公開鍵暗号の最近の話

1 楕円曲線暗号の安全性について

岡本 龍明　内山 成憲
NTT情報通信研究所

暗号技術の革命—公開鍵暗号—

インターネットのようなオープンなネットワークで通信や商取引を行うとき，大きな問題となるのは，不特定な相手（それまで何の面識もない相手）といかに安全な（秘匿性のある）通信を行うか，また相手もしくは相手のメッセージが本当に正しいものかをどのように確かめるかといったことである．このようなインターネット時代に我々が直面している問題を解決してくれるのが公開鍵暗号であり，一方，公開鍵暗号の概念を使わないでこのような問題を解決することは難しいように思われる．つまり，電子商取引や電子マネーを実現する上で，公開鍵暗号は必須の技術なのである．

このような公開鍵暗号の概念は，1976年にDiffieとHellmanにより提案された．公開鍵暗号の発見のインパクトは計り知れないほど大きく，これによりそれまでの暗号とは一線を画す「現代暗号」とでも呼べる1つの学問分野が創始されたといっても過言ではない．

さて，公開鍵暗号には，大きく秘匿通信のための機能（狭義の公開鍵暗号）と認証の機能（いわゆるディジタル署名）に分けられるが，本稿では秘匿機能，つまり狭義の公開鍵暗号を中心に話を進めることにする．

DiffieとHellmanの論文以来，どのように公開鍵暗号を実現するかが大きな関心を集めてきた．そのため，この20年以上の間，数学や計算機科学，情報理論，電気通信工学といったさまざまな分野から多くの研究者が実にさまざまなアイデアを提案してきた．しかしながら，その中の多くの方式がすでに破られており，現時点において実用的でありかつ安全であると思われている方式はそれほど多くない．現在，安全で実用的であると考えられている（つまり実際に広く使われている）公開鍵暗号は，いずれも整数論の問題に基づいた方式である．しかも，使われる整数論の問題は通常2つだけである．1つは，（通常の整数の）素因数分解問題であり，もう1つは，（ある有限群の）離散対数問題である．このように非常に特定の問題の上でしか実用的かつ安全な公開鍵暗号がうまく構成できないことは，ある意味で驚くべきことである．

一方，暗号の歴史は，暗号方式を作る・解読するという繰り返しであった．しかし，このようなことを単に繰り返しているだけでは，この分野はいつまでたっても技法（art）の集まりの域を出ない．暗号を1つの体系だった学問分野とするためには，暗号の要である安全性に対する深い理解と理論化が必要とされることはいうまでもないだろう．そのような方向を目指して，1980年代初めより公開鍵暗号の安全性を理論的に定式化して，ある種の暗号方式が安全であることを証明しようという理論研究が着実に進展してきた．

最近，以上のような公開鍵暗号の研究分野において，さまざまな興味深い進展がありこの分野の研究者の関心を集めている．そこで，本稿では，2回に分けて最近のこの分野の進展について解説しよう．ポイントは，以下である．

1. 最近よく耳にする楕円曲線暗号とはどういうものか？
   また，楕円曲線暗号の安全性（解読法）の現状は？
2. 公開鍵暗号が安全である（安全でない）とはどういう意味か？
   安全であることをどのように定義するか？　また，証明するか？
   安全であると証明された公開鍵暗号にはどのようなものがあるか？

今回は1．の楕円曲線暗号について解説しよう．2．については次回解説する．

公開鍵暗号とは

まず，公開鍵暗号の原理について簡単に紹介しておこう[10]．現在，我々がインターネットなどで利用する暗号技術は大きく2つの方式に分類できる．1つは，秘密鍵暗号方式であり，もう1つは公開鍵暗号技術である．

秘密鍵暗号（共通鍵暗号ともいう）とは，暗号化するための鍵（暗号化鍵）と復号化するための鍵（復号化鍵）が同一である．つまり，ドアを閉めるための鍵（暗号化鍵に対応）と開けるための鍵（復号化鍵に対応）が同一であるという意味で，通常のドアや金庫の鍵と同じである．

