解　説　論　文

ペアリングに関する最近の研究動向

Recent Research Activities on Pairing

岡本栄司 Eiji OKAMOTO　　岡本　健 Takeshi OKAMOTO
金山直樹 Naoki KANAYAMA

1．はじめに ― ペアリング登場の背景 ―

本稿でいうペアリングとは，2入力1出力関数であって，各入力に対して線形性が成り立つ，いわゆる双線形関数である．具体的なペアリングとしては，入力がだ円曲線上あるいは超だ円曲線上の2点で，出力はある有限体の元であるものが提案されている．

ペアリングと暗号の出会いは，1993年のだ円曲線上の離散対数問題解法が最初である[(1)]．これは，いわば暗号の解読に用いられたものである．暗号設計については，2000年にJouxによってDiffie-Hellman公開鍵配送方式が三者に拡張され[(2)]，境・大岸・笠原によって，IDに基づく暗号に適用された[(3)]．

その後，ペアリングを用いた暗号の研究は増えており，特にペアリングをブラックボックスとして扱い，その双線形性のみを利用した暗号プロトコルの提案が増加している．

一方，ペアリング自体の実装についても積極的に研究が行われるようになってきている．これは，今までペアリング計算処理速度がRSAなどのべき乗剰余演算よりも数倍遅かったためであり，せめて同程度にしなければ利用されないからである．現在,活発な研究によりソフトウェア実装あるいはハードウェア実装において，演算速度も上がってきている．

以上の現状を踏まえ，ここでは，ペアリングそのものに主に焦点を当てて概説を行い，最後に各種プロトコルに触れる．

2．ペアリングとは

現在暗号で用いられているペアリングはある種のだ円曲線上に定義される関数である．入力はだ円曲線上の2点，出力はある有限体の元である．そこで，まずだ円曲線を簡単に紹介し，その上でペアリングを定義する．

岡本栄司　正員：フェロー　筑波大学大学院システム情報工学研究科
E-mail　okamoto@risk.tsukuba.ac.jp
岡本　健　正員　筑波大学大学院システム情報工学研究科
E-mail　ken@risk.tsukuba.ac.jp
金山直樹　正員　筑波大学大学院システム情報工学研究科リスク工学専攻
E-mail　kanayama@risk.tsukuba.ac.jp
Eiji OKAMOTO, Fellow (Graduate School of Systems and Information Engineering, University of Tsukuba, Tsukuba-shi, 305-8573 Japan), Takeshi OKAMOTO, and Naoki KANAYAMA, Members (Graduate School of Systems and Information Engineering, University of Tsukuba, Tsukuba-shi, 305-8573 Japan).
Fundamentals Review Vol.1 No.1 pp.51-60 2007年7月

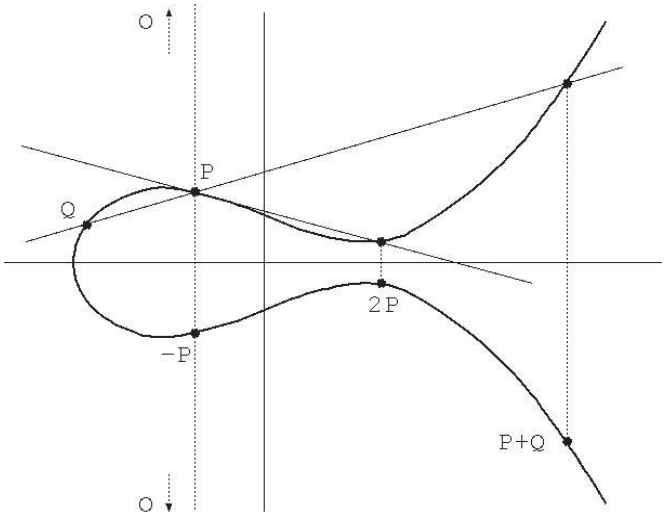

図1　だ円曲線における加算＋

2．1 だ円曲線

本文で扱うだ円曲線は$y^2=x^3+ax+b$を満たす有限体F_qの元の座標(x, y)の集合に無限遠点Oを追加した集合$E(F_q)$である：

$$E(F_q)=\{(x,y)\in F_q{}^2 : y^2=x^3+ax+b\}\cup\{O\}$$

ただし，曲線は非特異（どの点でも必ず接線が一本だけ引ける）とする．この集合は次に示す演算＋により加法群をなす．図1において，PとQを通る直線が$y^2=x^3+ax+b$と交わる第3の点のx軸に関する線対称点が$P+Q$となる．

$P=Q$のときはPにおける接線を用いる．Oが零で，$-P$はPのx軸に関する線対称点となる．すなわち，$P=(x, y)$とすると，逆元は$-(x, y)=(x, -y)$となり，容易に求められる．これは有限体F_qと大きく異なる点である．

代数的に示せば次のようになる．だ円曲線上の2点$P=(x_1, y_1)$，$Q=(x_2, y_2)$に対して，その和$P+Q=(x_3, y_3)$を$x_3=\lambda^2-x_1-x_2$，$y_3=\lambda(x_1-x_3)-y_1$で与える．ここで，λは直線の傾きで

$$\lambda=\begin{cases}\frac{y_2-y_1}{x_2-x_1} & if\ P\neq Q\\ \frac{3x_1{}^2+a}{2y_1} & if\ P=Q\end{cases}$$

である．なお，$x_1 = x_2$かつ$y_1 \neq y_2$のときは$P + Q = O$となる．

2. 2ペアリングの定義

暗号で利用されているペアリングとしてWeilペアリングとTateペアリングがある．Weilペアリングは1946年にWeilによって，整数論の分野において導入されたもので，文献(3)でも用いられた．しかし，Tateによって導入されたTateペアリングの方が計算コストは小さいので，現在ではTateペアリングの方が主流である．以後はTateペアリングに話を限定する．

