筑波大学大学院博士課程

システム情報工学研究科修士論文

ペアリング演算の高速化に関する研究

松田　誠一

(リスク工学専攻)

指導教員　岡本 栄司

2007年3月

概要

ペアリングとは楕円曲線上で定義される双線形写像であり，2000 年以降，暗号プリミティブとして広く利用されるようになった．具体例として ID を公開鍵として利用可能な Identity Based Encryption，既存方式より短い署名長で済む Short Signature などがあり，従来にない特性を有するプロトコルを構成することが可能である．しかし，主要な暗号要素技術と比較して計算コストが大きく，効率的な演算アルゴリズムが求められている．

楕円曲線の中でも Supersingular Curve は distortion map を持つなどペアリングに非常に適しており，その曲線上で定義される Eta ペアリングは現在最も高速なペアリングである．しかし，Supersingular Curve はパラメータ設定の際に重要となる埋め込み次数が固定値であるため，より高い安全性水準にも柔軟に対応可能な Oridnary Curve における効率的なペアリングが必要となる．Eta ペアリングを一般化した Ate ペアリング，Twisted Ate ペアリングは Ordinary Curve において定義可能であり，一般的に Tate ペアリングより高速に計算可能である．ただし，Ate ペアリングにおいては $\deg(t) \geq \deg(r)$, Twisted Ate ペアリングにおいては $(t-1)^e > r$ のとき，Tate ペアリングよりも計算コストが大きいという点において未だ不十分である．

本稿では，Ordinary Curve における Ate ペアリング及び Twisted Ate ペアリングに対して，Eta ペアリングのループ回数削減手法を適用し，ループ長を短縮した Optimized Ate ペアリング及び Optimized twisted Ate ペアリングを提案する．また提案手法の有用性を評価するために計算コストの推定及びソフトウェア実装による性能評価を行い，提案したペアリングは常に Tate ペアリングよりも高速に計算可能であることを示す．

目 次

第 1 章　序論 **1**
1.1 背景 1
1.2 目的 2
1.3 構成 2

第 2 章　数学的準備 **3**
2.1 整数論 3
2.1.1 群 3
2.1.2 環 5
2.1.3 体 6
2.2 楕円曲線理論 8
2.2.1 楕円曲線 8
2.2.2 twist 13
2.2.3 因子 15
2.2.4 引き戻し 18

第 3 章　ペアリング **20**
3.1 ペアリングの定義 20
3.1.1 Tate ペアリング 20
3.1.2 Weil ペアリング 21
3.1.3 Miller’s Algorithm 23
3.2 ペアリングを利用した方式における安全性 24
3.2.1 暗号系における安全性 24
3.2.2 離散対数問題 25
3.3 ペアリングを利用した応用プロトコル 27
3.3.1 ID に基づく方式 27
3.3.2 応用プロトコルにおける計算コスト 28

第 4 章　ペアリング演算 **29**
4.1 楕円曲線の生成手法 29
4.1.1 Pairing-friendly Curves 29
4.1.2 Supersingular Curve 30

4.1.3 Ordinary Curve . . . 31
4.2 有限体における演算 . . . 34
4.2.1 Pairing-friendly field . . . 34
4.2.2 Karatsuba-Ofman 法 . . . 34
4.2.3 Toom-Cook 法 . . . 35
4.3 演算アルゴリズム . . . 37
4.3.1 BKLS アルゴリズム . . . 37
4.3.2 Duursma and Lee アルゴリズム . . . 39
4.3.3 Eta ペアリング . . . 41

第 5 章 提案手法 46
5.1 Ate ペアリング . . . 46
5.2 Twisted Ate ペアリング . . . 49
5.3 Optimized Ate & optimized twisted Ate ペアリング . . . 50

第 6 章 実装方式 53
6.1 プログラム構成 . . . 53
6.2 パラメータ設定 . . . 54
6.2.1 安全性基準 . . . 54
6.2.2 楕円曲線 . . . 54
6.2.3 twist . . . 57
6.3 ペアリング演算 . . . 59
6.3.1 逐次拡大体 . . . 59
6.3.2 楕円曲線における演算 . . . 60
6.3.3 Miller Operation . . . 61

第 7 章 性能評価 63
7.1 理論値による評価 . . . 63
7.1.1 計算コスト推定 . . . 63
7.1.2 性能評価 . . . 64
7.1.3 各演算の計算コスト . . . 65
7.2 実測値による評価 . . . 66
7.2.1 実測環境 . . . 66
7.2.2 実測結果 . . . 66

第 8 章 結論 67

謝辞 68

参考文献 69

図 目 次

2.1 楕円曲線における点の加算 9
2.2 写像の引き戻し 19

3.1 数学的問題の帰着関係 25
3.2 離散対数問題の計算量と有限体のサイズ 26

6.1 プログラム構成 53
6.2 拡大体 $\mathbb{F}_{p^6}, \mathbb{F}_{p^8}, \mathbb{F}_{p^{12}}$ の構成 59

表 目 次

2.1 オイラー関数 $\varphi(n)$ 5

3.1 離散対数問題の計算量 26
3.2 応用プロトコルにおける計算コスト 28

4.1 種数 1 の Supersingular Curve 30
4.2 MNT Curve 32
4.3 2,3 次拡大体における乗算・2 乗算の計算コスト 36

6.1 MOV secuirty/Group order に対する埋め込み次数と定義体のサイズの関係 . . 54
6.2 埋め込み次数 k に対する生成可能な曲線の ρ 55
6.3 楕円曲線上の演算の計算コスト 61
6.4 直線式の計算コスト 62

7.1 ペアリングの計算コスト 64
7.2 各演算の計算コスト 65
7.3 実測環境 66
7.4 ペアリングの演算時間 66

第1章　序論

1.1　背景

本来，ペアリングは楕円曲線暗号に対する攻撃手法 (MOV attack [31]) の 1 つとして認識されていたが，2000 年にペアリングを利用した事前準備不要の鍵共有方式 [33]，3 者間鍵共有方式 [21] が提案され，その有用性が明らかとなり，ペアリングを応用したプロトコルの研究が活発に行われるようになった．公開鍵として ID を利用可能な Identity Based Encryption(IBE) [6]，既存方式より短い署名長で済む Short Signature [8] などに代表されるように，双線形性と呼ばれるペアリング特有の性質を効果的に利用することにより，従来技術では実現不可能な機能の創出，より少ない情報量でのプロトコルの構成が可能となった．しかし，RSA 暗号におけるべき乗剰余演算や楕円曲線暗号における点のスカラー倍演算など主要な暗号要素技術と比較して，より多くの計算コストを要するため効率的なペアリング演算アルゴリズムが求められている．

2002〜2006 年までに提案された主要なペアリング演算アルゴリズムは以下の通りである．

2002 年：BKLS アルゴリズム [2]

2003 年：Duursma and Lee アルゴリズム [15]

2004 年：Eta ペアリング [1]

2006 年：Ate ペアリング，Twisted Ate ペアリング [20]

BKLS アルゴリズムとはペアリング演算として最も一般的な Miller's Algorithm の最適化を実現したアルゴリズムである．Duursma, Lee [15] は標数 p の有限体上で定義される Supersingular Curve である次数 p の超楕円曲線における Tate ペアリングを求めるアルゴリズムを提案している．これは標数 p の有限体及び Supersingular Curve の性質を最大限利用し，超楕円曲線の研究分野の成果を導入した画期的なアルゴリズムである．その翌年に Barreto ら [1] は Duursma and Lee アルゴリズムを小標数の有限体におけるすべての Supersingular Curve で動作可能となるように一般化した双線形写像 η (Eta) ペアリングを提案している．また，そのアルゴリズムのループ回数を半減させた η_T ペアリングも提案している．一方，Hess ら [20] によって提案された Ate ペアリングは Ordinary Curve 上で定義可能な双線形写像である．入力となる群 $\mathbb{G}_1 = E(\mathbb{F}_q)[r], \mathbb{G}_2 = E(\mathbb{F}_{q^k})[r]$ の入れ替えにより，演算アルゴリズムのループ回数は群位数ではなく trace に依存する．また，twist と呼ばれる楕円曲線を利用し，Eta ペアリングを一般化した Ordinary Curve における Twisted Ate ペアリングも提案している．

1.2 目的

現在の安全性水準では Supearingular Curve における η_T ペアリングが最速である．しかし，Supersingular Curve はパラメータ設定の際に重要となる埋め込み次数が固定であるため，より高い安全性水準にも柔軟に対応可能な Oridnary Curve における効率的なペアリングが必要となる．よって，本稿では Ordinary Curve における Ate ペアリング，Twisted Ate ペアリングの高速化について議論する．

Tate ペアリング，Ate ペアリング，Twisted Ate ペアリングの演算アルゴリズムの構造はほぼ同一であり，そのループ回数はそれぞれ $\lfloor \log_2 r \rfloor$，$\lfloor \log_2(t-1) \rfloor$，$\lfloor \log_2(t-1)^e \rfloor$ である．ここで部分群の位数 r，楕円曲線の trace t，twist は有限体 $\mathbb{F}_{q^e}$ 上で定義されているものとする．一般的には，Ate, Twisted Ate ペアリングは Tate ペアリングより高速に計算可能であるが，Ate ペアリングにおいて $\deg(t) \geq \deg(r)$, Twisted Ate ペアリングにおいて $(t-1)^e > r$ のとき，従来の Tate ペアリングよりも計算コストが大きいという点において未だ不十分である．

本稿では Eta ペアリングのループ回数削減手法を適用し，ループ長を短縮した Optimized Ate ペアリング及び Optimized twisted Ate ペアリングを提案する．また提案手法の有用性を評価するために計算コストの推定及びソフトウェア実装による性能評価を行い，提案したペアリングは常に Tate ペアリングよりも高速に計算可能であることを示す．

1.3 構成

本稿の構成は以下の通りである．2 章ではペアリングを理解する上で必要となる整数論，楕円曲線理論を説明する．3 章ではペアリングの定義を示し，ペアリングを利用した方式における安全性，計算コストに関して述べる．4 章では効率的なペアリング演算方法に関して楕円曲線・有限体・演算アルゴリズムについて説明する．5 章では提案手法となる Optimized Ate ペアリング，Optimized twisted Ate ペアリングについて説明する．6 章ではペアリング実装におけるプログラムの構成を示す．7 章では計算コスト推定及びソフトウェア実装による性能評価を行う．最後に 8 章でまとめる．

第2章　数学的準備

ペアリングを理解するために必要となる整数論及び楕円曲線理論について概説する．整数論では，いくつかの重要な定理を示すともに暗号設計に不可欠な群・環・体と呼ばれる代数的構造を持つ集合の定義を行う．楕円曲線理論では，楕円曲線における演算，写像，twist について述べ，ペアリングに深く関係する因子とその演算について説明する．

2.1　整数論

2.1.1　群

定義 2.1 群 (Group)
ある集合 $\mathbb{G}$ が以下の *4* つの性質を満足するとき，$\mathbb{G}$ を群と呼ぶ．

1. 閉法則
   $a, b \in \mathbb{G} \Rightarrow a \circ b \in \mathbb{G}$
2. 結合則
   $a \circ (b \circ c) = (a \circ b) \circ c$
3. 単位元の存在
   すべての元 a に対して $a \circ e = e \circ a = a$ を満足する単位元 e が存在する．
4. 逆元の存在
   すべての元 a に対して $a \circ a^{-1} = a^{-1} \circ a = e$ を満足する逆元 a^{-1} が存在する．

さらに可換則 $a \circ b = b \circ a$ を満足する群 $\mathbb{G}$ を可換群あるいはアーベル群と呼ぶ．

演算に関して加法を定義可能な群を加法群，乗法を定義可能な群を乗法群と呼ぶ．群 $\mathbb{G}$ の元の個数 $\sharp\mathbb{G}$ を $\mathbb{G}$ の位数といい，位数が有限な群を有限群と呼ぶ．

定義 2.2 部分群
群 $\mathbb{G}$ の部分集合 $\mathbb{H}$ が次の条件を満足すれば，$\mathbb{H}$ を $\mathbb{G}$ の部分群と呼ぶ．

$$a, b \in \mathbb{H} \Rightarrow ab^{-1} \in \mathbb{H}$$

ある元 $g \in \mathbb{G}$ からなる部分群 $\mathbb{H}$ を $\langle g \rangle = \{g^k | k \in \mathbb{Z}\}$ と表現する．g の位数は $g^l = 1$ となる最小の整数 l，あるいは部分群 $\langle g \rangle$ の位数として定義される．有限群 $\mathbb{G}$ と部分群 $\mathbb{H}$ に関して次の定理が成立する．

定理 2.1 ラグランジェの定理

1. 部分群 $\mathbb{H}$ の位数は群 $\mathbb{G}$ の位数の約数である．

2. 群 $\mathbb{G}$ の各元 g の位数 l は群 $\mathbb{G}$ の位数 n の約数である．すなわち，$g^n = 1$ が成立する．

群 $\mathbb{G}$ が 1 つの元 g で生成されるとき，すなわち $\mathbb{G} = \langle g \rangle$ であるとき，g を $\mathbb{G}$ の生成元といい，$\mathbb{G} = \{g^k | k \in \mathbb{Z}\}$ を巡回群と呼ぶ．また，群 $\mathbb{G}$ 自身が有限個の元で生成されるとき，$\mathbb{G}$ は有限生成であるという．以下に群構造に関する定理を示す.

定理 2.2 群構造
有限生成なアーベル群は有限個の巡回群の直積と同型である．

$$\mathbb{G} \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_s}$$

ここで $n_i | n_{i+1}, (i = 1, 2, \ldots, s)$ であり，群 $\mathbb{G}$ によって n_i は一意に定まる．

定義 2.3 準同型写像・同型写像・同型
群 $\mathbb{G}$ から群 $\mathbb{G}'$ への写像 $f : \mathbb{G} \to \mathbb{G}'$ について，

$$f(ab) = f(a)f(b) \quad (a, b \in \mathbb{G})$$

が成立するとき，f を群 $\mathbb{G}$ から群 $\mathbb{G}'$ への準同型写像と呼ぶ．特に準同型写像 f が全単射であるとき，f を同型写像と呼ぶ．2 つの群 $\mathbb{G}, \mathbb{G}'$ の間に同型写像が存在するとき，それらを同型といい，$\mathbb{G} \cong \mathbb{G}'$ と表現する．

群 $\mathbb{G}$ を $\mathbb{G}$ 自身へ移す準同型写像を自己準同型写像，群 $\mathbb{G}$ を $\mathbb{G}$ 自身へ移す同型写像を自己同型写像と呼び，その全体の集合をそれぞれ $\mathrm{End}(\mathbb{G})$,$\mathrm{Aut}(\mathbb{G})$ と表記する．また，準同型写像の kernel(核) を次のように定義する．

定義 2.4 準同型写像の kernel
また，準同型写像 $f : \mathbb{G} \to \mathbb{G}'$ に対して，単位元 $e' \in \mathbb{G}'$ の逆像

$$\mathrm{Ker}(f) = \{a \in \mathbb{G} | f(a) = e'\}$$

を f の核あるいは kernel と呼ぶ．$\mathrm{Ker}(f) = \{e\}$ を自明な kernel と呼ぶ.

群 $\mathbb{G}$ の準同型写像 f に関して次の定理が重要である．

定義 2.5 準同型定理
群 $\mathbb{G}$ から群 $\mathbb{G}'$ への準同型写像 f の kernel を $\mathrm{Ker}(f)$ とすると，$\mathbb{G}/\mathrm{Ker}(f) \cong \mathbb{G}'$ が成立する．

$\mathbb{G}/\mathrm{Ker}(f)$ は剰余類全体の集合であり，剰余類は次小節にて説明する．準同型定理より，準同型写像 f は群 $\mathbb{G}$ 自身から構成される $\mathbb{G}/\mathrm{Ker}(f)$ への写像と同値となる．

2.1.2 環

定義 2.6 環 (Ring)
ある集合 $\mathbb{R}$ が以下の 3 つの性質を満足すれば，$\mathbb{R}$ を環と呼ぶ.

1. 加法に関して $\mathbb{R}$ は可換群である．加法の単位元を零元と呼ぶ.
2. 乗法に関して閉法則及び結合則が成立する.
3. 加法と乗法に関して分配法則が成立する.
   $(a+b)c = ac+bc, a(b+c) = ab+ac$

さらに可換則 $ab = ba$ を満足する環 $\mathbb{R}$ を可換環と呼ぶ.

自己準同型写像 $f, g \in \mathrm{End}(\mathbb{G})$ において，加法 $(f+g)(x) = f(x)+g(x)$，乗法 $(f \circ g)(x) = f(g(x))$ をと定めると $\mathrm{End}(\mathbb{G})$ は環となり，これを自己準同型環と呼ぶ．また，整数全体 $\mathbb{Z}$ は加法について可換群，乗法について結合則を満たすので環となる．これを整数環と呼ぶ．可換環で単位元を持ち，零元以外に零因子を持たない環を整域と呼び，具体例として，整数環と後述する多項式環がある.

ここで，整数 a, b の差 $a-b$ が自然数 n で割り切れるとき，a, b は法 n に関して合同であるといい，$a \equiv b \bmod n$ と表現する．互いに合同な整数全体の集合を剰余類という．a を含む剰余類を $\overline{a} = \{b | a \equiv b \pmod n\}$ と表現すると，剰余類全体の集合を $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$ とする．2 つの元 $a, b \in \mathbb{Z}/n\mathbb{Z}$ について，和 $\overline{a}+\overline{b} = \overline{a+b}$, 積 $\overline{a}\overline{b} = \overline{ab}$ と定めれば，集合 $\mathbb{Z}/n\mathbb{Z}$ は可換環となり，法 n に関する剰余環という．また，剰余環 $\mathbb{Z}/n\mathbb{Z}$ に属する剰余類の代表元による集合を $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$ と定義する．さらに，法 n と互いに素な整数で代表される剰余類を法 n に関する既約剰余類といい，$(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} | \gcd(a, n) = 1\}$ と表現する．元の個数を $\varphi(n)$ で表現し，これをオイラーの関数と呼ぶ.

$$\varphi(n) = \sharp(\mathbb{Z}/n\mathbb{Z})^* = \sharp\{a | 1 \leq a \leq n, \gcd(a, n) = 1\}$$

オイラー関数について次が成立する.

1. $\gcd(m, n) = 1$ のとき，$\varphi(mn) = \varphi(m)\varphi(n)$
2. 素数 p について，$\varphi(p^k) = p^{k-1}(p-1), k \geq 1$
3. m の素因数分解を $m = p_1^{e_1} \cdots p_r^{e_r}$ とするとき,
   $\varphi(m) = m(1-\frac{1}{p_1}) \cdots (1-\frac{1}{p_r})$

表 2.1: オイラー関数 $\varphi(n)$

n	1	2	3	4	5	6	7	8	9	10	11	12
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

定理 2.3 オイラーの定理
n を正整数, a を n と互いに素な整数とするとき，オイラーの関数 $\varphi(n)$ として，

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

オイラーの定理で n が素数 p と等しいとき，$\phi(p) = p - 1$ であるため，以下のフェルマーの小定理を得る．

定理 2.4 フェルマーの小定理
p を素数，a を p と素な整数とするとき，

$$a^{p-1} \equiv 1 \pmod{p}$$

2.1.3 体

定義 2.7 体 (Field)
ある集合 $\mathbb{F}$ が以下の *3* つの性質を満足すれば，$\mathbb{F}$ を体と呼ぶ．

1. 加法に関して，$\mathbb{F}$ は可換群である．
2. 乗法に関して，$\mathbb{F}$ は群である．
3. 加法と乗法に関して，分配法則が成立する．
   $(a+b)c = ac + bc, a(b+c) = ab + ac$

p を素数とするとき，剰余環 $\mathbb{Z}/p\mathbb{Z}$ は位数が p となる有限体となり，$\mathbb{F}_p$ と表現する．一般に，体 K において n 個の 1 の和が零となるような正整数 n が存在するとき，その中で最小の整数を体 K の標数 (characteristic) と呼び, $\mathrm{char}(K)$ と表現する．そのような整数が存在しない場合，標数を 0 とする．有理数体，実数体，複素数体の標数は 0 である．ここで，有限体 $\mathbb{F}_p$ による乗法群 $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ において離散対数問題を定義する．

定義 2.8 離散対数問題 (Discrete Logarithm Problem)
Given: $g, g^a \in \mathbb{F}_p^*$
Answer: $a \in \mathbb{F}_p$

体 K において，K の元を係数とする多項式 f を考える．

$$f = a_0 X^n + a_1 X^{n-1} + \cdots + a_n, \quad a_i \in K \tag{2.1}$$

n を f の次数, $f(a) = 0$ のとき，a を f の零点または根と呼ぶ．$f = (x-a)^e g, g(a) \neq 0$ のとき，e を f の零点 a における重複度 (multiplicity) と呼ぶ．
(2.1) の全体を $K[X]$ と表現すると，$K[X]$ の元 f を形式的に

$$f = \sum_{k=0}^{\infty} b_k X^k$$

と表現し，和と積を次のように定義する．

$$\sum_{k=0}^{\infty} b_k X^k + \sum_{k=0}^{\infty} c_k X^k = \sum_{k=0}^{\infty} (b_k + c_k) X^k, \quad (\sum_{k=0}^{\infty} b_k X^k)(\sum_{k=0}^{\infty} c_k X^k) = \sum_{k=0}^{\infty} \sum_{j=0}^{k} b_j c_{k-j} X^k$$

すなわち，$K[X]$ は整域であり，可換環である．$K[X]$ を K 上の多項式環と呼ぶ．$K[X]$ において，多項式 f が定数でない多項式 g, h の積 $f = gh$ で表現されるとき，f は (K 上で) 可約 (reducible) であるという．f が可約でないとき，f は (K 上で) 既約 (irreducible) であるという．f が既約な $f \in K[X]$ を法とする多項式環 $K[X]/f(X)$ は体となる．このとき，f の次数を n とすると，体 $K[X]/f(X)$ は K を基礎体とする n 次拡大体であり，n を拡大次数と呼ぶ．

定理 2.5 拡大体 (extension field)
次数が n の既約な $f \in K[X]$ を法とする多項式環 $K[X]/f(X)$ は K の n 次拡大体となる．

拡大体 L に含まれる体 K を部分体といい，最小の部分体を素体と呼ぶ．有限体 $\mathbb{F}_p$ は素体である．また代数的閉体を次のように定義する．

定義 2.9 代数的閉体
ある体 K を与えられたとき，$K[X]$ のいかなる元も体 K の拡大体 L 上で一次式の積の形に因数分解可能なとき，L を代数的閉体と呼ぶ．体 K の代数的閉体を $\overline{K}$ で表現するものとする．

方程式 $X^n - 1 = 0$ の解を 1 の n 乗根という．ζ_n が 1 の n 乗根で，かつ，n 乗して初めて 1 となるとき，ζ_n を 1 の原始 n 乗根であるという．一般に原始 n 乗根はたかだか n 個しかなく，原始 n 乗根全体の集合は ζ_n を生成元とする位数 $\varphi(n)$ の巡回群となる．ここで円分多項式を定義する．

定義 2.10 円分多項式

$$\Phi_n(X) = \prod_{1 \le k < n, \gcd(k,n)=1} (X - \zeta_n^k)$$

また，$n \geqq 1$ のとき，次式が成立する．

$$X^n - 1 = \prod_{d|n, d \ge 1} \Phi_d(X)$$

$n = 12$ までの円分多項式を以下に示す．

$n = 1 : x - 1$　　$n = 7 : x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
$n = 2 : x + 1$　　$n = 8 : x^4 + 1$
$n = 3 : x^2 + x + 1$　　$n = 9 : x^6 + x^3 + 1$
$n = 4 : x^2 + 1$　　$n = 10 : x^4 - x^3 + x^2 - x + 1$
$n = 5 : x^4 + x^3 + x^2 + x + 1$　　$n = 11 : x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
$n = 6 : x^2 - x + 1$　　$n = 12 : x^4 - x^2 + 1$

2.2 楕円曲線理論

2.2.1 楕円曲線

楕円曲線は Weierstrass form と呼ばれる以下の等式で表現される曲線である．

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.2}$$

ある体 K に対して係数 $a_1, a_2, a_3, a_4, a_6 \in K$ を満たすとき，楕円曲線 E は体 K 上で定義されていると表現し，E/K と表記する．このとき，体 K を楕円曲線 E の定義体と呼ぶ．$\mathrm{char(K)} \neq 2, 3$ のとき，(2.2) ではなく，Wierstrass short form と呼ばれる次式を用いて表現可能である．

$$E : y^2 = x^3 + Ax + B \tag{2.3}$$

E が体 K 上で定義されているとき，$L \supseteq K$ に対して $x, y \in L$ となる E 上の点 $P = (x, y)$ を L-有理点と呼ぶ．無限遠点を $\mathcal{O}$ で表記すると，L-有理点全体 $E(L)$ は次にように定義される．

$$E(L) = \{\mathcal{O}\} \cap \{(x, y) \in L \times L | y^2 = x^3 + Ax + B, 4A^3 + 27B^2 \neq 0\}$$

以降，K の代数的閉体 $\overline{K}$ として，$\overline{K}$-有理点全体 $E(\overline{K})$ を E とする．

楕円曲線における演算を次のように定義する．点 $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ とすると，その和 $P_1 + P_2$ は P_1 と P_2 を結ぶ直線 l と楕円曲線の交点 P_3' を x 軸に対して対称に移動させた点 $P_3 = P_1 + P_2$ である (図 2.1 参照のこと).

