円暗号へのガイダンス

辻井　重男[†]　　趙　晋輝[††]

A Guidance for Elliptic Curve Cryptosystems

Shigeo TSUJII[†] and Jinhui CHAO[††]

あらまし　まず，暗号技術の全般的な状況を説明した後，その中での楕円暗号の位置付けと概念を従来の公開鍵暗号と対比させながら平易に解説する．

キーワード　楕円曲線，超楕円曲線，公開鍵暗号，楕円暗号，虚数乗法

1. まえがき

本学会会員等の研究成果によって，いわゆるサイバースペースが我々の生活空間の大きな部分空間となりつつあるが，我々自身の身体がサイバースペースに入っていくわけにはいかず，個々にその身代わりを立ててサイバースペースで様々な活動を行わせねばならない．この身代わりになり，電子的化身となって身分証明を行うもの，いわばサイバーパスポートを保証する技術が暗号である．

自治体のワンストップサービスや電子投票などは，人々の利便性を高め，行政システムを広域的に効率化するが，これらは，暗号のもつ認証（署名）機能による本人確認に基づいて初めて可能になる．

また，電子マネーをはじめとする電子商取引は経済システムを効率化するが，電子マネーとは，「暗号のもつ認証（署名）機能によって，その金額情報が保証された現金」であり，暗号なしには電子マネーは存在し得ない．

あるいは物流システムも，暗号による改ざん防止機能を埋め込んだ半導体チップの利用によって物品の状態管理を誤りなく行うことにより合理化が大いに進められよう．

[†] 中央大学理工学部情報工学科，東京都
Department of Information and System Engineering, Faculty of Science and Engineering, Chuo University, Tokyo, 112–8551 Japan
[††] 中央大学理工学部電気・電子工学科，東京都
Department of Electrical and Electronic Engineering, Faculty of Science and Engineering, Chuo University, Tokyo, 112–8551 Japan

このように，暗号技術は，人に限らず，情報サービス，金・決済，物，更には時刻の真偽を確認し，それらの状態を正確に把握することによって社会・経済システムを著しく効率化する力を秘めている [1].

情報社会は自由が拡大する反面，安全性が問題化する社会である．暗号は安全性を高める技術であるといわれるが，安全性を保障しつつ自由を拡大していくという両面性をもっており，攻めと守りの 2 面性をもっている．このように，情報社会における暗号の役割は本質的であり，その信頼性の向上に我々は最大限の関心を払わねばならない．ちなみに OECD の暗号政策ガイドラインでは，その 8 原則の第 1 条で，暗号に対する信頼感の醸成をうたっている．こうした背景の中で，その安全性の高さのゆえに，最近，楕円暗号は暗号の中の暗号としての風格を備えてきた．

しかし，その理論構築に代数曲線論が駆使されるだけに，公開鍵暗号の中でもとりわけ理解されがたい分野であることも事実である．

本論文は，暗号の専門家ではないが数理に興味をもたれる多くの会員に読んで頂けるよう，理論や方式構成の詳細は他の著者に譲り，楕円暗号へのガイダンスに徹することとしたい．

2. 暗号最前線の状況

“暗号には共通鍵方式と公開鍵方式があって” というような説明から始めるとたちまち割当て頁数が尽きてしまいそうだが，楕円暗号の位置付けと役割を理解して頂くために，暗号に関する最近の動向について簡単に触れておきたい．

まず，共通鍵暗号であるが，最近，ポスト DES とし

て，AESが話題を呼んでいる．DES（Data Encryption Standard）は，今から20年余り前，1977年1月，米国政府の標準暗号として制定されたものである．それまでの暗号は，アルゴリズムも鍵もすべて秘密であった．DESはアルゴリズムと鍵の区別を明確化し，鍵のみを送・受信者間の共通秘密として，アルゴリズムは公開して標準化するという運用方式をとることにより，不特定多数の間の秘匿通信を容易にし，情報社会対応を図ったものである．

1990年前後から，Biham，Shamirによる差分解析や松井による線形解析など，共通鍵暗号に対する解読法が進み，DESに対する信頼感が揺らぎ始めた．もっともDESのように多くの研究者のチェックを受けてきた暗号が，これらの解析法により，解読されることは，実際の使用状況のもとでは考えがたく，可能性があるとすれば，鍵の総当りにより解読されることである．DESの鍵は56ビットであるから，鍵の総数は$2^{56} \doteqdot 10^{17}$であり，1日が約10^{17}ピコ秒であることと，最近のコンピュータの進歩と普及を考えると，鍵の総当りによる解読も不可能ではなくなってきた．

こうした背景のもとに，NIST（米国標準技術局）は，今後20年以上の使用に耐えられるポストDESとして，AES（Advanced Encryption Standard）を2000年を目途に制定することとし，海外からも次世代の暗号アルゴリズムを公募して，その第1回発表会を1998年8月に開催した．

我が国からはNTTがE2暗号を提案している．AESでは鍵長は128ビット以上となっており，鍵の総当り攻撃では，仮に1ピコ秒で一つの鍵を試すとしても1兆年以上を要する計算になる．もちろん，総当り法以外に差分解析や線形解析にも耐える方式でなければならない．

さて，楕円暗号は，公開鍵方式に属するものであるが，話を共通鍵暗号から始めたのは，講演会などで，以上のような共通鍵暗号の鍵長について説明すると，“1024ビットという話も聞きますが”という類の質問を受けたりすることも少なくないからである．1024ビットは公開鍵暗号の代表格であるRSA暗号の鍵長の例である．

公開鍵暗号は多くの面で共通鍵暗号と様相や趣を異にする．研究者としての好みの問題から極論すれば，共通鍵暗号をやる人は暗号の好きな人，公開鍵暗号をやる人は数学（特に数論）の好きな人といえるくらいの違いが感じられる．特に，次世代の公開鍵暗号としての期待を担う楕円暗号の研究には多くの数学出身者が参入している．例えば，中央大学では，企業数社の研究者と学生が集まって楕円暗号ゼミを開いているが，学外からの参加者のほとんどが，数論や代数幾何を大学院で修めた経歴をもつ人々である．

もっとも，これまで公開鍵暗号市場を独占してきたRSA暗号については，その秘密鍵をつくり出す公式，いわゆるEuler関数が，1761年のEulerに先駆けて，和算家久留島義太によって発見されていることからもわかるように，それほど高度な数学を知らなくても一通りの理解は可能である．

そうはいっても，RSA暗号が依拠する素因数分解に楕円曲線が利用されることもあるし，RSA暗号の安全性の追求についてもレベルの高い理論構築がなされており，そう簡単なものでもない．