Tateペアリングeは，整数rに対して

$$e : E(F_q)[r] \times E(F_{q^k}) \Big/ rE(F_{q^k}) \to \mu_r$$
$$e(P,Q) = f_P(Q)^{\frac{q^k-1}{r}}$$

で定義される関数である．ここで，

$$E(F_q)[r] = \{P \in E(F_q) \mid rP = O\}$$
$$\mu_r = \{x \in F_{q^k} \mid x^r = 1\}$$

であり，kは

$$r \mid q^k - 1$$

を満たす最小数で，埋込次数と呼ばれる．

Tateペアリングの定義式における$(q^k-1)/r$によるべき乗は，$f_P(Q)$における任意性の除去のためである．すなわち，$f_P(Q)$の計算結果には係数として$F_{q^k}{}^r$の任意性が残るが$(q^k-1)/r$でべき乗することにより1となる．

f_Pはx，yの有理関数であるが，それを取り扱うには次の因子の概念を必要とする．

だ円曲線$E(F_q)$上の因子とは，曲線の点の整数係数形式和

$$D = \sum_{A \in E(F_q)} a_A (A)$$

であり，その集合に和

$$\left(\sum_{A \in E(F_q)} a_A (A) \right) + \left(\sum_{A \in E(F_q)} b_A (A) \right) := \sum_{A \in E(F_q)} (a_A + b_A)(A)$$

を定義して得られる群を因子群$Div(E)$という．ここで，因子上の二つの写像$\deg(D)$と$sum(D)$を

$$\deg(D) = \sum_i a_i \in Z$$

$$sum(D) = \sum_i a_i A_i \in E(F_q)$$

で定義する．また零因子群を

$$Div_0(E) = \{D \mid sum(D) = O\}$$

で定義する．

一方，x，yに関する有理関数fに対して，因子が次のように定義でき，これを主因子という．

$$div(f) = \sum_{A \in E(F_q)} ord_A(f)(A)$$

ここで，$ord_A(f)$はAにおけるfとEの多重度で，Aにおけるfの位数と呼ばれる．例えば，fの零点$A(\neq O)$に対しては

$$ord_A(f) = \begin{cases} 1; & f = 0 \text{と} E \text{が交差} \\ 2; & f = 0 \text{が} E \text{に接し}, 3A \neq O \\ 3; & f = 0 \text{が} E \text{に接し}, 3A = O \end{cases}$$

となる．fの極$A(\neq O)$に対しては

$$ord_A(f) = -ord_A(f^{-1})$$

Oに対しては

$$ord_O(x) = -2$$
$$ord_O(y) = -3$$

となる[4]．

例えば，直線lがだ円曲線上においてP，Q，Rで交差する場合，P, Q, Rにおける位数が1，Oにおける位数が-3なので，

$$div(l) = (P) + (Q) + (R) - 3(O)$$

となる．なお，和の定義から$R = -(P+Q)$である．また，$P = (x_1, y_1)$とその逆元$-P = (x_1, -y_1)$は直線$x - x_1 = 0$の点であることより

$$Div(x - x_1) = (P) + (-P) - 2(O)$$

と表せる．

このとき，零因子群について次の重要な性質が成り立つ．

性質　$Div_0(E)$において，

$$\deg(D) = 0 \Leftrightarrow {}^{\exists} f; div(f) = D$$

位数rの点Pについての因子$(D)=r(P)-r(O)$は上記性質の条件を満たすので，

$div(f_P)=r(P)-r(O)$

となる有理関数f_Pが存在する．このf_Pを用いてペアリングが定義されている．

このf_Pの具体的な計算法は4．に示すが，log$r$の多項式時間で計算できる．だが，すべてのだ円曲線に対してペアリングが効率的に計算できるわけではないことに注意する必要がある．多くのだ円曲線は一般に埋込次数kが大きい値をとる（文献(5)を参照）ため，大きなサイズの体の中で計算しなければならないからである．効率的に計算できるだ円曲線の代表例は超特異曲線であるが，そのほかにも幾つかある．超特異曲線の場合，$q=p$（2，3以外の素数）なら$k=2$であり，$q=2^m$なら$k=4$，$q=3^m$なら$k=6$である．これらの値はペアリングの実装上，重要なパラメータとなる．以下，ペアリングが効率的に計算できるだ円曲線に限定して話を進める．

2. 3ペアリングの性質

ペアリングには次の性質がある．証明については紙面の制約のため割愛するが，例えば文献(4)を参考にされたい．

(1) 非縮退性

任意のP（またはQ）に対して$e(P, Q)=1$ならば$Q=O$（または$P=O$）

(2) 双線形性

$e(P_1+P_2, Q)=e(P_1, Q)\,e(P_2, Q)$

$e(P, Q_1+Q_2)=e(P, Q_1)\,e(P, Q_2)$

(3) 計算可能性

多項式時間で計算可能

これらの性質の中で，他の暗号プリミティブにない重要な性質は双線形性である．この性質により，例えば，

$e(aP, bQ)=e(P, Q)^{ab}=e(bP, aQ)$

という等式が成り立ち，暗号プロトコルとして大いに力を発揮する．

2. 4ペアリングの安全性

ペアリングの安全性には幾つかの定式化があるが，ここでは代表例を示す．ペアリングを用いたプロトコルはこれらの安全性の仮定が成り立つとして組み立てている．まず，ペアリングを用いたプロトコルで用いられる安全性根拠となる各種の問題を示す．

双線形計算DH問題[BCDH]

だ円曲線上で，与えられた入力組(P, aP, bP, cP)に対して$e(P, P)^{abc}$，を出力すること．

双線形判定DH問題[BDDH]

だ円曲線上で，与えられた入力組(P, aP, bP, cP, T)に対して$T=e(P, P)^{abc}$か否かを判定すること．

これらは有限体上における次の問題のペアリング版である．

計算DH問題[CDH]

有限体上で，与えられた入力組(g, g^a, g^b)に対してg^{ab}を出力すること．

判定DH問題[DDH]