定義 2.11 楕円曲線における演算
楕円曲線 $E : y^2 = x^3 + Ax + B$ とする．無限遠点でない 2 点を $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ とする．$P_1 + P_2 = P_3 = (x_3, y_3)$ は次のようにして求める．

1. $x_1 \neq x_2$ のとき
   $\lambda = (y_2 - y_1)/(x_2 - x_1), \quad x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda(x_1 - x_3) - y_1$
2. $x_1 = x_2, y_1 \neq y_2$ のとき
   $P_1 + P_2 = \mathcal{O}$
3. $P_1 = P_2, y_1 \neq 0$ のとき
   $\lambda = (3x_1^2 + A)/2y_1, \quad x_3 = \lambda^2 - 2x_1, \quad y_3 = \lambda(x_1 - x_3) - y_1$
4. $P_1 = P_2, y_1 = 0$ のとき
   $P_1 + P_2 = \mathcal{O}$

さらに，楕円曲線上のすべての点 P に対して次式が成立する．

$$P + \mathcal{O} = \mathcal{O} + P = P$$

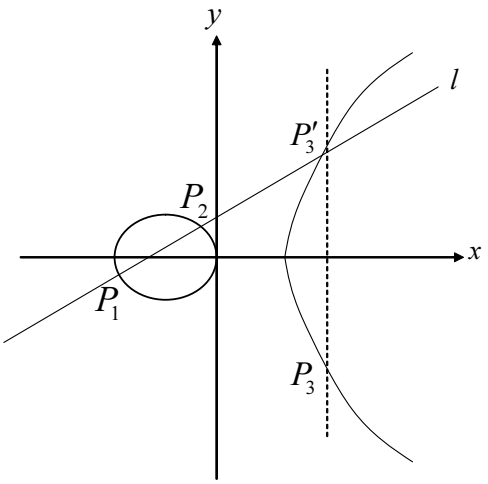

図 2.1: 楕円曲線における点の加算

$P = (x, y)$ に対する逆元は (2.3) では $P = (x, -y)$ だが，(2.2) では $-P = (x, -a_1x - a_3 - y)$ となる．L-有理点全体 $E(L)$ は加法に関して群の定義を満足するため，加法群となる．

定理 2.6 加法群 $E(L)$
$E(L)$ は加法群の定義である以下の *4* つの性質を満足する．$P, Q, R \in E(L)$ とする．

1. 閉法則
   加法 “+” に対して演算が閉じている
2. 単位元の存在
   $P + \mathcal{O} = \mathcal{O} + P = P$
3. 逆元の存在
   $P + (-P) = \mathcal{O}$
4. 結合則
   $(P + Q) + R = P + (Q + R)$

さらに，可換則 $(P + Q = Q + P)$ を満足するため，アーベル群でもある．

次に，$a(\in \mathbb{Z})$ 個の点を加算するスカラー倍算を以下のように定義する．

定義 2.12 スカラー倍算

$$aP = \underbrace{P + \cdots + P}_{a}, \quad 0P = \mathcal{O}, \quad -aP = a(-P)$$

一般にスカラー倍 aP は 2 進展解法と呼ばれる以下のアルゴリズムにより効率よく計算可能である．

Algorithm 2.1: Double and Add Method

INPUT: $a \in \mathbb{Z}, P \in E(L)$
OUTPUT: $Q = aP \in E(L)$
If $a < 0$ **then** $P \leftarrow -P$
$Q \leftarrow \mathcal{O}, a = \sum_{i=0}^{l-1} a_i 2^i, a_i \in \{0, 1\}$
for $j \leftarrow l - 1$ **downto** 0 **do**
　　$Q = 2Q$
　　If $a_j = 1$ **then**
　　$Q = Q + P$
return Q

上記のアルゴリズムを用いることにより，与えられた a, P から aP を容易に計算可能であるが，P, aP から a を求めることは計算量的に困難である．有限体 F_q 上で定義される楕円曲線 E に対して，楕円曲線における離散対数問題を次のように定義する．

定義 2.13 楕円曲線における離散対数問題 (Elliptic Curve Discrete Logarithm Problem:ECDLP)
Given: $P, aP \in E(\mathbb{F}_q)$
Answer: a

n-Torsion Point による群 $E[n]$ を次のように定義する．

定義 2.14 Torsion Point

$$E[n] = \{P \in E : nP = \mathcal{O}\}$$

また，$E(K)$ における n-torsion point による部分群 $E(K)[n]$ を以下のように定義する．

$$E(K)[n] = \{P \in E(K) : nP = \mathcal{O}\}$$

定理 2.7 (Washington [48])
体 K で定義される楕円曲線 E, 正整数 n とする．体 K の標数が n を割り切らない，あるいは零であれば,

$$E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$$

体の標数が $p > 0$，かつ $p \mid n$ であれば，$p \nmid n'$ となる $n = p^r n'$ とすると,

$$E[n] \simeq \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'} \quad or \quad \simeq \mathbb{Z}_n \oplus \mathbb{Z}_{n'}$$

である．

すなわち，$E[n]$ のすべての元は基底 P_1, P_2 を用いて $n_1P_1 + n_2P_2(n_1, n_2 \in \mathbb{Z})$ の形で表現可能であることを意味している．また n と p が互いに素であれば，$\sharp E[n] = n^2$ である．これに関連して，Ordinary Curve 及び Supersingular Curve の定義を以下に与える．

定義 2.15 Ordinary Curve, Supersingular Curve
標数 p の体で定義される楕円曲線 E に対して，$E[p] \simeq \mathbb{Z}_p$ のとき，E を Ordinary Curve と呼び，$E[p] \simeq 0$ のとき Supersingular Curve と呼ぶ.

一般に暗号に用いる楕円曲線の定義体は $q = p^m$ 個の要素からなる有限体 $\mathbb{F}_q$ である．以降，有限体 $\mathbb{F}_q$ 上で定義された楕円曲線 $E/\mathbb{F}_q$ として議論していくものとする．$lP = \mathcal{O}$ を満足する最も小さい自然数 l を点 $P \in E(\mathbb{F}_q)$ の位数と呼ぶ．$E(\mathbb{F}_q)$ の元の個数を $E(\mathbb{F}_q)$ の位数と呼び，$\sharp E(\mathbb{F}_q)$ と表記する．$E(\mathbb{F}_q)$ の群構造に関する定理を以下に示す.

定理 2.8 Washington [48]
ある整数 $n \geq 1$，あるいは $n_1 \mid n_2$ を満足する整数 $n_1, n_2 \geq 1$ に対して，次式が成立する．

$$E(\mathbb{F}_q) \simeq \mathbb{Z}_n \quad or \quad \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$$

$t = q + 1 - \sharp E(\mathbb{F}_q)$ となる t を Frobenius(次頁参照) の trace と呼ぶ．楕円曲線理論の中でも非常に重要な定理である Hasse の定理を以下に示す.

定理 2.9 Hasse's bound [47]
楕円曲線の trace t は以下の式を満足する．

$$|t| \leq 2\sqrt{q}$$

○ j-不変量

定義 2.16 楕円曲線 E の j-不変量

$$j = j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}$$

$j = 0, 1728$ のとき，楕円曲線は以下に示す形で表現され，自己同型写像を持つことが知られている．自己同型写像とは曲線から曲線自身への全単射な群準同型写像であり，楕円曲線が後述する Supersingular Curve であれば，distortion map と呼ばれる写像に相当する．

1. $j = 0$

$$y^2 = x^3 + B$$
$$\phi : (x, y) \mapsto (\zeta x, -y), \quad \zeta\text{:非自明な 1 の 3 乗根}$$

2. $j = 1728$

$$y^2 = x^3 + Ax$$
$$\phi : (x, y) \mapsto (-x, iy), \quad i^2 = -1$$

体 K で定義される異なる 2 つの楕円曲線が等しい j-不変量を持っているとき，それらの楕円曲線を互いに twist と呼ぶ．§2.2.2 にて twist について詳述する．

○自己準同型写像

楕円曲線 E における自己準同型写像とは有理関数で与えられる準同型写像 $\alpha : E \to E$ である．すなわち，$P_1, P_2 \in E$ に対して，$\alpha(P_1 + P_2) = \alpha(P_1) + \alpha(P_2)$ が成立する．すべての $(x, y) \in E$ に対して，自己準同型写像 α は係数が $\overline{K}$ の元となる有理関数 $r_1(x), r_2(x)$ を用いて

$$\alpha(x, y) = (r_1(x), r_2(x)y)$$

と表現される．準同型写像であるため，$\alpha(\mathcal{O}) = \mathcal{O}$ である．$r_1(x) = p(x)/q(x)$ で表現されるとき，ある点 (x, y) において $q(x) = 0$ であれば, $\alpha(x, y) = \mathcal{O}$ とする．$q(x) \neq 0$ であれば，同時に $r_2(x)$ が定義され，有理関数 α が定義される．非自明な α の次数を次のように定義する．

定義 2.17 自己準同型写像の次数

$$\deg(\alpha) = \mathrm{Max}\{\deg p(x), \deg q(x)\}$$

$\alpha = 0$ であれば，$\deg(0) = 0$ とする．

定義 2.18 Separable な自己準同型写像
$r_1(x)$ の形式的導関数 $r_1'(x)$ が恒等的に零でなければ，非零な α を separable な自己準同型写像と呼ぶ．Separable でない写像を inseparable な自己準同型写像と呼ぶ.

標数 p のとき，導関数が零となる多項式の次数は p である．一般的に標数 p においては p 倍写像となる自己準同型写像 $\alpha(Q) = pQ$ は次数 p^2 であり，separable ではない．次に自己準同型写像と kernel の位数に関する定理を示す.

定理 2.10 (Washington [48])
$\alpha \neq 0$ は楕円曲線 E の separable な自己準同型写像とすると，

$$\deg(\alpha) = \sharp\mathrm{Ker}(\alpha)$$

が成立し，$\mathrm{Ker}(\alpha)$ は準同型写像 $\alpha : E \to E$) の kernel である．$\alpha \neq 0$ が separable でなければ,

$$\deg(\alpha) > \sharp\mathrm{Ker}(\alpha)$$

となる．

自己準同型写像の中でも最も重要な Frobenius 写像 π_q を定義する．

定義 2.19 Frobenius 写像 π_q
有限体 $\mathbb{F}_q$ で定義される楕円曲線 E を想定する．

$$\pi_q(x,y) = (x^q, y^q), \quad \pi_q(\mathcal{O}) = \mathcal{O}$$

Frobenius 写像 π_q は次数 q の自己準同型写像であり，inseparable である．また，$(x,y) \in E(\mathbb{F}_q)$ であれば，$\pi_q(x,y) = (x,y)$ であり，逆もまた成立する．Frobenius の trace t と Frobenius 写像 π_q は等式 $\pi_q^2 - t\pi_q + q = 0$ により関連付けられる．すなわち，任意の点 $P = (x,y) \in E(\overline{\mathbb{F}}_q)$ に対して，

$$(x^{q^2}, y^{q^2}) - t(x^q, y^q) + q(x,y) = \mathcal{O}$$

が成立する．さらに，$X^2 - tX + q$ を特性多項式と呼び，これを用いて $\sharp E(\mathbb{F}_q)$ から任意の $n \in N$ に対する $\sharp E(\mathbb{F}_{q^n})$ を計算可能である．

定理 2.11 (Washington [48])
$\sharp E(\mathbb{F}_q) = q + 1 - t$ とする．特性多項式 $X^2 - tX + q$ の根を $\alpha \in \mathbb{C}$ とすれば，すべての $n \geq 1$ に対して，次式が成立する．

$$\sharp E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \overline{\alpha}^n)$$

2.2.2 twist

p を素数とする $q = p^m$ 個の要素からなる有限体 $\mathbb{F}_q$ 上で定義される楕円曲線 E が Ordinary Curve であるとすると，以下の定義で与えられる twist が存在する．

定義 2.20 twist
$\mathbb{F}_q$ 上で定義されている楕円曲線 E, E' において，$\mathbb{F}_{q^d}$における 同型写像 $\phi_d : E' \to E$ が存在し，d が最小の整数であれば，E' を d 次の twist と呼ぶ．

ここで σ は $\mathbb{F}_q$ の代数的閉体 $\overline{\mathbb{F}}_q$ における q 乗 Frobenius 自己同型写像とすると，同型写像 ϕ_d の係数に σ を適用させて得られる ϕ_d^σ に対して $\phi_d^\sigma \circ \phi_d^{-1} \in \mathrm{Aut}(E)$ が成立する．さらに d は最小の整数であるので，この自己同型写像の位数は d となるため，E' が E の位数 d の twist であれば，$\mathrm{Aut}(E)$ は必ず位数 d の元を含む．[47] によれば，有限群 $\mathrm{Aut}(E)$ の位数は常に 24 を割り切り，$p > 5$ のときは $\sharp\mathrm{Aut}(E)|6$ を満足する．すなわち，$p > 5$ のとき，twist の位数は $d = 2, 3, 4, 6$ のみ存在する．このとき，楕円曲線 E の twist の集合は $\mathbb{F}_q^*/(\mathbb{F}_q^*)^d$ と標準的に同型 (同型写像が唯一に存在する) であり，$j(E) \neq 0, 1728$ であれば $d = 2$，$j(E) = 1728$ であれば $d = 4$，$j(E) = 0$ であれば $d = 6$ である．すなわち，1 の d 乗根全体の集合を μ_d とすると，

$\mathrm{Aut}(E) \cong \mu_d$ であり，$\mathbb{F}_q$ 上で定義された楕円曲線 $E : y^2 = x^3 + Ax + B$ において，同型写像 $[\zeta]$ が定義可能である．

$$[\cdot] : \mu \to \mathrm{Aut}(E) : \zeta \mapsto [\zeta] \ \text{ with } \ [\zeta](x, y) = (\zeta^2 x, \zeta^3 y)$$

$D \in \mathbb{F}_p^*$ であり，$D \bmod (\mathbb{F}_q^*)^d$ に対応する位数 d の twist を示す．

$$\begin{aligned}
d = 2 \qquad & E : y^2 = x^3 + Ax + B \\
& E' : y^2 = x^3 + A/D^2 x + B/D^3 \\
& \phi_d : E' \to E : (x, y) \mapsto (Dx, D^{3/2} y) \\
d = 4 \qquad & E : y^2 = x^3 + Ax \\
& E' : y^2 = x^3 + A/Dx \\
& \phi_d : E' \to E : (x, y) \mapsto (D^{1/2} x, D^{3/4} y) \\
d = 3, 6 \qquad & E : y^2 = x^3 + B \\
& E' : y^2 = x^3 + B/D \\
& \phi_d : E' \to E : (x, y) \mapsto (D^{1/3} x, D^{1/2} y)
\end{aligned}$$

位数 d の twist を用いる場合，$\mathbb{F}_q^*/(\mathbb{F}_q^*)^d$ が d 個の要素を有する，すなわち $q \equiv 1 \bmod d$ を満足する必要がある．

○群位数

d 次の twist E' を持つ楕円曲線 E を想定する．$\mathbb{F}_{q^d}$ 上において E, E' は同型であり，$\sharp E(\mathbb{F}_{q^d}) = \sharp E'(\mathbb{F}_{q^d})$ を満足する．定理 2.11 より，任意の $\zeta \in \mu_d$ に対して，$\alpha = \zeta\alpha'$ が成立するため，たかだか d 通りの $\sharp E'(\mathbb{F}_q)$ しか存在しない．実際は ζ は 1 の原始 d 乗根のため，位数 d の E' は $\varphi(d)$ 通りの群位数を持つ．twist の群位数 $\sharp E'(\mathbb{F}_q)$ を以下に示す．

$$\begin{aligned}
d = 2 : & \sharp E'(\mathbb{F}_q) = q + 1 + t \\
d = 3 : & \sharp E'(\mathbb{F}_q) = q + 1 - (3f - t)/2, \quad t^2 - 4q = -3f^2 \\
& \sharp E'(\mathbb{F}_q) = q + 1 - (-3f - t)/2, \quad t^2 - 4q = -3f^2 \\
d = 4 : & \sharp E'(\mathbb{F}_q) = q + 1 + f, \quad t^2 - 4q = -f^2 \\
& \sharp E'(\mathbb{F}_q) = q + 1 - f, \quad t^2 - 4q = -f^2 \\
d = 6 : & \sharp E'(\mathbb{F}_q) = q + 1 - (3f + t)/2, \quad t^2 - 4q = -3f^2 \\
& \sharp E'(\mathbb{F}_q) = q + 1 - (-3f + t)/2, \quad t^2 - 4q = -3f^2
\end{aligned}$$

○構造定理

楕円曲線 E における Frobenius 写像を π_q, twist E' における Frobenius 写像を π'_q とする．同型写像 ϕ_d は同型環

$$\Phi_d : \mathrm{End}(E') \to \mathrm{End}(E) : f \mapsto \Phi_d(f) = \phi_d \circ f \circ \phi_d^{-1}$$

となる．任意の有理関数 $h : E' \to E'$ に対して，$\pi'_q \circ h = h^\sigma \circ \pi_q$ が成立するので，

$$\Phi_d(\pi'_q) = \phi_d \circ \pi'_q \circ \phi_d^{-1} = \phi_d \circ (\phi_d^{-1})^\sigma \circ \pi_q$$

前述したように，次数 d なので，$\phi_d \circ (\phi_d^{-1})^\sigma$ は位数 d の $\mathrm{Aut}(E)$ である．E の次数 d の twist E_i を $i = 0$ から $i = d-1$ までラベリングし，ζ_d を任意の固定された原始 d 乗根，$\pi_{q,i}$ を E_i における Frobenius 写像とすると，同型写像 $[\cdot] : \mu_d \to \mathrm{Aut}(E)$ を用いて，同型写像 $\phi_i : E' \to E$ に対応する同型環を $\Phi_i(\pi_{q,i}) = [\zeta_d^i]\pi_q$ と表現可能である．E における $\mathbb{F}_q$-有理点集合は $E(\mathbb{F}_q) = \mathrm{Ker}(\pi_q^d - 1)$ と表現されるので，同様にして，

$$E_i(\mathbb{F}_q) \simeq \mathrm{Ker}([\zeta_d^i]\pi_q - 1) \tag{2.4}$$

と表現される．よって，以下の twist に関する構造定理が成立する．

定理 2.12 twist に関する構造定理
有限体 $\mathbb{F}_q$ 上で定義された d 次の twist を持つ楕円曲線を E，d を割り切る E の d 個の twist をそれぞれ $E_i, (i = 0, \cdots, d-1)$ とする．

$$\forall p_i \mid d, (p_i\text{は素数}) : \sharp E(\mathbb{F}_q) \not\equiv \mathrm{mod} p_i$$

$\sharp E(\mathbb{F}_q)$ が上式を満足するなら，

$$E(\mathbb{F}_{q^d}) \cong \bigoplus_{i=0}^{d-1} E_i(\mathbb{F}_q)$$

が成立する．

この定理から，$l \mid\mid \sharp E(\mathbb{F}_q)$ かつ $l^2 \mid\mid \sharp E(\mathbb{F}_{q^d})$ となる素数 $l > d$ に対して，$l \mid \sharp E_i(\mathbb{F}_q)$ を満足する位数 d の twist E_i が唯一存在することがいえる．記号 $\mid\mid$ は $l \mid \sharp E(\mathbb{F}_q)$ となる最小の整数 l を意味する．

2.2.3 因子

点 $P \in E$ に対する形式的な記号として (P) を導入する．楕円曲線 E における因子 D は整数係数を持つ形式的な記号 (P) の和として定義される．

定義 2.21 楕円曲線 E における因子 D

$$D = \sum_{P \in E} n_P(P), n_P \in \mathbb{Z}$$

因子は生成元 (P) によって生成されるアーベル群の元であり，加算は次のようになる．

$$\sum_{P \in E} n_P(P) + \sum_{P \in E} m_P(P) = \sum_{P \in E} (n_P + m_P)(P)$$

因子 $D = \sum_{P \in E} n_P(P)$ の位数 $\deg(D)$, 及び $\mathrm{sum}(D), \mathrm{supp}(D)$ を次のように定義する．

定義 2.22 因子 D の次数 $\deg(D), \mathrm{sum}(D), \mathrm{supp}(D)$

$$\begin{aligned}\deg(D) &= \sum_{P\in E} n_P \in \mathbb{Z}\\ \mathrm{sum}(D) &= \sum_{P\in E} n_P P \in E\\ \mathrm{supp}(D) &= \{P \in E | n_P \neq 0\}\end{aligned}$$

因子による群を $\mathrm{Div}(E)$，位数 0 の因子による群を $\mathrm{Div}^0(E)$ と表記すると，$\mathrm{Div}^0(E)$ は $\mathrm{Div}(E)$ の部分群を成す.