更に，共通鍵暗号の立場で弁明すれば数学的な理論が不要というわけではなく，最近では特定の攻撃に対する証明可能安全性という用語も定着しているし，また，Gröbner基底などを用いる代数的解析法も研究されている．

しかし，共通鍵暗号が，換字と転置を繰り返すような回路構造を基本とし，その数学的構造を明示しがたい方式が多いのに対し，公開鍵暗号は，明快な数学的構造をもっていることは間違いない．

性能面や機能面でも両者に各々特徴があることはいうまでもなく，今，それらを逐一説明するゆとりはないので，概要を表1に示しておく[1]．

公開鍵暗号における最近の話題としては次の二つが挙げられよう．

（1） 素因数分解や有限体上の離散対数問題の困難性に基づく公開鍵暗号のプロトコル環境における安全性向上

インターネット上での電子商取引の普及に伴い，SSL（Secure Socket Layer）のような暗号プロトコルが組み込まれた実際的状況のもとで，能動的攻撃（例えばRSAの秘密鍵を探ろうとしてしかける不正な攻撃）で破られる可能性が示唆されたこともあって，公開鍵暗号の安全性をこうしたプロトコル環境の中で向上させたOAEP [20]，EPOC [21], Cramer-Shoup暗号 [22]などの諸方式が提案されている．実用面でもOAEPはSET（Secure Electronic Transactions，インターネット上でのクレジットカード決済を実現する技術仕様）に採用されている．

（2） そして，公開鍵暗号に関する最大の話題は本

表 1　共通鍵暗号と公開鍵暗号
Table 1　Comparison of common key cryptosystems and public key cryptosystems.

	共通鍵暗号	公開鍵暗号
主用途	ﾃﾞｰﾀの秘匿・保護 認証も可能（ｾﾝﾀｰによる加入者の秘密鍵管理が必要，不特定多数には不向き）	認証（署名，改ざん防止） 共通鍵暗号の鍵配送
鍵の構造	暗号化鍵=復号化鍵 (=秘密鍵)	秘密鍵から公開鍵を生成 (公開鍵から秘密鍵を割り出すことは困難)
暗号化速度	高速（ｿﾌﾄｳｪｱでも数百 Mb/s 可能）	低速（共通鍵に比べて 2〜3 桁遅い）
例	DES，RC5，AES(策定中)，FEAL, MULTI, MISTY, CIPHERUNICORN 等	RSA, Rabin,黒澤, ElGamal(有限体,楕円), EPOC 等

論文の主題である楕円暗号であろう．

3. 有限体上の離散対数問題と ElGamal の公開鍵暗号

公開鍵暗号という名称は鍵を公開するところから付けられたものであるが，鍵を全部見せてしまっては暗号にならない．鍵を 2 重構造にしておき，外側の鍵は公開し，内側の鍵は自分だけの秘密にするのである（図 1 参照）．外側の鍵を公開鍵と呼び，内側の鍵を秘密鍵と呼ぶ．個人個人が秘密鍵と公開鍵をペアでもつという点が，人類が数千年来用いてきた共通鍵暗号と全く異なっている．共通鍵の共通とは送信者 A と受信者 B のペアが定まったとき，そのペアに対して，A と B の間で秘密の鍵を一つ共通にもつという意味であり，鍵には内側も外側もなく 1 重構造である．

公開鍵暗号の 2 重構造の作り方には様々な方法が考えられるが，それらの中で，図 2 に示すように素因数分解を利用する RSA 型と離散対数問題の ElGamal 型がよく知られている．ElGamal 暗号は 1982 年，その名のとおり，ElGamal によって提案された方式である（アラブ語で El は定冠詞，Gamal はラクダを意味するそうである）．これは，図 3 のように有限体上の離散対数問題の困難性を利用する方式として発表された．有限体上の離散対数問題を小さな例について見てみよう．素数 31 を法とする有限体の中で，原始元として 3 を選び，$y = 3^x \bmod 31$ をグラフとして示したのが図 3 である．実数体における離散対数問題と異なり，x に対して y は予測しがたい動きを示し，法 p と原始元 g，更に y の値が公開されていても x の値を知ることは，法 p が大きくなるにつれて困難となる．現在，知られているアルゴリズムでは与えられた p，g，y に対して，x を求めるための計算量は，p のけた $(\log_{10} p)$ に対し，準指数時間の

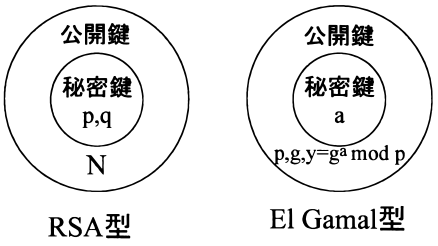


図 1　公開鍵の構造
Fig. 1　Structure of public key cryptosystems.

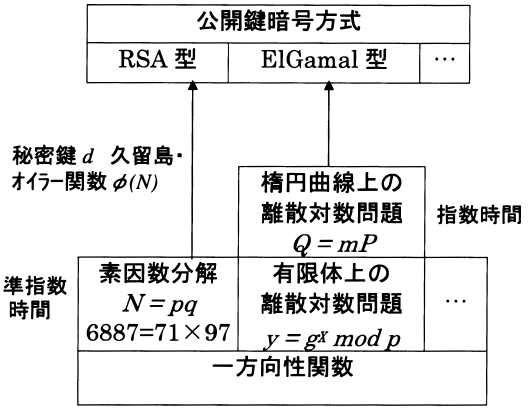


図 2　公開鍵暗号の構成
Fig. 2　Construction of public key cryptosystems.

表 2　有限体上と楕円曲線上の ElGamal 暗号方式
Table 2　ElGamal public key cryptosystems over finite fields and elliptic curves.