与えられた入力組(g, g^a, g^b, T)に対して$T=g^{ab}$か否かを判定すること．

なお，多くの暗号の安全性の基礎となっているのは次の有限体上の離散対数問題である．

離散対数問題[DL]

与えられた入力組(g, g^a)に対してaを出力すること．

これらの問題の困難さには依存関係があり，帰着関係と呼ばれる．

・離散対数問題が解ければ計算DH問題が解ける．

・計算DH問題が解ければ判定DH問題が解ける．

・判定DH問題が解ければ双線形判定DH問題が解ける．

・双線形計算DH問題が解ければ双線形判定DH問題が解ける．

すなわち，この中では双線形判定DH問題が相対的に他の問題より易しい（または同程度に難しい）．帰着関係で言えば

双線形判定DH問題→判定DH問題→計算DH問題→離散対数問題

また，

双線形判定DH問題→双線形計算DH問題→離散対数問題

となる．ここで，問題A，Bに対して，A→Bとは「AはBに帰着する」ことを意味する．

暗号プロトコルの設計に際してはこれらの問題がすべて困難であるとしている．実際，これまでに効率良く解くアルゴリズムは報告されていない．

3．ペアリングの計算法

3.1 ペアリング計算の基本アルゴリズム

ペアリングの計算は，定義式

$$e(P,Q)=f_P(Q)^{\frac{q^k-1}{r}}$$

から分かるように，次の条件を満たす有理関数f_Pの計算に帰着される．

$div(f_P)=r(P)-r(O)$

さて，f_hを

$div(f_h)=h(P)-(hP)-(h-1)(O)$

を満たす有理関数とし，これを用いて再帰的に$f_P=f_r$を求める方法を示す．基本となる公式は

$$div(f_{i+j}) - div(f_i) - div(f_j) = div\left(\frac{l_{iP,jP}}{v_{(i+j)P}}\right)$$

である．これは次のようにして示される．iPとjPを通る直線を$l_{iP,\,jP}$とし，$(i+j)P$を通る垂線を$v_{(i+j)P}$とすると，直線の主因子の公式

$$div\,(l_{R,S}) = (R) + (S) + (-(R+S)) - 3\,(O)$$

より，

$$\begin{aligned} div\left(\frac{l_{iP,jP}}{v_{(i+j)P}}\right) &= div(l_{iP,jP}) - div(v_{(i+j)P}) \\ &= \{(iP) + (jP) + (-(i+j)P) - 3(O)\} \\ &\quad -\{(i+j)P + (-(i+j)P) - 2(O)\} \\ &= (iP) + (jP) - (i+j)P - (O) \end{aligned}$$

となる．一方f_hの定義から

$$\begin{aligned} &div(f_{i+j}) - div(f_i) - div(f_j) \\ &= \{(i+j)(P) - ((i+j)P) - (i+j-1)(O)\} \\ &\quad -\{i(P) - (iP) - (i-1)(O)\} - \{j(P) - (jP) - (j-1)(O)\} \\ &= (iP) + (jP) - ((i+j)P) - (O) \end{aligned}$$

が得られ，両者は等しくなる．

したがって，

$$div(f_{i+j}) = div(f_i) + div(f_j) + div\left(\frac{l_{iP,jP}}{v_{(i+j)P}}\right) = div(f_i f_j \frac{l_{iP,jP}}{v_{(i+j)P}})$$

より，再帰的公式

$$f_{i+j} = f_i f_j \frac{l_{iP,jP}}{v_{(i+j)P}}$$

が得られた．これをもとにして，$f_P = f_r$を求める．なお，上記再帰的公式は正確には定数倍の任意さがあるが，Tateペアリングにおける最終べき乗で消えるので，省略してよい．

Millerアルゴリズム

$e\,(P, Q)$の計算

$r = (r_{t-1}, \cdots, r_0)_2, f = 1, V = P$
for $i = t-1$ to 0 do
$f = f^2 \frac{l_{V,V}(Q)}{v_{2V}(Q)}$ and $V = 2V$
if $r_i = 1$ then $f = f \frac{l_{V,P}(Q)}{v_{V+P}(Q)}$ and $V = V + P$
end for
return $f^{\frac{q^k-1}{r}}$

ここで，$r = (r_{t-l}, \cdots, r_0)_2$は$r$の2進展開を表している．

3. 2 実装上の留意点

実装上，考慮する点が幾つかある．

(1) 曲線の選び方

ペアリング計算に使いやすいだ円曲線として超特異曲線が挙げられる．この場合，曲線の群位数は簡単に求められる．例えば，

$q = p$のときは，$y^2 = x^3 + 1$（ただし$p \equiv 2 \bmod 3$）や$y^2 = x^3 + x$（ただし$p \equiv 3 \bmod 4$）が超特異曲線で，$|E(F_q)| = p + 1$

$q = 2^m$のときは，$y^2 + y = x^3 + x$や$y^2 + y = x^3 + x + 1$が超特異曲線で，$|E(F_q)| = 2^m + 1 \pm 2^{\frac{m+1}{2}}$

$q = 3^m$のときは，$y^2 = x^3 - x \pm 1$が超特異曲線で，

$$|E(F_q)| = 3^m + 1 \pm 3^{\frac{m+1}{2}}$$

である．超特異曲線でない例としては，MNT曲線がよく知られている[6]．更に，通常の曲線を使う方法も提案されている[7]．

(2) $E\,(F_q)\,[r]$における点Pの求め方

ここでは$q = p$の場合を示す．このとき，Pは$E\,(F_q)$上の任意の点Rに対し$P = ((p+1)/r)\,R$で求められる．なぜなら，$|E\,(F_q)| = p + 1$より$rP = (p+1)\,R = O$だからである．rは定義より$r \mid p^2 - 1$を満たし$r \mid p - 1$は満たさないので，$r \mid p + 1$であることに注意する．ただし，$P = O$のときは使えないのでRを選び直す必要がある．なお，rが素数ならばrはPの位数にもなっている．