秘密鍵暗号では送り手と受け手で同じ鍵を持つ必要があるので，暗号通信をする前に外部に盗まれないように鍵データを配送し，通信者が同じ鍵データを保有する必要がある．しかも，通信する相手ごとに，鍵データを共有しなくてはならない．このため，複数のユーザと通信する場合は，通信相手の数だけ，鍵データを保管しなくてはならない．インターネットでの通信のように，それまで一面識もない不特定の相手と突然暗号通信を行いたいといったような場合，どのように鍵データを送るかが問題となることに注意しよう．

この鍵配送の問題を解決する暗号方式が，公開鍵暗号である．公開鍵暗号では，暗号化するための鍵（暗号化鍵）と復号化するための鍵（復号化鍵）が異なり，そのうちの暗号化鍵を公開し，それに対応する復号化鍵は秘密に保持する．つまり，ドアを閉める鍵だけを公開し，開ける鍵は秘密にする．これにより，誰でもオートロックのドアを閉められるように公開の暗号化鍵を用いて暗号文を作り送ることが可能となった．そして，その暗号文を復号できるのは，秘密鍵を持っている本人のみである．

公開鍵暗号を実現するには，公開鍵と秘密鍵という別の鍵を利用して，暗号化したものを復号するという循環性を保持する必要性があるため，単にデータをかき混ぜるといった仕掛け（秘密鍵暗号は主にこの仕掛けだけで構成可能である）だけではなく，ある程度数学的な構造の入った仕掛けが必要となる．このような仕掛けとしては，整数論に基づくものと組合せ論に基づくものに大別できるが，先に述べたように現在実用に使われている公開鍵暗号はいずれも整数論に基づいている（組合せ論に基づく方式はほとんどがすでに解読されているか，実用的でないかのいずれかであり，現在のところ実用化されているものはほとんどない）．

整数論に基づく仕掛けとしては，素因数分解問題に基づく方式と離散対数問題（およびその類似問題）に基づく方式に大別できる．

素因数分解問題とは，整数Nを与えてその素因数を求める問題である．たとえば，15が与えられたとき，15の素因数である3と5(15=3×5)を求めることである．この問題は，Nの桁数が大きくなると（たとえば，10進数で300桁），大変難しい問題となる．

離散対数問題とは，$Y=G^X \bmod P$としたとき，(Y, G, P）からXを求める問題である．なお，ここでPは素数として，$A=B \bmod P$は，BをPで割った余りがAであることを意味する．たとえば，$5=47 \bmod 7$である．離散対数問題の例としては，(1, 4, 7）が与えられたとき，その離散対数は，3となる．なぜならば，$1=4^3 \bmod 7$であるから．ここで，この離散対数問題は，有限体（たとえば，$\mathbf{F}_7$）の乗法の上で定義されていることに注意されたい．

離散対数問題は上で紹介したような有限体の乗法の上（乗法群）以外でもさまざまな演算（有限群）の上で定義できる．たとえば，楕円曲線と呼ばれる3次の代数曲線上の点の間で演算が定義できる（通常，楕円曲線上の加法と呼ばれる）．この楕円曲線上の加法に関する離散対数問題を楕円離散対数問題と呼ぶ．

素因数分解問題に基づく公開鍵暗号としては，RSA暗号方式，Rabin暗号方式，EPOC暗号方式などがある．また，離散対数問題に基づく公開鍵暗号としては，Diffie-Hellman鍵配送方式，ElGamal暗号方式，Cramer-Shoup暗号などがある（EPOC暗号，Cramer-Shoup暗号については，安全性の証明のついた方式として次回紹介する）．

楕円曲線と楕円離散対数問題について

楕円曲線の理論は数学の中でも最も美しくかつ重要なものの1つであり，また20世紀数学を代表する理論でもある．その深遠さについては，数年前にA. Wilesによって完成されたフェルマーの大定理の証明が楕円曲線の理論に基づいていることなどからその一端を伺うことができよう．ただし本稿では紙数などの制約から楕円曲線の理論そのものについては述べず，単に暗号への応用のみを紹介しよう．なお，楕円暗号が登場する以前に暗号で使われた数学は（19世紀初頭に完成していた）初等整数論がほとんどであり，楕円曲線は20世紀の数学が暗号に使われた最初の例である．