2 変数 x, y による多項式環 $K[x, y]$ の元 r を

$$r(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$$

と定義する. r による楕円曲線上における多項式環を

$$\overline{K}[E] = \overline{K}[x, y]/(r)$$

とする．関数 $l \in \overline{K}[E]$ を標準形で

$$l(x, y) = v(x) + yw(x), \quad v(x), w(x) \in \overline{K}[x]$$

と表現し，その有理関数を $f \in \overline{K}(E)$ とする．$f(P) = 0$ であれば，関数 f は点 P において零点，$f(P) = \infty$ であれば，関数 f は点 P において極を持つと表現する．また，ある点 P において $u_P(P) = 0$ となる “uniformizer” と呼ばれる関数が存在し，すべての関数 $f(x, y)$ は次の形で表現可能である.

$$f = u_P^r g, r \in \mathbb{Z}, g(P) \neq 0, \infty$$

定理 2.13 (Menezes [46])
$P \in E$ とする．$l : ax + by + c = 0$ が点 P を通る接線ではない直線であれば，直線 l は点 P における uniformizer である.

定理 2.13 より u_P は次のようになる.

$$u_P = \begin{cases} x - c & \text{if } P = (c, d) \notin E[2]\\ y & \text{if } P = (c, 0) \in E[2]\\ x/y & \text{if } P = \mathcal{O}\end{cases}$$

点 P における関数 f の位数を次のように定義する.

定義 2.23 点 P における関数 f の位数

$$\mathrm{ord}_P(f) = r$$

すなわち，$\mathrm{ord}_P(f)$ は関数 f の点 P における零点あるいは極の重複度を表現しており，$\mathrm{ord}_P(f) > 0$ のとき，関数 f は点 P において $\mathrm{ord}_P(f)$ 位の零点，$\mathrm{ord}_P(f) < 0$ のとき，関数 f は点 P において $|\mathrm{ord}_P(f)|$ 位の極を持つという．$\mathrm{ord}_P(f) = 0$ であれば，関数 f は点 P において零点も極も持たない．

定義 2.24 関数 f の因子 $\mathrm{div}(f)$

$$\mathrm{div}(f) = \sum_{P \in E} \mathrm{ord}_P(f)(P) \in \mathrm{Div}(E)$$

$\mathrm{div}(f) = 0$ と関数 f が定数であることは同値であり，関数 f_1, f_2 に対して次式が成立する．

$$\mathrm{div}(f_1 f_2) = \mathrm{div}(f_1) + \mathrm{div}(f_2)$$

定理 2.14 Weil′s reciprocity
$f, g \in \overline{K}(E)$ とすると，$f(\mathrm{div}(g)) = g(\mathrm{div}(f))$ が成立する．

$D = \mathrm{div}(f)$ を満足する関数 f が存在する因子 $D \in \mathrm{Div(E)}$ を主因子と呼ぶ．さらに，$D_1 - D_2$ が主因子となる 2 つの因子 $D_1, D_2 \in \mathrm{Div(E)}$ は線形同値であると表現し，$D_1 \sim D_2$ と表記する．このとき，ある有理関数 f を用いて $D_1 = D_2 + \mathrm{div}(f)$ が成立する．主因子に関して以下の定理が成立する．

定理 2.15 (Silverman [47])
因子 $D = \sum_{P \in E} n_P(P)$ とする．D が主因子であれば,

$$\deg(D) = 0 \text{ かつ } \mathrm{sum}(D) = \mathcal{O}$$

が成立し，逆もまた成立する．

$\mathrm{supp}(\mathrm{div}(f)) \cap \mathrm{supp}(D)$ を満足する関数 $f \in \overline{K}(E)$ に引数として因子 $D = \sum_{P \in E} n_P(P)$ を与えたとき，次のようにして値 $f(D)$ を求めることができる．

$$f(D) = \prod_{P \in \mathrm{supp}(D)} f(P)^{n_P} \tag{2.5}$$

補題 2.1
因子 $D \in \mathrm{Div}^0(E)$, 関数 $f_1 \in \overline{K}(E)$ は $\mathrm{supp}(\mathrm{div}(f_1)) \cap \mathrm{supp}(D) = \emptyset$ を満たすものとする．$c \in \overline{K}^*$ とすると，有理関数 $f_2 = cf_1$ は

$$f_2(D) = f_1(D)$$

を満たす.

$D \sim (P) - (\mathcal{O}) \in \mathrm{Div}^0(E)$ とする．このとき，一意に定まる関数 $f \in \overline{K}(E)$ を用いて，次のように表現できる．これを標準形と呼ぶこととする．

$$D = (P) - (\mathcal{O}) + \mathrm{div}(f)$$

標準形で表現された 2 つの因子 $D_1, D_2 \in \mathrm{Div}^0(E)$ の加算を考える．

$$D_1 = (P_1) - (\mathcal{O}) + \mathrm{div}(f_1)$$
$$D_2 = (P_2) - (\mathcal{O}) + \mathrm{div}(f_2)$$

$P_1 + P_2 = P_3$ とする．点 P_1, P_2 を通る直線を $l : l_1 y + l_2 x + l_3$, 点 P_3 を通る垂線を $v : x + v_1 = 0$ とする．$P_1 = P_2$ ならば，l は点 P_1 における接線であり，$P_3 = \mathcal{O}$ ならば，$v = 1$ である．直線 l は点 $P_1, P_2, -P_3$ で 1 位の零点，無限遠点 $\mathcal{O}$ で 3 位の極を持ち，垂線 v は点 $P_3, -P_3$ で 1 位の零点，無限遠点 $\mathcal{O}$ で 2 位の極を持つので，

$$\begin{aligned}\mathrm{div}(l) =& (P_1) + (P_2) + (-P_3) - 3(\mathcal{O}) \\ \mathrm{div}(v) =& (P_3) + (-P_3) - 2(\mathcal{O})\end{aligned}$$

よって，因子の和 $D_1 + D_2$ は $f_3 = l/v$ として次のように書ける．

$$\begin{aligned}D_1 + D_2 =& (P_1) + (P_2) - 2(\mathcal{O}) + \mathrm{div}(f_1 f_2) \\ =& (P_3) - (\mathcal{O}) + \mathrm{div}(l) - \mathrm{div}(v) + \mathrm{div}(f_1 f_2) \\ =& (P_3) - (\mathcal{O}) + \mathrm{div}(f_1 f_2 f_3)\end{aligned}$$

2.2.4 引き戻し

ここで，提案手法の証明に必要となる因子の引き戻しについて述べる．まず，写像の引き戻しについて説明する．E_1, E_2 は体 K 上で定義された楕円曲線，$K(E_1), K(E_2)$ は E_1, E_2 の K 係数の有理関数全体のなす体とする．また，ϕ を E_1 から E_2 への K-係数有理写像とすると，以下の ϕ^* を “ϕ に関する f の引き戻し” と呼ぶ．図 2.2 に示す．

$$\phi^* : \begin{cases} K(E_2) & \to K(E_1) \\ f & \mapsto f \circ \phi \end{cases}$$

すなわち，ϕ^* は E_2 上の有理関数を E_1 上の有理関数に写像する関数であり，f の引き戻し $\phi^* f$ は合成写像 $f \circ \phi$ と等しくなる．

定義 2.25 分岐指数 (Ramification Index) [47]
写像 $\phi : E_1 \to E_2$，$P \in E_1(K)$ とする．P についての ϕ の分岐指数 $e_\phi(P)$ は

$$e_\phi(P) = \mathrm{ord}_P(\phi^* u_{\phi(P)})$$

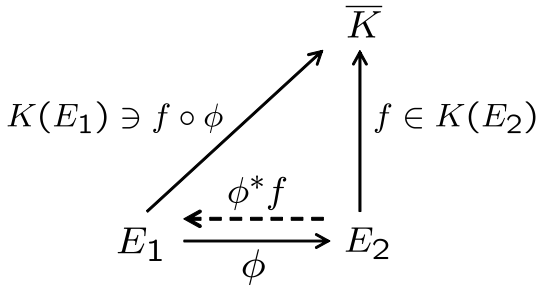

図 2.2: 写像の引き戻し

で与えられる．ここで，$u_\phi(P) \in K(E_2)$ は点 $\phi(P)$ における uniformizer である．$e_\phi(P) \geq 1$ であり，$e_\phi(P) = 1$ のとき，点 P について ϕ は非分岐であるといい，さらに E_1 におけるすべての点で非分岐のとき，ϕ は非分岐であるという．

分岐指数 $e_\phi(P)$ に関して，次式が成立する．

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg(\phi)$$

E_1, E_2 における因子の群をぞれぞれ $\mathrm{Div}(E_1), \mathrm{Div}(E_2)$ とする．$\mathrm{Div}(E_2)$ から $\mathrm{Div}(E_1)$ への因子群の間の写像を

$$\Psi : \begin{cases} \mathrm{Div}(E_2) & \to \mathrm{Div}(E_1) \\ (P) & \mapsto \sum_{Q \in \phi^{-1}(P)} e_\phi(Q)(Q) \end{cases}$$

と定義すると，非零な関数 $f \in K(E_2)^*$ に対して，

$$\Psi(\mathrm{div}(f)) = \mathrm{div}(f \circ \phi)$$

が成立する．ここで Ψ は ϕ に関する因子の引き戻しである．なお，$D \in \mathrm{div}(E_2)$ に対して，$\deg(\Psi D) = \deg(\Psi) \cdot \deg(D)$, $f \in K(E_2)^*$ に対して，$\phi^*(\mathrm{div} f) = \mathrm{div}(\phi^* f)$ が成立する．

第3章　ペアリング

本章では Tate ペアリング, Weil ペアリングの定義，性質及びその演算アルゴリズムについて述べる．ペアリングを利用した方式における安全性について言及し，計算量的に安全な小標数の有限体のサイズを示す．ペアリングを利用した応用プロトコルとして境・笠原らの方式を示し，さらに応用プロトコル間における計算コストの比較方法について説明する．

3.1　ペアリングの定義

3.1.1　Tate ペアリング

$\mathbb{F}_q$ は p を素数とする $q = p^m$ 個の要素からなる有限体，E は $\mathbb{F}_q$ 上で定義された楕円曲線とする．$\sharp E(\mathbb{F}_q) = hr = q + 1 - t$ において部分群の位数 r は大きな素数，h を cofactor とし，$r|q^k - 1$ を満足する最小の整数 k を埋め込み次数と呼ぶ．$r^2 \nmid q^k - 1$ とする．$P \in E(\mathbb{F}_q)[r]$ に対して $\mathrm{div}(f_{r,P}) = r(P) - r(\mathcal{O})$ となる有理関数 $f_{r,P} \in \mathbb{F}_q(E)$ が存在する．すべての点を r 倍して得られる異なる点の集合を $rE(\mathbb{F}_{q^k})$ とすると，その剰余類全体の集合を $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$ と表現する．剰余類の代表元を Q として，$D \sim (Q) - (\mathcal{O})$ となる因子 $D \in \mathrm{Div}^0(E)$ を選択する．$\mathrm{supp}(\mathrm{div}(f_{r,P})) \cap \mathrm{supp}(D) = \emptyset$ を満足するようにランダムに選んだ点 $R \in E(\mathbb{F}_{q^k})$ を利用して $D = (Q + R) - (R)$ とおくと，$f_{r,P}(D)$ を計算可能である．Tate ペアリングは次のように定義可能である．

定義 3.1 Tate ペアリング

$$\langle \cdot, \cdot \rangle_r : \begin{cases} E(\mathbb{F}_q)[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) & \to \mathbb{F}^*_{q^k}/(\mathbb{F}^*_{q^k})^r \\ (P, Q) & \mapsto \langle P, Q \rangle_r = f_{r,P}(D) \end{cases}$$

Tate ペアリングの値は剰余類全体の集合 $\mathbb{F}^*_{q^k}/(\mathbb{F}^*_{q^k})^r$ に属しており，一意に定まらない．すなわち，2 つの元 $a, b \in \mathbb{F}^*_{q^k}$ が元 $c \in \mathbb{F}_{q^k}$ を用いて $a = bc^r$ と表現可能なとき，a, b は合同 ($a \equiv b$) となる．ペアリングを利用する方式では $\mathbb{F}^*_{q^k}$ における一意に定まる値が必要であるため，c^r を消去する必要がある．$a^{q^k-1} = 1, a \in \mathbb{F}_{q^k}$ の性質を利用して，Tate ペアリングの値に最終べき乗 $(q^k - 1)/r$ を行うことにより，ユニークな値を得ることが可能である．Tate ペアリングの値を最終べき乗した reduced Tate ペアリングを次のように定義する．

定義 3.2 Reduced Tate ペアリング
$P \in E(\mathbb{F}_q)[r], Q \in E(\mathbb{F}_{q^k}), \mu_r = \{x \in \mathbb{F}_{q^k}^* | x^r = 1\}$ とする．

$$\tau(P,Q) = \langle P,Q \rangle_r^{(q^k-1)/r} = f_{r,P}(Q)^{(q^k-1)/r} \in \mu_r$$

[17] によれば，Reduced Tate ペアリングの重要な性質として $N = h'r$ に対して次式が成立する．

$$\tau(P,Q) = \langle P,Q \rangle_r^{(q^k-1)/r} = \langle P,Q \rangle_N^{(q^k-1)/N} \tag{3.1}$$

(3.1) によって，r を Hamming Weight が小さい $N = h'r \in \mathbb{N}$ に変更することにより, Miller's Algorithm におけるループ回数は部分群の位数 r を用いる場合に比べ増加するが，アルゴリズムの総計算量の低減が期待できる．Tate ペアリングの性質として以下の 3 つの性質が挙げられる．

1. 定義可能性
   すべての点 $Q \in E(\mathbb{F}_{q^k})$ に対して，$\langle \mathcal{O}, Q \rangle_r = 1$ が成立する．また，すべての点 $P \in E(\mathbb{F}_q)[r]$ および $Q \in rE(\mathbb{F}_{q^k})$ に対して，$\langle P,Q \rangle_r \in (\mathbb{F}_{q^k}^*)^r$ が成立する．

2. 非退化性
   無限遠点を除くすべての点 $P \in E(\mathbb{F}_q)[r] \setminus \{\mathcal{O}\}$ に対して，$\langle P,Q \rangle_r \notin (\mathbb{F}_{q^k}^*)^r$ を満足する点 $Q \in E(\mathbb{F}_{q^k})$ が存在する．

3. 双線形性
   すべての点 $P, P_1, P_2 \in E(\mathbb{F}_q)[r]$ および $Q, Q_1, Q_2 \in E(\mathbb{F}_{q^k})$ に対して，$\langle P_1 + P_2, Q \rangle_r \equiv \langle P_1, Q \rangle_r \langle P_2, Q \rangle_r$ および $\langle P, Q_1 + Q_2 \rangle_r \equiv \langle P, Q_1 \rangle_r \langle P, Q_2 \rangle_r$ が成立する．

3.1.2 Weil ペアリング

Weil ペアリングよりも Tate ペアリングの方が効率よく計算可能なため，一般的には Tate ペアリングを用いる場合が多い．しかし，Scott ら [34] によりペアリングの値が属する拡大体 $\mathbb{F}_{q^k}$ のサイズが 4096 ビット以上あれば，Weil ペアリングの方が高速であるとのソフトウェア実装による実測結果が報告されており，今後，研究のトレンドが Tate ペアリングから Weil ペアリングにシフトする可能性も考えられる．そこで，本小節では Tate ペアリングとの比較を通じて Weil ペアリングの定義，性質およびその計算手法について説明する．

$S, T \in E[r]$ に対して，$mT' = T$ となる点 $T' \in E$ を選択し，有理関数 $g \in K(E)$ は次式を満足するものとする．

$$\mathrm{div}(g) = \sum_{R \in E[r]} (T' + R) - (R)$$

定義 3.3 Weil ペアリング

$$e : \begin{cases} E[r] \times E[r] & \to \mu_r \\ (P, Q) & \mapsto g(X+S)/g(X) \end{cases}$$

ここで $X \in E$ は $g(X+S), g(X) \neq 0, \infty$ を満足する点であり，μ_r は $\overline{K}$ における単位元の r 乗根からなる乗法群である．

Weil ペアリングは関数 g および点 X の選び方に依存せず，点 S, T が互いに線形独立な点であれば，非自明 ($e(S,T) \neq 1$) となる．以下に Weil ペアリングの性質に関する定理を示す．

定理 3.1 *(*Silverman [47])
$S_1, S_2, S, T_1, T_2, T \in E[r]$ とすると，定義 *3.3* により定義される Weil ペアリングは以下の性質を満足する．

1. 双線形性
   $e(S_1 + S_2, T) = e(S_1, T)e(S_2, T)$
   $e(S, T_1 + T_2) = e(S, T_1)e(S, T_2)$
2. 恒等射
   $e(S, S) = 1$
3. 交互性
   $e(S, T) = e(T, S)^{-1}$
4. 非退化性
   すべての点 $S \in E[r]$ に対して $e(S, T) = 1$ が成立するならば，$T = \mathcal{O}$ である．

また Weil ペアリングには定義 3.3 よりも効率的に計算可能な別の定義が存在する．点 $S, T \in E[r]$ とする．因子 D_S, D_T は $\mathrm{supp}(D_S) \cap \mathrm{supp}(D_T) = \emptyset$ を満足するものとし，それぞれ $D_S \sim (S) - (\mathcal{O}), D_T \sim (T) - (\mathcal{O})$ とおく．S, T は r-torsion point であるため，rD_s, rD_T は主因子である．よって，$\mathrm{div}(f_{r,S}) = rD_S, \mathrm{div}(f_{r,T}) = rD_T$ を満足する関数 $f_{r,S}, f_{r,T} \in E$ が存在する．Weil ペアリング e' は以下のように定義可能である．

定義 3.4 Weil ペアリング *2*
定義 *3.3* と同じ表記とする．

$$e' : \begin{cases} E[r] \times E[r] & \to \mu_r \\ (S, T) & \mapsto f_{r,S}(D_T)/f_{r,T}(D_S) \end{cases}$$

次小節で説明する Miller's Algorithm により効率よく $f_{r,S}(D_T), f_{r,T}(D_S)$ を計算可能である．正確には定義 3.3，定義 3.4 により定義される Weil ペアリングの値は異なっており，$e(S,T) = 1/e'(S,T) = e'(T,S)$ となる．これらは Weil ペアリングの性質である交互性を満足する関係にあり，Weil ペアリング e' も定理 3.1 を満足する．

3.1.3 Miller's Algorithm

現在までに提案されているペアリング演算アルゴリズムのベースとなっているのが，1986年に Miller [28] によって提案された Miller's Algorithm である．これは Miller's Formula に基づく部分群の位数 r の 2 進展開法によるアルゴリズムである．

点 $U, V \in E(\mathbb{F}_{q^k})$ を通る直線 $g_{U,V} : l_1 y + l_2 x + l_3 = 0$ とする．$U = V$ のとき，$g_{U,V}$ は接線であり，U, V の片方が無限遠点であれば，$g_{U,V}$ は他方の点を通る垂線である．$g_{U,-U}$ を g_U と記述する．Miller's Algorithm の中で重要な位置づけを占める Miller's Formula を以下に示す．

定理 3.2 Miller's Formula
$P \in E(F_{q^k})$ とし，有理関数 f_c は $\mathrm{div}(f_c) = c(P) - (cP) - (c-1)(\mathcal{O})$ を満足するものであるとする．すべての $a, b \in \mathbb{Z}$ に対して，以下の等式が成立する．

$$f_{a+b,P} = f_{a,P} \cdot f_{b,P} \cdot g_{aP,bP} / g_{(a+b)P}$$

証明 $D_1 = a(P) - a(\mathcal{O}), D_2 = b(P) - b(\mathcal{O})$ とおく．D_1, D_2 は標準形で以下のように表現可能である．

$$D_1 = (aP) - (\mathcal{O}) + \mathrm{div}(f_{a,P})$$
$$D_2 = (bP) - (\mathcal{O}) + \mathrm{div}(f_{b,P})$$

和 $D_1 + D_2 = (a+b)(P) - (a+b)(\mathcal{O})$ は標準形として次式で与えられる．

$$(a+b)(P) - (a+b)(\mathcal{O}) = ((a+b)P) - (\mathcal{O}) + \mathrm{div}(f_{a,P} \cdot f_{b,P} \cdot g_{aP,bP} / g(a+b)P)$$

ここで $g_{aP,bP}/g_{(a+b)P}$ は §2.2.3 の $f_3 = l/v$ に対応している．$((a+b)P) - (\mathcal{O})$ を左辺に移行すれば，次式を得る．

$$\mathrm{div}(f_{a+b,P}) = \mathrm{div}(f_a \cdot f_b \cdot g_{aP,bP} / g_{(a+b)P})$$ □

Miller's Formula を利用して，点 $P \in E(\mathbb{F}_q)$ に対する $\mathrm{div}(f_{r,P}) = r(P) - r(\mathcal{O})$ を満足する有理関数 $f_{r,P}$ を r の 2 進展開法により求める．$\mathrm{div}(f_{1,P}) = 0$ より，$f_{1,P} = 1$ とおく．$i > 0$ のとき，

$$f_{i+1,P} = f_i \cdot g_{iP,P} / g_{(i+1)P}$$
$$f_{2i,P} = f_i^2 \cdot g_{iP,iP} / g_{2iP}$$

関数 $f_{r,P}$ の導出後，点 Q による因子 D を与えて (2.5) により $f_{r,P}(D)$ を計算するよりも，導出した中間値 $f_{i,P}(D)$ の積から求めたほうが効率が良い．因子 $D \sim (Q) - (\mathcal{O})$ はある点 $Q' \in E(F_{q^k})$ として $D = (Q + Q') - (Q')$ とすれば，2 進展開法における加算ステップ, 2 倍算ステップの中間値は次のようになる．

$$f_{i+1,P}(D) = f_{i+1,P}(Q+Q') / f_{i+1,P}(Q') = f_i(D) \cdot \frac{g_{iP,P}(Q+Q') g_{(i+1)P}(Q')}{g_{(i+1)P}(Q+Q') g_{iP,P}(Q')}$$
$$f_{2i,P}(D) = f_{2i,P}(Q+Q') / f_{2i,P}(Q') = f_i(D)^2 \cdot \frac{g_{iP,iP}(Q+Q') g_{2iP}(Q')}{g_{2iP}(Q+Q') g_{iP,iP}(Q')}$$

上述の方法をまとめたものを Miller's Algorithm として以下に示す.