(3) 点Qの選び方

Pは$E\,(F_q)$から選ぶが，Qは$E\,(F_q)$でなく$E\,(F_{q2})$から選ばなくてはならない．そうしなければ，$e\,(P, Q)$がF_qに属し，$(q^2 - 1)/r = \{(p+1)/r\}\,(q-1)$で最終べき乗すると消えてしまう．

このための最も簡単な方法はDistortion写像φを使う方法である．例えば，$q = p \equiv 3 \bmod 4$の場合

$$\varphi(x, y) = (-x,\ \sigma y)$$

はだ円曲線$y^2 = x^3 + x$上の同形写像であり，$E\,(F_q)$の点をその外へ写像する．ここで，σは$F_{qk} - F_q$の元である．

$p \equiv 3 \bmod 4$ならば-1は非平方数であるので$\sigma^2 + 1 = 0$となるσとすればよい．標数2や3の拡大体でもこのような写像が存在する．

このとき，$E\,(F_q)$の点Qに対する$\varphi(Q)$を改めてQとして用いればよい．

3. 3 ペアリング計算の高速化

(1) Millerアルゴリズムの簡単化

Millerアルゴリズムに現れる分母はx座標しか現れない．上記の場合は

$\varphi(x, y) = (-x, \sigma y)$

の形の写像を用いるが，そのとき分母にはσが現れない．したがって最終べき乗の中の$(p-1)$により，分母はすべて消えてしまう．このことから，この場合のMillerアルゴリズムは簡単化できる．

簡単化Millerアルゴリズム

$e(P, Q)$の計算

$r = (r_{t-1}, \cdots, r_0)_2, f = 1, V = P$
for $i = t-1$ to 0 do
$f = f^2 \cdot l_{V,V}(\varphi(Q))$ and $V = 2V$
if $r_i = 1$ then $f = f \cdot l_{V,P}(\varphi(Q))$ and $V = V + P$
end for
return $f^{\frac{q^k-1}{r}}$

このほかにも幾つかの細かな改良手法があり，これらを合わせると，計算処理速度は約1けた上がる[8]．

(2) $E(F_{3^m})$における高速化手法とη_Tペアリング

標数3に限ると，高速処理上有利となる性質が幾つか知られている．対象とするだ円曲線は超特異曲線$y^2 = x^3 - x + b$，$b = \pm 1$とする．

・3倍点$Q = 3P$の計算が容易となる．

$$3(x, y) = (x^9 - b, -y^9)$$

・rの3進数表現$r = (r_{t-1}, \cdots, r_0)_3$において$r_i = 0, \pm 1$とでき，2を用いるよりアルゴリズムが簡単化できる．これは点の逆元を利用できることに起因する．

・有理関数f_iを求める再帰式は，3進展開では

$$f_{3j} = f_j^3 \frac{l_{jP,2jP}}{v_{3jP}} \cdot \frac{l_{jP,jP}}{v_{2jP}}$$

となるが，そこに現れる4直線の組合せ有理関数の代りに，$h_V = \beta^3 y - (\alpha^3 - x + b)^2$の形の二次曲線が使える[9]．

・rよりも小さいTに関して，$\eta_T(P, Q) = f_T(P, \varphi(Q))$で定義される$\eta_T$は双線形性を持ち，Tateペアリングとの間には次の関係が成り立つ．

$$(\eta_T(P,Q)^M)^{3T^2} = e(P,\varphi(Q))^L$$
$$T = -b3^{(m+1)/2} - 1,\ L = -b3^{(m+3)/2}$$
$$M = (3^{6m} - 1)/(3^m + b3^{(m+1)/2} + 1)$$

これをη_Tペアリングという．Tの長さはmの約半分なので，再帰回数を半減できる[10]．したがって，Tateペアリングでなくこのη_Tペアリングを求めることが多くなってきている．なお，η_Tペアリングは標数3以外にも提案されている．

標数3におけるこれらの性質を利用したη_Tペアリング計算法が次のアルゴリズムである．ここには，Distortion写像も含まれている．

η_Tペアリングアルゴリズム

$\eta_T(P, Q)$の計算

$P = (x_p, y_p), Q = (x_q, y_q)$
if $b = 1$ then $y_p \leftarrow -y_P$
$f \leftarrow \sigma y_q + y_p(\rho - x_p - x_q - 1)$
for $j \leftarrow 0$ to $(m-1)/2$ do
$u \leftarrow x_p + x_q + b$
$g \leftarrow \sigma y_p y_q - u^2 - \rho u - \rho^2$
$f \leftarrow fg$
$x_p \leftarrow x_p^{1/3}, y_p \leftarrow y_p^{1/3}$
$x_q \leftarrow x_q^3, y_q \leftarrow y_q^3$
end for
return f

ここでσ，ρは$\sigma^2 + 1 = 1$，$\rho^3 - \rho - b = 0$を満たす六次拡大体の元である．mが6と互いに素ならばこれらを添加することにより拡大できる．

もしTateペアリング$e(P, \varphi(Q))$が必要ならば上記の関係式$(\eta_T(P, Q)^M)^{3T^2} = e(P, \varphi(Q))^L$から求めればよい．三乗根は多項式計算量で求められる．

η_Tペアリングアルゴリズムには三乗根演算があるが，その計算はそれほど困難ではないにしても，三乗に比べればやはり多い．そこで，上記アルゴリズムで三乗根演算を取り除いたアルゴリズムが提案されている[11]．基本的アイデアは，η_Tペアリングアルゴリズムの中のループの途中に，新たに三乗操作を導入することにより三乗根演算を除去することにある．