楕円曲線とは，ある体の要素となるx, yに関して$y^2=x^3+ax+b$で表せる3次曲線であり（a, bは曲線のパラメータ），この曲線上の点に仮想的な無限遠点を加えた点の集合の上で群が定義できる[17), 9), 10)]．楕円曲線暗号を構成するときは，有限体$\mathbf{F}_q$上の楕円曲線を用いる．上記3次式を満足する$(x,y) \in \mathbf{F}_q^2$と無限遠点を加えたもの，すなわち$\mathbf{F}_q$-有理点の集合を$E(\mathbf{F}_q)$と表記する．また，楕円曲線上の2点の間の群演算（楕円曲線上の加法と呼び，+と表記する）が定義され，無限遠点がその加法演算の単位元（零元）になる（**図-1**）．

この加法により楕円曲線$E(\mathbf{F}_q)$は有限可換群になる．

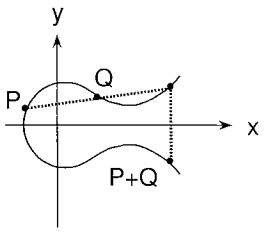

図-1　楕円曲線上の加法

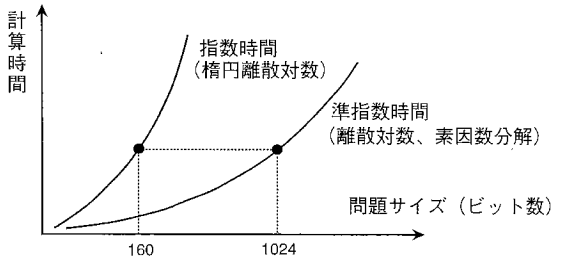

図-2　計算時間と鍵サイズの比較

この有限群$E(\mathbf{F}_q)$の元の数は，$q+1-t\,(2\sqrt{q}\le t\le 2\sqrt{q})$となる．元の数は，有限群を特徴付ける最も重要なパラメータであり，暗号に利用したときの安全性がこのパラメータにより定まる．このとき，tの値は，トレースと呼ばれる．

有限群$E(\mathbf{F}_q)$上では，有限体の乗法群と同様に離散対数問題が定義され，それを楕円離散対数問題と呼ぶ．つまり，$E(\mathbf{F}_q)$上の元（点：ベースポイント）をG，ならびにxを正整数，$Y=xG(=G+\ldots+G$: つまりGをx回加算したもの）とすると，$E(\mathbf{F}_q)$上の離散対数問題とは，$(E(\mathbf{F}_q), G, Y)$が与えられたとき，xを求める問題である．

楕円曲線暗号とその利点

楕円曲線暗号（楕円暗号と省略されて呼ばれることも多い）は，1985年にアメリカの数学者であるKoblitzとMillerにより独立に提案された方式である．彼らは，乗法群上の離散対数問題に基づき構成された暗号方式を楕円離散対数問題上で再構築する方法を提案した．これが，いわゆる楕円曲線暗号である．たとえば，Diffie-Hellman鍵配送方式やElGamal暗号方式に基づき，楕円Diffie-Hellman鍵配送方式や楕円ElGamal暗号方式が作れる．したがって，楕円曲線暗号とは，特定の1つの方式を意味するわけではなく，楕円Diffie-Hellman鍵配送方式や楕円ElGamal暗号方式など楕円離散対数問題に基づき構成された暗号方式の総称であることに注意されたい．

楕円曲線暗号が注目を集めている理由は，通常の（有限体の乗法群上の）離散対数問題に比べ楕円離散対数問題がより難しい問題と考えられている（期待されている）ことによる．

通常の（乗法群上の）離散対数問題および素因数分解問題は，指数計算法（index calculus）という強力な手法が適用でき，計算時間が準指数時間となるような解読法を持つ[9), 16)]（準指数時間とは，問題のサイズがnのとき，計算時間が$2^{cn^{1/3}}$のように，nのべき根のオーダーが指数となるものである．cはある定数）．