	(受信者 A の)準備	暗号化(送信者 B)	復号(受信者 A)
有限体上の ElGamal 暗号（秘匿目的）	素数 p,原始元 g を公開 ランダム数 a を秘密 $y = g^a \bmod p$ を計算, y を公開	平文 M_B ランダム数 k を生成 暗号文$(g^k,\ M_B\ y^k) \bmod p$ を送信	$(g^k)^a = y^k \bmod p$ $\frac{M_B\, y^k}{y^k} = M_B \bmod p$
楕円曲線上の ElGamal 暗号（秘匿目的）	素数 p ベース点 P を公開 ランダム数 m を秘密 Q=mP を計算, Q を公開	平文 M_B ランダム数 k を生成 暗号文(kP, M_B+kQ)を送信	m(kP) = kQ $M_B + kQ - kQ$ $= M_B$

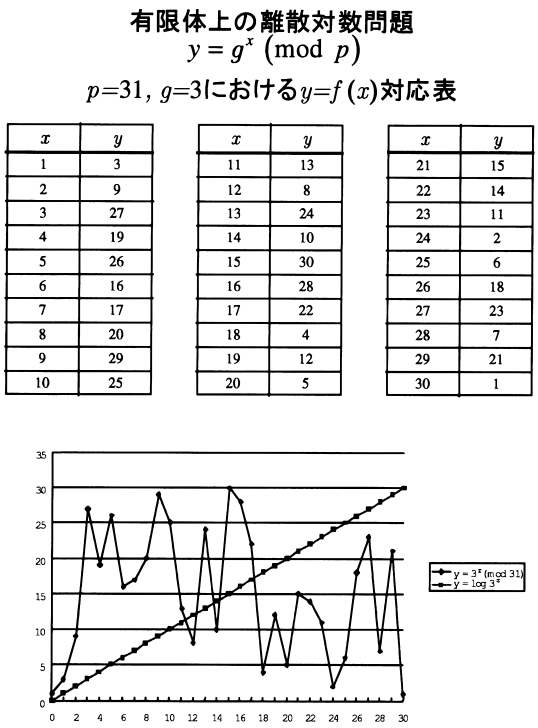


図 3　有限体上の離散対数問題
Fig. 3　Discrete logarithm problem over finite field.

オーダとなっている（c を定数とし，計算のオーダが $\mathcal{O}(\exp\{c(\log p)^b(\log\log p)^{1-b}\}), (0 < b < 1)$ で表されるとき，その計算量は準指数時間のオーダであるという．また，$\mathcal{O}(\exp(c \cdot \log p))$ のとき指数関数時間のオーダという）．p が 10 進数で 200 けた程度以上となると現在のコンピューティングパワーを用いて現実時間で解くことは不可能と考えられる．つまり，

$$y = f(x) = g^x \bmod p$$

は一方向性関数となる．したがって，図 1 のように $y = g^a \bmod p$ を公開しても a を秘密に保てるのである．この一方向性関数を落とし戸として公開暗号系を表 2 のように構成したのが ElGamal である．表 2 において，k は送信者が勝手に決める使い捨て乱数である．離散対数問題の困難性によって，k は解読者にはもちろん，受信者にもわからない．しかし，受信者は自分だけの秘密 a で $g^k \bmod p$ をべき乗して $(g^k)^a = (g^a)^k = y^k \bmod p$ を得，その値で第 2 項 $My^k \bmod p$ を割ることにより，平文 M を得ることができる．

ElGamal 暗号の問題点は平文 M（$p-1$ より小）に対し，暗号文の長さが 2 倍程度になることである．なお，ElGamal 暗号は確かに公開鍵暗号方式ではあるが，送信者は乱数 k を共通鍵方式における鍵として離散対数に託して秘密配送しているようでもあり，共通鍵暗号方式の名残りをとどめていると解釈することもできる．また，同一の平文でも，送信のつど k を変えることにより，異なる暗号文となる．このような性質をもつ暗号を確率的暗号と呼んでいる．

4.　楕円曲線上の離散対数問題と楕円暗号

楕円暗号という呼称が広く使われているので，本論文でもそのように呼んできたが，正確には，楕円暗号とは，楕円曲線上の離散対数問題の困難性を利用した公開鍵暗号の総称である．また楕円曲線とは限らず，超楕円曲線，あるいは一般に Abel 多様体上の群構造を利用する暗号系も広い意味で楕円暗号と呼ぶことも多い．

さて，楕円曲線とは，例えば，

$$y^2 = x^3 + 1 \qquad (1)$$

のように「$y^2 = x$ の 3 次式（重根をもたない）」と

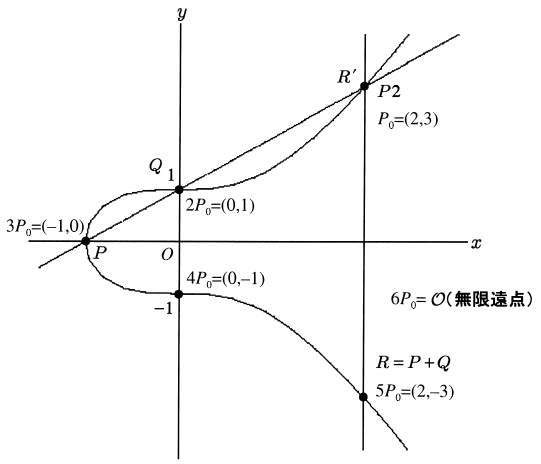


図 4　楕円曲線とその上の加法
（$y^2 = x^3 + 1$ の場合）
Fig. 4　Additive law over an elliptic curve.

して表される代数曲線である．簡単のため複素数体上で考えて，x, y を実数として描けば図 4 のように x 軸に関して対称なグラフになる．この曲線上で，2 点 P と Q を図 4 のようにとれば，$P = (x_1, y_1)$ と $Q = (x_2, y_2)$ を通る直線は，曲線上のもう一つの点 R' と交わる．この R' と無限遠点を通り，y 軸と平行な直線は，x 軸に関して R' と対称な点 $R = (x_3, y_3)$ で交わる．ここで，

$$P + Q = R$$

と定義する．具体的には簡単な計算によって，

$$\begin{cases} x_3 = -x_1 - x_2 + \lambda^2 \\ y_3 = -\lambda(x_3 - x_1) - y_1 \\ \lambda = \dfrac{y_2 - y_1}{x_2 - x_1} \end{cases} \tag{2}$$

となることがわかる．また，点の整数倍も定義することができ，例えば，図 4 では，$Q = 2P_0$ となる．一般に P と Q を任意の 2 点とし，上のようにして定まる第 3 の点 R を P と Q の和と定義すれば，x, y が有理数のとき，驚くべきことに曲線上の点の集合に無限遠点を加えた集合は，有限生成の加法群をなすことが 1922 年，Mordell によって示された．楕円曲線という幾何学的存在が代数的構造をもっていることがわかったのである．曲線上の点としては，複素数，有理数，代数的数などが考えられるが，暗号としては，有限体上の点を使うことになる．もっとも設計段階では，代数体上で考え，有限体上に還元したりするので，有限体上の議論だけですむわけではない．