表1　Optimized（Twisted）Ateペアリング性能評価

パラメータ	ペアリング	演算時間(ms)	
		Standard	Optimized
$k = 6, \log_2 q \sim 512, \log_2 r \sim 256$ MOV security ～ 3072	Tate	38.2	
	Twisted Ate	38.9	19.3
$k = 8, \log_2 q \sim 384, \log_2 r \sim 256$ MOV security ～ 3072	Tate	64.1	
	Twisted Ate	96.8	48.2
$k = 12, \log_2 q \sim 256, \log_2 r \sim 256$ MOV security ～ 3072	Tate	84.8	
	Twisted Ate	84.1	59.1

改良 η_T ペアリングアルゴリズム

$\eta_T(P,Q)^{3^{(m+1)/2}}$ の計算
if b = 1 then $y_p \leftarrow -y_p$
$u \leftarrow x_p + x_q + b$
$d \leftarrow b$
$f \leftarrow \sigma y_q - u y_p + \rho y_p$
for $j \leftarrow 0$ to $(m-1)/2$ do
$u \leftarrow x_p + x_q + d$
$g \leftarrow \sigma y_p y_q - u^2 - \rho u - \rho^2$
$f \leftarrow (fg)^3$
$y_p \leftarrow -y_p$
$x_q \leftarrow x_q^9, y_q \leftarrow y_q^9$
$d \leftarrow d - b \bmod 3$
end for
return f

この出力 $\eta_T(P,Q)^{3^{(m+1)/2}}$ から $\eta_T(P, Q)$ を求めるのは容易である．これは $F_{3^{6m}}$ においては，3のべき乗根をわずかな加減算のみで計算できるからである[11]．

(3) Ateペアリング / Twisted Ateペアリングとその高速化

Tateペアリングでは

$$e : E(F_q)[r] \times E(F_{q^k}) \Big/ rE(F_{q^k}) \rightarrow \mu_r$$
$$e(P,Q) = f_{r,P}(Q)^{\frac{q^k-1}{r}}$$

から分かるように，P と Q の定義体が異なる．この2点を入れ替えた形の $f_{T,Q}(P)$ をもとにした

$$a_T(Q,P) = f_{T,Q}(P)^{c_T(q^k-1)/N}$$

もまた双線形性を持つことが示される．ここで，$T = t-1$（t はトレース $q+1-\#E(F_q)$），$N = \gcd(T^k-1, q^k-1)$，$c_T = \sum_{i=0}^{k-1} T^{k-i-1} q^i$ である．この $a_T(Q,P)$ はAteペアリングとよばれる．この命名は η のスペルを逆読みしたことによるとのことである．

一般にトレース t のサイズは q のサイズの半分になるので，$r \approx q$ ならTateペアリング（Millerアルゴリズム）のループ回数を半減できる．

また，だ円曲線におけるTwistという写像を用いることにより，Ateペアリングの定義域の順序を元に戻したTwisted Ateペアリングも定義でき，k の約数 e が $-r \le T^e \le r$ を満たせばループ回数はTateペアリングに比較して削減できる．ここで $e = k/GCD(k, \#Aut(E))$ である $\#Aut(E)$ は E 上の自己同形写像の個数）[7]．

このAteペアリングとTwisted Ateペアリングに対して，ループ回数を更に減らし，Twisted Ateペアリングにおける $-r \le T^e \le r$ という条件を外すことにより，適用可能な曲線を大幅に増やすことが可能である[12]．

Ateペアリングに対していえば，

$$a_S(Q,P) = f_{S,Q}(P)^{c_S(q^k-1)/N}$$

で定義される関数は双線形性を満たす．これをOptimized Ateペアリングと言う．ここで，$S = q \bmod r$，$N = \gcd(S^k-1, q^k-1)$，$c_T = \sum_{i=0}^{k-1} S^{k-i-1} q^i$ である．S を適切に選ぶことにより，ループ回数を半減でき，実際，実装した結果表1にもそれが現れている．なお，パラメータの設定上，拡大体のサイズを3072ビットとしている．

同様の手法はTwisted Ateペアリングを改良したOptimized Twisted Ateペアリングにも適用できる．$|T^e| \ge r$ の場合は整数 n を用いて $|S| \le r$ となるように $S = T^e - n \cdot r$ をとり，この S に対して改めてTwisted Ateペアリングを考えればよい．しかし，最後のべき乗のべき指数は変化する（詳細は文献(12)参照）．

4. ペアリング実装例と計算ツール

最近，η_T ペアリングの実装をソフトウェアとハードウェア

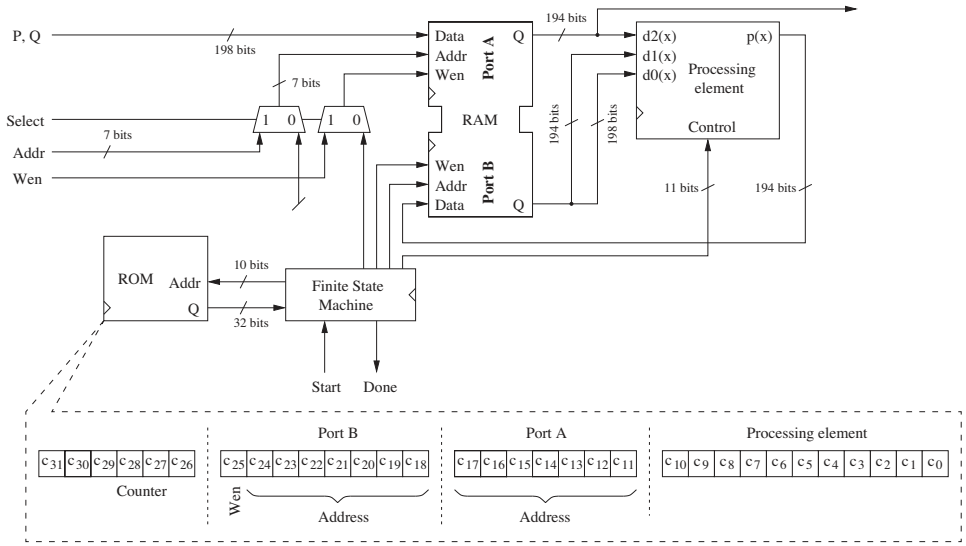

図2　改良 η_T ペアリング計算回路

それぞれについて行ったので，紹介する．

4. 1 ソフトウェア実装

我々は，科学技術振興調整費・重要課題解決型研究の推進“セキュリティ情報の分析と共有システムの開発”において，η_TペアリングのライブラリとAPI設計を行い，WindowsやUnix環境上で実装した[13]．ライブラリは下記のサイトに公開している．