ところが，楕円離散対数問題に対しては，現在のところ計算時間が指数時間の解読法しか見つかっていない（指数時間とは，問題のサイズがnのとき，計算時間が2^{cn}のように，nのオーダーが指数となるものである）．ただし，指数時間とはいっても，総当たり攻撃（2^n）よりは効率的な解読法が知られている（Pohlig-Hellman-Silverアルゴリズム[11)]，ShanksによるBSGS（baby-step-giant-step）アルゴリズム[15)]などで，$2^{n/2}$のオーダーである）．

離散対数問題や素因数分解問題が指数計算法に対して解読困難であるためには，その問題のサイズが少なくとも1024ビット程度であることが必要とされている．つまり，それらの問題に基づくRSA暗号方式やDiffie-Hellman鍵配送方式，ElGamal暗号方式の鍵のサイズは，少なくとも1024ビット程度である必要がある．

ところが，楕円離散対数問題では指数計算法が適用できないために，同等の安全性を確保するために問題のサイズがたった160ビット程度で十分なのである．つまり，楕円曲線暗号（楕円Diffie-Hellman鍵配送方式，楕円ElGamal暗号方式）の鍵のサイズが160ビット程度でいいことになる（**図-2**）．

また，鍵サイズが短くできることに応じて，処理速度が高速となる．たとえば，RSA暗号方式やDiffie-Hellman鍵配送方式，ElGamal暗号方式に比べて，楕円曲線暗号の暗号処理時間は数倍から100倍程度高速となる．したがって，楕円曲線暗号は，ICカードのようにメモリサイズならびに処理能力が限定された装置に適した方式といえよう．

楕円曲線暗号の攻撃法（安全でない曲線）

先ほど述べたように，楕円曲線暗号は，1985年にKoblitzとMillerによって独立に提案されたが，彼らはいずれも特殊な楕円曲線を利用することを提案した．それは，超特異（supersingular）と呼ばれる曲線である．先ほど述べたように楕円曲線$E(\mathbf{F}_q)$の元の数は，$q+1-t$となるが，トレースtがとり得る範囲$(-2\sqrt{q}\le t\le 2\sqrt{q})$のちょうど真ん中であるとき，つまりトレース$t=0$のときが超特異である（もう少し正確には，$\mathbf{F}_q$の標数を$p$としたとき，$t\equiv 0 \pmod p$のときである）．彼らが，楕円曲線暗号を構成するために超特異曲線を推奨した理由は，それが最も代表的であり

かつよく研究されている曲線であるため曲線のパラメータを容易に選定できること，また元の数がq+1と自明であること（さもなくば，tを計算する必要がある），群構造が分かっており，たとえば$\mathbf{F}_q$が素体の場合は$E(\mathbf{F}_q)$が巡回群であること（離散対数の群のサイズが，qと同等のサイズであることが保証されている．さもなくば，最悪の場合，離散対数の群のサイズがqの半分程度にまでなることがあり，その場合qを2倍程度大きくする必要が生じる），暗号・復号演算を高速化する特殊な手法が使えるなどの理由による．

ところが，1990年にMenezes，岡本，Vanstoneは，超特異楕円曲線上の離散対数問題に対して準指数時間の解読法があることを発見した[6]．それまで，楕円離散対数問題に対しては，指数時間の解読法しか知られていなかったこと，ならびにKoblitz，Millerにより超特異曲線が楕円曲線暗号の構成に推奨されていたことの両面からこの発見は注目された．彼らの手法は，Weil対（Weil pairing）を用いて，超特異曲線の楕円離散対数問題を効率よく（通常の）離散対数問題に帰着させるものである（MOV帰着）．

