# 代数曲線上の公開鍵暗号

松尾 和人* 有田 正剛† 趙 晋輝‡

## より効率的な公開鍵暗号をめざして

インターネット等の不特定多数ディジタル通信を利用して電子商取引等を安全に行うためには，秘密通信，個人のプライバシーの保護，個人認証等の情報セキュリティ技術が不可欠である．中でも公開鍵暗号アルゴリズムは，このような安全な情報通信サービスを提供する基盤技術として必須のものであり，電子決済，電子政府，電子医療など，社会，生活全般にわたるインフラストラクチャの核となる技術である．

公開鍵暗号アルゴリズムは 1976 年に Diffie と Hellman によって提案された．このアルゴリズムは暗号化と復号に異なる鍵を用いるものであり，更には暗号化に用いる鍵（暗号鍵）を秘匿する必要が無いものである．したがって、このアルゴリズムにより不特定多数間の秘密通信が容易に実現可能となった．

Diffe と Hellman のアルゴリズムは，それまでに知られていた暗号アルゴリズムとは異なり，数論的問題を解くことに要する計算量を安全性の根拠とした．特に彼らは安全性の根拠として以下に示す離散対数問題を用いた．

**定義 1 (離散対数問題)** $G$ を有限可換群，$N$ を $G$ の位数，$\alpha, \beta \in G$ とする．$\alpha = m\beta$ を満足する $m \in [0, N-1]$ を求めよ．

彼等は有限可換群 $G$ として有限体の乗法群を用いた[1]．このとき $\beta$ を固定すれば，$m$ から $\alpha$ は容易に計算可能であるが，$N$ が十分に大きいとき，$\alpha$ から $m$ を求めることは困難である．このような性質を持つ関数を「一方向性関数」という．その後，一方向性関数に整数の素因数分解を用いた RSA 暗号や有限体の乗法群上の離散対数問題を用いた ElGamal 暗号，署名等のアルゴリズムが提案された．1990 年代に入ると，インターネットの長足な発展とともに公開鍵暗号への需要が急激に増加し，RSA 暗号が公開鍵暗号のデファクトスタンダードとして広く利用されるようになった．しかし，整数の素因数分解と有限体の乗法群上の離散対数問題には，共に準指数時間計算量 [3] の解法が知られており，近年のコンピュータ能力の指数関数的な進歩が，RSA 暗号や Dffie-Hellman 暗号，ElGamal 暗号にとって両刃の剣となった．すなわち，計算速度の急激な向上によって暗号解読時間もまた急激に短くなり，安全性確保のために数論的問題のサイズ[2] を準指数関数的に増加させる必要が生じ，結果として暗号化速度の面でコンピュータ性能の進歩を完全には享受できないこととなった．

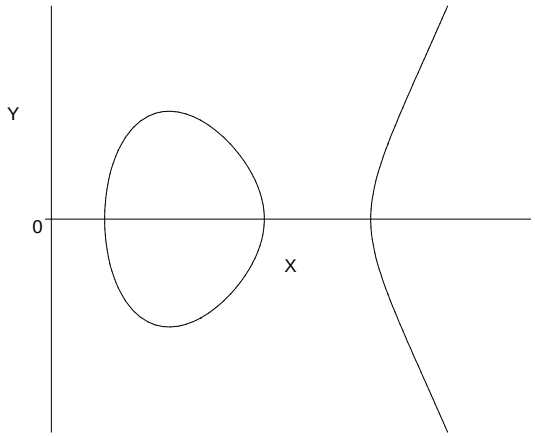


図 1: 楕円曲線の例

このようなコンピュータ性能の進歩によるアルゴリズム性能の劣化が生じない暗号アルゴリズムとして，楕円曲線暗号知られている [1]．楕円曲線暗号は，離散対数問題を定義する有限可換群 $G$ に有限体上の楕円曲線（図 1）の有理点集合を選んだアルゴリズムである．現在に至るまで，注意深く選んだ楕円曲線上の離散対数問題に対しては，指数関数時間アルゴリズム以外の解読アルゴリズムは知られていない．また，このよう