Algorithm 3.1: Miller's Algorithm

INPUT: $P \in E(\mathbb{F}_q)[r], Q \in E(\mathbb{F}_{q^k})$
OUTPUT: $f \in \mathbb{F}_{q^k}$
$Q' \in_R E(\mathbb{F}_{q^k}), S = Q + Q' \in E(\mathbb{F}_{q^k})$
$f \leftarrow 1, V \leftarrow P$ and $r = \sum_{i=0}^{l-1} r_i 2^i, r_i \in \{0, 1\}$
for $j \leftarrow l - 1$ **downto** 0 **do**
    $f \leftarrow f^2 \cdot (g_{V,V}(S)g_{2V}(Q'))/(g_{2V}(S)g_{V,V}(Q'))$ and $V \leftarrow 2V$
    if $r_j = 1$ **then**
        $f \leftarrow f \cdot (g_{V,P}(S)g_{V+P}(Q'))/(g_{V+P}(S)g_{V,P}(Q'))$ and $V \leftarrow V + P$
return f

3.2 ペアリングを利用した方式における安全性

3.2.1 暗号系における安全性

RSA 暗号やエルガマル暗号などに代表される公開鍵暗号方式の安全性は数学的問題の困難性を仮定することにより証明される．厳密にはあるプロトコルにおいて攻撃者に圧倒的に有利な環境を与えたとしても，数学的問題を破ることができなければ，ある確率以下でしか攻撃は成功しないことを示す．これを証明可能安全性と言い，その安全性の強度は安全性の目的 [強秘匿性 (Semantic Secure), 頑強性 (Non-Malleable) , 識別不可能性 (INDistinguishable)] と攻撃者の条件 [選択暗号文攻撃 (CCA), 適応的選択暗号文攻撃 (CCA2) など] の組み合わせで表現される．現在，理論上攻撃に最も頑強かつ安全な方式は IND-CCA2(NM-CCA2) を満足する方式である．本稿では，詳細な安全性証明手法については述べず，安全性の基盤となる数学的な問題について議論する．以下に群 $\mathbb{G}$ に対する離散対数問題に関する数学的問題を列挙する．ここで，素数位数 l の群 $\mathbb{G}$ の元を g とする．

定義 3.5 Computational Diffie-Hellman (CDH) 問題
Given: g, g^a, g^b for some $a, b \in Z_l^*$
Answer: g^{ab}

定義 3.6 Decisional Diffie-Hellman (DDH) 問題
Given: g, g^a, g^b, g^c for some $a, b, c \in Z_l^*$
Answer: Yes if $c = ab \mod l$ otherwize no

楕円曲線上における加法群 $\mathbb{G}$ では CDH 問題を解くことは非常に困難だが，DDH 問題はペアリングの双線形性の性質を利用することにより簡単に解くことができる．このような CDH 問題と DDH 問題の困難性に差が生じるようなクラスを Gap Diffie-Hellman (GDH) クラスと呼ぶ.

また，双線形写像 (Bilinear map) e に関する Diffie-Hellman 問題を同様に定義できる．素数位数 q の加法群，乗法群をそれぞれ $\mathbb{G}_1, \mathbb{G}_2$ とし，$P \in \mathbb{G}_1$ とおく．

定義 3.7 Bilinear Diffie-Hellman (BDH) 問題
Given: P, aP, bP, cP for some $a, b, c \in Z_l^*$
Answer: $e(P,P)^{abc}$

定義 3.8 Decisional Bilinear Diffie-Hellman (DBDH) 問題
Given: P, aP, bP, cP, r for some $a, b, c \in Z_l^*, r \in \mathbb{G}_2$
Answer: Yes if $r = e(P,P)^{abc}$ otherwize no

図 3.1 に上述した数学的問題の帰着関係について示す．帰着関係とはある問題 A が別の問題 B に帰着する場合，問題 B が解ければ問題 A を解くことが可能な関係を言い，下図では $A \rightarrow B$ と表現される．ここで ECDLP, DLP をそれぞれ加法群 $\mathbb{G}_1$，乗法群 $\mathbb{G}_2$ における離散対数問題 $DL_{\mathbb{G}_1}, DL_{\mathbb{G}_2}$ と表現する．

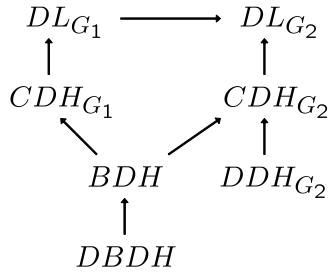

図 3.1: 数学的問題の帰着関係

ペアリングを利用した方式で定義される数学的な問題はすべて離散対数問題 $DL_{\mathbb{G}_1}, DL_{\mathbb{G}_2}$ に帰着する．すなわち，他の数学的な問題は離散対数問題の困難性を仮定したことを前提として成立する問題であると言える．次小節では離散対数問題の困難性について説明する．

3.2.2 離散対数問題

楕円曲線上の離散対数問題（ECDLP）には特殊な場合を除いて準指数関数時間で解読可能なアルゴリズムは存在しない．基本的には後述する一般の有限群上の離散対数問題に対するアルゴリズムを適用する．

有限体の離散対数問題に対する攻撃法は一般の有限群に適用できる一般法と有限体における乗法群の性質を用いる指数計算法 (Index Calculus 法) の 2 種類に分類される．一般法には Pohlig-Hellman 法, Baby-Step/Giant-Step 法 ($\sqrt{N}$)，Pollard 法 ($\sqrt{\pi N/2}$) があり，いずれも群位数ビット長の指数時間アルゴリズムである．指数計算法は数体ふるい法（素因数分解アルゴリズムの数体ふるい法を応用したもの）と関数体ふるい法があり，どちらも準指数時間アルゴリズムである．1984 年，Coppersmith [12] が標数 2 の有限体上における離散対数問題を効

率よく解読するアルゴリズムを提案したことにより，ハードウェア実装に適した標数 2 の有限体の離散対数問題の危険性が指摘されるようになった．Coppersmith 法は上述した関数体ふるい法の特別な場合と位置づけられ，一般に小標数の有限体における離散対数問題は関数体ふるい法を利用して標数が大きな素数の場合よりも効率よく解読可能である．

次に小標数の有限体における離散対数問題の計算量を算出し，計算量的に安全と考えられる有限体のサイズを導出する．有限体上の離散対数問題を解読するために必要な計算量を

$$L_n[a,c] = exp[(c+O(1))(\log_e n)^a(\log_e \log_e n)^{1-a}]$$

とする． [52] によれば，有限体 $\mathbb{F}_{p^k}$ の離散対数問題の計算量は以下のようになる．

表 3.1: 離散対数問題の計算量

条件 ($\varepsilon > 0$)	アルゴリズム	計算量
$k < (\log_2 p)^{1/2-\varepsilon}$	数体ふるい法	$L_{\mathbb{F}_{p^k}}[1/3, (64/9)^{1/3}]$
$k \geq (\log_2 p)^2$	関数体ふるい法	$L_{\mathbb{F}_{p^k}}[1/3, (32/9)^{1/3}]$

1024 ビットサイズの素体 $\mathbb{F}_p$ における離散対数問題の計算量 $L_{\mathbb{F}_{p^k}}[1/3, (64/9)^{1/3}]$ と同等の計算量を有する小標数の有限体のサイズを導出するため，標数 2,p の有限体のサイズとその離散対数問題の計算量の関係を図 3.2 に示す．素体における計算量は $L_{\mathbb{F}_p,|p|=1024}[1/3, (64/9)^{1/3}] = 1.316 \times 10^{26}$ と算出され，同等の計算量を持つ標数 2 の有限体の拡大次数を計算すると 1751 ビットとなる．なお，2007 年現在の解読記録は 2001 年の Thomé [40] による関数体ふるい法を利用した $\mathbb{F}_{2^{607}}$ における解読，2005 年の Joux ら [22] による数体ふるい法を利用した 130 桁の素数 p を標数に持つ有限体 $\mathbb{F}_p$ における解読などがある．

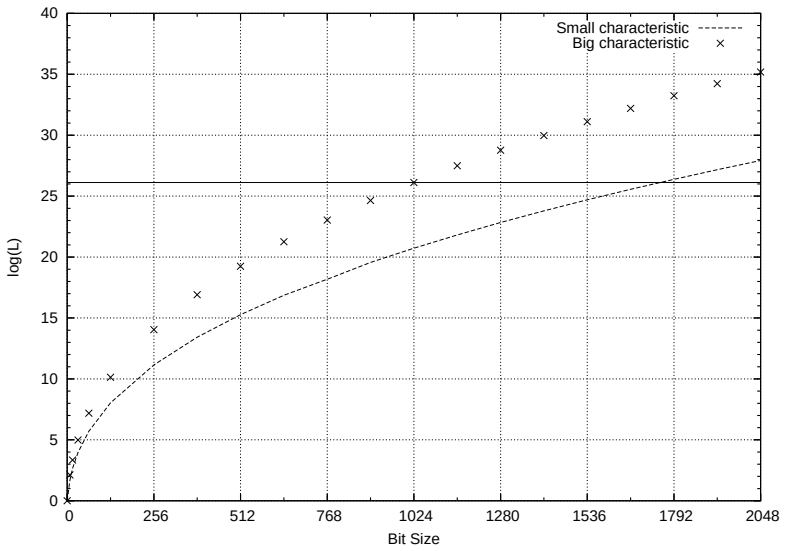

図 3.2: 離散対数問題の計算量と有限体のサイズ

3.3 ペアリングを利用した応用プロトコル

3.3.1 ID に基づく方式

2000 年に境・笠原らによって提案された ID に基づく鍵共有方式 [33] はペアリングの双線形性を効果的に利用した初めての方式である．以降，ペアリングの双線形性を利用した暗号方式に関する研究が活発に行われるようになった．

代表的な ID に基づく暗号方式として Identity Based Encryption(IBE) [6] があり，既に Voltage Security 社によって「Voltage SecureMail」 [55] として商品化されている．一般に IBE 方式では ID を公開鍵としてメッセージを暗号化することが可能であり，従来の PKI における証明書の取得や失効リストの発行などの管理・運用コストが削減され，また公開鍵を覚えやすいことからユーザにとって利用しやすいという特徴を有する．また，メッセージの署名を ID によって検証可能な ID ベース型署名方式 (IBS) [19] なども提案されている．また，ペアリングの双線形性を利用することにより，既存方式よりもプロトコルの簡略化・通信データ量の削減などの大幅なパフォーマンス向上が期待できる．広く知られた応用例として，署名長が従来方式の半分で済む Short Signature [8] や Joux による 1 ラウンドの三者間鍵共有方式 [21] がある．また，正規のユーザーに対してセッションキーを効率的に配送することを目的とした放送用暗号方式において，2005 年，Boneh ら [7] によってユーザの秘密鍵のサイズ，伝送量のサイズがユーザ数に依存せずに固定長となる方式が提案されている．この方式は計算量的な側面で問題を抱えているが，同研究分野において重要な位置づけを占める方式である．

ペアリングを利用した方式の一例として，境・笠原らによる ID に基づく鍵共有方式 [33] を示す．

【事前準備】

ユーザー i の ID 情報を ID_i，ID_i を加法群 $\mathbb{G}$ における元 P_i に写像する関数 (**MapToPoint**) を H, ペアリングを $e(\cdot,\cdot) \in \mathbb{G}_T$ とする．ここで $ID_i, H, e(\cdot,\cdot)$ は公開情報，$\mathbb{G}_T$ は乗法群である．センターは秘密情報となる乱数 l を生成し，ユーザー i の秘密鍵 $S_i = lP_i$ を計算，ユーザー i に送信する．

ここでは，ユーザー A, B の ID 情報を ID_A, ID_B として 2 者間の事前準備不要の鍵共有方式を紹介する．

【鍵共有】

ユーザー A は ID 情報 ID_B を用いて MapToPoint H により加法群 $\mathbb{G}$ における元 P_B を生成する．ユーザー A が得る共通鍵 $K_{AB} \in \mathbb{G}_T$ は,

$$K_{AB} = e(S_A, P_B) = e(P_A, P_B)^l$$

となる．同様の処理を行うことにより，ユーザー B は以下の共通鍵 K_{BA} を得る．

$$K_{BA} = e(S_B, P_A) = e(P_B, P_A)^l$$

よって $K_{AB} = K_{BA}$ となり，ユーザー A, B は同じ鍵を共有する．

3.3.2 応用プロトコルにおける計算コスト

ペアリングを利用した方式には主要な演算が 3 つあり，楕円曲線上のスカラー倍算，ペアリング演算，有限体におけるべき乗剰余演算である．また，ID 情報を楕円曲線上の点に写像する MapToPoint は従来のハッシュ関数と比較して複雑な処理を行うため，その計算コストは無視できない．そこで，スカラー倍算 (aP)，ペアリング演算 ($e(P,Q)$)，べき乗剰余演算 ($g^x \bmod p$)，MapToPoint のそれぞれの 1 回の演算コストを M, P, E, H を単位として表現し，本章で紹介した方式の計算コストを表 3.2 に示す．n はユーザー数，[ ] は事前計算可能であること表す．

表 3.2: 応用プロトコルにおける計算コスト

方式	計算コスト		
	事前準備	暗号化/署名	復号化/検証
ID に基づく鍵共有方式 [33]	$2P + 2H$		
3 者間鍵共有方式 [21]	$3M + 3P + 3E$		
Identiby Based Encryption [6]	$(n+1)M + nH$	$1M + 1P + 1E + 1H$	$1P$
Short Signature [8]	$1M$	$1M + 1H$	$1P + 1H$
Identity Based Signature [19]	$(n+1)M + nH$	$1M + [1P] + 1E$	$[1P] + 1P + 1E$

事前準備において ID に基づく方式ではユーザー数に応じたスカラー倍算，MapToPoint の処理が必要であるが，どの方式でもペアリング演算は不要である．本来，事前準備は管理者が潤沢な計算機環境を利用して，システムの運用開始の際に一度行うのみであり，計算コストの大きさはそれほど問題とはならない．一方，暗号化・復号化，署名・検証に段階ではモバイル環境などリソースが限られた環境で計算処理を行う状況も想定され，より計算コストの小さい方式が望まれる．また，ペアリングの演算を外部の計算機に委託する手法 [27] や複数の署名を同時検証可能な Batch Verification 技術 [9] などの研究も行われている．

一方で上述した性能評価方法では $P >> M, E, H$ という曖昧な指標を基準として計算コストの比較が行っているが，同様の機能を有するプロトコル間における計算コストの性能評価は行いやすい．しかし，システム設計においては，単純に計算コストの大きな演算のみ考慮するのではなく，計算コストと演算回数の積が最大となる演算をボトルネックとみなしてシステム構成する必要がある．その場合に明確な値として計算量を推定することが非常に重要であり，ある一つの基本算術を単位としてプロトコル全体の総計算量を算出することが求められる．§7.1.3 では上述した 4 つの演算手法について，有限体における乗算を基本算術として計算コストの推定を行う．

第4章　ペアリング演算

ペアリング演算に関連するものとして楕円曲線，有限体，演算アルゴリズムの 3 つが挙げられる．4.1 節ではペアリングに適した楕円曲線の生成方法，4.2 節では有限体における効率的な演算手法を紹介する．4.3 節では現在までの提案された主要なアルゴリズムとして BKLS アルゴリズム，Duursma and Lee アルゴリズム，Eta ペアリングについて説明する．

4.1　楕円曲線の生成手法

4.1.1　Pairing-friendly Curves

楕円 ElGamal 暗号系や ECDSA(Elliptic Curve Disital Signature Algorithm) などに代表される楕円曲線を用いる方式ではランダムに生成された楕円曲線を利用してシステムの構築が行われているが，ペアリングを利用した方式においてはパラメータ設定の点からそれらの曲線は利用できない．一般にペアリングに適した楕円曲線を Pairing-friendly Curve と呼び，ペアリングの有用性が明らかになると同時に Pairing-friendly Curve の生成に関する研究も活発に行われるようになった．

定義 4.1 Pairing-frinedly Curve
有限体 $\mathbb{F}_q$ 上で定義される楕円曲線 E を想定する．次の *2* 点を満足する楕円曲線 E を Pairing-friendly Curve と呼ぶ．
1. $\sharp E(\mathbb{F}_q)$ を割り切る素数 $r \geq \sqrt{q}$ が存在する．
2. 部分群の位数となる r に対する楕円曲線の埋め込み次数 k は $k < (\log_2 r)/8$ を満足する．

楕円曲線の生成においては，部分群の位数 r と楕円曲線の定義体 $\mathbb{F}_q$ のサイズの比 $\rho = \log q / \log r$ および埋め込み次数 k が非常に重要な要素となる．一般に ρ の値は小さいほど定義体のサイズも小さくなるため，楕円曲線上のスカラー倍演算が高速処理が可能である．特に定義体が署名長となる Short Signature [8] などでは $\rho \sim 1$ であることが望まれる．また，埋め込み次数 k が偶数であれば，後述する高速化手法 (§**??**参照のこと) を適用可能である．

Pairing-friendly Curve は Supersingluar Curve と Ordinary Curve のに分類することができる．Supersingular Curve は distortion map が必ず存在するなどの利点があるが，埋め込み次数 k は楕円曲線であれば，$k \leq 6$ であることが知られている [31]. よって，より大きい埋め込み次数が必要であれば，任意の埋め込み次数を持つような Oridnary Curve の生成が必要となる．

4.1.2 Supersingular Curve

Supersingular Curve は IBE [6] や Short Signature [8] などの方式で用いられ，また，その特性を利用した後述する高速なアルゴリズムが提案されている．

埋め込み次数が偶数で容易に曲線が得られる Supersingular Curve を以下に示す．定義体 $\mathbb{F}_q$ における Supersingular Curve は $r \mid q+1$ を満足することが条件となるため，素数 r，cofactor h のサイズを自由に決定できるという利点を持つ．一方，小標数における Supersingular Curve は群位数が大きな素数を持つか判定する必要がある．また拡大次数 m が素数となる 3 項から構成される Trinomial な既約多項式により生成される拡大体はソフトウェア実装に適しており，reduction などを効率よく行うことができる．

表 4.1: 種数 1 の Supersingular Curve

定義体	楕円曲線	distortion map ψ	条件	trace	k
$\mathbb{F}_q$	$y^2 = x^3 + ax$	$(x,y) \mapsto (-x, iy)$ $i^2 = -1$	$p \equiv 3 \pmod 4$	0	2
$\mathbb{F}_q$	$y^2 = x^3 + b$	$(x,y) \mapsto (\zeta x, y)$ $\zeta^3 = 1, \zeta \neq 1$	$p \equiv 2 \pmod 3$	0	2
$\mathbb{F}_{2^m}$	$y^2 + y = x^3 + x$	$(x,y) \mapsto (x + s^2, y + sx + t)$ $s^2 + s + 1 = 0, t^2 + t + s = 0$	$m \equiv \pm 3 \pmod 8$ otherwise	$t = \sqrt{2q}$ $t = -\sqrt{2q}$	4
$\mathbb{F}_{2^m}$	$y^2 + y = x^3 + x + 1$	$(x,y) \mapsto (x + s^2, y + sx + t)$ $s^2 + s + 1 = 0, t^2 + t + s = 0$	$m \equiv \pm 1 \pmod 8$ otherwise	$t = \sqrt{2q}$ $t = -\sqrt{2q}$	4
$\mathbb{F}_{3^m}$	$y^2 = x^3 - x + 1$	$(x,y) \mapsto (\rho - x, \sigma y)$ $\sigma^2 + 1 = 0, \rho^3 - \rho - b = 0$	$4 \nmid m - 1$ otherwise	$t = \sqrt{3q}$ $t = -\sqrt{3q}$	6
$\mathbb{F}_{3^m}$	$y^2 = x^3 - x - 1$	$(x,y) \mapsto (\rho - x, \sigma y)$ $\sigma^2 + 1 = 0, \rho^3 - \rho - b = 0$	$4 \mid m - 1$ otherwise	$t = \sqrt{3q}$ $t = -\sqrt{3q}$	6

Supersingular Curve には distortion map と呼ばれる同型写像が存在する．distortion map とは埋め込み次数 k を持つ楕円曲線 E における $\mathbb{F}_q$-有理点を $\mathbb{F}_{q^k}$-有理点に写す関数であり，点 $P \in E(\mathbb{F}_q)$ と独立した点 $\psi(P) \in E(\mathbb{F}_{q^k})$ を容易に導出できる．すなわちペアリングの値が非自明となる Modified Tate ペアリングを定義可能である．

定義 4.2 Modified Tate ペアリング
$P, Q \in E(F_q)[r]$ とすると，Modified Tate ペアリング $\hat{\tau}$ は次式で与えられる．

$$\hat{\tau}(P,Q) = \tau(P, \psi(Q))$$

非自明とは同じ点を入力として与えても単位元を出力をしない, すなわち，$\hat{\tau}(P,P) \neq 1$ となることを意味しており，暗号系で用いる際には安全性の面から非自明なペアリングが不可欠である．また，ペアリングの入力を同一の群 ($E(\mathbb{F}_q)$) から取れ，また，distortion map ψ とスカラー倍が可換 ($m\psi = \psi m$) であるため，拡大体におけるスカラー倍を処理するモジュールが不用となり，コンパクトなシステム設計が可能となる．

一方で Supersingular Curve は楕円曲線の中でも非常に特異な曲線であることなどから漠然と脆弱性を有するのではないかという推測がなされているが，現時点では具体的な攻撃方法は見つかっておらず，Pairing-friendly Curve に分類される Ordinary Curve と同程度の安全性を有すると考えられている [24].

