C_{ab} 曲線上のペアリングと暗号への応用

吉野 絵美　（指導教官：金子 晃）

1　はじめに

1990 年代初頭に楕円曲線暗号の攻撃手段として登場したペアリングは，暗号プロトコルの構成手段としての利用価値を見出されて後，非常に大きな関心を集める主題へと急速な成長を遂げた．そして現在，従来は実現不可能と思われていた暗号プロトコルがペアリングの性質を利用することで，現実的な方式として数多く提案されている．それに伴い，ペアリングを暗号へ応用した際の安全性や，ペアリングの計算の効率性もまた詳しく調べる必要が生じている．その中で，楕円曲線より高い種数を持つ超楕円曲線上でのペアリングを暗号へ応用する提案が自然になされた．本稿では，更に楕円曲線・超楕円曲線の一般化である C_{ab} 曲線上でのペアリング及び，その実装方法について考察する．

2　C_{ab} 曲線

K を任意の体とするとき $\overline{K}$ で K の代数閉体を表す．

定義 1 $a,b\in\mathbb{N}$ を $2\le a<b$ を満たす互いに素な自然数とする．任意の有限体 $\mathbb{F}_q(q=p^l,\ p$ は素数 $)$ 上の次の形の多項式を定義方程式に持つ曲線を C_{ab} 曲線と呼ぶ；

$$M(X,Y):=\sum_{ai+bj\le ab}\lambda_{i,j}X^iY^j\quad,$$

$$\text{ただし }\lambda_{i,j}\in\mathbb{F}_q,\lambda_{0,a}\neq 0,\lambda_{b,0}\neq 0.$$

C_{ab} 曲線 $M(X,Y)=0$ の表示を

$$Y^a+\sum_{ai+bj<ab,i\ge 0,j\ge 1}\lambda_{ab-ai-bj}X^iY^j = X^b+\sum_{0\le i<b}\lambda_{ab-ai}X^i\quad,\ \text{ただし}\lambda_i\in\mathbb{F}_q.$$

と変形すれば $(a,b)=(2,3)$ のとき楕円曲線の Weierstrass の標準形と一致し，$(a,b)=(2,2g+1)$ のときは種数が g 以下の超楕円曲線の標準形となる．以下，$M(X,Y)$ は非特異（即ち，$M(X,Y)=M_X(X,Y)=M_Y(X,Y)=0$ を満たす $(X,Y)\in\overline{\mathbb{F}}_q\times\overline{\mathbb{F}}_q$ は存在しない）とし，C を $M(X,Y)$ で定義された C_{ab} 曲線として固定する．このとき，曲線 C の種数は $g=(a-1)(b-1)/2$ に等しい．
K を $\mathbb{F}_q$ の任意の拡大体とする．X,Y を形式的文字とする K 上の多項式環 $K[X,Y]$ の剰余環

$$K[C]:=K[x,y]=K[X,Y]/(M(X,Y))$$

を K 上の C の座標環と呼ぶ．ここで $(M(X,Y))$ は多項式 $M(X,Y)\in K[X,Y]$ で生成される $K[X,Y]$ のイデアルを表す．$\overline{\mathbb{F}}_q[C]$ の元を C 上の多項式関数と呼ぶ．$M(X,Y)$ は $\overline{\mathbb{F}}_q[X,Y]$ において既約であることが示せ，従って，$K[C]$ は整域であることがわかる．座標環 $K[x,y]$ の商体を $K(x,y)=K(C)$ と書いて K 上の C の関数体と呼ぶ．$\overline{\mathbb{F}}_q(C)$ の元を C 上の有理関数と呼ぶ．