*情報セキュリティ大学院大学
†情報セキュリティ大学院大学
‡中央大学理工学部情報工学科

[1] 乗法群なので離散対数問題は $y = x^m$ を満足する $m$ を求める問題になる．

[2] 例えば離散対数問題では $\log N$

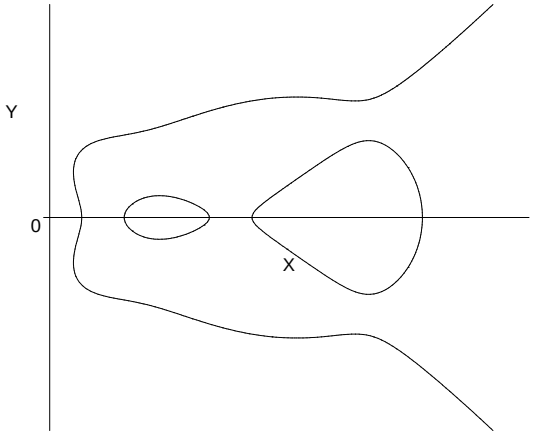


図 2: $C_{45}$ 曲線の例

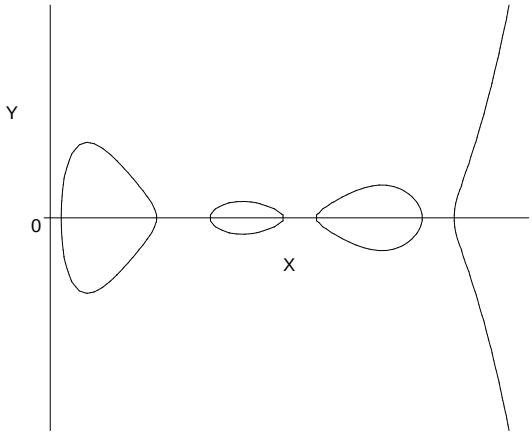


図 3: 種数 3 の超楕円曲線の例

な曲線は豊富に存在する．したがって，楕円曲線暗号は RSA 暗号等の準指数時間の攻撃法が存在する暗号アルゴリズムと比較し明らかに優位なアルゴリズムであるが，最近まで広く実社会において使われることはなかった．この原因の一つに，約十年前までは，現実的な安全性を得るための数論的問題のサイズを最小に固定したとき，RSA 暗号のほうが楕円曲線暗号より高速な暗号化が可能であったことがある．しかし，現在では，楕円曲線暗号に必要なサイズが 160bit であるのに対し，RSA 暗号には 1024bit が必要であるとされており，楕円曲線暗号は RSA 暗号と比較し数十倍高速な暗号化が可能である．また，よりコンパクトな実装が可能である．したがって，最近国内外で盛んに行われている公開鍵暗号の標準化作業では，RSA 暗号と共に楕円曲線暗号がリストアップされるようになった．

楕円曲線暗号は現在では最も優れた公開鍵暗号アルゴリズムであるが，楕円曲線自体は代数曲線の中の非常に小さなクラスの一つに過ぎない．そこで，最近では，より効率的な公開鍵暗号アルゴリズムをめざして，より一般的な代数曲線上の離散対数問題を用いた暗号アルゴリズムの研究も盛んに行われるようになった．

## 楕円曲線，超楕円曲線，$C_{ab}$ 曲線

暗号応用に関して幾らかの結果が知られている代数曲線に $C_{ab}$ 曲線がある．有限体 $\mathbf{F}_q$ 上の $C_{ab}$ 曲線とは以下の定義式をもつ非特異アフィン曲線である（図 2）．

$$C : F(X) = \sum_{0 \le i \le b, 0 \le j \le a, ai+bj \le ab} f_{i,j} X^i Y^j = 0$$

ここで，$f_{i,j} \in \mathbf{F}_q$ であり，$a$ と $b$ は互いに素な自然数である．$C_{ab}$ 曲線に対し「種数」と呼ばれる不変量が $g = \frac{(a-1)(b-1)}{2}$ で定義される．$F(x,y) = 0$ を満足する $\mathbf{F}_q$ の要素の対 $(x,y) \in \mathbf{F}_q$ と唯一の無限遠点 $\infty$ を，$C$ の有理点という．代数曲線の暗号応用では専らこの有理点の集合を扱う．

$\mathbf{F}_q$ 上の種数 $g$ の超楕円曲線 $C$ は，$C_{ab}$ 曲線のサブセットとして，

$$C : Y^2 = X^{2g+1} + \sum_{0 \le i \le 2g} f_i X^i, f_i \in \mathbf{F}_q$$

で与えられる（図 3）．楕円曲線とは，種数が 1 の超楕円曲線のことである．

これらの曲線上で離散対数問題を定義するには，曲線上で有限可換群 $G$ が定義される必要がある．大雑把にいって，$\mathbf{F}_q$ の $g$ 次拡大体上の $g$ 個の有理点の集合を一つの要素とみたとき，それら全体の集合には加法が定義され，この集合は有限可換群になる[3]．したがって，楕円曲線に対しては有理点集合そのものが有限可換群になる．このようにして得られた有限可換群 $G$ 上の離散対数問題を「代数曲線上の離散対数問題」と呼ぶ．また $G$ 上の加法は実際に効率的に計算可能であり，さらに暗号アルゴリズムの速度に直接影響することから多くの研究が行われ，その速度は日進月歩に向上している．

## 代数曲線上の離散対数問題の解法

代数曲線暗号の解読には様々な方法が考えられるが，最も直接的な方法は代数曲線上の離散対数問題を解く

[3]正確な定義は，[2, 6] 等を参照頂きたい．

ことである．代数曲線上の離散対数問題の解法アルゴリズムは大きく二つに分類される．一つは square-root 法と呼ばれる，代数曲線上に限らず離散対数問題一般に適用可能な方法であり，もう一つは代数曲線上の離散対数問題に特化した方法である．Square-root 法は，$G$ の位数 $N$ の最大素因子を $N_{max}$ としたとき，計算量 $O(\sqrt{N_{max}})$ のアルゴリズムである．代数曲線暗号の暗号化速度には $N$ の大きさが影響するので，実装効率を考慮すれば，$N$ はほぼ素数[4]である必要がある．したがって，