4.1.3 Ordinary Curve

ほぼすべての楕円曲線は CM 法 (Complex Multiplication method) に基づいて生成され，Superpersingular Curve でも前小節で紹介した曲線以外は CM 法を用いる必要がある．CM アルゴリズムは素数べき q と整数 n を入力に与えると，n 個の $\mathbb{F}_q$-有理点を有するような $\mathbb{F}_q$ 上で定義される楕円曲線 E を出力するアルゴリズムである．曲線生成に関する研究の多くは任意の埋め込み次数 k を有するような q, n を生成することを目的とする．これらは個別にパラメータを生成する手法と多項式表現による楕円曲線族を生成する手法の 2 通りに分類されるが，Supersingular Curve は前者に属する．本小節では後者の手法によるパラメータ生成について述べ，CM アルゴリズムの詳細については触れないものとする．

パラメータの生成は CM 等式 (4.1) を満足する x, y を求める必要がある．D は “CM discriminant” と呼ばれ，ある固定された正整数とする．以下，q, t, r などをパラメータ x の関数と考え，$q(x), t(x), r(x)$ などと表記する．

$$Dy^2 = 4q(x) - t(x)^2 \tag{4.1}$$

また，$hr = q + 1 - t$ により，次のような変形も可能である．h を cofactor と呼ぶ.

$$Dy^2 = 4hr(x) - (t(x) - 2)^2 \tag{4.2}$$

CM 等式を満足する解 (x, y) は指数関数的に値が上昇するが，その値を元に得られる曲線族を Sparse な曲線族，いかなる x に対しても CM 等式が成立するように y を x による多項式表現したとき得られる曲線族を Complete な曲線族と呼ぶ [16].

Pairing-friendly Curve の先駆的な研究と知られる宮地ら [30] による曲線生成 (MNT Curve) は Sparse な曲線族に分類される．$k = 3, 4, 6$ を持つ素数位数の Ordinary Curve に対する q, t の条件を $x \in \mathbb{Z}$ による多項式で表現し，CM 等式に代入して一般的ペル方程式 (4.3) に変形する．

$$x^2 - Dy^2 = N \tag{4.3}$$

一般的ペル方程式は $(P_0 + \sqrt{D})/Q_0$ を連分数展開する PQa アルゴリズムを用いた LMM アルゴリズムにより解くことができる．詳細は [32] を参照して欲しい.

MNT Curve 生成の手順はある D に対する一般的ペル方程式の解 X, Y を導出，得られる $q, r = q + 1 - t$ が素数であるか判定し，素数でなければ，D を再度選択するアルゴリズムとなる．埋め込み次数 $k = 3, 4, 6$ に対する q, t, 一般的ペル方程式とそのときの X の値, 計算効率を向上させるための D の条件を表 4.2 に示す.

表 4.2: MNT Curve

k	q	t	一般的ペル方程式	X	D
3	$12x^2-1$	$-1\pm 6x$	$X^2-3Dy^2=24$	$6x\pm 3$	$D\equiv 19 \pmod{24}$
4	x^2+x+1	$-x,(x+1)$	$X^2-3Dy^2=-8$	$3x+2,(3x+1)$	D is square-free
6	$4x^2+1$	$1\pm 2x$	$X^2-3Dy^2=-8$	$6x\mp 1$	$D\equiv 3 \pmod{8}$

MNT Curve の生成手法を拡張した手法がいくつか提案されているが，Scott ら [36] は cofactor h の値を柔軟に変更可能な曲線生成アルゴリズムを提案している．すなわち，(4.2) において $r=\Phi_k(t-1)/d, t=x+1$ を代入することにより，

$$Dy^2 = 4h\frac{\Phi_k(x)}{d} - (x-1)^2 \tag{4.4}$$

となり，これを x の線形置換により変形し，一般的ペル方程式を得る．曲線生成は MNT Curve と同様のアルゴリズムに従う．

Complete な曲線族では CM 等式の左辺が常に D と完全平方の積で表現できる，すなわち，y を x による多項式で表現することによりいかなる x に対しても CM 等式が成立するように $D, t(x), q(x)$ を選択する．現在，Sparse な曲線族より活発に研究がなされており，様々な曲線生成手法が提案されている．ここでは，§7.1.3 の性能評価で用いる $4,6$ 次の twist を有する楕円曲線を容易に生成可能な手法について紹介する．

$D=1,2,3$ のとき，有限体 $\mathbb{F}_q$ における以下の楕円曲線を得られることが知られている [16].

$$\begin{aligned}
E_1: &\quad y^2 = x^3 + ax && (D=1)\\
E_2: &\quad y^2 = x^3 - 30a^2x + 56a^3 && (D=2)\\
E_3: &\quad y^2 = x^3 + a && (D=3)
\end{aligned}$$

ここで q は 6 と互いに素，$a\in\mathbb{F}_q^*$ である．特に $D=1,3$ のとき，それぞれ E_1, E_2 は 4,6 次の twist を持つ楕円曲線であり，後述する Ate ペアリング，Twisted Ate ペアリングを効率よく構成可能である．一方で $D=1,3$ における効率的な Pollard 法が存在しており, ECDLP の安全性が数ビット程度低下することが知られている．ここでは小さな値の D に伴う脆弱性よりも twist を容易に得られる点を重視する．

Barreto ら [5] は $D=3$ となる CM 等式を満足する $k=12$ における素数位数の楕円曲線のパラメータ q,t を次のような多項式表現で与え，簡略化した CM 法に基づくアルゴリズムを提案している．

$$\begin{aligned}
t &= 6z^2+1\\
n &= 36z^4+36z^3+18z^2+6z+1\\
p &= 36z^4+36z^3+24z^2+6z+1\\
DV^2 &= 3(6z^2+4z+1)^2
\end{aligned}$$

以下に示すアルゴリズムは p, n のおおよそビット長 m を入力とし，生成元 $G = (1, y)$ となる $\mathbb{F}_p$ 上で定義された位数 n の楕円曲線 $y^2 = x^3 + B$ のパラメータ p, n, B, y を出力する．与えられたビット長 m から初期値 x_0 を生成，$p(x_0), r(x_0)$ が素数であれば，$D = 3$ における CM 法は $E(F_p) : y^2 = x^3 + B, B \neq 0$ の曲線を生成する．また，$B + 1$ が平方剰余となる最小の B を探索することにより，$nG = \infty$ を満足するベースポイント $G = (1, (B + 1)^{1/2} \bmod p)$ を容易に生成することができる．

Algorithm 4.1: Constructiong a curve of prime order with $k = 12$

Input: the size m of curve order (in bits)
Output: p, n, B, y such that $y^2 = x^3 + B$ has order n over $\mathbb{F}_p$ and the base point $G = (1, y)$

Let $P(z) \equiv 36z^4 + 36z^3 + 24z^2 + 6z + 1$
Compute the smallest $z \approx 2^{m/4}$ such that $\lceil \log_2 P(-z) \rceil = m$
loop
    $t \leftarrow 6z^2 + 1$
    $p \leftarrow P(-z), n \leftarrow p + 1 - t$
    if p and n are prime **then**
        exit loop
    end if
    $p \leftarrow P(z), n \leftarrow p + 1 - t$
    if p and n are prime **then**
        exit loop
    end if
    $z \leftarrow z + 1$
end loop
$B \leftarrow 0$
repeat
    repeat
        $B \leftarrow B + 1$
    until $B + 1$ is a quadratic residue $\bmod p$
    Compute y such that $y^2 = B + 1 \bmod p$
    $G \leftarrow (1, y)$ on the curve $E : y^2 = x^3 + B$
until $nG = \mathcal{O}$
return p, n, B, y

あらかじめ得られる曲線の形が決まっているものに関しては，上記のアルゴリズムは適当な行を修正することにより他の埋め込み次数の場合にも応用可能である．効率的にペアリング演算が可能な $k = 4, 6, 8$ のケースにおいても楕円曲線パラメータの多項式表現が示されており，同様にして曲線生成が可能である．

4.2 有限体における演算

4.2.1 Pairing-friendly field

ペアリングの値は楕円曲線の埋め込み次数 k を拡大次数に持つ有限体 $\mathbb{F}_{p^k}$ の元となるため，乗算・2 乗を効率よく行えるような拡大体を用いる必要がある．Koblitz ら [24] は以下に示すペアリング演算に適した有限体として Pairing-friendly field を導入している．Pairing-friendly field を用いることにより，既約多項式を規定する定数による乗算が効率よく行え，また，有限体の乗算コストの分析も容易となり，理論的なペアリング演算コスト算出が可能になる．

定義 4.3 Pairing-friendly field
1. 標数 p は素数であり, $p \equiv 1 \pmod{12}$ を満足する．
2. 埋め込み次数 k は $k = 2^i 3^j, i \geq 0, j > 0$ で表現可能である．
上記 *2* 点を満足する有限体 $\mathbb{F}_{p^k}$ を Pairing-friendly field と呼ぶ．

β は平方数でもない立方数でもない $\mathbb{F}_p$ の元とする．2 項式 $X^k - \beta$ は $\mathbb{F}_p[X]$ における既約多項式となり，k 次拡大体 $\mathbb{F}_{p^k}$ が定まる．このとき，β の平方根あるいは立方根が解となる 2 項式を既約多項式として逐次的に拡大体 $\mathbb{F}_{p^k}$ を構成することが可能である．さらに，$j = 0$ であれば，$p \equiv 1 \pmod{4}$ の条件で 2 次拡大による再帰的な構成も可能となる．以降，有限体における効率的な演算手法，拡大体構成方法について説明する．計算コストの算出にあたって，素体 $\mathbb{F}_p$ における乗算，2 乗，加算（減算），β による定数倍をそれぞれ M, S, A, B で表現する．

4.2.2 Karatsuba-Ofman 法

最も単純な教科書法による n ビットの整数同士の乗算は $O(n^2)$ の計算量が必要とされる．Karatsuba-Ofman 法 (KO 法) では与えられた整数を 2 分割するにより 2 項多項式を生成，少ない乗算回数で多項式演算することで，より小さい計算量 $O(n^{\lg(3)}) \approx O(n^{1.585})$ で乗算を行うことが可能である．しばしば 2 次拡大体の乗算に適用される．Toom [41] と後の Cook [11] は Karatsuba 法を拡張し，与えられた整数を 3 分割することによる効率的な乗算アルゴリズム (Toom-Cook 法) を提案し，さらに小さい計算量 $O(n^{1.46})$ で乗算可能となった．こちらは 3 次拡大体の乗算に適用されることが多い．

素体 $\mathbb{F}_p$ における k 次の既約多項式による拡大体 $\mathbb{F}_{p^k}$ の元は $k-1$ 次の多項式 $a_0 + a_1 X + \cdots + a_{k-1} X^{k-1}$ で表現される．すなわち，拡大体における演算とは $k-1$ 次以下の多項式同士の乗算のことを意味する．演算結果は $2k-2$ 次の多項式となるが，既約多項式による剰余を計算することにより $k-1$ 次の多項式を得る．2 つの元 $a, b \in \mathbb{F}_{p^k}$ の乗算は最も単純な教科書法では，$X^k - \beta$ を既約多項式として，

$$c = ab = (\sum_{i=0}^{k-1} a_i X_i)(\sum_{i=0}^{k-1} b_i X_i) \pmod{(X^k - \beta)}$$

と定義される．最終的に得られる多項式 c の係数 c_i は次の式で表される．

$$c_i = \sum_{j=0}^{i} a_j b_{i-j} + \beta(\sum_{j=i+1}^{k-1} a_j b_{i-j+k}) \pmod{p}$$

Karatsuba 法による 2 次拡大体 $\mathbb{F}_{p^2}$ における乗算は次のようになる．$c = ab \in \mathbb{F}_{p^2}$ とすると，$v_0 = a_0 b_0, v_1 = a_1 b_1$ を最初に求め，

$$c_0 = v_0 + \beta v_1$$
$$c_1 = (a_0 + a_1)(b_0 + b_1) - v_0 - v_1$$

と計算することにより，教科書法では 4 回必要だった乗算回数が 3 回に削減される．3 次拡大体 $\mathbb{F}_{p^3}$ における乗算にも KO 法を適用することが可能である．$c = ab \in \mathbb{F}_{p^3}$ とすると，$v_0 = a_0 b_0, v_1 = a_1 b_1, v_2 = a_2 b_2$ を事前計算しておき，

$$c_0 = v_0 + \beta((a_1 + a_2)(b_1 + b_2) - v_1 - v_2)$$
$$c_1 = (a_0 + a_1)(b_0 + b_1) - v_0 - v_1 + \beta v_2$$
$$c_2 = (a_0 + a_2)(b_0 + b_2) - v_0 + v_1 - v_2$$

として乗算を行う．Weimerskirch ら [42] は任意の次数の多項式に KO 法を適用する一般的方法について述べている．

4.2.3 Toom-Cook 法

Toom-Cook 法は $2k-1$ 個の異なる点における $k-1$ 次の多項式の値を計算する多項式補完法に基づくアルゴリズムである．2 つの元 $a, b \in \mathbb{F}_{p^k}$ の積は $2k-2$ 次の多項式 $a(x)b(x)$ で与えられるが，$2k-1$ 個の異なる元 $x_i \in \mathbb{F}_p$ を選択，$a(x_i)b(x_i)$ を計算すると多項式補完法により $ab \in \mathbb{F}_p[X]$ が一意に決定する．この値を Reduction することにより $c = ab \in \mathbb{F}_{p^k}$ を得る．Toom-Cook 法の効率性は選ばれる x_i と多項式補完法に依存しており，大きい次数の多項式に対する実装方法は厳密に示されていない．

Toom-Cook 法による 3 次拡大体 $\mathbb{F}_{p^3}$ における乗算は次のようにして求められる．$a(x), b(x) \in \mathbb{F}_{p^3}$ とすると，$\{0, \pm 1, 2, \infty\}$ の 5 点における $a(x)b(x)$ の計算は以下の通りである．

$$v_0 = a(0)b(0) = a_0 b_0$$
$$v_1 = a(1)b(1) = (a_0 + a_1 + a_2)(b_0 + b_1 + b_2)$$
$$v_2 = a(-1)b(-1) = (a_0 - a_1 + a_2)(b_0 - b_1 + b_2)$$
$$v_3 = a(2)b(2) = (a_0 + 2a_1 + 4a_2)(b_0 + 2b_1 + 4b_2)$$
$$v_4 = a(\infty)b(\infty) = a_2 b_2$$

Lagrange の多項式補完法により,

$$c_0 = v_0 + \beta((1/2)v_0 - (1/2)v_1 - (1/6)v_2 + (1/6)v_3 - 2v_4)$$
$$c_1 = -(1/2)v_0 + v_1 - (1/3)v_2 - (1/6)v_3 + 2v_4 + \beta v_4$$
$$c_2 = -v_0 + (1/2)v_1 + (1/2)v_2 - v_4$$

を得る．上記の場合，補完するときに 2,3,4,6 による逆元が必要となるが，ペアリング演算においては最終べき乗の処理により $\mathbb{F}_{p^k}$ の部分体の元の定数倍は単位元となるため (§4.3.1 参照のこと)，6 倍することで逆元処理を省略することが可能である．このようにして最適化した Toom-Cook 法を Toom-Cook-x 法と呼ぶ [13]. 教科書法，KO 法，Toom-Cook 法による 2,3 次拡大体における乗算・2 乗算の計算コストを以下に示す.

表 4.3: 2,3 次拡大体における乗算・2 乗算の計算コスト

	2 次拡大体		3 次拡大体	
	乗算	2 乗算	乗算	2 乗算
教科書法	$4M + 2A + B$	$M + 2S + 2A + B$	$9M + 6A + 2B$	$3M + 3S + 6A + 2B$
KO 法	$3M + 5A + B$	$3S + 4A + 2B$	$6M + 13A + 2B$	$6S + 13A + 2B$
Toom-Cook-3 法	-	-	$5M + 33A + 2B$	$5S + 33A + 2B$

○拡大体の構成

素体から 4 次以上拡大する拡大体の構成方法は素体から k 次の既約多項式を用いて直接 k 次拡大体を構成する方法と k の因数による逐次拡大，すなわち，KO 法や Toom-Cook 法が効率的に適用可能な 2,3 次拡大体を利用して構成する方法の 2 つがある．

前者の手法により構成された有限体の演算は一般に Toom-Cook 法が用いられる．しかし，前小節で述べたように拡大次数が大きい場合には効率的な多項式補完法の実装が難しい．ただし，4,6 次拡大体の場合に関しては Dahab ら [13] により示されている．また，前者では同型写像による楕円曲線上の点の導出の際に乗算処理が不要となり，さらにその導出された点は sparse な構造を有するため効率的なペアリング演算が可能である [5].

逐次拡大の構成方法は，例えば 6 次拡大体であれば，2 次拡大体を 3 次拡大する手法と 3 次拡大体を 2 次拡大する手法の 2 通りがある．[13] によれば，前者の方が乗算では 23 回の加算，2 乗算では 25 回の加算 (β 倍算は 4 回増加) だけ計算コストが小さい．しかし，後述するように部分体 $\mathbb{F}_{p^{k/2}}$ を利用して最終べき乗の高速化を実現するため，$k = 6$ であれば後者の方が効率的であるといえる．それ以外のケースであれば，前者を用いる方が望ましい．また，逐次拡大は理論的にペアリング演算コストを算出し易いという利点があり，埋め込み次数 $k = 2^i 3^j$ となる有限体 $\mathbb{F}_{p^k}$ の乗算コストは $M_k = 3^i 5^j$ として表現される．

4.3 演算アルゴリズム

4.3.1 BKLS アルゴリズム

Supersingular Curve における Reduced Tate ペアリングの高速化手法が Barreto ら [2] によっていくつか提案されており，それらを適用したアルゴリズムを BKLS アルゴリズムと呼ぶ.

【部分体の要素による乗算】

補題 4.1 Irrelevant Factors
埋め込み次数 k の因子を d とすると, ペアリングの値を変えずに非零な要素 $x \in \mathbb{F}_{q^d}$ を $f_{r,P}(Q)$ に乗じることが可能である.

証明 $q^k - 1 = (q^d - 1)\sum_{i=0}^{k/d-1} q^{id}$ と因数分解可能であり，$k > 1$ のとき $r \mid q^k - 1, r \nmid q^d - 1$ となるため，$r \mid \sum_{i=0}^{k/d-1} q^{id}$ である．すなわち，$(q^k - 1)/r$ は因子として $q^d - 1$ を必ず含んでいる．よって，$f_{r,P}(Q)$ は最終べき乗 $(q^k - 1)/r$ の処理を行うことにより，フェルマーの小定理より乗じた値 $x^{(q^k-1)/r} = 1$ となる． □

【点による因子の置換】

ペアリングの値は，引数として与える $Q \in E(\mathbb{F}_{q^k})$ とランダムに選択される $R \in E(\mathbb{F}_{q^k})$ から構成される因子 $D = (Q + R) - (R)$ を用いて計算されるが，因子 D を点 Q と置換しても正しく計算可能である.

定理 4.1
$P \in E(\mathbb{F}_q)[r], Q \in E(\mathbb{F}_{q^k})$ は線形独立な点とする．このとき，*(4.5)* が成立する.

$$e(P, Q) = f_{r,P}(Q)^{(q^k-1)} \tag{4.5}$$

証明 点 $R \in E(\mathbb{F}_q)$ は $R \notin \{\mathcal{O}, -P, Q, Q - P\}$，関数 $f'_{r,P}$ は $\mathrm{div}(f'_{r,P}) = r(P + R) - r(R) \sim \mathrm{div}(f_{r,P})$ を満足するものとする．このとき，$D = (Q) - (\mathcal{O})$ に対して $\mathrm{supp}(\mathrm{div}(f')) \cap \mathrm{supp}(D) = \emptyset$ を満足し，$e(P, Q) = f'_{r,P}((Q) - (\mathcal{O}))^{(q^k-1)/r}$ が成立する．関数 f' は無限遠点 $\mathcal{O}$ において零点も極も持たないため，$f'_{r,P}(Q)/f'_{r,P}(\mathcal{O})$ となる．また $P \in E(\mathbb{F}_q)$ より $f'_{r,P}$ は $\mathbb{F}_q$ 上で定義され，$f'_{r,P}(\mathcal{O}) \in \mathbb{F}_q^*$ である．さらに，埋め込み次数の定義から $(q^k - 1)/r$ は必ず $q - 1$ を因子として持つため，フェルマーの小定理より $f'_{r,P}(\mathcal{O})^{(q^k-1)/r} = 1$ となり，$e(P, Q) = f'_{r,P}(Q)$ が成立する.