さて，有限体 $\mathbf{F}_q$ 上で定義された楕円曲線上で，上のような加法によって，P を m 回加えた結果を

$$Q = mP \tag{3}$$

と表すこととする．点 P をベースポイントという．点 P の位数が大きな素数を含む場合，2 点 P と Q が与えられていても m を求めることは難しい．これは，先に述べた有限体上で

$$y = g^x \bmod p \tag{4}$$

において p，g，y が与えられていても x を求めることが難しいのと似ている（表 2 参照）．そこで，m を求める問題を楕円曲線上の離散対数問題といい，その困難性を利用して，有限体上の ElGamal 暗号と同様に公開鍵暗号を構成することができる（図 5 参照）．このように楕円曲線等を利用した公開鍵暗号を総称して，通常，楕円暗号と呼んでいるのである．したがって，楕円暗号という名称は，暗号方式ではなく，数学的素材に由来するものである（図 2 参照）．

なお，上に説明した ElGamal 暗号はデータの秘密を目的とするものであるが，公開鍵暗号にとってより重要な認証のための方式も離散対数問題を利用して構成できる．

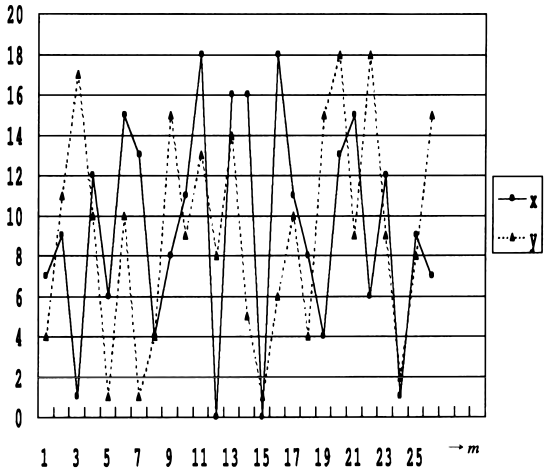
5.　楕円暗号の優位性

有限体上の離散対数問題と楕円曲線上の離散対数問題とはどちらが難しいのだろうか．

先に述べたように，有限体上の離散対数問題の難しさは特別な場合（例えば $p - 1$ が小さな因数の積からなる場合）を除いて，準指数時間である．これに対し，楕円曲線上の離散対数問題についても多くの研究者が努力を傾けているが，極めて特殊な場合を除けば，その計算量は現在知られているアルゴリズムでは，有限体のサイズに対し指数時間オーダである．楕円暗号に関しても，将来，準指数時間アルゴリズムが出現する可能性が全くないわけではないが（その不可能性を証明することも不可能だろうが），それをいえば，有限体上の場合でも，準指数時間が多項式時間に下がる可能性を全く否定することもできない．そこで，有限体上の場合は準指数時間，楕円曲線上の場合は指数時間として両者を比較してみよう．

Q = mP	P	2P	3P	4P	5P	6P	7P	8P	9P	10P	11P	12P	P13
(x,y)	7,4	9,11	1,17	12,10	6,1	15,10	13,1	4,4	8,15	11,9	18,13	0,8	16,14

14P	15P	16P	17P	18P	19P	20P	21P	22P	23P	24P	25P	26P	27P
16,5	0,1	18,6	11,10	8,4	4,15	13,18	15,9	6,18	12,9	1,2	9,8	7,15	0



(a) GF(19)上定義された楕円曲線$y^2 = x^3 + 2x + 1$における
Q(x,y) = mP　P = (7,4)(生成元)のx,y座標
（水野弘文:“情報数理の基礎”, 培風館, 1996,
p 110の数値を図表化したものである。）

公開鍵　P = (7,4), Q = 6P = (15,10)
秘密鍵　m = 6
暗号化 ——暗号通信——→ 復号
k = 3（ランダムに選ぶ）
平　文: M
暗号文; (3P, M+3Q)を作成

$$M + 3Q - 6(3P)$$
$$= M + 3Q - 3Q$$
$$= M$$

(b) (a)に示す楕円曲線を用いたElGamal暗号

図 5　楕円曲線上の離散対数問題と暗号方式の例
Fig. 5　Cryptosystem based on discrete logarithm over an elliptic curve.

現在，広く利用されている RSA 暗号が依拠する素因数分解に要する計算量も準指数時間であり，現在話題を呼んでいるのは，RSA 暗号と楕円暗号について，両者の解読に要する計算量を同等としたときの所要鍵長の比較である．RSA 暗号の場合，様々な認証に要する法 N のビット数は，今後 10 年以上のコンピュータの進歩と普及を考えると 1024 ビットは必要とされている．これに対し楕円暗号の場合は，安全性を同程度とするには 160 ビット〜170 ビット程度あればよいと評価されている（表 3 参照）．

こうした違いから，IC カード型電子マネーについていえば，現在の LSI 技術では，RSA 暗号を実装するにはコプロセッサが必要となるが，楕円暗号ならコプロセッサは不要となる．このような背景のもとに，1980 年中ごろ，Miller [33] や Koblitz [2] によって始められた楕円暗号がインターネットの商用化に伴って数年前から脚光を浴び始めたのである．

更に，今後のコンピュータの進歩と普及を考えると，準指数時間と指数時間の差は，年とともに大きく効いてくる．仮に，コンピュータパワーが年々，指数時間的に向上し，それが続くものとすれば，準指数時間レベルの解読困難性をもつアルゴリズムでは，コンピュータに追いつくためには素数，あるいは合成数を年とともに大幅に増大させることが必要となる．この点，楕円暗号であれば素数（mod p の p）は小幅な増加ですむわけである（図 6 参照）．

表 3　解読時間の比較推定例
Table 3　Comparison of estimated time required for exhaustive attack.

解読時間	楕円暗号	RSA 暗号	共通鍵暗号
30 日	100bit	512bit	56bit
100 万年	170bit	1024bit	80bit
1000 兆年	220bit	2048bit	112bit

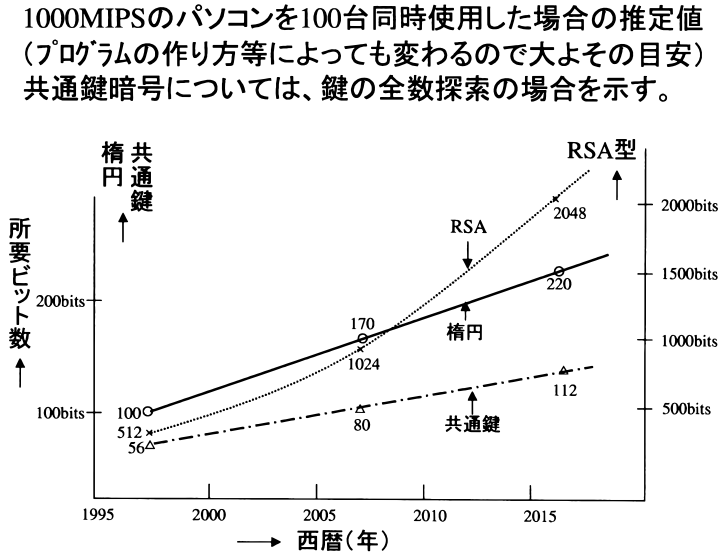


図 6　コンピュータのパワーが毎年 2 倍増と仮定した場合の所要ビット数の経年変化の比較例
Fig. 6　Comparison of required bits of key length.