1997年，今度は素体（要素数が素数pである有限体）$\mathbf{F}_p$上でトレースが1の楕円曲線（anomalous 曲線と呼ばれる）に対する解読法がSmartおよび佐藤，荒木により独立に発見された[18), 13)]．後に，Semaevがすでに同様の結果を得ており，論文誌に投稿済みであったことが分かったため[14)]，この解法はSemaev–Smart–佐藤–荒木（SSSA）アルゴリズムと呼ばれる．なお，Semaevの手法は代数幾何学的であり，Smartおよび佐藤–荒木の手法は代数的整数論的である．これらの解法は，大変効率がよく多項式時間（サイズの3乗）である．Semaevの結果は，Rück[12)]によって，楕円曲線上の群の一般化であるJacobi多様体上の離散対数問題に対して一般化された．

一方，1994年にFrey[☆1]とRückは，MOV帰着を一般化し，Jacobi多様体上の離散対数問題を通常の（乗法群上の）離散対数問題に帰着させる方法を示した[4)]．この帰着では，Weil対の代わりにTate対を用いており，ここではこの帰着をFR帰着と呼ぶことにする．

さらに，1998年に内山と齋藤[19)]は，MOV帰着とFR帰着の効果の比較によって，トレースが2の楕円曲線上の楕円離散対数問題に対してのみMOV帰着とFR帰着は差があり，それ以外では等価であることを示した．つまり彼らは，トレースが2のときにはMOV帰着は有効でないが，FR帰着により準指数時間の解読法があることを明示的に示した（ここでは，これをUSアルゴリズムと呼ぶ）．

また，一般に，MOV帰着（FR帰着）が超特異曲線以外のどういうクラスの楕円曲線に対して効果的であるか，あまり知られていなかったが，最近，Balasubramanian，Koblitz[2)]によって，楕円暗号によく用いられるパラメータの楕円曲線をランダムに選んだとき，その曲線に対してMOV帰着（FR帰着）が効果的となる確率は非常に小さい（無視できる）ことが示された．

以上のことを特に素体上の楕円曲線で整理すると以下のようになる．

1. トレース0の曲線（超特異曲線）：準指数時間解読法あり（MOV帰着）
2. トレース1の曲線（anomalous曲線）：多項式時間解読法あり（SSSAアルゴリズム）
3. トレース2の曲線：準指数時間解読法あり（FR帰着: USアルゴリズム）
4. それ以外：MOV帰着（FR帰着）が効果的となる曲線は非常に少ない（つまり，現在分かっている手法により準指数時間で解読される曲線は非常に少ない）．

以下で，上の結果のもう少し詳しい解説を行う．

MOV帰着とFR帰着の有効な曲線について

MOV帰着とFR帰着のアルゴリズムを説明することは，本稿の範囲を越えるため行わない（MOV帰着については，文献9），6），7）を，FR帰着については，文献4），19）を参考にされたい）．ここでは，どのような楕円曲線に対してMOV帰着とFR帰着が適用できるかに関する結果のみを述べる．

いま暗号で用いる楕円曲線$E(\mathbf{F}_q)$が与えられたとき，MOV帰着とFR帰着のいずれも，ある適当な拡大次数kを選択し，その楕円曲線Eの$\mathbf{F}_{q^k}$–有理点の集合$E(\mathbf{F}_{q^k})$から拡大体の乗法群$\mathbf{F}^{\times}_{q^k}$への埋め込み写像（Weil対およびTate対を使った写像）を利用する．さて，ここでこれらの帰着を実際に使って離散対数を解く場合に問題となるのは，kがどの位の大きさの値であるかということである．

つまり，もしkが非常に大きい値であった場合（たとえば，k=100であったとしよう），楕円離散対数問題が通常の（乗法群の）離散対数に帰着できても，100次拡大体$\mathbf{F}_{q^{100}}$上の離散対数問題（qのサイズを160ビットとした場合16000ビットのサイズの離散対数問題）を解く必要がある．明らかに，この場合は帰着を用いないで直接楕円離散対数問題を解いた方が効率的であることはいうまでもないだろう．

それでは，どのような曲線に対してkが小さな値となるのであろうか？　まず楕円曲線$E(\mathbf{F}_q)$が超特異の場合は，MOV帰着に関して$k \leq 6$であることが示された[6)]．すなわち，この場合には，$\mathbf{F}_{q^k}$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（特に，素体の場合には，k=2である）．