C 上の K 有理点の集合を $M(X,Y)=0$ の K における解全体と無限遠点 P_∞ からなる集合と定め，

$$C(K):=\{(X,Y)\in K\times K\mid M(X,Y)=0\}\cup\{P_\infty\}$$

で表す．特に $K=\overline{\mathbb{F}}_q$ のとき $C(\overline{\mathbb{F}}_q)=C$ と記す．

3　C_{ab} 曲線上のペアリング

曲線 C の因子類群を

$$J_C:=\mathrm{Div}_C^0/\mathrm{Princ}_C$$

とおき，因子 $D\in\mathrm{Div}_C^0$ に対応する因子類を $\bar{D}\in J_C$ で表す．また，座標環 $K[C]$ のイデアル類群を

$$\mathcal{H}(K[C]):=\mathcal{I}(K[C])/\mathcal{P}(K[C])$$

とおき，$I\in\mathcal{I}(K[C])$ に対応するイデアル類を $\bar{I}\in\mathcal{H}(K[C])$ で表す．$\mathcal{H}(K[C])$ の各同値類はその代表元として座標環 $K[C]$ のイデアルを選ぶことができる．実際，各 $I\in\mathcal{I}(K[C])$ に対して，0 でない $f\in I$ を任意に取ると，$(f)I^{-1}\subset K[C]$ より 0 でない有理関数 $h\in I^{-1}$ を多項式関数 $fh\in K[C]$ の無限遠点 P_∞ での極位数が最小になるように選ぶ．このような h は f の取り方に依らず，0 でない定数倍を除いて一意に決まる．この h を I の被約化関数と呼び，I と同じイデアル類に属する $K[C]$ のイデアル $(h)I\subset K[C]$ を I の被約イデアルと呼ぶ．$\bar{I}\in\mathcal{H}(K[C])$ の対応する被約イデアルを $\rho(I)\subset K[C]$ で表す．集合 $\rho(\mathcal{H}(K[C]))$ に

$$\rho(\bar{I}_1)\odot\rho(\bar{I}_2):=\rho(\bar{I}_1\bar{I}_2)$$

として演算 $\odot$ を定義する．$n\in\mathbb{Z}$ と $I\in\mathcal{I}(K[C])$ に対して

$$I^{\odot n}:=\rho(\bar{I}^n)$$

とし，I^n の被約化関数を $g_{n,I}\in K(C)$ とするとき $h_{n,I}=1/g_{n,I}\in K(C)$ と書くことにする．即ち，$I^n=(h_{n,I})I^{\odot n}$ である．曲線 C 上の因子類群とイデアル類群は自然な対応 $D\mapsto\{r\in K(C)\mid \mathrm{ord}_P r\ge -\mathrm{ord}_P(D)\quad\forall P\in C\setminus\{P_\infty\}\}$ によって，同型になる．r を，$\mathcal{H}(K[C])$ の位数の素因数で q と互いに素なものとする．k を（r に関する）埋め込み次数（すなわち $r\mid(q^k-1)$ を満たす最小の $k\in\mathbb{Z}$）とする．従って，1 の原始 r 乗根のなす群 μ_r は $\mathbb{F}_{q^k}$ に含まれる．$\mathcal{H}(\mathbb{F}_{q^k}(C))$ の r 捩れ元全体を

$$\mathcal{H}(\mathbb{F}_{q^k}(C))[r]:=\{\bar{I}\in\mathcal{H}(\mathbb{F}_{q^k}(C))\mid\rho(\bar{I}^r)=1\}$$

とおく．このとき Tate-Lichtenbaum ペアリング が well-defined な非退化双線形写像

$$\langle\ ,\ \rangle_r:\mathcal{H}(\mathbb{F}_{q^k}(C))[r]\times J_C(\mathbb{F}_{q^k})/rJ_C(\mathbb{F}_{q^k})\to\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r$$

として次のように定義できる．$\bar{I}_1\in\mathcal{H}(\mathbb{F}_{q^k}(C))[r]$，$\bar{D}_2\in J_C(\mathbb{F}_{q^k})$ に対して $I_1\in\bar{I}_1$，$D_2\in\bar{D}_2$ が $\mathrm{supp}(I_1)\cap$