6. 楕円暗号から超楕円暗号へ

6.1 超楕円暗号とは

超楕円曲線とは楕円曲線を一般化したものであり，体 F の上の超楕円曲線 C は

$$C/\mathrm{F} : y^2 + h(x)y = x^n + a_1x^{n-1} + \cdots + a_n \tag{5}$$

によって定められる非特異な曲線である．体 F の標数 $(Char\mathrm{F})$ について
$Char\mathrm{F} > 2$ のとき $h(x) = 0$ であり

$$y^2 = x^n + a_1x^{n-1} + \cdots + a_0. \tag{6}$$

このとき，

$$g = \begin{cases} \dfrac{n-1}{2} & n : \text{奇数} \\ \dfrac{n-2}{2} & n : \text{偶数} \end{cases} \tag{7}$$

で定められる g を超楕円曲線 C の種数と呼ぶ．

楕円曲線は，$Char\mathrm{F} \neq 2, 3$ のとき式 (6) において $n = 3$，とおいたものであり，また，式 (7) より $g = 1$ であるから，種数 1 の超楕円曲線である．なお，$n = 4$ の場合も双有理変換によって $n = 3$ の曲線，つまり楕円曲線に帰着される．

暗号に直接利用する曲線は有限体上の曲線であるが，見やすくするため，実数体上の場合について，$n = 5$，$g = 2$ の超楕円曲線を示すと図 7 のようになる．数学的な説明は成書を参照して頂くとして，複素数体上では楕円曲線はドーナツ（あるいは 1 人用浮き袋）に対応しており，種数が g の超楕円曲線は，穴が g 個の g 人用浮き袋に対応している．

このように楕円曲線は超楕円曲線の特別の場合といえるが，暗号技術の面からは，超楕円曲線を用いた暗号は，現在，研究途上にあり，いまだ技術として成熟していないこともあって，超楕円暗号という呼び方は

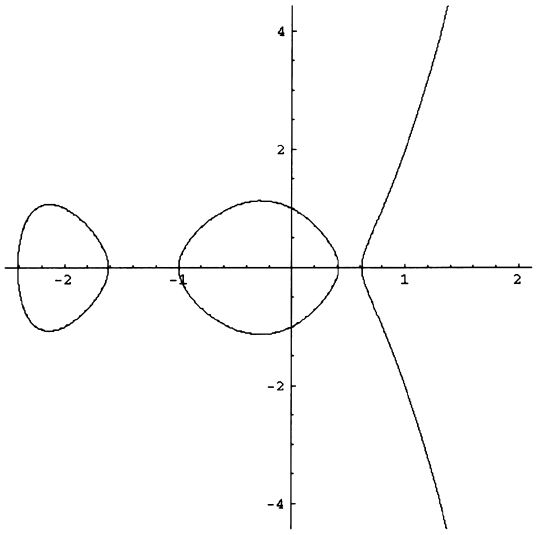


図 7　超楕円曲線の例
$(y^2 = x^5 + 4x^4 + 3x^3 - 3x^2 - 2x + 1)$
Fig. 7　An example of hyperelliptic curve.

余り聞かれず，超楕円曲線あるいは C_{ab} 曲線 [25] のような曲線も含めて，これらの代数曲線を利用する暗号を通常，楕円暗号と呼んでいる．

さて，超楕円曲線を楕円曲線のような形で公開鍵暗号に利用するためには，曲線上の $\mathbf{F}_q$-有理点（$\mathbf{F}_q$ の要素を x, y 座標とする点）の全体から加法群を定義して，加算を効率良く行う必要がある．このため，$g \geqq 2$ の場合は，$\mathbf{F}_q$-有理点そのものではなく，超楕円曲線 C の Jacobi 多様体 $\mathcal{J}(C)/\mathbf{F}_q$ が用いられる．

曲線 C に対して，因子群 $Div(C)$ が定義されることから，Jacobi 多様体 $\mathcal{J}(C)/\mathbf{F}_q$ が，代数群の構造をもつ Abel 多様体として定義されるのである（詳しくは [27], [31] を参照されたい）．

$g = 1$，すなわち楕円曲線の場合は，曲線上の点と Jacobi 多様体の点が 1 : 1 対応している．$g = 2$ の場合は，例えば，複素数体のような代数的閉体についていえば，曲線上の 2 点のペアが Jacobi 多様体の点に対応しているというイメージになる．

超楕円曲線（の Jacobi 多様体）上の離散対数問題，更に一般的な代数曲線 [31]（の Jacobi 多様体）上の離散対数問題も，楕円曲線の場合と同じような形で次のように定義される．

$$Given \quad P, Q \in \mathcal{J}(C),$$
$$find \quad m \in Z \quad s.t. \quad P = mQ$$

6.2　超楕円暗号の利点と安全性

このように定義された超楕円曲線上の離散対数問題も Elgamal 暗号方式に利用できることは明らかであるが，暗号としての安全性や暗号・復号化処理の点で楕円暗号と比較して利点があるのだろうか．

種数 g の Jacobi 多様体 $\mathcal{J}/\mathbf{F}_q$ の位数（要素の個数）$\#\mathcal{J}(\mathbf{F}_q)$ は，

$$(q^{1/2} - 1)^{2g} \leqq \#\mathcal{J}(\mathbf{F}_q) \leqq (q^{1/2} + 1)^{2g} \qquad (8)$$

を満たすことが知られている．上式で，$g = 1$ とおけば，

$$q - 2\sqrt{q} + 1 \leqq \#C \leqq q + 2\sqrt{q} + 1 \qquad (9)$$

となって，楕円曲線上で，Hasse の定理としてよく知られた $\mathbf{F}_q$-有理点の位数がとり得る範囲を示す式が得られる．

そこで，$\#\mathcal{J}(\mathbf{F}_q)$ が十分大きな素数を含むような，ある一定の数 N とすれば，つまり安全性を同程度とすれば，式 (8) において g が大きいほど，有限体の大きさ q は小さくてすむことがわかる．