☆1 Frey曲線の提案により，A. WilesによるFermatの最終定理の解決のきっかけを作ったG. Freyである．

$k < \log q$であれば，現在の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って，$|q|$の準指数時間アルゴリズムとなることが示せる[19]．一方，素体$\mathbf{F}_q(q>2)$上定義された楕円曲線で，その元の数が素数となるものに対しては，そのような楕円曲線をランダムに選んだとき，MOV帰着が準指数時間アルゴリズムとなる確率Probの評価が$\mathrm{Prob} < O\left(\frac{(\log q)^9 (\log\log q)^2}{q}\right)$で与えられた[2]．すなわち，このような楕円曲線をランダムに選んだ場合，MOV帰着が効果的となる確率は無視できるほど小さいことが分かる．

次に，MOV帰着とFR帰着が有効となる（小さな拡大次数kを持つ）曲線を比較しよう．そのために，まず楕円曲線が超特異でないとして，MOV帰着の場合のkに関する必要十分条件を以下に示そう[2), 19)]．ここで，lは$\sqrt{q}$よりも十分に大きい素数とし，lは$E(\mathbf{F}_q)$の元の数$(q+1-t)$の約数とする$(l|(q+1-t))$．

定理1

$E(\mathbf{F}_q)$にMOV帰着が適用可

$$\Leftrightarrow \begin{cases} q^k \equiv 1 \pmod{l},\ l \nmid (q-1), \\ k \equiv 0 \pmod{l},\ l \mid (q-1). \end{cases}$$

また，FR帰着の場合の拡大次数に関する必要十分条件は以下である[4), 19)]．

定理2

$E(\mathbf{F}_q)$にFR帰着が適用可$\Leftrightarrow q^k \equiv 1 \pmod{l}$．

以上より，MOV帰着とFR帰着で差があるのは$l|(q-1)$の場合だけであることが分かる．このとき，lの大きさなどの条件よりトレースtが2となることに注意．

この場合$(l|(q-1))$，MOV帰着では$k \equiv 0 \pmod{l}$がkに対する必要十分条件である．このとき明らかにkはlと同等以上の大きさとなり（入力サイズの指数オーダーとなり），MOV帰着は有効でないことが分かる．

一方，FR帰着では，$q^k \equiv 1 \pmod{l}$がkに対する必要十分条件である．この場合$(l|q-1)$，$k=1$はこの必要十分条件を満足する．つまり，FR帰着では拡大次数1で（つまり，元の体$\mathbf{F}_q$のままで）楕円離散対数問題を$\mathbf{F}_q^{\times}$上の離散対数問題に帰着できることになる．

よって，次の結果を得る[19]：

定理3

MOV帰着とFR帰着の効果は，トレース2の楕円曲線を除き等価である．つまり，楕円離散対数問題において，トレース2の楕円曲線のみがFR帰着が有効でかつMOV帰着が有効でない楕円曲線である．

これによって，楕円離散対数問題に関するFR帰着の存在意義は，トレース2の楕円曲線に対してのみにあることが分かる．

まとめ

実際に楕円暗号に使われている楕円曲線は，その定義体の標数が2でない場合は，素体の場合が多いので，楕円暗号として安全でない特殊な楕円曲線とそれに対して有効な攻撃法を，素体$\mathbf{F}_q$上の楕円曲線に限って，トレースで場合分けすれば次のようになる：

$$\begin{cases} t=0\ (\text{超特異曲線}) & \Leftarrow \text{MOV帰着(FR帰着)} \\ t=1\ (\text{Anomalous曲線}) & \Leftarrow \text{SSSAアルゴリズム} \\ t=2 & \Leftarrow \text{FR帰着} \\ & \quad (\text{USアルゴリズム}) \\ t\cdots \exists k[q^k \equiv 1 \pmod{l} \wedge k < \log q] & \\ & \Leftarrow \text{MOV帰着(FR帰着)} \end{cases}$$

