超楕円曲線における Weil 数について

永田　清

概要

高度情報化社会において公開鍵暗号は情報の秘匿のみならず，改ざん防止，認証，非否認性などさまざまな応用範囲を持つ。そのような公開鍵暗号方式のうちで，次世代方式と呼ばれているのが超楕円曲線の Jacobi 群によるものである。本論文では，超楕円曲線の構成法を数学的理論との係わりを中心に概観し，その中で重要な役割を果たす Weil 数についての考察を行う。

1. はじめに

公開鍵暗号方式は，1976年に W. Diffie と M. Hellman[1]によって提案された。その原理は，鍵を２つにしてその１つを公開することである。それによって，鍵が１つの暗号方式（“秘密鍵暗号方式”，または“共通鍵暗号方式”と呼ばれる）における鍵配送の問題を解決するだけでなく，現在の情報ネットワーク社会において欠くことのできない，改ざん防止，認証および非否認性などのさまざまな技術への応用が可能になった。

彼等のアイデアは，1978年に３人の数学者 R. Rivest，A. Shamir および L. Adleman[2]によってＲＳＡ公開鍵暗号方式として実現され，現在でも広く使われている。これを第１世代公開鍵暗号方式とすれば，1986年頃 V. Miller[3]と N. Koblitz[4]の二人によって独立に提案された，楕円曲線を用いる方法が第２世代に当たる。ＲＳＡ方式の概略，楕円曲線法のＲＳＡ法に対する利点，および虚数乗法をもつ楕円曲線の生成などに関しては[5]で述べたが，ここでも超楕円曲線との関係で復習しておこう。

ＲＳＡ法の計算が行われる領域（ここでは“場”と呼ぶことにする）は整数の剰余環であり，ある決められた元のべき乗が計算される。それは，共通鍵暗号方式のほとんどが２進数の足し算と論理演算を繰り返すだけであることに比べると，非常に大きな計算量を必要とする。復号化の原理は Euler の定理であり，公開鍵に対応する秘密鍵を見つけるためには，剰余の法となる整数

が素因数分解されれば良い。法となる整数 n は公開するので，安全性を確保するためには n の素因数分解が計算量的に不可能でなければならない。現在のところ，n として1024ビット程度のものが使われているが，共通鍵暗号では64ビットから128ビットくらいが主流なのに比べると非常に大きな“場”での計算が要求され，計算処理能力だけ出なくメモリの点からもみても効率が悪い。また“Index Calculus”のような，素因数分解を行わずに解読しようとする試みもなされてきた[6][7]。

楕円曲線法や超楕円曲線法では，最も基本となる“場”は素体か素体の有限次拡大であるが，安全性を与える“場”はその上の加法群である。ＲＳＡでは多くの乗法計算を行わなければならなかったが，これらの方法では加法とより少ない乗法計算ですむ。また基本的な“場”である有限体上の Abel 多様体の加法群としての構造を利用するのであるから，有限体が小さい場合にも大きな加法群を構成することができる。ここにおける離散対数問題，つまり $Q=nP$ から n を求めること，は P の位数が大きい場合は難しいと考えられるので，暗号として利用できる。その上，“Index Calculus”も有効には働かないと考えられている。

楕円曲線と超楕円曲線の違いは，代数曲線としては種数が１か２以上かということであるが，定義体が同じ場合は種数が大きいほうが，より大きな加法群を構成できる。実際に，代数幾何符号の構成方法として研究されていた C_{ab} 曲線（楕円曲線や超楕円曲線を含む）を暗号に使おうとする試みがなされた[8]。しかし，逆に種数が大きい場合に定義体の小さな曲線の離散対数問題に帰着されてしまう場合もあるので，一般には種数が２，３，４くらいまでが適当といわれている。

楕円曲線の場合は，［５］で示したように最も次数の低いＣＭ体である虚２次体を使って安全性の高い曲線を構成する理論的方法があり，これは超楕円曲線の場合にも拡張される。一方で与えられた楕円曲線に対しその Mordell–Weil 群の位数を計算する高速なアルゴリズムもあり，曲線を順次与えていって適当な位数を持つものを決める方法が実際には主流である。

楕円曲線の場合と異なり，超楕円曲線に対しては Mordell–Weil 群に対応する Jacobi 群の位数を求める十分に高速なアルゴリズムがまだ開発されていないのが現状である。したがって，現在のところ，ＣＭ体を用いる方法が実現可能な方法であるが，後に示すようにいくつかの問題点があり，その意味でも次世代の公開鍵暗号系と呼ばれている。