また，暗号システムの運用上，位数が異なる曲線の数が多いことが望ましいが，その数は，

$$\#\{\mathcal{J}(\mathbf{F}_q)\} = \mathcal{O}(4gN^{1-1/2g})$$

となることが知られている．したがって，同じ定義体でも種数 g の大きい場合は，安全な曲線がより豊富に存在していることがわかる．

楕円曲線にしろ超楕円曲線にしろ，安全な曲線は世界に 1 本あれば十分ではないかという主張も聞かれるので，ここで，安全な曲線を豊富に生成することの意義について触れておきたい．

暗号方式を設計するに際して，同一の曲線あるいは同じ位数を有する曲線であっても，ベースポイント P の取り方を変えることにより，異なる離散対数問題，したがって，異なる ElGamal 暗号を設計することができるから，安全な位数をもつ曲線は 1 本あればよいという主張は確かに一理あるが，運用面からは漠然とした不安を抱くのが暗号センスというものだろう．

また，数理的な面からも，いつでもどこでも同じ曲線を用いることに対して，次のような問題も指摘されている．現在，先に述べたような特殊な場合を除けば，楕円・超楕円暗号に対する最も強力な攻撃法は Baby Step-Giant Step と呼ばれる方法であるが，この攻撃法を拡張することにより，曲線のベースポイントだけ

を変えた離散対数問題を，もとの暗号系のデータベースを生かすことによって，より効率的に解くことができるというものである [32].

こうしたことも考慮すると，楕円・超楕円曲線はできるだけ容易にかつ豊富に生成できることが望ましい．

超楕円曲線上の暗号が，楕円曲線上の暗号に比べてより安全であると推察される状況証拠を挙げておこう．

楕円曲線や超楕円曲線上の点を有理数体上に持ち上げて，index calculus 法により離散対数問題を解く可能性が考えられる．この持上げは極めて困難であり，また仮に成功したとしても有理点の height は爆発的に大きくなり，計算は難しい．更に，rank が大きくなれば，この解法は成功しない．ここまでは，楕円，超楕円の区別なくいえることである．

さて，楕円曲線については，現在発見されている rank の最大値は 20 を少し超える程度であり，現在のところ index calculus 法の適用は不可能であるが，rank の理論上の上界は知られていない．

また，g が 4 以上の場合は，有限体の Jacobi 多様体の持上げは一般に代数体上の Jacobi 多様体にはならないことが，1986 年，関口ら [35] によって示されている．例えば "Canonical Lifting" がないことなどを考えると，超楕円は楕円より持上げは一般的に難しいといえる．1986 年といえば，楕円暗号が提案されたころであり，関口らは工学への応用など念頭になかったに違いないが，こうした数学最前線の知的資産が，現在，暗号の方式設計に一つの示唆を与えているのは興味深い．

しかし，余り g を大きくすると，超楕円曲線上の離散対数問題が準指数時間等に落ちてしまうことが Adleman らによって示されている．1992 年，Adleman ら [23] は

$$\log q < 2g + 1 \tag{10}$$

のとき，index calculus 法の関数体版ともいえる方法によって，準指数時間攻撃が可能であると主張したが，その証明はヒューリスティックな仮定に基づいていた．1997 年，Müller ら [34] は，実 2 次合同関数体の類群が，スムースな，つまり次数の小さな素イデアルによって生成されていることを一般化 Rieman 予想のもとで証明することにより，準指数時間性をより厳密に示している．

なお，楕円曲線について，特殊な位数をもつ場合，Weil 対による定義体の乗法群への埋込みを利用した MOV 還元 [38] により離散対数問題は準指数時間となり，また，位数が定数体の標数と互いに素でない（anomalous，異常な）楕円曲線のそれは，佐藤，荒木ら [39], [40] により多項式時間で解かれているが，これらの攻撃法は Jacobi 多様体に対しても拡張されている．前者については，Frey らにより Weil 対の代わりに Tate 対が用いられ [29]，後者に関しては，Rück が，対数微分を用いて $\mathcal{O}(\log q)$ の時間で，p 可除群上の離散対数を $\mathbf{F}_q^{2g-1}$ に埋め込んでいる [36].

以上のように，超楕円曲線も，特殊な位数や非常に大きな種数を避ければ，現在のところ，解読に要する手間は指数時間であり，かつ，有限体のサイズを一定にすれば，楕円曲線より格段に安全となり，逆に安全性を一定に保つとすれば，有限体のサイズはかなり小さくなって，ハード，ソフトいずれで構成するにしても有利性を秘めている．

そこで，次に考えるべきことは

（i） 安全な超楕円曲線の生成法

（ii） 超楕円曲線上で群演算（加算）を効率良く行うアルゴリズム

の 2 点である．（ii）については Cantor のアルゴリズム [26] をはじめとして多くの研究 [7], [28], [30], [37] が進められているが，本論文では説明を割愛し，（i）について研究動向をみておこう．

6.3 安全な超楕円曲線の生成法

楕円・超楕円曲線の生成法として次の 3 通りを挙げることができる．

（a） Weil Conjecture を用いる方法

（b） Schoof のアルゴリズムなどにより位数を繰り返し計算する方法

（c） 虚数乗法（CM Complex Multiplication）をもつ曲線（CM 曲線）を用いる方法

（a）の Weil Cojecture を用いる方法 [45] は，もともと標数の小さな体上で定義された楕円曲線を拡大体へ持ち上げる方法であり，得られる曲線数が少なく，また，任意の位数を得がたいという制約がある．超楕円曲線についても Koblitz によって生成されている．

（b）の Schoof のアルゴリズムとは与えられた曲線の位数を計算するアルゴリズムである [43], [44]．計算した結果位数を得ることができるが，この位数が大きな素数を含む（almost prime な）数でなければ，安全な暗号系を構成することはできない．Almost prime とは，大きな素数以外は小さな因数からなる合成数である．このような位数を得るまで，多数回の計算を行

う必要があるのが，方法（b）の欠点である．

楕円曲線については，Schoofのアルゴリズムと計算環境の改良により，almost primeな曲線を得るまでの時間は年々短縮されており，学会の場でも時間短縮競争が続いている．

超楕円曲線についても位数を計算する方法が研究されているが，現在知られているアルゴリズムでは，例えば，計算量が $\mathcal{O}((\log p)^{g^6})$ のように [24]，種数の指数時間オーダとなっている．現在のところ，超楕円曲線については，位数計算法が実用的になる見込みは立ってない．