ここで，lは$\sqrt{q}$よりも十分に大きい素数とし，$l|(q+1-t)$．

また，曲線をランダムに選んだ場合は，MOV帰着やFR帰着が有効となる確率は非常に小さい．

以上，楕円曲線暗号の安全性研究に関する最近の進展について紹介した．紙面の都合で紹介できなかったが，暗号に適した楕円曲線の構成法や高速算法，楕円曲線をより一般化した超楕円曲線などを用いた暗号の研究も活発に行われている[3), 1)]．

楕円曲線暗号の安全性が活発に研究されはじめたのは，1990年代になってからであり，安全性の研究はこれからもさらに大きく進展するだろう．この分野における最も重要な未解決問題は，楕円離散対数問題に対して指数計算法が適用できない本質的な理由があるのかどうかを明確にすることである．

参考文献

1) Adleman, L.M., DeMarris, J. and Huang, M.D.: A Subexponential Algorithms for Discrete Logarithms over the Rational Subgroup of the Jacobians of Large Genus Hyperelliptic Curves over Finite Fields, Proc. of ANTSI, LNCS 877, Springer-Verlag, pp.28-40 (1994).
2) Balasubramanian, R. and Koblitz, N.: Improbability that an Elliptic Curve has Subexponential Discrete Log Problem under the Menezes-Okamoto-Vanstone Algorithm, Journal of Cryptology, 2, 11, pp.141-145 (1998).
3) Chao, J., Matsuda, N. and Tsujii, S.: Efficient Construction of Secure Hyperelliptic Discrete Logarithm Problems, Proc. of ICICS'97, LNCS 1334, Springer-Verlag, pp.291-301 (1997).
4) Frey, G. and Rück, H.G.: A Remark Concerning m-divisibility and The Discrete Logarithm in The Divisor Class Group of Curves, Math. Comp., 62, 206, pp.865-874 (1994).
5) Koblitz, N.: Elliptic Curve Cryptosystems, Math. Comp., 48, 177, pp.203-209 (1987).
6) Menezes, A., Okamoto, T. and Vanstone, S.: Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field, IEEE Transaction on Information Theory, IT-39, 5, pp.1639-1646 (1993).
7) Menezes, A.: Elliptic Curve Public Key Cryptosystem, Kluwer Academic Publishers (1993).
8) Miller, V.S.: Use of Elliptic Curves in Cryptography, Proc. of Crypto'85, LNCS 218, Springer-Verlag, pp.417-426 (1985).
9) 岡本龍明，太田和夫編：暗号・ゼロ知識証明・数論，共立出版

付録：用語の解説

■群と体

群とは，算法（演算）を持った集合で，その算法に関して，結合法則，単位元の存在，逆元の存在が示せるもの．たとえば，“たし算”，“ひき算”が自由にできるような集合．特に，算法が$a+b=b+a$のように可換なものを可換群という．たとえば，整数の全体$\mathbf{Z}=\{\cdots,-1,0,1,\cdots\}$は通常の足し算に関して可換群をなす．

体（可換体）とは，2つの異なる算法を持った集合で，一方を加法，他方を乗法と呼ぶことにすると，加法に関して可換群，その集合から加法に関する単位元（零元）を除いた集合が，乗法に関して可換群をなし，さらに分配法則を満たすものをいう．平たく言えば，“たし算”，“ひき算”，“かけ算”，“わり算”が自由にできる集合のこと．たとえば，有理数の全体は，通常の足し算，掛け算に関して体をなす．また，素数pを法とした剰余類の全体$\mathbf{Z}/p\mathbf{Z}=\{0,\cdots,p-1\}$は，$a+b=a+b \bmod p$，$a\times b=a\times b \bmod p$で定義される算法$+,\times$に関して体をなす．これは有限体と呼ばれ，$\mathbf{F}_p$などと表される．

■準指数時間アルゴリズム

準指数時間アルゴリズムとは，入力のサイズをnとした時，その実行時間が$O(2^{cn^s})$（ただし，s $(0<s<1)$，cは定数）と書けるものをいう．これは，実行時間が$O(n^c)$などと表される多項式時間アルゴリズムと，$O(2^{cn})$などと表される指数時間アルゴリズムの中間的なものである．