2. 楕円曲線の構成法

超楕円曲線の構成法を理解しやすくするために，ここでは虚数乗法（Complex Multiplication；ＣＭ）を持つ楕円曲線の構成法について簡単な復習をしておこう。

まず，有理数体上の総虚な２次拡大である虚２次体 $k=\mathbb{Q}(\sqrt{-D})$ を一つ決める。この体には，ちょうどその類数 h_k 個の簡約された２次無理数（上半平面 H の $SL_2(\mathbb{Z})$ による基本領域に入る２次の無理数）が存在し，その対応は次で与えられる。

$$\overline{A} = z < a, \frac{-b+\sqrt{-D}}{2} > \in C_k \leftrightarrow \tau = \frac{-b+\sqrt{-D}}{2a} \in H/SL_2(Z)$$

h_k 個の簡約された2次無理数を，重さ0のモジュラー関数体の生成元である j-関数に代入した値は互いに共役で，それらを根に持つ多項式（Hilbert 多項式）は有理整数係数の多項式となる。

$$H_D(X) = \prod (X - j(\omega_r)^{\sigma_c}),\ j(\omega_r)^{\sigma_c} = j(\omega(c_r)^{\sigma_c}) = j(\omega(c^{-1}c_r))\ \ (c, c_r \in C_k)$$

今 k において相異なる二つの単項イデアルに完全分解するような素数 p を取ると，Hilbert 多項式は mod p で h_k 個の相異なる解を持ち，一つを j_0 として楕円曲線 E を次のように構成する。

$$E : y^2 = x^3 + 3tx + 2t,\ t = \frac{j_0}{1728 - j_0}$$

このとき，素体 F_p 上で定義された楕円曲線 E の Mordell-Weil 群の位数は

$$\#E(F_p) = p + 1 - Tr(\pi_p)$$

となる。ここで，π_p は Frobenius 写像を表すが，それは k における p の素因子と同一視できる。

この群を暗号に用いる場合，その安全性を確保するために位数が大きく，できれば素数に近いもの（大きな素数×小さな数）であって欲しい。そのためには p を与えたとき，2変数2次不定方程式 $X^2 + DY^2 = 4p$ が解けるかどうか調べ，もしも解けるならばその解 X=A に対し，

$$\#E(F_p) = p + 1 \pm A$$

を計算し，これが素数に近いかどうか調べる。幸いにして $X^2 + DY^2 = 4p$ は，p がかなり大きな数でも，解の判定を含めて解く高速なアルゴリズムが知られている。

3. 種数2の超楕円曲線の構成

安全性の高い種数2の超楕円曲線を構成する方法は，ドイツ Essen 大学の Frey 教授の大学院生だった Anne-Monika Spallek[9]や同大学の Annegret Weng[10]（現在は Johannes Gutenberg-Universität, Fachbereich Mathematik）などによってまとめられている。日本においても中央大学の辻井教授（現情報セキュリティ大学院大学学長）や趙教授のもとで多くの研究がなされた[11]。どちらも基礎となる部分では，CMを持つ Abel 多様体の理論が使われている。これは楕円曲線の場合の拡張であり，種数2の場合は実2次体上の総虚2次拡大の整数環（またはその部分環）と同型な準同型環を持つような Abel 多様体（実際には曲線 $y^2 = f(x)\ (deg(f(x)) = 5, 6)$ の生成が目標である。

楕円曲線の場合と同様，CMを持つものを考える。一般に種数が g のときは対応する CM体は，有理数体上の総実な g 次拡大 k_0 上の総虚2次拡大 k である。このような体で適当なものを一つ

決め，楕円曲線の場合に行った類体構成のような手法を用いるのだが，一般のgに対してはHilbert多項式に対応するものが簡単には求まらない。しかしg＝2のとき，CM体から求まる周期行列を使ってまずθ関数の値を計算し，そこから井草不変量[12]を求め，更にMestre不変量[13]が計算できる。θ関数や井草不変量は，いわゆるGlobalな領域の話であり，CM体上の類体構成問題と関係が深い。Mestre不変量の計算時点でmod pの領域への移行がなされ，目的とする曲線$y^2=f(x)\,(deg(f(x))=5,6)$を得ることができる。つまり，$\theta$関数の値や井草不変量を計算するときには，誤差の範囲に気を使い，途中で現れる類多項式の係数を整数化する必要がある。