（c）のCM曲線を利用する方法では，まず，代数体上のCM曲線を構成する．(a), (b) の二つの方法はいずれも有限体上のみに閉じた世界で曲線を生成していた．暗号に利用するのは有限体上の曲線であるから，うまくいけばそれでよいのだが，不十分であれば，いったん世界を拡げてみることが有効な場合も少なくない．

楕円曲線 E が任意の整数 n に対して n 倍写像以外の自己準同型写像をもつとき E は虚数乗法（CM）をもつという．超楕円曲線の場合もこれを拡張した形でCMをもつ曲線が定義される．

なお，虚数乗法という呼び方は，複素数体上の場合は，周期（楕円曲線は楕円関数でパラメトライズされ，楕円関数は2重周期関数である [41]）が複素数倍の場合もあるということで直観的にわかりやすいが，一般の体上の場合にも，この呼称を拡張して用いていることに注意されたい．

CMによる方法では，あらかじめ，代数体上で曲線を構成した上で，還元された有限体上で安全な位数をもつように，これを有限体上に還元するのである．代数体上のCM曲線をうまく構成できれば，短時間に安全な曲線が生成できる効率の良い方法である．

楕円曲線に対するCM法については，その実用的意義を評価する声も高い反面，曲線にCMをもつというような制限することは望ましくないという感覚的批判を受けやすい．しかし，楕円曲線の場合は，Schoofのアルゴリズムによる方法も高速化が進んでいるのに対し，超楕円曲線については，位数計算法はいまだ実用にはほど遠い．したがって，数学的にも未開拓ともいえる超楕円曲線についての知見を広げるためにも，CM法による生成法の研究を進めることは有意義であろう．

7. 楕円暗号の魅力

暗号は，サイバースペースという無色透明な世界で自己証明を行い，相手を確認し，なりすましや文書の改ざん・偽造を防ぎ，情報の盗取を防止するための基盤技術である．そのため，我田引水的表現になるが，様々な技術の中で，暗号ほど学際的・業際的な分野も珍しく，暗号技術を中心に電子決済，電子法制，国際情報戦略の歴史と将来，情報倫理などの社会的課題へと果てしなく興味は広がっていく．その一方で，暗号理論，特に楕円暗号は数学との交わりを深めており，Gauss，Jacobi，Abelなど数学史上の巨人達が築いてきた数論や楕円曲線論のような奥深く美しい理論がインターネットの普及等をきっかけに，正に唐突に電子社会に利益をもたらす技術に利用され始めたのである．

数年前，Fermatの最終定理（予想）が360年ぶりに解決されたことは記憶に新しいが，それは，代数的整数論の範囲では遂に決着を見ることなく，「楕円曲線はモジュラーであろう」という谷山・志村・Weil予想のWilesによる本質的解決の副産物として証明された．そのきっかけは，n を3以上の自然数として，

$$a^n + b^n = c^n$$

を満たす自然数解 a, b, c の存在問題が，Freyにより

$$y^2 = x(x - a^n)(x - b^n)$$

なる楕円曲線が存在するかという問題に言い換えられたことによって与えられた．その数学者Freyらも暗号に適した超楕円曲線の生成法について研究を続けている．Freyに限らずこうした気鋭の数学者に対して，工学者がどこまで活動できるのかと思われるかも知れないが，工学者は，技術に対する感覚や価値観が純粋数学者と異なる面もあり，実用的理論を構築するためには，両者が緊密に協力することが望ましい．

楕円暗号は難解な分野であるだけに誤解もされやすい．例えば，極めて特殊な楕円曲線上の離散対数問題が多項式時間で解かれたというニュースに，暗号研究者（楕円を専門としない）までが，“楕円も危ないのではないか” という反応を見せたりする．こうした誤解を防ぎ，楕円暗号の安全性に対する正しい認識を広めるためにも数学系・工学系の研究者が協力していくべきであろう．

8. 楕円曲線と楕円暗号へのブックガイド

暗号全般については文献 [1] の巻末にあるブックガ

イドを見て頂くとして，まず，楕円曲線について寝転んで（失礼）読める本として，文献 [4], [5] を薦めたい．数学的背景は最小限にして，楕円暗号そのものを早く理解したい人には文献 [6] が良いようだ．数論については高木貞治の名著 [8] は今でも健在だが，最近，文献 [9]〜[11] をはじめ多くの読めばわかる（?）良書が出版されている．代数幾何については文献 [12] の第 II 部第 1 章（第 2 章の代数曲面は飛ばして），第 3，4 章が面白い．2 次元以上のトーラスが，どのような条件のもとで代数多様体となるかがスリリングに導かれている（これは楕円曲線ではなく超楕円曲線に関係した話だが）．同一著書（上野）による文献 [13] も平易に書かれているが「デカルトの精神 ···」のような魅力はやや薄れている．

楕円曲線の本ならいくらでも書けると Lang が "Elliptic Curves: Diophantine Analysis"（Springer, 1978）の序文にて書いているが，和訳も出ている本としては [14]〜[16] が挙げられる．そのほか，本特集号の桂による "代数曲線の基礎" [31] を参照されたい．

超楕円暗号については，文献 [7] の Menezes らによる付録の記述が，抽象論にとどまらず，具体性があって有用であろう．

虚数乗法論についてはこの分野の理論を築いた志村，谷山による文献 [17] が古典的名著であるが絶版となっている．最近，新しい内容が加えられた英語版が出版されている [18]．その後の成果も加えた成書として文献 [19] が挙げられる．

そのほか数論アルゴリズムの文献 [42] など専門書は枚挙にいとまがないが，この辺にとどめておこう．

文　献

[1] 辻井重男，暗号–ポストモダンの情報セキュリティ，講談社（選書メチエ），1996.

[2] N. Koblitz, "Elliptic Curve Cryptosystems," Math. Comp., vol.48, no.177, pp.203–209, 1987.

[3] 水野弘文，情報数理の基礎，培風館，1966.

[4] 足立恒雄，フェルマーの大定理が解けた!，講談社（ブルーバックス），1995.

[5] 加藤和也，解決!フェルマーの最終定理，日本評論社，1995.

[6] A.J. Menezes, Elliptic Curve Public Key Cryptosystems, Kluwer Academic Publishers, 1993.

[7] N. Koblitz, Algebraic Aspects of Cryptography, Springer, 1997.

[8] 高木貞治，代数的整数論第 2 版，岩波書店，1971.

[9] 山本芳彦，岩波講座（現代数学への入門）数論入門 1，2，1996.