1. $N$ はほぼ素数
2. $N$ は十分に大きい（現状では最低 160 bit 程度）
3. その上の離散対数問題に対し，square-root 法より効率的な解法が知られていない

が，安全な暗号系を構成するための曲線 $C$ の必要条件となる．

一方，代数曲線上の離散対数問題に特化した解法には，この離散対数問題を $\mathbf{F}_q$ の拡大体の乗法群上の離散対数問題に変換し，これを解く方法と，$\mathbf{F}_q$ の加法群上の離散対数問題に変換し，これを解く方法が知られている．前者の計算量は準指数時間であり，後者は低次多項式時間である．ただし，これらが効果を持つ曲線は極めて稀に存在するのみである．また，これらが効果を持つか否かは，$N$ から簡単に判定可能である．これらとは別に，種数の大きな曲線に対しては有限体上の乗法群上の離散対数問題に対する準指数時間アルゴリズムの類推が働くことが知られている．このアルゴリズムは，種数が $N$ と共に大きくなるという仮定の下で準指数時間アルゴリズムであるが，固定された $g$ に対しては指数時間アルゴリズムである．また，$g \geq 3$ のとき square-root 法より計算量が小くなる．しかし，種数 3 程度の曲線に対する効果については議論の余地がある．また，$\mathbf{F}_q$ のサイズを通常より大きくとれば，square-root 法に対し必要な耐性よりも大きな耐性を確保でき，安全な暗号系を構成可能である．このように，現実的な安全性の議論には，各解法に対する計算量の詳細評価が必要である．

## 安全な代数曲線の構成

以上で見たように，安全な代数曲線を構成するためには，$N$ を知る必要がある．この $N$ は曲線 $C$ のパラメータ設定により，$q^g$ 付近で変動することが知られており，ランダムに与えた $C$ は高い確率で square-root 法に対する安全性要件を満足しない．逆に，ランダムに与えた $C$ に対する $N$ の計算を $O(\log N)$ 回繰り返せば安全な代数曲線が得られる．したがって，安全な代数曲線の構成には，$C$ に対する $N$ を計算するアルゴリズムが必要である．このアルゴリズムの構成は困難な課題であるが，楕円曲線に対しては効率的なアルゴリズムが提案されており，安全な曲線を豊富に構成可能である [5]．また，$\mathbf{F}_q$ の標数が小さい場合のアルゴリズムは近年目覚しい進歩を遂げ，この場合には，安全な超楕円曲線も豊富に得られるようになった．この分野も暗号応用というモチベーションを得て急速に発展しており，$\mathbf{F}_q$ の標数が大きい場合についても，安全な曲線を豊富に得られる日は遠くないであろう [6]．

## 最近の話題

代数曲線の暗号応用の近年の話題の一つに，楕円曲線等の種数の小さな曲線上の離散対数問題を種数の大きい曲線上の離散対数問題に変換して解く，Weil descent 法と呼ばれる代数曲線上の離散対数問題の解法アルゴリズムがある．これまでのところ，どのような曲線に対しこのアルゴリズムが効果を持つか等不明な点が多く，現在盛んに研究がされている．もう一つの大きな話題に，ペアリング暗号がある．これは代数曲線上の離散対数問題を $\mathbf{F}_q$ の拡大体の乗法群上の離散対数問題に変換して解く際に用いられるペアリングと呼ばれる写像を用いた暗号アルゴリズムであり，逆転の発想といえるもので大変興味深い．これの詳細については提案者等の著書 [4] を参照頂きたい．

[4] 大きな素数と小さな整数の積

### 参考文献


[1] Blake, I., Seroussi, G. and Smart, N.: *Elliptic Curves in Cryptography*, LMS 265, Cambridge U. P. (1999).

[2] Koblitz, N.: *Algebraic Aspects of Cryptography*, Algorithms and Computation in Mathematics, No. 3, Springer-Verlag (1998).

[3] 岡本龍明, 内山成憲: 楕円曲線暗号の安全性について, 情報処理, Vol. 39, No. 12, pp. 1252–1257 (1998).

[4] 笠原正雄, 境隆一: 暗号〜ネットワーク社会の安全を守る鍵, 共立出版 (2002).

[5] 佐藤孝和: 有限体上の楕円曲線の位数計算アルゴリズム, 日本応用数理学会論文誌, Vol. 13, No. 2, pp. 273–288 (2003).

[6] 松尾和人, 有田正剛, 趙晋輝: 代数曲線暗号, 日本応用数理学会論文誌, Vol. 13, No. 2, pp. 231–243 (2003).