有限体へ移行する時点では素数pの選択が必要で，暗号に用いる場合の安全性を考慮する必要がある。そのためには，曲線に対応するJacobi群の位数が素数に近いものを選ばなければならない。この位数とpは，楕円曲線の場合と同様に，pのkにおける分解と密接に関係しており[14]，どのようなpが適当かが示されている。本論文の目的は，このような素数pを決定するための方向性を示すことである。

以下では，有理数体上の実2次拡大を$k_0=Q(\sqrt{d})$，その上の2次拡大で総虚となり，しかも有理数体上Galois拡大にならないものを$k=k_0(\sqrt{-\alpha})(\alpha=a+b\sqrt{d})$とする。つまり，$d>0, \alpha>0, \alpha'=a-b\sqrt{d}>0, b\neq 0, \sqrt{\alpha\alpha'}\notin k$である。

また簡単のために，それぞれの整数環O_{k_0}，O_kの基底は次のような場合を考える。

$$O_{k_0}={}_Z<1,\sqrt{d}>, O_k={}_Z<1,\sqrt{d},\sqrt{-\alpha},\sqrt{-d\alpha}>$$

4. Weil数

前節で示したように，種数が2の超楕円曲線を素体F_pに移行したときにそのJacobi群の位数が取るであろう値は，4次のCM体kにおけるpの分解を用いて記述することができる。しかし，どのような素数pでも良いというわけではなく，次のような素数が必要になる。

定義（Weil数）

kの整数ωで，$\omega\bar{\omega}=p$となるものをWeil数と呼ぶ。ここで，$\bar{\omega}$はωの複素共役を表すものとする。

Weil数を求めることによりJacobi群の位数が計算され，それが安全性を満たすものならば採用し，そうでなければ別のWeil数を探すことになる。素数pとして少なくともある程度の大きさの素数（例えば十進60桁以上）が必要であるが，一般の4次体においてそのような大きな素数を分解できるような高速なアルゴリズムは，筆者の知る限り存在しない。前節で述べたいくつかの超楕円曲線生成法においては，素数を与えるのではなく，kの整数ωを与えてその絶対値を計算し，それが素数ならば候補として採用している。素数の分布に関するGaussの定理を考察すれば，与えた桁の多項式時間で素数が見つかるはずである。

我々はこの立場を取らず，与えられた素数 p に対し Weil 数 ω を計算するアルゴリズムを目標にしている。本論文では，素数 p に対して Weil 数が存在するための条件と，それがどのような形をしていなければならないかを示す。

5. Weil 数を含むイデアル

体 k を含む有理数体上の最小 Galois 拡大を L とすると，$L = k(\sqrt{-\alpha'})$ となり，次のような Galois 群を持つ。

$$Gal(L/Q) =< \sigma, \tau >, Gal(L/k) =< \tau >, Gal(L/k_0) =< \sigma^2, \tau >$$

$$\sigma : (\sqrt{-\alpha}, \sqrt{-\alpha'}) \mapsto (\sqrt{-\alpha'}, -\sqrt{-\alpha}), \sigma^2 = \rho$$

$$\tau : (\sqrt{-\alpha}, \sqrt{-\alpha'}) \mapsto (\sqrt{-\alpha}, -\sqrt{-\alpha'})$$

（ただし，ρ は複素共役を表す）

以後 Weil 数に対応する素数 p は L において不分岐であるとする。つまり，p を割る任意の L の素イデアル $\wp$ に対しその分岐群 $T_\wp = \{e\}$ である。

$K = Q(\sqrt{d}, \sqrt{\alpha\alpha'})$ とすると，これは L に含まれる有理数体上の Galois 拡大（Abel 拡大）で，$Gal(L/K) =< \sigma^2 > (\sigma^2 = \rho)$ であり，$\omega \in k \subset L, N_{L/K}\omega = \omega\omega^\rho = p$ となる。素数 p と ω によって生成される単項イデアル(ω)の L における分解は，次のようになる。

p の K における分解	P		P_1P_2		$P_1P_2P_3P_4$	
P_i の L における分解	$\wp$	$\wp\,\wp^\rho$	$\wp_1\wp_2$	$\wp_1\wp_1{}^\rho\wp_2\wp_2{}^\rho$	$\wp_1\wp_2\wp_3\wp_4$	8 個の素イデアルに完全分解
(ω)の L における分解	$\wp$	$\wp$	$\wp_1\wp_2$	$\wp_1\wp_2$		$\wp_1\wp_2\wp_3\wp_4$
$N_{L/K}(\omega)$	p^2	p	p^2	p	p^2	p