$(P + R) - (R) \sim (P) - (\mathcal{O})$ より，関数 $f'_{r,P}$ はある有理関数 g を用いて $\mathrm{div}(f'_{r,P}) = r((P + R) - (R)) = r((P) - (\mathcal{O}) + \mathrm{div}(g))$, すなわち，$f'_{r,P} = f_{r,P}g^r$ と書ける．点 Q は $f_{r,P}, f'_{r,P}$ の零点でも極でもないので，$f'_{r,P}(Q)^{(q^k-1)/r} = f_{r,P}(Q)^{(q^k-1)/r} g(Q)^{(q^k-1)} = f_{r,P}(Q)^{(q^k-1)/r}$ が成立する． □

【分母消去】

Supersingular Curve であれば，$Q'_1 \in E(\mathbb{F}_q)$ に distortion map を適用させることにより，$Q_1 = \psi(Q'_1) \in E(\mathbb{F}_{q^k})$ を得る．Ordinary Curve であれば，twist E' 上の点 $Q'_2 \in E(\mathbb{F}_{q^e})$ から $Q_2 =$

$\psi(Q_2') \in E(\mathbb{F}_{q^k})$ を得る．ここで，$m = gcd(k,d), e = k/m$ である．$Q_i = (x_i, y_i)$ とすれば，§2.2.2, §4.1 より $x_i \in E(\mathbb{F}_{q^{k/2}})$ であることが確認できる．よって，以下の定理が成立する．

定理 4.2 Denominator Elimination
$Q = (x,y) \in E(\mathbb{F}_{q^k})$ において $x \in \mathbb{F}_{q^{k/2}}$ となるとき，Miller's Algorithm の 2 倍算・加算ステップに出現する分母の要素 g_{2V}, g_{V+P} は $e(P,Q)$ の値を変更することなく省略可能である．

証明 Miller's formula に出現する分母を $g_U(Q)$ とおく．g_U は点 $U = (u_x, u_y) \in E(\mathbb{F}_q)$ を通る垂線であり，$g_U(Q) = x - u_x$ で求められるが，$x \in \mathbb{F}_{q^{1/2}}$ より，$g_U(Q) \in \mathbb{F}_{q^{1/2}}$ である．補題 *4.1* より分母の値 $g_U(Q)$ は最終べき乗により単位元となり，省略可能である． □

【群位数の Hamming Weight】

Miller's Algorithm は部分群の位数 r に対する 2 進展開法に基づき，ペアリングの値を計算しているため，加算ステップの処理回数は r の Hamming Weight(2 進展開した値における 1 の総数) に依存する．ランダムに選択された r の平均的な Hamming Weight はビット長の半分程度となるが，部分群の位数として Solinas Prime [39] と呼ばれる $r = 2^\alpha \pm 2^\beta \pm 1$ を選択することにより，ペアリング演算コストを大幅に抑えることが可能である．

【最終べき乗の高速化】

Pairing-friendly field $\mathbb{F}_{q^k}$ における最終べき乗 $(q^k-1)/r$ を想定する．k 次の円分多項式 $\Phi_k(p)$ とすれば，$r \mid q^k - 1$ であるため，

$$f^{(q^k-1)/r} = (f^{(q^k-1)/\Phi_k(q)})^{(\Phi_k(q)/r)}$$

と変形できる．拡大体 $\mathbb{F}_q[X]/(X^k - \beta)$ において $X^{qi} \pmod{X^k - \beta}$ を事前計算しておけば，$(q^k-1)/\Phi_k(q)$ 乗の計算コストは数回の逆元と数回の乗算コストとなる．最終べき乗のコストは $(\Phi_k(q)/r)$ 乗のコストと同等，$(\Phi_k(q)/r)$ のビット長は $\frac{\varphi(k)}{k}\log_2(q^k) - \log_2(r)$ となる．

Supersingular Curve の distortion map ψ を利用して分母消去の手法を適用した BKLS アルゴリズムを以下に示す．Ordinary Curve の場合，$Q' \in E'(F_q)$ として, distortion map ではなく twist の同型写像 ϕ_d を用いる．

Algorithm 4.2: BKLS Algorithm

INPUT: $P, Q \in E(\mathbb{F}_p)[r]$
OUTPUT: $f \in \mathbb{F}_{p^k}$
$f \leftarrow 1, V \leftarrow P$ and $r = \sum_{i=0}^{l-1} r_i 2^i, r_i \in \{0,1\}$
for $j \leftarrow l-1$ **downto** 0 **do**
  $f \leftarrow f^2 \cdot g_{V,V}(\psi(Q))$ and $V \leftarrow 2V$
  if $r_j = 1$ **then**
    $f \leftarrow f \cdot g_{V,P}(\psi(Q))$ and $V \leftarrow V + P$
return f

【基底の変更】

$\mathbb{F}_{3^m}$ の有限体上で定義される Supersingular Curve $y^2 = x^3 - x + b$ 上の 3 倍算は，$P = (x, y), 3P = (x_3, y_3)$ とすれば,

$$x_3 = (x^3)^3 - b$$
$$y_3 = -(y^3)^3$$

で計算可能である．標数 3 の有限体における 3 乗算の計算コストは乗算と比較して小さく，効率よく 3 倍算を求めることができる．部分群の位数 r を 3 進展開し，3 倍算に対する Miller's fomula を求めることにより，Miller's Algorithm の計算が可能となる．また distortion map ψ により，分母消去の手法が適用可能である．

Algorithm 4.3: BKLS Algorithm for Supersingular curve on $\mathbb{F}_{3^m}$

INPUT: $P, Q \in E(\mathbb{F}_{3^m})[r]$
OUTPUT: $f \in \mathbb{F}_{3^{6m}}$
$f \leftarrow 1, V \leftarrow P$ and $r = \sum_{i=0}^{l-1} r_i 3^i, r_i \in \{-1, 0, 1\}$
for $j \leftarrow l - 1$ downto 0 do
    $f \leftarrow f^3 \cdot g_{V,-3V}(\psi(Q))$ and $V \leftarrow 3V$
    if $r_j = 1$ **then**
        $f \leftarrow f \cdot g_{V,P}(\psi(Q))$ and $V \leftarrow V + P$
    else if $r_j = -1$ **then**
        $f \leftarrow f \cdot g_{V,-P}(\psi(Q))$ and $V \leftarrow V - P$
return f

【ペアリング値の圧縮】

ペアリング値の圧縮とは安全性を低下させずにペアリングの値から数学的冗長性を除き，より小さいデータ量で値を表現する手法である．圧縮したペアリングの値を利用することにより，通信データ量が減少することに加え，素体，あるいは 2 次体における算術のみで演算アルゴリズムを構成可能である．代表的な手法として，標数 3 の Supersingular Curve において 6 次拡大体の元の trace を計算することによりペアリングの値を 1/3 に圧縮する Compressed Pairing [35] や Torus を利用する手法 [18], 素体上における埋め込み次数 12 の BN Curve を利用してペアリングを 1/6 に圧縮する手法 [5] などがある．

4.3.2 Duursma and Lee アルゴリズム

Duursma ら [15] は有限体 $\mathbb{F}_{p^m} (p \geq 3, \gcd(m, 2p) = 1)$ 上で定義された種数 $\frac{p-1}{2}$ の超特異代数曲線 $C : y^2 = x^p - x + d$ における Tate ペアリングの演算アルゴリズムを提案している．特に $p = 3$ のとき，標数 3 の有限体における埋め込み次数 $k = 6$ を持つ Supersingular Curve に対する演算アルゴリズムとなる．Reduced Tate ペアリングの性質より，群位数 r を基底 p に

おいて Hamming Weight が 2 となる値 $p^{mp}+1$ と置換，最終べき乗を Frobenius 写像と 1 回の逆元で計算可能な値 $(p^{2mp}-1)/(p^{pm}+1)=(p^{mp}-1)$ と置換する．この手法により，Miller's algorithm の処理及び最終べき乗が著しく簡略化され，さらに mp 回のループ回数を m 回への削減も実現している．

超楕円曲線 $y^2=x^p-x+d, d=\pm 1, p\equiv 3 \pmod 4$ を $C/\mathbb{F}_{p^m}$ とする．Duursma and Lee アルゴリズムでは, 点を通る直線 g を導出して Miller's formula から導出せず，ある因子を持つ関数より値を計算する．$P\in C(\mathbb{F}_{p^m})$ とすると，因子 $(p^{pm}+1)((P)-(\mathcal{O}))$ は主因子となる．すなわち，$\mathrm{div}(f_{p^{pm}+1,P})=(p^{pm}+1)(P)-((p^{pm}+1)P)-(p^{pm})(\mathcal{O})$ となる関数 $f_{p^{pm}+1,P}$ を求める．以降，x^{p^i} を $x^{(i)}$ と表記するものとする．

補題 4.2
$P\in(\alpha,\beta)\in C$ とする．関数

$$h_P=\beta^p y-(\alpha^p-x+d)^{(p+1)/2}$$

は因子 $\mathrm{div}(h_V)=p(V)+(-pV)-(p+1)(\mathcal{O})$ を持つ．ここで，$-pV=(\alpha^{(2)}+d^p+d,\beta^{(2)})$ である．

上記補題により，楕円曲線では関数 $g_V(x,y)=y_V^3y-(x_V^3-x+b)^2$ は因子 $\mathrm{div}(g_V)=3(V)+(-3V)-4(\mathcal{O})$ を持つことが分かる．よって，次の定理が成立する．

定理 4.3 (Duursma & Lee [15])
超楕円曲線 $C/\mathbb{F}_{p^m} y^2=x^p-x+d, d=\pm 1, p\equiv 3 \pmod 4$ において，埋め込み次数 $k=2p$, distortion map $\psi(x,y)=(\rho-x,\sigma y), \rho^p-\rho+2d=0, \sigma^2+1=0$ とする．$P=(\alpha,\beta), Q=(x,y)\in C(\mathbb{F}_{p^m})$ のとき，次式が成立する．

$$f_P(\psi(Q))=\prod_{i=1}^{m}(\beta^{(i)}y^{(m+1-i)}\hat{\sigma}-(\alpha^{(i)}+x^{(m+1-i)}-\rho+d)^{(p+1)/2}))$$

証明 補題 *4.2* より，

$$f_P(\psi(Q))=\prod_{i=1}^{pm}(h_{p^{i-1}P}(\psi(Q)))^{(pm-i)}$$

3 倍算の公式，$h_V, \psi(Q)$ として，

$$\begin{aligned}h_P(Q)&=\beta^p y-(\alpha^p-x+d)^{(p+1)/2}\\ p^{i-1}P&=(\alpha^{(2i-2)}+(i-1)2d,(-1)^{i-1}\beta^{(2i-2)})\\ \psi&=(\rho-x,\sigma y)\end{aligned}$$

を代入すると，

$$\prod_{i=1}^{pm}((-1)^{i-1}\beta^{(2i-1)}(\sigma y) - (\alpha^{(2i-1)} + (i-1)2d - (\rho - x) + d)^{(p+1)/2})^{(pm-i)}$$
$$= \prod_{i=1}^{pm}((-1)^{i-1}\beta^{(i-1)}\sigma^{(pm-i)}y^{(pm-i)}$$
$$- (\alpha^{(i-1)} + (i-1)2d - (\rho - (pm-i)2d - x^{(pm-i)}) + d)^{(p+1)/2})$$

また，$\alpha, \beta, x, y \in \mathbb{F}_{p^m}$ であり，i の値に関わらず，$(-1)^{i-1}\sigma^{(pm-i)} = \sigma$ が成立するので，

$$\prod_{i=1}^{m}(\beta^{(i-1)}y^{(m-i)}\sigma - (\alpha^{(i-1)} - \rho + x^{(m-i)} + d)^{(p+1)/2})^p$$
$$= \prod_{i=1}^{m}(\beta^{(i)}y^{(m+1-i)}\hat{\sigma} - (\alpha^{(i)} + x^{(m-i)} - \rho^p - d)^{(p+1)/2})$$

さらに，$-\rho^p - d = -\rho + d$ により，定理 *4.3* を得る． □

以下に標数 3 の有限体上で定義される Supersingular Curve における Tate ペアリングを求める Duursma and Lee アルゴリズムを示す．

Algorithm 4.4: $f_{3^{3m+1},P}(\psi(Q))$ on $E(\mathbb{F}_{3^m}) : y^2 = x^3 - x + d$

INPUT: $P = (\alpha, \beta), Q \in E(\mathbb{F}_{3^m})[r]$
OUTPUT: $f_{3^{3m+1},P}(\psi(Q)) \in \mathbb{F}_{3^{6m}}$
for $j \leftarrow 1$ **to** m **do**
　　$\alpha \leftarrow \alpha^3, \beta \leftarrow \beta^3$
　　$g \leftarrow \beta y\hat{\sigma} - (\alpha + x - \rho + d)^{(p+1)/2}$
　　$f \leftarrow f \cdot g$
　　$x \leftarrow x^{1/3}, y \leftarrow y^{1/3}$
end for
return f

4.3.3 Eta ペアリング

定義 4.4 Eta ペアリング
$T \in \mathbb{Z}$ に対して，Eta ペアリングを次のように定義する．

$$\eta_T(D, D') = f_{T,D}(\psi(D'))$$

Eta ペアリングは常に非退化性かつ双線形性を満足する写像ではないため，適切な T を選択する必要がある．定義 4.4 において，Duursma and Lee による手法では $T = q = 3^m$ と選

択しており，このときに定義される Eta ペアリングを η ペアリングと呼ぶ．すなわち，η ペアリングは標数 3 の Supersingular Curve における Duursma and Lee の手法を一般化したものであり，小標数の有限体上で定義される Supersingular Curve のとき定義可能である．さらに Barreto ら [1] は $N \in \mathbb{N}$ として $T = q - N$ と設定した Eta ペアリングを η_T ペアリングとして提案している．この手法をループ回数削減手法と呼び，η_T ペアリングは η ペアリングの約半分のループ回数で計算可能である．また，標数 2,3 の有限体における演算は非常に高速に実装可能なことから，現在，最も高速なペアリングであるといわれている．

C は有限体 $\mathbb{F}_q$ 上で定義される埋め込み次数 $k \geq 2$ の Supersingular Curve(超楕円曲線も含む) とする．Supersingular Curve であるため, Distortion map ψ を利用して分母消去が可能である．

定義 4.5 被約因子
C を種数 g の代数曲線とする．次の形の次数 *0* の因子

$$D = \sum_{P_j \in C} m_j(P_j) - \{\sum_{P_j \in C} m_j\}(\mathcal{O})$$

が $\sum_{P_j \in C} \leq g$ を満たす時，D を被約因子という．

$n \in \mathbb{N}$ とする．nD と合同な被約因子を D_n とし，ある $m \in \mathbb{N}$ に対して $nD - D_n - m(\mathcal{O})$ を因子に持つ関数を $f_{n,D}$ とする．本節では関数 $f_{n,D}$ の因子を $(f_{n,D})$ と表記することとする．楕円曲線の場合，$D = (P) - (\mathcal{O})$ なので，$D_n = (nP) - (\mathcal{O})$，$f_{n,D}$ は定理 3.2 により与えられる．代数曲線 C における Tate ペアリングは因子を引数として与える $\langle D, D' \rangle_N$ と定義される．

定理 4.4 Eta ペアリング有限体 $\mathbb{F}_q$ 上で定義される曲線 C は埋め込み次数 k 及び distortion map ψ を持つものとする．因子 D の位数は N を割り切るものとする．$M = (q^k - 1)/N$ と定義する．

1. 曲線 C の自己同型写像 γ に対して，$TD \equiv \gamma(D)$ が成立する．
2. すべての点 $Q \in C(\mathbb{F}_q)$ に対して，γ 及び ψ は $\gamma\psi^q(Q) = \psi(Q)$ を満足する．
3. ある $a \in \mathbb{N}$ 及び $L \in \mathbb{Z}$ に対して，$T^a + 1 = LN$ が成立する．
4. ある $c \in \mathbb{Z}$ に対して，$T = q + cN$ が成立する．

上記の *4* つの条件を満足する $T \in \mathbb{Z}$ に対して，Eta ペアリング η_T は Tate ペアリングと等式が成立する．

$$(\langle D, \psi(D) \rangle_N^M)^L = \eta_T(D, D')^{MaT^{a-1}}$$

$TD \equiv \gamma(D)$ より $D_{T^i} = \gamma^i(D)$ が成立するので，$D = \sum_{j=1}^{d}(P_j) - d(\mathcal{O})$ とすれば，$D_{T^i} = \sum_{j=1}^{d}(\gamma^i(P_j)) - d(\mathcal{O})$ となる．

補題 4.3
$TD \equiv \gamma(D)$ となる因子 D に対して，次式が成立する．

$$f_{T,D}(\psi(D'))^{TM} = f_{T,TD}(\psi(D'))^M$$

証明 定義より，$(f_{T,D}) = TD - D_T - (T-1)d(\mathcal{O}), (f_{T,D}^T) = T(f_{T,D}), (f_{T,TD}) = TD_T - D_{T^2} - (T-1)d(\mathcal{O})$ とする．自己同型写像 γ による因子の引き戻しにおいて，γ は次数 *1* の separable な写像であるから，

$$\gamma^*(\sum_P n_P(P)) = \sum_P \sum_{Q \in \gamma^{-1}(P)} n_P e_\gamma(Q)(Q) = \sum_P n_P(\gamma^{-1}(P))$$

が成立する．よって，

$$\begin{aligned}\gamma^*(f_{T,TD}) &= \gamma^*(TD_T - D_{T^2} - (T-1)d(\mathcal{O})) \\ &= TD - D_T - (T-1)d(\mathcal{O}) \\ &= (f_{T,D})\end{aligned}$$

また，$\gamma^*(f_{T,TD}) = (\gamma^* f_{T,TD}) = (f_{T,TD} \circ \gamma)$ であり，補題より，

$$f_{T,TD} \circ \gamma = f_{T,D}$$

を得る．$\psi(D')$ を代入し，両辺を TM 乗すると，

$$f_{T,TD}(\gamma(\psi(D')))^{TM} = f_{T,D}(\psi(D'))^{TM}$$

$T = q + cN, NM = (q^k - 1)$ より，NM 乗はすべて単位元となるため，

$$f_{T,D}(\psi(D'))^{TM} = f_{T,TD}(\gamma(\psi(D')))^{qM}$$

q 乗は Frobenius 写像と相当し，$f_{T,TD}, \gamma, D'$ は $\mathbb{F}_q$ 上で定義されていることから，

$$f_{T,D}(\psi(D'))^{TM} = f_{T,TD}(\gamma(\psi^q(D')))^M$$

さらに定理 *4.4* の条件 *3* $\gamma\psi^q = \psi$ より，

$$f_{T,D}(\psi(D'))^{TM} = f_{T,TD}(\psi(D'))^M$$

□

補題 4.4

$$(f_{T^a,D}) = (f_{T,D}^{T^{a-1}} f_{T,TD}^{T^{a-2}} \cdots f_{T,T^{a-1}D})$$

証明

$$\begin{aligned}(f_{T,D}^{T^{a-1}} f_{T,TD}^{T^{a-2}} \cdots f_{T,T^{a-1}D}) =& T^{a-1}(f_{T,D}) + T^{a-2}(f_{T,TD}) + \cdots + (f_{T,T^{a-1}D}) \\ =& T^{a-1}(TD - D_T - (T-1)d(\mathcal{O})) + T^{a-2}(TD_T - D_{T^2} \\ & - (T^2-1)d(\mathcal{O})) + \cdots + TD_{T^{a-1}} - D_{T^a} - (T^a-1)d(\mathcal{O}) \\ =& T^aD - D_{T^a} - (T^a-1)d(\mathcal{O}) \end{aligned}$$

□

補題 4.5

$$\mathrm{div}(f_{N,D}(\psi(D')) = (f_{T,D}(\psi(D')))^{MaT^{a-1}}$$

証明 Reduced Tate ペアリングの定義より，$f_{N,D}^L = f_{LN,D} = f_{T^a+1,D}$ となる．$T^a + 1 = LN$ より，$(T^a+1)D \equiv 0$ となり，$T^aD \equiv -D$ を得る．よって，

$$f_{T^a+1,D} = f_{T^a,D} \cdot v$$

ここで，v は $D, -D$ を通る垂線である．$\psi(D')$ を代入，M 乗する. ψ により分母消去可能なので，

$$f_{N,D}(\psi(D'))^{ML} = f_{T^a,D}(\psi(D'))^M \cdot v(\psi(D'))^M = f_{T^a,D}(\psi(D'))^M$$

補題 *4.4* より，

$$f_{T^a,D}(\psi(D'))^M = \prod_{j=0}^{a-1} f_{T,T^jD}(\psi(D'))^{MT^{a-1-j}}$$

補題 *4.3* における D に T^jD に代入すると，

$$f_{T,T^jD}(\psi(D'))^{MT^{a-1-j}} = f_{T,D}(\psi(D'))^{MT^{a-1}}$$

□

定理 4.4 より，標数 2,3 の有限体における η_T ペアリングの定義は次のようになる．

定義 4.6 $\mathbb{F}_{2^m}$ における η_T ペアリング
埋め込み次数 $k = 4$ を持つ有限体 $\mathbb{F}_{2^m}$ 上で定義された Supersingular Curve $E : y^2 + y = x^3 + x + b, (b \in \{0,1\}, m : odd)$ とする．位数 $N = \sharp E(F_{2^m}) = 2^m \pm 2^{(m+1)/2} + 1$, $\psi(x,y) = (x+s^2, y+sx+t), s^2 = s+1, t^2 = t+s$ で与えられ，$\phi(x,y) = (x+1, y+x), \gamma = \phi^m = [2^m]$ とする．$T = 2^m - N$ とおけば，$M = (2^{4m}-1)/N = (2^m \mp 2^{(m+1/2)} + 1)(2^{2m}-1)$ となる．$P, Q \in \mathbb{F}_{2^m}$ に対して，η_T ペアリングは Tate ペアリングとの等式により与えられる．

$$(\eta_T(P,Q)^M)^T = \langle P, \psi(Q)\rangle_N^M$$

Algorithm 4.5: $\eta_T(P,Q)$ on $E(\mathbb{F}_{2^m}) : y^2 + y = x^3 + x + b, m \equiv 3 \pmod 8$

INPUT: $P, Q \in E(\mathbb{F}_{2^m})[r]$
OUTPUT: $\eta_T(P,Q) \in \mathbb{F}_{(2^m)^k}$
$u \leftarrow x_P + 1$
$f \leftarrow u \cdot (x_P + x_Q + 1) + y_P + y_Q + b + 1 + (u + x_Q)s + t$
for $i \leftarrow 1$ **to** $(m+1)/2$ **do**
    $u \leftarrow x_P, x_P \leftarrow \sqrt{x_P}, y_P \leftarrow \sqrt{y_P}$
    $g \leftarrow u \cdot (x_P + x_Q) + y_P + y_Q + x_P + (u + x_Q)s + t$
    $f \leftarrow f \cdot g$
    $x_Q \leftarrow x_Q^2, y_Q \leftarrow y_Q^2$
return $f^{(2^{2m}-1)(2^m - 2^{(m+1)/2}+1)}$