$\mathrm{supp}(D_2)=\emptyset$ を満たすとする．このとき，$h_{r,I_1}\in\mathbb{F}_{q^k}(C)^*$ は $(h_{r,I_1})=I_1^r$ を満たす．このとき，$\bar{I}_1$ と $\bar{D}_2$ の Tate-Lichtenbaum ペアリングは

$$\langle \bar{I}_1,\bar{D}_2\rangle_r \equiv h_{r,I_1}(D_2):=\prod_{P\in C} h_{r,I_1}(P)^{\mathrm{ord}_P(D_2)}.$$

ここで，$\equiv$ は $(\mathbb{F}_{q^k}^*)^r$ を法として等しいということを意味する．因子 D_2 の次数が 0 なので，h_{r,I_1} のゼロでない定数倍は相殺されるので，この結果は h_{r,I_1} の選び方によらない．ペアリングの計算結果が剰余類ではなく，一意に決まるよう修正したペアリング $e(\ ,\ )$ を被約 Tate-Lichtenbaum ペアリングと呼び，次のように定義する；

$$e(\bar{I}_1,\bar{D}_2)=\langle \bar{I}_1,\bar{D}_2\rangle_r^{(q^k-1)/r}\in\mu_r\subset\mathbb{F}_{q^k}^*.$$

ペアリングの計算，即ち $h_{r,I_1}(D_2)$ を求めるアルゴリズムを以下に与える．

アルゴリズム 1 Miller のアルゴリズム
入力：$\mathbb{N}\ni n=\sum_{j=0}^{w} n_j 2^j\ n_j\in\{0,1\}, n_w=1, \bar{I}_1\in\mathcal{H}(\mathbb{F}_{q^k}(C))$, $\bar{D}_2\in J_C(\mathbb{F}_{q^k})$, $\bar{I}_1$,$\bar{D}_2\in J_C$ の代表元で $\mathrm{supp}(I_1)\cap\mathrm{supp}(D_2)=\emptyset$ なる $I_1\in\mathcal{I}(\mathbb{F}_{q^k}(C)), D_2\in \mathrm{Div}_C^0$
出力：$h_{n,I_1}(D_2)$

$I\leftarrow I_1, c\leftarrow 1$
for $j=w-1$ **down to** 0 **do**
  $I\leftarrow I^{\odot 2}$
  $c\leftarrow c^2 G_{I,I}(D_2)$
  if $n_j=1$ **then**
    $I\leftarrow I\odot I_1$
    $c\leftarrow cG_{I,I_1}(D_2)$
  end if
end for
Return c

4 T-基底

ペアリングを実際に暗号へ応用する為には，ペアリングが定義されている群の演算が効率的に行えることが必要である．曲線 C 上の因子類群の各イデアル類は代表元に $K[C]$ のイデアルを持つので，因子類群とイデアル類群の自然な対応によって因子類群の計算を，イデアル計算を用いて実現出来る．C_{ab} 曲線に対する計算に対しては従来，多項式環の任意のイデアルが持つ Gröbner 基底が利用されていた．一方で，超楕円曲線の場合では，各因子類を一変数多項式のペアで表すことが出来る（Mumford 表現）．C_{ab} 曲線の各因子類を Gröbner 基底を用いて表現すると最大 a 個の元が必要となり，超楕円曲線と C_{ab} 曲線との計算効率に大きな差が出来てしまう．しかし，次の補題から $K[C]$ のイデアルは高々2 元で生成されることが保証されているので，Gröbner 基底を用いずに各因子類を表現することを考えたい．

補題 1 $I\in\mathcal{I}(K[C])$ を可逆な分数イデアルとすると，任意に選んだ 0 でない $u\in I$ に対して，$v\in I$ が存在して $I=(u,v)$ とできる．