この表で $N_{L/K}(\omega)$行が p であるものは 2，4，6 列目であるが，2 及び 4 列目の場合は，k における分解を考えることによって除くことができる。したがって次の命題を得る。

命題 1

素数 p に対して Weil 数が存在するためには，p が L において完全分解する必要がある。またこのとき，$(\omega) = PP^\sigma$ となる。

次にイデアル(ω)の $O_k =_Z < 1, \sqrt{d}, \sqrt{-\alpha}, \sqrt{d\alpha} >$ における生成元を考えよう。素数 p の k_0における完全分解性から，ある整数 s が存在して $d \equiv s^2 \bmod p$ となる。また k における完全分解性を考慮することにより，ある整数 t および u が存在して，$-(a + bs) \equiv t^2 \bmod p, -(a - bs) \equiv u^2 \bmod p$ となる。これらの整数から

$$\begin{cases} v = & tu \\ w = & t+u \end{cases} (\mathrm{mod}\, p)$$

を定義すると，$(\omega) = PP^{\sigma} =_{Ok} (p, v-\alpha+w\sqrt{-\alpha})$ となる。この生成元を用いて整数環上の基底を計算することができ，次のようになる。

命題 2

$(\omega) = PP^{\sigma} =_{Z} < p, p\sqrt{-\alpha}, b_2 w - \sqrt{d} + 2b_2\sqrt{-\alpha}, 2b_2 v + b_2 w\sqrt{-\alpha} + \sqrt{d\alpha} >$

ただし，$b_2 \equiv 2^{-1}b^{-1}w \bmod p$ である。

（証明の方針）

$(\omega) =_{Ok} (p, v-\alpha+w\sqrt{\alpha})$ より，$\omega \equiv a_0 + a_1\sqrt{d} + a_2\sqrt{-\alpha} + a_3\sqrt{-d\alpha} \bmod p$ と表す。ここで v, w, α の関係を用いることによって，a_0, a_1, a_2, a_3 の関係式が求まり，それらを整理することによって，基底が求まる。

更に上記のイデアル基底を使って，$O_{k_0} =_{Z} < 1, \sqrt{d} >$ 上の生成元を求めることができる。この環は一般には単項イデアル環とならず，必ずしも基底が存在するとは言えない。しかしここで得られた結果は，Weil 数で生成されるイデアルが O_{k_0} 上の基底を持つことを示している。

命題 3

$$(\omega) = PP^{\sigma} =_{Ok_0} < p, l + m\sqrt{d} + \varepsilon\sqrt{-\alpha}, >$$

ここで，ε は任意の単数で $\varepsilon = n + o\sqrt{d}$ と表したとき，l, m は次の式で決まる整数である。

$$\begin{pmatrix} l \\ m \end{pmatrix} \equiv \begin{pmatrix} n & -od \\ o & -n \end{pmatrix} \begin{pmatrix} 2^{-1}w \\ bw^{-1} \end{pmatrix} \bmod p$$

（証明の方針）

$$p(x_0 + x_1\sqrt{d}) + ((l + m\sqrt{d}) + (n + o\sqrt{d})\sqrt{-\alpha})(x_2 + x_3\sqrt{d})$$
$$= (px_0 + lx_2 + mdx_3) + (px_1 + mx_2 + lx_3)\sqrt{d}$$
$$+ (nx_2 + odx_3)\sqrt{-\alpha} + (ox_2 + nx_3)\sqrt{-d\alpha}$$

より，$PP^{\sigma} \subseteq_{Ok_0} < p, l + m\sqrt{d} + \varepsilon\sqrt{-\alpha}, >$ であるための条件は，

$^{\exists}M \in M_4(Z) s.t.$

$$\begin{pmatrix} p & 0 & l & md \\ 0 & p & m & l \\ 0 & 0 & n & od \\ 0 & 0 & o & n \end{pmatrix} M = \begin{pmatrix} p & 0 & b_2 w & 2b_2 v \\ 0 & 0 & -1 & 0 \\ 0 & p & 2b_2 & b_2 w \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