http://www.cipher.risk.tsukuba.ac.jp/pairing_lib/

ライブラリの実装に当たっては，体演算ライブラリ，だ円曲線ライブラリ，ペアリングライブラリをそれぞれ実装した．ペアリングを実装する場合は，最も下位層に有限体（拡大体）ライブラリを実装しなくてはならない．ペアリングやだ円曲線演算の構成法は，大きな素数を標数とする体（以下，標数p）を利用するか，標数が小さな（例えば，標数が2や3など）体の拡大体を利用するかによって大きく異なる．我々は，安全性，性能などを考慮して，標数p及び標数3の体演算ライブラリを実装し，その上で動作するだ円曲線ライブラリ，及びペアリングライブラリを実装した．拡大体の次数も選べるようになっている．

計算例を挙げると，計算環境

OS：Red Hat Linux 9

CPU：Pentium 4 3.4GHz

メモリ：1GByte

のもとでの1回の処理時間は，

η_T：$E(F_{3^{97}})\times E(F_{3^{6\cdot 97}})\rightarrow F_{3^{6\cdot 97}}$　　4. 32ms

であった．ちなみに，同環境で

$E(F_{3^{97}})$上スカラ倍	1. 31ms
1024ビットべき乗剰余演算	8.69ms

であるので，かなり実用的な計算処理速度が得られている．

なお，当サイトでは，公開文献（14）に記載のグループ署名方式も同時に実装し，公開している．

4. 2 ハードウェア実装

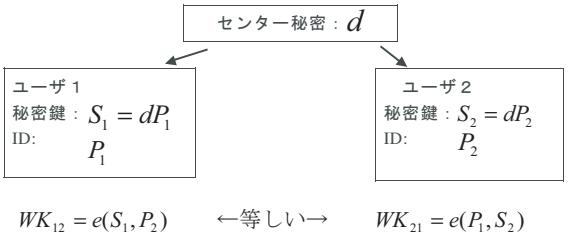

図3　IBE

η_Tペアリング（改良形を含む）のハードウェア実装は，新エネルギー・産業技術総合開発機構（NEDO）半導体アプリケーションチッププロジェクト，“Pairing Liteの研究開発”で進めており，標数3でmが97のケースをFPGA（Field Programmable Gate Array）に実装済みである．

プロセッサを9個持つタイプと，1個のみを持つタイプの2種類で実現している．プロセッサは乗算，加減算，3乗算，累算を一つで行えるものを2676 LE（Logic Element）で構成しており，ほぼ最小に近い形である．

マルチプロセッサタイプ

Cyclone II EP2C35
9プロセッサ
18,000スライス
クロック周波数　147MHz
計算時間　27 μ s

シングルプロセッサタイプ

Vertex- II Pro4
1プロセッサ
1,888スライス
クロック周波数　147MHz
計算時間　222 μ s

これらを比較すると，当然マルチプロセッサタイプが高速であるが，シングルプロセッサタイプは論理回路素子が非常に少ないので，応用上はシングルプロセッサタイプが好まれる可能性がある．その回路ブロック図を図2に示す[15]．

5. ペアリングの優位性を利用したプロトコル

ペアリングの持つ双線形性ゆえに，多くの暗号プロトコルが提案されている．ここでは，年代順に代表的な適用例を簡単に示そう．

5. 1 MOV帰着[1]

有限体上の離散対数問題DLについては，現時点の最良解法アルゴリズムは準指数的計算量であるが，だ円曲線上では指数的計算量アルゴリズムしか知られていない．ここに，ペアリングを持つだ円曲線上では有限体に射影することにより準指数的計算量に変換するのが，MOV帰着である．

ペアリングを持つだ円曲線上の離散対数問題（Bilinear Elliptic Curve Discrete Logarithm Problem）が次のように与えられたとする．

BECDLP：与えられた入力組(P, aP)に対してaを出力すること．

ここで，MOV帰着

$g = e(P, P)$

$$e\,(P, aP) = e\,(P, P)^a = g^a$$

を用いると，与えられた入力組 (g, g^a) に対して a を出力する，というように有限体上の離散対数問題に変換することができる．

有限体上の離散対数問題は準指数計算量で解けるので計算量は少なくなると期待できる．ただし，有限体といってもだ円曲線の基礎となる体 F_q ではなく，その k 次拡大体 F_{q^k} であることに注意する必要がある．したがって，k が余り大きいと，準指数計算量といっても F_q 上の指数的計算量より多くなる．

5. 2 三者間公開鍵配送[2]

DiffieとHellmanによって提案されたいわゆるDH公開鍵配送方式は二者間の鍵配送方式である．それが2000年にJouxによって，ペアリングを用いることにより三者間に広げられた．

三人のユーザをA, B, C とする．各々の秘密鍵と公開鍵のペアを，(a, P_A)，(b, P_B) (c, P_C) とする．ここで，秘密鍵と公開鍵の間には次のような関係がある．

$$P_X = xP$$

P はだ円曲線上のある固定点である．

このとき，この三者間での共有鍵は次のようにして得ることができる．

ユーザA：$WK_A = e\,(P_B, P_C)^a$
ユーザB：$WK_B = e\,(P_C, P_A)^b$
ユーザC：$WK_C = e\,(P_A, P_B)^c$