上の補題 1 における $0\neq u$ は任意に選んでよいので，特に $I\cap K[x]$ から取ることができる．従って各 $I\in\mathcal{I}(K[C])$ に対して $0\neq f(x)\in K[x]$ と $0\neq u(x,y)\in K(x,y)$ で $I=(f(x),u(x,y))$ なるものが存在する．このように一方が x だけの式からなる I の 2 元の生成系 $\{f(x),u(x,y)\}$ を T-基底と呼ぶ．

定義 2 I を可逆な $K[C]$ のイデアルとする．以下の条件を満たす関数のペア $\{f(x),u(x,y)\}$ を被約 T-基底と呼ぶ；

1. $\{f(x),u(x,y)\}$ は T-基底
2. $f(x)\in I$ はモニックかつ $I\cap K[x]$ で C_{ab} 次数最小
3. $u(x,y)\in I$ はモニックかつ $(f^2,u)=I$ を満たし，$(f^2,u)=I$ を満たす中で C_{ab} 次数最小

上の定義 2 において，$f(x)\in I\cap K[x]$ は，I に対して一意に決まるが，$u(x,y)\in I$ は一般には一意でないことに注意する必要がある．Mumford 表現を用いた効率的な超楕円曲線上の群演算のアルゴリズムが T-基底を利用することで，C_{ab} 曲線に対して拡張できる．このことは次に挙げる補題から導かれる．

補題 2 $\{f(x),u(x,y)\}$ を被約イデアル I の被約 T-基底とする．$f(x)\in K[x]$ を互いに共通因子を持たない $f_1(x)$, $f_2(x)\in K[x]$ の積 $f(x)=f_1(x)f_2(x)$ で書けているとする．このとき $(f(x),u(x,y))=(f^2(x),u(x,y))$ が成り立つことと，$(f_1(x),u(x,y))=(f_1^2(x),u(x,y))$ かつ $(f_2(x),u(x,y))=(f_2^2(x),u(x,y))$ が成り立つことは同値．

補題 3 $\{f(x),u(x,y)\}$ を被約イデアルの被約 T-基底とする．$f(x)\in K[x]$ を互いに共通因子を持たない $f_1(x)$, $f_2(x)\in K[x]$ の積 $f(x)=f_1(x)f_2(x)$ で書けているとする．このとき

$$(f(x),u(x,y))=(f_1(x),u(x,y))(f_2(x),u(x,y))$$

が成り立つ．

補題 4 $\{f(x),u(x,y)\},\{h(x),v(x,y)\}$ をそれぞれ異なる被約イデアルの被約 T-基底とする．$f(x)$,$h(x)$ は共通因子を持たないとし，$a(x),b(x)\in K[x]$ で $a(x)f(x)+b(x)h(x)=1$ と書けているとすると

$$(f(x),u(x,y))(h(x),v(x,y))$$
$$=(f(x)h(x),a(x)f(x)v(x,y)+b(x)h(x)u(x,y))$$

が成り立つ．

補題 5 $\{f(x),u(x,y)\},\{h(x),v(x,y)\}$ をそれぞれ被約イデアルの被約 T-基底とする．$K[C]$ のイデアル $(f(x))$, $(h(x))$ の根基が等しい（即ち，$f(x)$ と $h(x)$ は同じ因子しか持たない）とすると

$$(f(x),u(x,y))(h(x),v(x,y))$$
$$=(f(x)h(x),u(x,y)v(x,y))$$

が成り立つ．

5 まとめと今後の課題

C_{ab} 曲線上の群に対してペアリングを構成し，T-基底を導入することで，ペアリング計算を高速化することを提案した．今後は，詳細なアルゴリズムを構成し，より効率的な計算方法を考えるとともに，楕円・超楕円曲線上のペアリングとの比較も行っていく．

参考文献

[1] Henri Cohen and Gerhard Frey, 「Handbook of Elliptic and Hyperelliptic Curve Cryptography」, Chapman & Hall/CRC, 2006
[2] 三浦晋示,“アフィン代数曲線上の線形符号,” 電子情報通信学会論文誌 (A), Vol.J81-A,no.10,pp.1398-1421,Oct.1998