定義 4.7 $\mathbb{F}_{3^m}$ における η_T ペアリング
埋め込み次数 $k = 6$ を持つ有限体 $\mathbb{F}_{3^m}$ 上で定義された Supersingular Curve $E : y^2 = x^3 - x + b, (b = \pm 1, \gcd(m, 6) = 1)$ とする．位数 $N = \sharp E(F_{3^m}) = 3^m \pm 3^{(m+1)/2} + 1$, $\psi(x,y) = (\rho - x, \sigma y), \sigma^2 = -1, \rho^3 = \rho + b$ で与えられ，$\phi(x,y) = (x - b, -y), \gamma = \phi^m = [3^m]$ とする．$T = 3^m - N$ とおけば，$M = (3^{6m} - 1)/N = (3^{3m} - 1)(3^{3m} + 1)(3^m \mp 3^{(m+1/2)} + 1)$ となる．$P, Q \in \mathbb{F}_{3^m}$ に対して，η_T ペアリングは次式により与えられる．

$$(\eta_T(P,Q)^M)^{3T^2} = \langle P, \psi(Q) \rangle_N^M$$

Algorithm 4.6: $\eta_T(P,Q)$ on $E(\mathbb{F}_{3^m}) : y^2 = x^3 - x + b, m \equiv 1 \pmod{12}$

INPUT: $P, Q \in E(\mathbb{F}_{3^m})[r]$
OUTPUT: $\eta_T(P,Q) \in \mathbb{F}_{(3^m)^k}$
$P_0 \leftarrow -P$
if $T < 0$ **then** $T \leftarrow -T, P \leftarrow -P$
let $P = (x_P, y_P), Q = (x_Q, y_Q)$
$l \leftarrow$ the line between $3^{(m+1)/2}$ and P_0
$f \leftarrow l(\psi(Q))$
for $j \leftarrow 1$ **to** $(m-1)/2$ **do**
    $u \leftarrow x_P + x_Q - b$
    $g \leftarrow \sigma y_P y_Q - u^2 - \rho u - \rho^2$
    $f \leftarrow f \cdot g$
    $x_P \leftarrow x_P^{1/3}, y_P \leftarrow y_P^{1/3}$
    $x_Q \leftarrow x_Q^3, y_Q \leftarrow y_Q^3$
return $f^{(3^{3m}-1)(3^m+1)(3^m - b3^{(m+1)/2}+1)}$

第5章　提案手法

Suprisingular Curve における η_T ペアリングを Oridinary Curve へと一般化・拡張した Ate ペアリングおよび twisted Ate ペアリングについて詳述する．次に η_T ペアリングのループ削減手法のアイデアを適用した Optimized Ate ペアリングおよび Optimized twisted Ate ペアリングを提案し，双線形性・非退化性を満足するペアリングであることを証明する．

5.1　Ate ペアリング

本章を通じて加法群 $\mathbb{G}_1 = E(F_q)[r]$ 及び $\mathbb{G}_2 = E(F_{q^k})[r]$ を次のように表現する．

$$\mathbb{G}_1 = E[r] \cap \mathrm{Ker}(\pi_q - 1)$$
$$\mathbb{G}_2 = E[r] \cap \mathrm{Ker}(\pi_q - q)$$

前章までに紹介したように，Tate ペアリングに与える入力は $P \in E(F_q)[r], Q \in E(F_{q^k})$ の場合が一般的であり，これは上記の表現を用いて $\mathbb{G}_1 \times \mathbb{G}_2$ における Tate ペアリングと表現される．Duursma and Lee によるペアリングを一般化した η ペアリング，η_T ペアリングは $\mathbb{G}_1 \times \mathbb{G}_2$ における Tate ペアリングに分類される．本節で紹介する Ate ペアリングは，$\mathbb{G}_1$ と $\mathbb{G}_2$ を入れ替えた $\mathbb{G}_2 \times \mathbb{G}_1$ における Tate ペアリングである．

有限体 $\mathbb{F}_q$ 上で定義された Ordinary Curve を E とし，部分群の位数 r は $r \geq 5$ を満足する大きな素数であるものとする．$\sharp E(\mathbb{F}_q) = q + 1 - t$ となる t は Frobenius の trace である．$P \in \mathbb{G}_1, Q \in \mathbb{G}_2$ とする．μ_r は単位元の r 乗根, $r|q^k - 1$ を満足する最小の整数を埋め込み次数 k とする．Ate ペアリングの定義は次の定理によって与えられる．

定理 5.1 Ate ペアリング
$T = t-1$ とおく．$N = \gcd(T^k - 1, q^k - 1), T^k - 1 = LN$ と定義する．$c_T = \sum_{i=0}^{k-1} T^{k-1-i} q^i \equiv kq^{k-1} \bmod r$ とおくと，

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

は $\mathbb{G}_2 \times \mathbb{G}_1 \to \mu_r$ となる双線形写像である．$f_{T,Q}(P)$ を Ate ペアリングと呼ぶ．Reduced Tate ペアリング τ に対して，

$$\tau(Q, P)^L = a_T(Q, P)$$

が成立するため，$r \nmid L$ のとき a_T は非退化性を満足する．

一般に trace t のサイズは定義体 $\mathbb{F}_q$ の位数 q のサイズの約半分となるため，$q \sim r$ のとき，Ate ペアリングは Tate ペアリングの約半分のループ長で計算可能である．2 つの補題を与え，定理 5.1 の証明を行う．

補題 5.1

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

証明 Reduced Tate ペアリングの定義より，$r \mid N \mid q^k - 1$ を満足する N に対して，

$$\tau(Q,P) = f_{r,Q}(P)^{(q^k-1)/r} = f_{N,Q}(P)^{(q^k-1)/N}$$

が成立する．t は $\sharp E(F_q) = hr = q+1-t$ を満足するので，$q \equiv t-1 \bmod r$ となり，両辺を k 乗して $q^k \equiv (t-1)^k \bmod r$，埋め込み次数の定義 $r|q^k-1$ より，$(t-1)^k \equiv 1 \bmod r$ を得る．

$$\begin{aligned}\tau(Q,P)^L &= f_{N,Q}(P)^{L(q^k-1)/N} \\ &= f_{LN,Q}(P)^{(q^k-1)/N} \\ &= f_{T^k-1,Q}(P)^{(q^k-1)/N}\end{aligned}$$

ここで $T^k - 1 = LN$ である．また，$Q \in E[r]$ であることから，因子 $\mathrm{div}(f_{T^k-1,Q})$ に関して，

$$\begin{aligned}\mathrm{div}(f_{T^k-1,Q}) &= (T^k-1)(Q) - ((T^k-1)Q) - (T^k-2)(\mathcal{O}) \\ &= (T^k)(Q) - (Q) - (T^k-1)(\mathcal{O}) \\ &= (T^k)(Q) - (T^kQ) - (T^k-1)(\mathcal{O}) = \mathrm{div}(f_{T^k,Q})\end{aligned}$$

となるため，補題より，$f_{T^k-1,Q} = f_{T^k,Q}$ である． □

また，補題 4.4 により，以下の等式 (5.1) を得る．

$$f_{T^k,Q} = f_{T,Q}^{T^{k-1}} f_{T,TQ}^{T^{k-2}} \cdots f_{T,T^{k-1}Q} \tag{5.1}$$

$Q \in \mathbb{G}_2$ より，$\pi_q(Q) = qQ = (t-1)Q = TQ$ となり，$\pi_q^i(Q) = T^iQ$ を得る．以下の補題によって f_{T,π_q^i} と $f_{T,Q}$ を関連付けることにより，上式の右辺は $f_{T,Q}$ の項により表現することが可能になる．

補題 5.2
すべての点 $Q \in \mathbb{G}_2$ に対して，

$$f_{T,\pi_q^i(Q)} = f_{T,Q}^{\sigma^i}$$

が成立する．ここで σ は代数的閉体 $\overline{\mathbb{F}_q}$ における q 乗 Frobenius 自己同型写像である．

証明 定義より，$\mathrm{div}(f_{T,\pi_q^i(Q)}) = T(\pi_q^i(Q)) - (\pi_q^{i+1}(Q)) - (T-1)(\mathcal{O})$ である．π_q に関する因子 $\mathrm{div}(f_{T,\pi_q^i(Q)})$ の引き戻しを考えると，

$$\begin{aligned}(\pi_q^i)^*\mathrm{div}(f_{T,\pi_q^i(Q)}) =&(\pi_q^i)^*\{T(\pi_q^i(Q)) - (\pi_q^{i+1}(Q)) - (T-1)(\mathcal{O})\}\\ =&T(\pi_q^i)^*(\pi_q^i(Q)) - (\pi_q^i)^*(\pi_q^{i+1}(Q)) - (T-1)(\pi_q^i)^*(\mathcal{O})\end{aligned}$$

となる．それぞれの項に関して π_q は次数 q の inseparable な自己準同型写像であることから，

$$T(\pi_q^i)^*(\pi_q^i(Q)) = T(\sum_{P\in(\pi_q^i)^{-1}(\pi_q^i(Q))} e_{\pi_q^i}(P)(P)) = T\deg(\pi_q^i)(Q) = q^iT(Q)$$

$$(\pi_q^i)^*(\pi_q^{i+1}(Q)) = (\sum_{P\in(\pi_q^i)^{-1}(\pi_q^{i+1}(Q))} e_{\pi_q^i}(P)(P)) = \deg(\pi_q^i)(\pi_q(Q)) = q^i(\pi_q(Q))$$

$$(T-1)(\pi_q^i)^*(\mathcal{O}) = (T-1)(\sum_{P\in(\pi_q^i)^{-1}(\mathcal{O})} e_{\pi_q^i}(P)(P)) = (T-1)\deg(\pi_q^i)(\mathcal{O}) = q^i(T-1)(\mathcal{O})$$

すなわち，

$$\begin{aligned}(\pi_q^i)^*\mathrm{div}(f_{T,\pi_q^i(Q)}) =&q^iT(Q) - q^i(\pi_q(Q)) - q^i(T-1)(\mathcal{O})\\ =&\mathrm{div}(f_{T,Q}^{q^i})\end{aligned}$$

さらに $(\pi_q^i)^*\mathrm{div}(f_{T,\pi_q^i(Q)}) = \mathrm{div}(f_{T,\pi_q^i(Q)}\circ\pi_q^i)$ なので，

$$f_{T,\pi_q^i(Q)}\circ\pi_q^i = f_{T,Q}^{q^i}$$

よって，$f_{T,Q}^{q^i} = f_{T,Q}^{\sigma^i}\circ\pi_q^i$ より，$f_{T,\pi_q^i(Q)} = f_{T,Q}^{\sigma^i}$ である． □

定理 5.1 の証明 $P\in\mathrm{Ker}(\pi_q - 1)$ なので，補題 *5.2* より，

$$f_{T,\pi_q^i(Q)}(P) = f_{T,Q}^{\sigma}(P) = (f_{T,Q}(P))^{q^i}$$

となり，(5.1) より，

$$f_{T^k,Q}(P) = f_{T,Q}(P)^{\sum_{i=0}^{k-1}T^{k-1-i}q^i}$$

を得る．上式を補題 *5.1* に代入して，

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

ここで $c_T = \sum_{i=0}^{k-1}T^{k-1-i}q^i \equiv kq^{k-1} \bmod r$ である．Reduced Tate ペアリング $\tau(Q,P)$ による等式で表現可能なことから，$f_{T,Q}(P)$ は双線形写像である．また，$r\nmid L$ のとき，$\tau(Q,P)$ 自身が単位元にならないため，非退化性を満足する． □

非退化性を満足する条件について補足説明する．一般に $t\sim\sqrt{q}$ であり，ほぼ全ての曲線は $t=0,2$ にならないため，k が偶数のとき，$T^k-1\neq 0$ を満足する．Tate ペアリングを用いる際には $r^2\nmid q^k-1$ という条件を仮定しているため，$q\equiv t-1 \bmod r$ より，$r^2\nmid T^k-1$ である．よって，$r\mid N$ なので，$r\nmid L$ が成立する．

5.2 Twisted Ate ペアリング

楕円曲線 E は d 次の twist を持つものとして仮定し，$m = \gcd(k, d), e = k/m$ とする．Tate ペアリングを定義する際に $q^k - 1$ は r で割れるが r^2 で割れないと仮定する．ここで $\sharp E(\mathbb{F}_{q^e})$ が r^2 で割れると仮定すると，ペアリングの定義から $r^2 \mid \sharp E(\mathbb{F}_{q^k})$ となる．ラグランジェの定理より位数 r^2 となる元 $R \in E(\mathbb{F}_{q^k})$ が存在する．$P \in E(\mathbb{F}_q)[r]$ とすると，ペアリングの準同型性より $\tau(P, R)$ は単位元の r^2 乗根となる．すなわち，位数 r^2 の元が $\mathbb{F}_{q^k}^*$ の中に存在するので，$r^2 \mid q^k - 1$ とならなければならないが，これは仮定に反する．よって，$E(\mathbb{F}_{q^e})$ の位数は r では割れるが r^2 では割れない．さらに，twist の構造定理より，$r \geq 7$ であれば，$r \mid \sharp E'(\mathbb{F}_{q^e})$ を満足する有限体 $\mathbb{F}_{q^e}$ 上で定義された楕円曲線 E の m 次の twist E' が唯一に存在する．位数が r で割り切れる群は 1 つしか存在しないので，群位数を調べることにより，唯一の m 次の twist を得ることができる．また，§2.2.2 より，

$$E'(\mathbb{F}_q) \simeq \mathrm{Ker}([\zeta_m]\pi_q^e - 1)$$

となる単位元の原始 m 乗根 ζ_m が唯一に存在する．$\mathrm{Ker}([\zeta_m]\pi_q^e - 1)$ は π_q^k において不変である．すなわち，$P \in \mathrm{Ker}([\zeta_m]\pi_q^e - 1)$ に対して，

$$\begin{aligned}[\zeta_m]\pi_q^e(P) = P \Leftrightarrow & [\zeta_m]^2\pi_q^{2e}(P) = [\zeta_m]\pi_q^e(P) = P \\ & \cdots \\ \Leftrightarrow & [\zeta_m]^m\pi_q^k(P) = P\end{aligned}$$

また，$\mathbb{G}_2 = E[r] \cap \mathrm{Ker}(\pi_q - q)$ の Kernel による群も同様にすると，π_q^k 上で不変であることが示せるので，$\mathrm{Ker}([\zeta_m]\pi_q^e - 1) \simeq \mathrm{Ker}(\pi_q - q)$ となり，$\mathbb{G}_2 = E[r] \cap \mathrm{Ker}([\zeta_m]\pi_q^e - 1)$ の表現が可能となる。

定理 5.2 Twisted Ate ペアリング
楕円曲線 E は d 次の twist を持つものとする．$m = \gcd(k, d), e = k/m, T^e = (t-1)^e$ とおく．$N = \gcd(T^k - 1, q^k - 1), T^k - 1 = LN$ と定義する．$c_{T^e} = \sum_{i=0}^{k-1} T^{e(m-1-i)}q^{ei} \equiv mq^{e(m-1)} \bmod r$ とおくと，

$$a_{T^e}^{\mathrm{twist}} : (P, Q) \mapsto f_{T^e,P}(Q)^{c_{T^e}(q^k-1)/N}$$

は $\mathbb{G}_1 \times \mathbb{G}_2 \to \mu_r$ となる双線形写像である．$f_{T^e,P}(Q)$ を twisted Ate ペアリングと呼ぶ．Reduced Tate ペアリング τ に対して，

$$\tau(P, Q)^L = a_{T^e}^{\mathrm{twist}}(P, Q)$$

が成立するため，$r \nmid L$ のとき a_T は非退化性を満足する．

$\mid T^e \mid \leq r$ のとき，twisted Ate ペアリング $f_{T^e,P}(Q)$ は Tate ペアリング $f_{r,P}$ よりも効率よく計算可能である．定理 5.2 の証明に関して，Ate ペアリングにおける補題 5.1 と (5.1) は同様に成り立つ．$[\zeta_m]$ は曲線の自己同型写像であり，以下の補題が成立する．

補題 5.3
すべての点 $P \in \mathbb{G}_1$ に対して,

$$f_{T^e,[\zeta_m]P} \circ [\zeta_m] = f_{T^e,P}$$

が成立する.

証明 $[\zeta_m]$ は曲線の自己同型写像であり，自明な kernel を持つことから，次数 *1* の separable な写像である．補題 *5.2* と同様に $[\zeta_m]$ による因子の引き戻しを考えると,

$$\begin{aligned}\mathrm{div}(f_{T^e,[\zeta_m]P} \circ [\zeta_m]) &= [\zeta_m]^* \mathrm{div}(f_{T^e,[\zeta_m]P}) \\ &= [\zeta_m]^* \{T^e([\zeta_m]P) - (T^e[\zeta_m]P) - (T^e - 1)(\mathcal{O})\} \\ &= T^e(P) - (T^e P) - (T^e - 1)(\mathcal{O}) \\ &= \mathrm{div}(f_{T^e,P})\end{aligned}$$ □

$\mathbb{F}_{T^e,P}$ は $\mathbb{F}_q$ 上で定義されているため，e 回の Frobenuis 写像 π_q^e と e 回の q 乗 Frobenius 写像は同じ操作となり，$f_{T^e,[\zeta_m]P} \circ [\zeta_m] \circ \pi_q^e = f_{T^e,P}^{q^e}$ を得る．$Q \in \mathbb{G}_2$ より，代入すると $f_{T^e,T^eP}(Q) = f_{T^e,[\zeta_m]P}(Q) = f_{T^e,P}(Q)^{q^e}$ となる．よって，定理 5.2 が証明される.

位数 r の $E'(\mathbb{F}_q)$ における部分群 $\mathbb{G}_2'$ に対して twist の同型写像 $\phi_d : E'(\mathbb{F}_{q^e}) \to E(\mathbb{F}_{q^k})$ を利用し，$\mathbb{G}_2$ を表現可能である．すなわち，$Q \in \mathbb{G}_2'$ に対して ϕ_d を適用し，$\phi_d(Q) \in \mathbb{G}_2$ を得る．これは同型写像 ϕ_d が Supersingular Curve における distortion map に相当しており，次のように Modified Ate ペアリング, Modified twisted Ate ペアリングを定義可能である.

定義 5.1 Modified Ate ペアリング, Modified twisted Ate ペアリング
$P \in \mathbb{G}_1, Q' \in \mathbb{G}_2'$ とすると, Modified Ate ペアリング $\hat{a}_T$, Modified twisted Ate ペアリング $\hat{a}_T^{\mathrm{twist}}$ は次の式で与えられる.

$$\hat{a}_T(\psi(Q), P) = a_T(Q, P) \qquad \hat{a}_T^{\mathrm{twist}}(P, \psi(Q)) = a_T^{\mathrm{twist}}(P, Q)$$

5.3 Optimized Ate & optimized twisted Ate ペアリング

前述したように Ate ペアリング，Twisted Ate ペアリングは常に Tate ペアリングより高速ではない．$\mathbb{G}_2 \times \mathbb{G}_1$ 型の Ate ペアリングでは演算アルゴリズム中で $f_{T,\phi(Q)} \in F_{q^e}(E)$ を導出する必要があり，$\mathbb{G}_1 \times \mathbb{G}_2$ 型のペアリングよりもループ 1 回に要するコストが大きい．ループ回数は常に T で抑えられるが，$t \sim r$ のとき Tate ペアリングよりも計算コストが大きくなることが分かる．一方，Twisted Ate ペアリングのループ 1 回の処理は Tate ペアリングと同一であるため，計算コストは完全にループ回数に依存する．よって，$(t-1)^e > r$ のとき，Twisted Ate ペアリングは Tate ペアリングよりも計算コストが大きくなる.