これらがすべて $e\,(P, P)^{abc}$ に等しいことは，ペアリングの双線形性から明らかである．この安全性は双線形計算DH問題[BCDH]の困難さによる．

5. 3 IDに基づく暗号

IDに基づく暗号（IBE）は1980年代に定式化され研究も行われた．しかし，予備通信が必要であったり，安全性上のしきい値があったりして，必ずしも満足のいくものではなかった．これらの問題は2000年になってペアリングの双線形性を利用することにより，境・大岸・笠原らによって解決された[3]．

IBEの基本となっている鍵配送方式を図3に示す．

鍵を共有するユーザ1, 2のほかに，信頼できるセンターCが必要となる．

センターCは秘密情報 d を持ち，ユーザ i はID情報に対応しただ円曲線上の点 P_i を持っている．ID情報はユーザを特定する情報ならば何でもよく，例えばメールアドレスなどがよく用いられる．ID情報からだ円曲線上の点への対応はMapToPointと呼ばれるが，公開写像で簡単に計算できるので，ここでは P_i 自身をIDとみなす．

ユーザ i は秘密鍵としてあらかじめセンターから

$$S_i = dP_i$$

を秘密に受け取っている．

さて，実際の鍵配送時には各ユーザは次のようにして共有鍵を計算する．

ユーザ1：$WK_{12} = e\,(S_1, P_2)$
ユーザ2：$WK_{21} = e\,(P_1, S_2)$

これらはペアリングの双線形性により等しい：

$$e\,(dP_1, P_2) = e\,(P_1, P_2)^d = e\,(P_1, dP_2)$$

なお，ここではベースになる方式を示したが，次のようにすることもできる．例えばユーザ1がユーザ2のメールアドレスで鍵を作成し，それでメールを暗号化してユーザ2に送ったとしよう．そのとき，ユーザ2はそのメールを受け取ってからセンターに秘密鍵を問い合わせる．このようにするとあらかじめユーザ2は秘密鍵をもらっておく必要はなくなる．

これらの方式では予備通信は不要であり，また結託攻撃により生じるしきい値も事実上存在しないため，従来のIBEの課題を解決している．安全性についての根拠は明確には示されていなかったが，Boneh・Franklinは2001年に安全性が双線形計算DH問題[BCDH]に依存する方式を与えた[16]．IBEというと，こちらの暗号方式を指す場合が多く，これをもってペアリングを用いたIDベース暗号はBoneh・Franklinによって最初に提案されたといわれることが多いが，正しい記述とは言えない．

5. 4 ショート署名

ペアリングを用いることにより署名長を従来より短くできる方式が幾つか提案されている．ここではBoneh・Lynn・Shachamによる方式を紹介する[17]．

本方式ではセンターは必要ない．署名生成者はだ円曲線上の点 P を定め，整数 s をランダムに生成して P, $V = sP$ を公開する．

メッセージ m の署名は

$$Q_m = sH(m)$$

となる．ここで H はMapToPointである．

検証は

$$e(V, H(m)) \stackrel{?}{=} e(P, Q_m)$$

が成立するか否かで行われる．双線形性より，正しいメッセージと署名に対してはこの等式は成立する．

署名Q_mはだ円曲線上の点であり，ビット長は$|q|$と同程度の短さである．

安全性について，Hが理想的なランダム関数であり，かつ双線形計算DH問題[BCDH]の困難性を仮定すれば，この方式は高い安全性を持つことが証明できる(17)．

5. 5 放送暗号

ペアリングを用いることにより，番組放送用のスクランブル鍵を効率的に配送できることを示す．すなわち，あらかじめ全加入端末に個別鍵をセットしておき，ある番組放送に際して鍵配送センターは希望視聴者のみに個別鍵で当該番組のスクランブル鍵を暗号化して配送する．

この場合，全体では希望視聴者数に比例した帯域が必要となるのが常識である．ところがBoneh・Gentry・Watersが示した方式(18)によると，加入者数にかかわらず一定のビット長で鍵を配送できる．希望視聴者をユーザ1からユーザnとする．

[セットアップ]

鍵配送センターはだ円曲線上の点Pを定め，ランダムな整数α，γを生成し，$P, P_1, P_2, \cdots, P_n, P_{n+2}, \cdots, P_{2n}, Q$を公開する．ここで，$P_i = \alpha^i P, Q = \gamma P$である．

ユーザiの秘密鍵は$D_i = \gamma P_i$である．

[暗号化]

センターは乱数tを生成し，

$$C_0 = tP$$

$$C_1 = t(Q + \sum_{j \in S} P_{n+1-j})$$

を全ユーザに送る．ここで，Sは復号を許可するユーザの集合を表す．

このとき，暗号化に用いる鍵は

$$K = e\ (P_{n+1}, P)^t$$

となる．

[復号化]

ユーザ$i \in S$は(C_0, C_1)を受け取り，

$$K = \frac{e(P_i, C_1)}{e(D_i + \sum_{\substack{j \in S \\ j \neq i}} P_{n+1-j+i}, C_0)}$$

より，鍵を求める．送受信側で鍵が一致することは，ペアリングの双線形性から明らかである．

同報通信されるデータ(C_0, C_1)のビット長はnや復号を許可した人数にかかわらず，一定であることに注意されたい．

安全性は，双線形計算DH問題[BCDH]に派生して生じたいわゆるℓ- BDHE問題に基づく．これは$(Q, P, \alpha P, \alpha^2 P, \cdots, \alpha^l P, \alpha^{l+2} P, \cdots, \alpha^{2l} P)$から$e\ (P,Q)^{\alpha^{l+1}}$を求める問題であり，この問題の困難性を仮定すれば，この方式は高い安全性を持つことが証明できる(18)．

6. あとがき

ペアリングに関して，基礎から実装，応用にわたる解説を試みた．ペアリングについては，まとまった一般向け解説が少なく，特に計算法や実装についての解説が少ないと思われたので，そこを重点的に解説したつもりである．なお，プロトコルについては紙面の関係もあり，簡単に触れるだけとし，特に安全性における攻撃と解読の定義については省略した．これらについては文献(19)などを参照するとよい．