■位数が160ビット程度となる楕円曲線の例

前に述べたように，（超特異等の危険な曲線を除く）楕円曲線の群の位数が160ビット程度であれば，その上での楕円曲線暗号は現時点では安全であると考えられている．そこで，群の要素の数（位数）が160ビット程度となるような楕円曲線のパラメータの例を示そう．

まず，有限体$\mathbf{F}_p$上定義された楕円曲線$y^2=x^3+Ax+B$のパラメータとして以下のような値を考えよう．ここではパラメータの値（整数）を16進で表記している．

p = 00446C3B15F9926687D2C40534FDB564000000000097,

A = 000D9F131F7A6840215F073340499D1D4340A43FD1BE,

B = 004148203409922959A1903DEA05D97B18B882E82B72.

この楕円曲線上の$\mathbf{F}_p$–有理点の個数は，0016CEBE5CA886222D46415A71753D65812F9B0B6869となる（この値は，166ビットである）．

この楕円曲線上の点として，たとえば以下のような座標の点$G=(X, Y)$がとれる．

X = 0042F39C1605DB5C6133DD46F92EDF0A762F9E41F86E,

Y = 000B1D4EBA24089591B44137FB2AF4A5924D61C92701.

この点Gの位数（Gで生成される巡回群の位数）は，

016CEBE5CA886222D46415A71753D65812F9B0B6869

となる（この値は，165ビットである）．つまりこのGをベースポイントとして楕円離散対数問題ならびに楕円曲線暗号を構成することができる．

(1995).
10) 岡本龍明, 山本博資著: 現代暗号, 産業図書 (1997).
11) Pohlig, S. and Hellman, M.: An Improved Algorithm for Computing Logarithms over GF(p) and Its Cryptographical Significance, IEEE Trans. Information Theory, 24, pp.106-110 (1978), pp.417-426 (1985).
12) Rück, H.G.: On the Discrete Logarithm in the Divisor Class Group of Curves, preprint (1997).
13) Satoh, T. and Araki, K.: Fermat Quotients and the Polynomial Time Discrete Log Algorithm for Anomalous Elliptic Curves, Commentarii Math. Univ. Sancti Pauli, 47, 1, pp.81-92 (1998).
14) Semaev, I.A.: Evaluation of Discrete Logarithms in a Group of p-torsion Points of an Elliptic Curve in Characteristic p, Math. Comp., 67, 221, pp.353-356 (1998).
15) Shanks, D.: Class Number, a Theory of Factorization, and Genera, Proc. Symposium Pure Mathematics, AMS (1985).
16) Schirokauer, O., Weber, D. and Denny, T.: Discrete Logarithms: The Effectiveness of the Index Calculus Method, Proc. of ANTSII, LNCS 1122, Springer-Verlag, pp.337-361 (1996).
17) Silverman, J.H.: The Arithmetic of Elliptic Curves, GTM 106, Springer-Verlag (1986).
18) Smart, N.P.: The Discrete Logarithm Problem on Elliptic Curves of Trace One, to appear in Journal of Cryptology.
19) Uchiyama, S. and Saitoh, T.: A Note on the Discrete Logarithm Problem on Elliptic Curves of Trace Two, Technical Report of IEICE, ISEC98-27, pp.51-57 (1998).

（平成10年10月13日受付）

訂　正

本誌前号（39巻12号）に掲載されました「公開鍵暗号の最近の話：1. 楕円曲線暗号の安全性について」の中で，p.1256の定理1に誤りがありましたので，下記のとおり訂正させていただきます．

（誤）

定理1

$E(\mathbf{F}_q)$にMOV帰着が適用可

$$\Leftrightarrow \begin{cases} q^k \equiv 1 \pmod{l}\ l \mid /(q-1), \\ k \equiv 0 \pmod{l}\ l \mid (q-1). \end{cases}$$

（正）

定理1

$E(\mathbf{F}_q)$にMOV帰着が適用可

$$\Leftrightarrow \begin{cases} q^k \equiv 1 \pmod{l}\ \ l \nmid (q-1)\text{のとき}, \\ k \equiv 0 \pmod{l}\ \ l \mid (q-1)\text{のとき}. \end{cases}$$