となる。ここで左辺 1 項目の逆行列を計算し，$N = n^2 - o^2 d$ とおくと，

$$M=\begin{pmatrix} 1 & -\frac{nl-omd}{N} & \frac{b_2 w}{p}-\frac{2b_2(nl-omd)}{pN} & \frac{2b_2\nu}{p}-\frac{b_2 w(nl-omd)}{pN}-\frac{(nm-ol)d}{pN} \\ 0 & -\frac{nm-ol}{N} & -\frac{1}{p}-\frac{2b_2(nm-ol)}{pN} & -\frac{b_2 w(nm-ol)}{pN}-\frac{nl-omd}{pN} \\ 0 & \frac{np}{N} & \frac{2b_2 n}{N} & \frac{b_2 nw}{N}-\frac{od}{N} \\ 0 & -\frac{op}{N} & -\frac{2b_2 o}{N} & -\frac{b_2 ow}{N}+\frac{n}{N} \end{pmatrix}$$

となる。この条件を考察することにより，$n+o\sqrt{d}$ が単数であることと，l, m の条件式が導き出される。

6. 終わりに

超楕円曲線の構成法とそのために必要な Weil 数について，その数学的性質を示したが，実際に命題２や命題３の基底をうまく使って Weil 数の計算を行うアルゴリズムを開発することが今後の課題である。例えば命題２をそのまま使っただけでは，４元４次の不定方程式を解かなければならない。それは楕円関数の場合の虚２次体と異なって高速解法アルゴリズムは知られておらず，特に素数が大きな場合は良い効果が得られない。

命題３は実２次体の類数が１ではない場合も成り立つので数学的には面白い。筆者は現在，この基底を用いたアルゴリズムを，具体的な例なども含めて研究中である。

注

[１] W. Diffie and M. E. Hellman, “New direction in Cryptography,” IEEE Transaction on Information Theory, v. IT–22, n.6, Nov. 1976, pp. 644–654.

[２] R. L. Rivest, A. Shamir, and L. M. Adleman, “A Method for Obtaining Digital Signature and Public–Key Cryptosystems,” Communication of the ACM, v.21, n.2, Feb. 1978, pp. 120–126.

[３] V. Miller, “Use of elliptic curves in cryptography,” Advances in Cryptology, Proceedings of CRYPTO 85, Springer–Verlag, 1986, pp. 417–426.

[４] N. Koblitz, “Elliptic curve cryptosystems,” Math. Comp., 48, 1987, pp. 203–209.

[５] 永田　清，“虚数乗法をもつ楕円曲線とｊ－不変量について”，大東文化大学紀要，第41号，＜自然科学＞，平成15年３月，pp.1–7.

[６] L. Adleman, “A subexponential algorithm for the discrete logarithm problem with applications to cryptography,” Proc. 20th IEEE Found. Comp. Sci. Symp., 1979, pp. 55–60.

[７] J. H. Silverman and Joe Suzuki, “Elliptic Curve Discrete Logarithms and Index Calculus,” Proceedings of Asiacrypt 98, Springer–Verlag, 1999, pp. 110–125.

[８] S.Arita, “Algorithms for computations in Jacobian group of C_{ab} curve and their application to discrete–log–based public key cryptosystems,” Conference on The Mathematics of Public Key Cryptography, Toronto, 1999.

[９] A.–M. Spallek, “Kurven vom Geschlicht 2 und ihre Anwendung in Public–Key–Kryptosystemen,” Ph.

D. thesis, Institut für Experimentelle Mathematik, Universität GH Essen, 1994.

[10] A. Weng, "Constructing hyperelliptic curves of genus 2 suitable for cryptography," Math. Comp. (72), 2003, p. 435–458

[11] J. Chao, K. Matsuo, H. Kawashiro and S. Tsujii, "Construction of Hyperelliptic Curves with CM and Its Application to Cryptosystems," Advances in Cryptology– ASIACRYPT 2000, LNCS 1976, pp. 259–273, 2000.

[12] J. Igusa, "Arithmetic Variety of Moduli for Genus Two," Annals of Mathematics, Vol.72, No. 3, November, 1960, pp.612–649.

[13] J. F. Mestre, "Construction de courbes de genre 2 a partir de leurs modulus," Prog. Math., Birkhauser, 94, 1991, pp.313–334.

[14] J. Tate, "Endomorphisms of Abelian Varieties over Finite Fields," Inventions Math. 2, 1966, pp.134–144.