ペアリングに基づいた暗号を研究している我々としては，今後更にペアリングの研究が進み，利用・普及も促進されることを期待する．

最後に，本解説に載せた幾つかの成果は我々の共同研究から生まれたことを付け加えておく．ここに，公立はこだて未来大学の高木　剛先生，白勢政明氏，情報セキュリティ大学院大学の土井　洋先生，NECの側高幸治氏，筑波大学のJean- Luc Beuchat氏，松田誠一氏(現ソニー)に深謝する．

文　献

(1) A. Menezes, T. Okamoto, and S. Vanstone, “Reducing elliptic curve logarithms to logarithms in a finite field,” IEEE Trans. Inf. Theory, vol.39, pp.1639-1646, 1993.
(2) A. Joux, “A one round protocol for tripartite Diffie-Hellman,” Proc. of Algorithmic Number Theory Symposium Ⅳ , Lect. Notes Comput. Sci., vol.1838, pp.385-294, 2000.
(3) R. Sakai, K. Ohgishi, and M. Kasahara, “Cryptosystems based on pairing,” Proc. of SCIS2000, 2000.
(4) L. C. Washington., Elliptic curves: Number Theory and Cryptography, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2003.
(5) R. Balasubramanian and N. Koblitz, “The Improbability that an elliptic curve has subexponential log problem under the Menezes-Okamoto-Vanstone algorithm,” J. Cryptol., vol.11, pp.141-145, 1998.
(6) A. Miyaji, M. Nakabayashi, and S. Takano, “New explicit conditions of elliptic curve traces for FR-Reduction,” IEICE Trans. Fundamentals, vol. E84-A, no.5, pp. 1234-1243, May 2001.
(7) F. Hess, N.P. Smart, and F. Vercauteren, “The eta pairing revisited,” IEEE Trans. Inf. Theory, vol.52, no.10, pp.4595-4602, Oct. 2006.
(8) S. Matsuda, A. Inomata, T. Okamoto, and E. Okamoto, “Performance evaluation of efficient algorithms for Tate pairing,” Proc. of PacRim2005, 2005.
(9) I. Duursma and H. S. Lee, “Tate pairing implementation for hyperelliptic cruves y^2=xp-x+d,” ASIACRYPT 2003, Lect. Notes Comput. Sci., vol. 2894, pp.111-123, 2003.
(10) P. S. L. M. Barreto, S. Galbraith, C. O. hEigeartaigh, and M. Scott, “Efficient pairing computation on supersingular abelian varieties,” To appear in Designs, Codes and Cryptography.
(11) 白勢政明，高木　剛，岡本栄司，“ペアリングの最終べきについて，”信学技報，ISEC2006-98, pp.19-26, Nov. 2006.
(12) 松田誠一，金山直樹，岡本　健，岡本栄司，“Twisted Ate ペアリングの高速化手法の提案，” 信学技報，ISEC2006-106, pp.29-34, Dec. 2006.
(13) 側高幸治，松田誠一，土井　洋，岡本　健，小松文子，岡本栄司，“匿名署名を実現するためのPairingを用いたグループ署

名ライブラリの実装," DICOMO2007, 2007.
(14) D. Boneh, X. Boyan, and H. Shacham, "Short group signatures," Proc. of Crypto2004, Lect. Notes Comput. Sci., vol. 3152, pp.41-55, 2004.
(15) J.-L. Beuchat, N. Brisebarre, J. Detrey, and E. Okamoto, "Arithmetic operators for pairing-based cryptography," IACR ePrint Archive, 2007/091, 2007.
(16) D. Boneh and M. Franklin, "Identity based encryption from the Weil pairing," Extended Abstract in Proceedings of Crypto '2001, Lect. Notes Comput. Sci., vol. 2139, pp. 213-229, 2001. (SIAM J. Comput., vol. 32, no. 3, pp. 586-615, 2003.)
(17) D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," Extended Abstract in Proceedings of Asiacrypt '01, Lect. Notes Comput. Sci., vol. 2248, pp. 514-532, 2001. (J. Cryptol., vol. 17, no. 4, pp. 297-319, 2004.)
(18) D. Boneh, C. Gentry and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," CRYPTO 2005, Lect. Notes Comput. Sci., vol. 3621, pp.258-275, 2005.
(19) T. Okamoto, "On pairing-based cryptosystems," Proc. of VIETCRYPT2006, Lect. Notes Comput. Sci., vol. 4341, pp.50-66, 2006.

岡本　栄司(正員：フェロー)

1973東工大・工・電子卒．1978東工大大学院博士課程了．工博．同年日本電気入社．その後，北陸先端大，東邦大を経て2002より筑波大教授，現在に至る．情報セキュリティを中心とする情報数理工学の教育・研究に従事．1990本会論文賞，1993情報処理学会ベストオーサ賞受賞．2003本学会フェロー、2004情報処理学会フェロー．著書「暗号理論入門」(共立出版)，「電子マネー」(岩波書店)など．IEEE, ACM,情報処理学会各会員，IJIS(International Journal of Information Security)編 集 長，IEEE Information Theory Society の Associate Editor.

岡本　健(正員)

2002北陸先端大大学院博士課程了．博士(情報科学)．同年東京電機大・理工・情報科学・助手．その後2003より筑波大・システム情報工学・講師，現在に至る．情報セキュリティ，暗号とその応用に関する研究に従事．著書に「科学大辞典 第2版」(丸善出版：分担執筆)「Linuxハンドブック」(オライリージャパン：共訳)など．

金山　直樹(正員)

1996早大・理工・数学卒．2001年同大学院博士課程中退．同年早大・理工・助手．整数論に関するアルゴリズムとその公開鍵暗号への応用についての研究に従事．

現在，筑波大研究員．博士(理学)．