[10] 加藤和也，黒川信重，斎藤　毅，岩波講座（現代数学の基礎）数論 1，2，1998.

[11] 黒川重信，栗原将人，斎藤　毅，岩波講座（現代数学の基礎）数論 3，1998.

[12] 飯高　茂，上野健爾，浪川幸彦，デカルトの精神と代数幾何，日本評論社，1993.

[13] 上野健爾，代数幾何入門，岩波書店，1995.

[14] J.S. Tate, "Rational Points on Elliptic Curves," Springer, 1994.（足立，木田，小松，田谷訳，楕円曲線論入門，シュプリンガー・フェアラーク，東京，1995.）

[15] J. Cassels, "Lectures on Elliptic Curves," Cambridge University Press, 1991（徳永訳，楕円曲線入門，岩波書店，1996.）

[16] N. Koblitz, "A Course in Number Theory and Cryptography," Springer.（櫻井幸一訳："数論アルゴリズムと楕円暗号理論入門," シュプリンガー・フェアラーク，東京.）

[17] 志村五郎，谷山　豊，近代的整数論，共立出版，1957.

[18] G. Shimura, Abelian Varieties With Complex Multiplication and Modular Functions, Princeton University Press, 1998.

[19] S. Lang, Complex Multiplication, Springer, 1983.

[20] M. Bellare and P. Rogaway, "Optimal asymmetric encryption," Advances in Cryptology—Proceedings of EUROCRYPTO '94, Lecture Notes in Computer Science, vol.950, pp.92–111, Springer-Verlag, 1995.

[21] T. Okamoto and S. Uchiyama, "A new public-key cryptosystem as secure as factoring," Advances in Cryptology—Proceedings of EUROCRYPTO '98, Lecture Notes in Computer Science, vol.1403, pp.308–318, Springer-Verlag, 1998.

[22] R. Cramer and V. Shoup, "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack," Advances in Cryptology—Proceedings of CRYPTO '98, Lecture Notes in Computer Science, vol.1462, pp.13–25, Springer-Verlag, 1998.

[23] L.M. Adleman and M.D.A. Huang, Primality Testing and Abelian Varieties Over Finite Fields, Springer-Verlag, 1992.

[24] L.M. Adleman and M.D. Huang, "Counting rational points on curves and abelian varieties over finite fields," Proc. of ANTS-2, Springer-Verlarg, LNCS1122, pp.1–16, 1996.

[25] S. Arita, "Public key cryptosystems with C_{ab} curve (II)," IEICE, Symposium on Cryptography and Information Security, SCIS '98, 7.1-B, 1998-1.

[26] D. Cantor, "Computing in the jacobian of hyperelliptic curve," Math. Comp., vol.48, pp.95–101, 1987.

[27] D. Cantor, "On the analogue of the division polynomials for hyperelliptic curves," J. Reine Angew. Math, vol.447, pp.91–145, 1994.

[28] S.D. Galbraith, S. Paulus, and N.P. Smart, "Arithmetics of of superelliptic curves," preprint, 1998.

[29] G. Frey and H. Rück, "A remark concering mdivisibility on the discrete logarithm in the divisor class group of curves," Math. of Comp. vol.42, no.206,

pp.865–874, April 1994.
[30] M.D. Huangs and D. Ierardi, “Efficient algrithms for the Riemann-Roch probrem and for addition in the Jacobian of a curve,” Proc. of 21st ACM Symp. on FOCS, pp.678–687, May 1991.
[31] 桂　利行，“代数曲線の基礎,” 信学論（A），vol.J82-A, no.8, pp.1191–1199, Aug. 1999.
[32] K. Kurotani, K. Matsuo, J. Chao, and S. Tsujii, “Consideration of security of hyperelliptic cryptosystems,” IEICE Symposium on Cryptography and Information Security, SCIS ’98, 4.1-D, Jan. 1998.
[33] V.S. Miller, “Use of elliptic curves in cryptography,” Advances in Cryptology Proc. of Crypto ’85, LNCS, 218, Springer-Verlag, pp.417–426, 1986.
[34] V. Müller, A. Stein, and C. Thiel, “Computing discrete logarithms in real quadratic congruence function fiels of large genus,” Mathematics of Computation, vol.68, pp.807–822, 1999.
[35] F. Oort and T. Sekiguchi, “The canonical lifting of an ordinary jacobian variety need not be a jacobian variety,” J. Math. Soc, Japan, vol.38, no.3, 1986.
[36] H.Rück, “On the discrete logarithm in the divisor class group of curves,” Mathematics of Computation, vol.68, no.226, pp.805–806, April 1999.
[37] E.J. Volcheck, “Computing in the Jacobian of a plane algebraic curve,” Proc. of ANT-1, pp.221–233, LNCS-877, 1994.
[38] A. Menezes, S. Vanstone, and T. Okamoto, “Reducing elliptic curve logarithms to logarithms in a finite fields,” Proc. of STOC, pp.80–89, 1991.
[39] T. Sato and K. Araki, “Fermat quatients and the polynomial time discrete log algorithm for anomalous elliptic curves,” Commentarii Math. Univ. Santoti, Pauli, vol.47, no.1, pp.81–92, 1998.
[40] N.P. Smart, “The discrete logarithm problem on elliptic curves of trace one,” to appear in Journal of Cryptology.
[41] 笠原正雄，“格子理論とその応用へのガイダンス,” 信学論（A），vol.J82-A, no.8, pp.1239–1252, Aug. 1999.
[42] H. Cohen, “A course in computational algebraic number theory,” GTM 138, Springer-Verlag, New York, 1993.
[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] R. Schoof, “Counting points on elliptic curves over finite fields,” Journal de The’orie des Nombres de Boreaux 7, pp.219–254, 1995.
[45] T. Beth and F. Schaefer, “Non supersingular elliptic curves for public key cryptosystems,” Advanced in Cryptology-EUROCRYPT ’91, pp.316–327, 1991.

（平成 11 年 3 月 19 日受付）

辻井　重男　（正員）

昭 33 東工大・工・電気卒．中大教授．東工大名誉教授．本会会長等歴任．郵政省電波管理審議会委員．本会功績賞，大川出版賞等受賞．著書「暗号—ポストモダンの情報セキュリティ」（講談社メチエ選書）など．

趙　　晋輝　（正員）

昭 57 中国西安電子科技大・電子卒．昭 63 東工大大学院博士課程了．工博．平 1 東工大助手．平 4 中央大助教授．平 8 同教授．楕円暗号理論，適応信号処理，3D 画像，ヒューマン情報処理などの研究に従事．本会論文賞（昭 63，平 2）．