本節では，η_T ペアリングのループ回数削減手法を Ate，Twisted Ate ペアリングに適用した Optimzied Ate ペアリング及び Optimized twisted Ate ペアリングを提案する．Ate，twisted Ate

ペアリングに対する Optimzied Ate，Optimized twisted Ate ペアリングの関係は Supersingular Curve における η ペアリングに対する η_T ペアリングの関係に対応する．具体的には $T = q, T^e = q^e$ に対して，部分群の位数 r を法として $S = q \bmod r, S_e = q^e \bmod r$ と設定する．

有限体 $\mathbb{F}_q$ 上で定義される楕円曲線 E，$P \in \mathbb{G}_1, Q \in \mathbb{G}_2$ として，Optimized Ate ペアリング及び Optimized twisted Ate ペアリングに関する定理を以下に示す．

定理 5.3 Optimized Ate ペアリング，Optimized twisted Ate ペアリング
整数 $S \equiv q \bmod r$，部分群の位数 $r \geq 5$ とする．$N = \gcd(S^k - 1, q^k - 1), L = \gcd(S^k - 1, q^k - 1)/N, c_S = \sum_{i=0}^{k-1} S^{k-1-i} q^i \bmod r$ とおく．

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

は $\mathbb{G}_2 \times \mathbb{G}_1 \to \mu_r$ となる双線形写像である．$k \mid \sharp \mathrm{Aut}(E)$ ならば，

$$a_S^{\mathrm{twist}} : (P, Q) \mapsto f_{S,P}(Q)^{c_S(q^k-1)/N}$$

もまた，$\mathbb{G}_1 \times \mathbb{G}_2 \to \mu_r$ となる双線形写像である．$r \nmid L$ のとき，a_S および a_S^{twist} は非退化性を満足する．

$a_S, a_S^{\mathrm{twist}}$ は S を適切に選択することにより，Ate ペアリング a_T，twisted Ate ペアリング a_T^{twist} よりも効率よく計算可能である．以降，Ate，twisted Ate ペアリングにおける同型写像 ψ を同一記号で記述し，より一般的な方法により Optimized Ate ペアリング, Optimized Twisted Ate ペアリングの証明を行う．

定理 5.3 の証明 同型写像 ψ は Ate ペアリングでは $\psi = \pi_q$, twisted Ate ペアリングでは $\psi = \gamma\pi_q$ とする．ここで，$\gamma \in \mathrm{Aut}(E)$ は位数 k の自己同型写像であり，$(\gamma\pi_q)(Q) = Q$,$(\gamma\pi_q)(P) = qP$ を満足する．Ate ペアリングでは P, Q を入れ替えることにより，$\psi(P) = P$, $\psi(Q) = qQ = SQ$ が成立する．補題 *5.1* より，

$$e(Q, P) = f_{r,Q}(P)^{(q^k-1)r} = f_{N,Q}(P)^{(q^k-1)/N}$$

を得る．また，

$$\begin{aligned} e(Q, P)^L &= f_{N,Q}(P)^{L(q^k-1)/N} = f_{LN,Q}(P)^{(q^k-1)/N} \\ &= f_{S^k-1,Q}(P)^{(q^k-1)/N} \\ &= f_{S^k,Q}(P)^{(q^k-1)/N} \end{aligned} \tag{5.2}$$

が成立する．補題 *4.4* より，

$$f_{S^k,Q} = f_{S,Q}^{S^{k-1}} f_{S,SQ}^{S^{k-2}} \cdots f_{S,S^{k-1}Q} \tag{5.3}$$

ψ は次数 q の inseparable な同型写像であるため, 補題 *5.3* より次式を得る．

$$f_{S,\psi^i(Q)} \circ \psi^i = f_{S,Q}^{q^i}. \tag{5.4}$$

$\psi^i(Q) = S^iQ, \psi^i(P) = P$ なので，(5.3) および (5.4) を統合して，

$$f_{S^k,Q}(P) = f_{S,Q}(P)^{\sum_{i=0}^{k-1} S^{k-1-i}q^i} \tag{5.5}$$

(5.5) を (5.2) に代入して，

$$e(Q,P)^L = f_{S,Q}(P)^{c_S(q^k-1)/N} \tag{5.6}$$

(5.6) より，a_S 及び a_S^{twist} は双線形写像であり，$r \nmid L$ のとき非退化性を満足する． □

$k \nmid \sharp\mathrm{Aut}(E)$ のとき，twisted Ate ペアリングの証明は有限体 F_{q^e} 上で定義された楕円曲線 E_1 を用いて行う．ここで $e = k/\gcd(k, \sharp\mathrm{Aut}(E))$ である．E_1 の部分群の位数 r に対する埋め込み次数は $m = k/e$ であり，$m \mid \sharp\mathrm{Aut}(E)$ となる．よって，定理 5.3 において E_1 における twisted Ate ペアリングに対して q を q^e, k を m, $S \equiv q^e \bmod r$ とおくことにより，Optimized twisted Ate ペアリングが定義可能となる．

第6章　実装方式

ソフトウェア実装におけるプログラム構成について述べる．ペアリングのパラメータ設定において安全性の基準となる MOV security について簡単に説明し，実際に生成した楕円曲線及びその twist のパラメータを示す．ペアリング演算としてアルゴリズム中の楕円曲線における演算及び Miller Operation の詳細について述べる．

6.1　プログラム構成

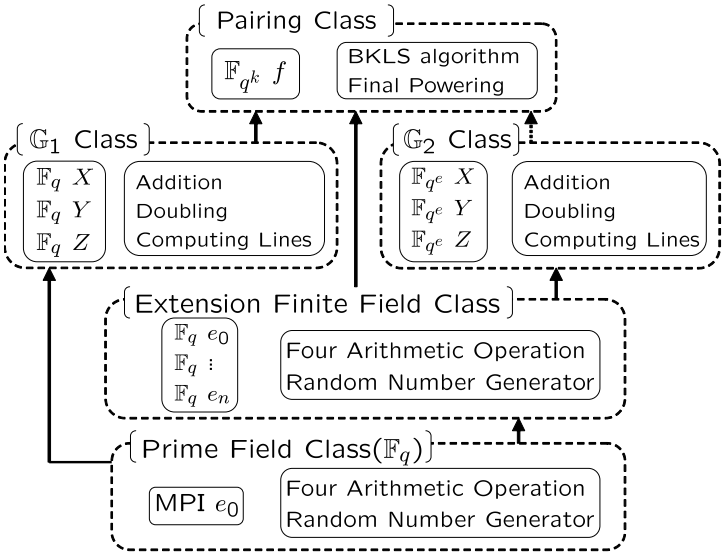

図 6.1: プログラム構成

ソフトウェア実装におけるプログラム構成を図 6.1 に示す．有限体クラス (Prime Field Class, Extension Field Class)，楕円曲線クラス ($\mathbb{G}_1$ Class, $\mathbb{G}_2$ Class), ペアリングクラス (Pairing Class) の 3 つのクラスにより構成される．有限体クラスは多倍長データ (multiple-precision integer) を持つ素体 (Prime field) と素体を基礎体として逐次拡大した拡大体 $\mathbb{F}_{q^2}, \mathbb{F}_{q^3}, \mathbb{F}_{q^4}, \mathbb{F}_{q^6}, \mathbb{F}_{q^8}, \mathbb{F}_{q^{12}}$ により構成される．詳細は §6.3.1 で説明する．楕円曲線クラスでは楕円曲線 E における $\mathbb{F}_q$-有理点群を $\mathbb{G}_1$, twist E' における $\mathbb{F}_{q^e}$-有理点群を $\mathbb{G}_2$ と設定する．ペアリングクラスでは楕円曲線クラスにおける加算・2 倍算及び直線式の計算モジュールを用いて，BKLS アルゴリズムを構成し，有限体クラスのべき乗剰余計算により Final Powering を行う．

6.2 パラメータ設定

6.2.1 安全性基準

ペアリングのパラメータ設定に関して，MOV security [31] を次のように定義する．

定義 6.1 MOV security
埋め込み次数 k を持つ有限体 $\mathbb{F}_q$ 上で定義される楕円曲線 E において，ペアリングの値域となる $\mathbb{F}^*_{q^k}$ のサイズを MOV security と呼ぶ．$\mathrm{MOVsecurity} = k \log_2 q$ となる．

1024 ビットの素因数分解問題 (IFP) と 1024 ビットの有限体における離散対数問題 (DLP) の困難性は同等であると言われており，現在の安全性水準では MOV security=1024 である．一方，楕円曲線上の離散対数問題 (ECDLP) は準指数時間解読アルゴリズムが存在せず，DLP に比べ短いビット長で済む．§3.1 で述べたように，ペアリングの安全性は DLP と ECDLP に帰着するため，どちらの問題も同等の困難性を有するようにパラメータを設定する必要がある．以下に DLP(MOV security) 及び ECDLP(Group order) の等価安全性と埋め込み次数・群位数・有限体の位数の関係について示す．楕円曲線の生成においては，埋め込み次数 k により $\rho = \log q / \log r$ の値が変動するため，常に下表のパラメータを満足する楕円曲線生成は可能ではない．

表 6.1: MOV secuirty/Group order に対する埋め込み次数と定義体のサイズの関係

	MOV security / Group order	k					
		2	4	6	8	10	12
$\log_2 q$	1024 / 160	512	256	171	-	-	-
	2048 / 224	1024	512	342	256	-	-
	3072 / 256	1536	768	512	384	308	256

6.2.2 楕円曲線

§4.1 で述べたように，$D = 1, 2, 3$ となる CM 等式 $4q - t^2 = DV^2$ を満足するパラメータ q, t により，CM アルゴリズムを適用することなく，曲線を生成することが可能である．しかし，前小節でも示したように埋め込み次数 k によって生成可能な曲線の $\rho = \log q / \log r$ の値は変動する．以下に，埋め込み次数 $k = 2^i 3^j, (i > 1, j \geqq 1)$ に対する $\rho = \log q / \log r$ の最小値を示す [16].

また，Ordinary Curve における Modified ペアリングは同型写像 ϕ_d を持つ d 次の twist E' を持つ楕円曲線 E を前提としている．d 次の twist の定義体の拡大次数 $e = k/m$ は $m = \gcd(k, d)$ より与えられるため，e が最小となるためには $d|k$ を満足する必要がある．$D = 1$ のとき $d = 4$, $D = 3$ のとき,$d = 6$ となる楕円曲線を生成可能なことから，$k = 4, 8$ のとき $D = 1, k = 6, 12$

表 6.2: 埋め込み次数 k に対する生成可能な曲線の ρ

	small D		variable D	
k	ρ	D	ρ	D
2	any^*	1,3	any^*	$3 \bmod 4$
4	1.500	3	1.000	some
	2.000	1	-	-
6	1.250	1	1.000	some
	2.000	3	-	-
8	1.250	3	-	-
	1.500	1	-	-
12	1.000	3	1.750	$2 \bmod 8$

$^* \cdots$ Supersingular Curve

のとき $D = 3$ となる楕円曲線が望まれる．twist の定義より，$p \equiv 1 \bmod d$ を満足する p が必要となる．これらは多項式表現されたパラメータが示されており，Algorithm 4.1 を利用して曲線生成が可能である．以下に，t, r, p の多項式パラメータとともに，Ate ペアリング，twisted Ate ペアリング，Optimized Ate ペアリング，Optimized twisted Ate ペアリングにおける T, T^e, S, S_e を示す．また，実際に曲線生成した楕円曲線のパラメータを示す [14, 5, 16]．以下の曲線のベースポイントはすべて $G = (1, 2)$ である．

$\mathbf{k = 4}$

$t = 4z^2 + 2z + 2$

$r = 4z^2 + 1$

$p = 8z^4 + 6z^2 + 2z + 1$

$DV^2 = 4z^2(2z^2 - 1)^2$

$\mathbf{k = 6}$

$t = 3z^2 + 1$

$r = 3z^2 - 3z + 1$

$p = 9z^4 - 9z^3 + 9z^2 - 3z + 1$

$DV^2 = 3(3z^2 - 2z + 1)^2$

$T = 3z^2$

$S = S_e = 3z - 1$

$E : y^2 = x^3 + 3$

$t = 110671499948136457898767062435634000244637879784610750455870242188027714479693$ (253-bit)

$r = 110671499948136457898767062435634000244061672790688939946147248795381456622967$ (256-bit)

$p = 122481809007703680033766248999768979446389676441464146308771057600294241077436877699849883979387314348641400328517665670374427869969661814657500069933888 23$ (510-bit)

k = 8

$t = -9z^3 - 3z^2 - 2z$

$r = 9z^4 + 12z^3 + 8z^2 + 4z + 1$

$p = \frac{1}{4}(81z^6 + 54z^5 + 45z^4 + 12z^3 + 13z^2 + 6z + 1)$

$DV^2 = (3z + 1)^2$

$T = -9z^3 - 3z^2 - 2z - 1$

$T^2 = 81z^6 + 54z^5 + 45z^4 + 30z^3 + 10z^2 + 4z + 1$

$S = T = -9z^3 - 3z^2 - 2z - 1$

$S_e = p^2 \bmod r = -18z^3 - 15z^2 - 10z - 4$

$E : y^2 = x^3 + 3x$

$t = -163709027938637861219753170334979117687752941020633770111 58$ (192-bit)

$r = 199840114516367894642706730642926707261845896462221274551748357376589671102786$ (257-bit)

$p = 670016145715342795308367097665050084865985211655660046808378284204960327759902939872204483433284019680961532461412 77$ (377-bit)

k = 12

$t = 6z^2 + 1$

$r = 36z^4 + 36z^3 + 18z^2 + 6z + 1$

$p = 36z^4 + 36z^3 + 24z^2 + 6z + 1$

$DV^2 = 3(6z^2 + 4z + 1)^2$

$T = 6z^2$

$T^2 = 36z^4$

$S = T = 6z^2$

$S_e = p^2 \bmod r = -36z^3 - 18z^2 - 6z - 1$

$E : y^2 = x^3 + 3$

$t =$ 340282366920936614211651523200128901127 (129-bit)

$r =$ 115792089237314936872688561244471742058035595988840268584488757999429535617037 (256-bit)

$p =$ 115792089237314936872688561244471742058375878355761205198700409522629664518163 (256-bit)

6.2.3 twist

○群位数

$k = 6, 12$ のとき，楕円曲線 $E/\mathbb{F}_q : y^2 = x^3 + B$ に対する twist は $E' : y^2 = x^3 + B/D$ の形で与えられ，立方元でない $\lambda \in \mathbb{F}_p$ 及び平方元でない $\mu \in \mathbb{F}_{p^2}$ を用いて，$1/D = \lambda^2\mu^3$ として定義するものとする．$k = 8$ のとき，平方元でない $\nu \in F_{p^2}$ を用いて，$1/D = \nu$ として twist $E' : y^2 = x^3 + (A/D)x$ を構成する．

また，d 次の twist の群位数 $E'(F_{q^e})$ は 2 通りの位数の可能性を持つが，§2.2.2 で述べたように，r で割り切れる位数を持つ twist $E'(\mathbb{F}_{q^e})$ は唯一に存在する．$k = 12, d = 6$ のとき，$\sharp E(\mathbb{F}_q) = q + 1 - t$ として twist 位数 $E'(\mathbb{F}_{q^2})$ は次のようにして求める．

1. $\sharp E(\mathbb{F}_{q^2})$ を計算し，$t' = t^2 - 2q$ として $\sharp E(\mathbb{F}_{q^2}) = q^2 + 1 - t'$ とおく．
2. $\sharp E'(\mathbb{F}_{q^2}) = q^2 + 1 - (\pm 3f + t')/2, t' - 4q = 3f^2$ を計算する．ただし，$d = 6$ のとき，CM 等式は $4q - t^2 = 3V^2$ で与えられる．
3. $E'(\mathbb{F}_{q^2}) = q^2 + 1 - (3tV + t^2 - 2q)/2$, $E'(\mathbb{F}_{q^2}) = q^2 + 1 - (-3tV + t^2 - 2q)/2$ の 2 つの位数を得るが，r で割り切れる方が求める twist の位数である．

$k = 6$

$E' : y^2 = x^3 + (3/D), 1/D = \lambda^2\mu^3 = -9, \mu^2 + 1 = 0, \lambda^3 - 3 = 0$

$\sharp E'(F_q) =$ 1224818090077036800337662489997689794463896764414641463087710576002942410774346642698509212502293390073926876485127786748486748730656416397476659782286164 (511-bit)

$k = 8$

$E' : y^2 = x^3 + (3/D)x, 1/D = \nu, \nu^2 + 2 = 0$

$\sharp E'(F_{q^2}) =$ 448921635519243469643787732844339106342260576

249477484956737817183543156613221480915711884717855 87

363283946019363379092931033471173190644330020508367 17

662346566810297667316781749134787140595139178105259 03

834358993533968393971196883 4 (766-bit)

$k = 12$

$E' : y^2 = x^3 + (3/D), 1/D = \lambda^2\mu^3 = -8 + 8i, \lambda = 2, \mu = 1 + i, i^2 + 1 = 0$

$\sharp E'(F_{q^2}) =$ 134078079299423056391018503686918023097301143

717770165660537515174441269911207046351102868331479 27

468008193153310432518778926023398110971494743542672 82

6693 (510-bit)

○ $Q \in E'(F_{q^e})$ の生成

一般に，x または y にランダムな値を代入し，その平方根もしくは立方根を計算することにより，楕円曲線上の点を生成する．有限体 $\mathbb{F}_q$ の標数 p の条件によっては平方根，立方根を容易に計算可能である．$p \equiv 3 \bmod 4$ のとき，ある $a \in \mathbb{F}_q = \mathbb{F}_p[X]/f(X)$ に対する平方根は $\sqrt{a} = a^{(p+1)/4} \bmod f(X)$ で与えられ，$p \equiv 2 \bmod 3$ のとき，ある $a \in \mathbb{F}_q = \mathbb{F}_p[X]/f(X)$ に対する立方根は $a^{1/3} = a^{(2p-1)/3} \bmod f(X)$ で与えられる．$k = 6$ の場合は $p \equiv 3 \bmod 4$ より，前者の手法を適用する．$k = 8, 12$ の場合の計算方法を以下に述べる．

【$k = 8$】

$p \equiv 5 \bmod 8$ のとき，ある $a \in \mathbb{F}_q = \mathbb{F}_p[X]/f(X)$ に対する平方根は，$\gamma = (2a)^{(p-5)/8}, i = 2a\gamma^2$ として，$\sqrt{a} = a\gamma(i-1) \bmod f(X)$ で与えられる．

【$k = 12$】

$p \equiv 4 \bmod 9$ のとき，2 次拡大体の立方剰余な元 $a \in \mathbb{F}_{p^2}$ の立方は $a^{1/3} = a^{(2p+1)/9} \bmod f(X)$ で与えられる [5].

さらに，また，ペアリングに与える点 $Q' \in E'(F_{p^e})[r]$ は r-torsion point である必要があるため，次のようにして計算する．

1. ランダムな x または y を与え，曲線の式を満足する $Q = (x, y)$ を計算する．
2. $Q' = [\sharp E'(F_{p^e})/r]Q$ が無限遠点でなければ，$Q' \in E(F_p)[r]$ である．

○同型写像 ϕ

d 次の twist の同型写像 ϕ_d は次のように与えられる．

$$d = 4 : \phi_d : E' \to E : (x, y) \mapsto (D^{1/2}x, D^{3/4}y)$$
$$d = 6 : \phi_d : E' \to E : (x, y) \mapsto (D^{1/3}x, D^{1/2}y)$$

前述のパラメータ表記を利用すると，$d = 4, 6$ のときはそれぞれ以下のように表現可能である．

$$d = 4 : \begin{cases} D^{1/2} = (\frac{1}{\nu})^{1/2} = (\frac{1}{\nu})\nu^{1/2} \\ D^{3/4} = (\frac{1}{\nu})^{3/4} = (\frac{1}{\nu})\nu^{1/4} \end{cases} \quad d = 6 : \begin{cases} D^{1/3} = (\frac{1}{\lambda^2\mu^3})^{1/3} = (\frac{1}{\lambda\mu})\lambda^{1/3} \\ D^{1/2} = (\frac{1}{\lambda^2\mu^3})^{1/2} = (\frac{1}{\lambda\mu^2})\mu^{1/2} \end{cases}$$

6.3 ペアリング演算

6.3.1 逐次拡大体

twist を定義する D の要素 μ, λ, ν を用いて，以下に示すように逐次拡大により拡大体を構成する．

$$\begin{array}{ccc} & & \mathbb{F}_{p^{12}} = \mathbb{F}_{p^6}[Z]/Z^2 - \mu \\ & \mathbb{F}_{p^8} = \mathbb{F}_{p^4}[Z]/Z^2 - \nu^{1/2} & \Big| 2 \\ \mathbb{F}_{p^6} = \mathbb{F}_{p^2}[Y]/Y^3 - \lambda & \Big| 2 & \mathbb{F}_{p^6} = \mathbb{F}_{p^2}[Y]/Y^3 - \lambda \\ \Big| 3 & \mathbb{F}_{p^4} = \mathbb{F}_{p^2}[Y]/Y^2 - \nu & \Big| 3 \\ & \Big| 2 & \\ \mathbb{F}_{p^2} = \mathbb{F}_p[X]/X^2 - \mu & \mathbb{F}_{p^2} = \mathbb{F}_p[X]/X^2 + 2 & \mathbb{F}_{p^2} = \mathbb{F}_p[X]/X^2 + 1 \\ \Big| 2 & \Big| 2 & \Big| 2 \\ \mathbb{F}_p & \mathbb{F}_p & \mathbb{F}_p \end{array}$$

図 6.2: 拡大体 $\mathbb{F}_{p^6}, \mathbb{F}_{p^8}, \mathbb{F}_{p^{12}}$ の構成

上記の構成によって twist の同型写像 ϕ_d により $Q \in E(\mathbb{F}_q)$ から sparce な成分で構成される $\phi_d(Q) \in E(\mathbb{F}_{q^k})$ を生成可能である．すなわち，twist の定義体 $\mathbb{F}_{p^e}$ における 2 つの元以外はすべて零元による構成となる．一例として，$k = 6, d = 6$ のとき同型写像により得られる点 $\phi_d(Q)$ を以下に示す．$\mathbb{F}_{q^6} = (a_0\mu^{1/2} + a_1)\lambda^{2/3} + (a_2\mu^{1/2} + a_3)\lambda^{1/3} + a_4\mu^{1/2} + a_5$ とすると，$Q' = (x, y) \in E(\mathbb{F}_p)$ に対して，

$$\psi(Q) = ((0, 0, \frac{x}{\lambda\mu}, 0, 0, 0), (0, 0, 0, 0, \frac{y}{\lambda\mu^2}, 0))$$

6.3.2 楕円曲線における演算

楕円曲線における演算はアフィン (Affine) 座標系と射影 (Projective) 座標系の 2 つに分類される．2.3 節で説明した演算は Affine 座標系に基づくものである．一般に，楕円曲線上の Projective 座標系の点は $P = (X : Y : Z)$ で表現され，斉次 Weierstrass 方程式

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

を満たす．$Z \neq 0$ のとき，Affine 座標の点 $(X/Z, Y/Z)$ に対応し，Affine 座標系から Projective 座標系の点は $Z = 1$ として容易に得られる．このとき，無限遠点は $\mathcal{O} = (0 : 1 : 0)$，逆元は $-P = (X : -Y : Z)$ と表現される．以下に Projective 座標系における楕円曲線の演算を示す．$P_1 = (X_1, Y_1, Z_1), P_2 = (X_2, Y_2, Z_2), P_1 + P_2 = P_3 = (X_3, Y_3, Z_3)$ とする．

$P_1 \neq \pm P_2$のとき

$$\begin{aligned}
X_3 &= vA \\
Y_3 &= u(v^2X_1Z_2 - A) - v^3Y_1Z_2 \\
Z_3 &= v^3(Z_1Z_2) \\
u &= Y_2Z_1 - Y_1Z_2, v = X_2Z_1 - X_1Z_2, A = u^2Z_1Z_2 - v^3 - 2v^2X_1Z_2
\end{aligned}$$

$P_1 = P_2$のとき

$$\begin{aligned}
X_3 &= 2hs \\
Y_3 &= w(4B - h) - 8Y_1^2s^2 \\
Z_3 &= 8s^3 \\
w &= aZ_1^2 + 3X_1^2, s = Y_1Z_1, B = X_1Y_1s, h = w^2 - 8B
\end{aligned}$$

次に重み付射影座標系と呼ばれる Jacobian 座標系について述べる．Jacobian 座標系における点は $P = (X : Y : Z)$ で表現され,

$$Y^2 = X^3 + aXZ^4 + bZ^6$$

の方程式を満たす．$z \neq 0$ のとき，Affine 座標系の点 $(X/Z^2, Y/Z^3)$ に対応する．無限遠点は $\mathcal{O} = (1 : 1 : 0)$, 逆元は $-P = (X : -Y : Z)$ で表現される．以下に Jacobian 座標系における楕円曲線の演算を示す．$P_1 = (X_1, Y_1, Z_1), P_2 = (X_2, Y_2, Z_2), P_1 + P_2 = P_3 = (X_3, Y_3, Z_3)$ とする．

$P_1 \neq \pm P_2$のとき

$$\begin{aligned}
X_3 &= -H^3 - 2U_1H^2 + r^2 \\
Y_3 &= -S_1H^3 + r(U_1H^2 - X_3) \\
Z_3 &= Z_1Z_2H \\
U_1 &= X_1Z_2^2, U_2 = X_2Z_1^2, S_1 = Y_1Z_2^3, S_2 = Y_2Z_1^3, H = U_2 - U_1, r = S_2 - S_1
\end{aligned}$$

$P_1 = P_2$のとき

$$X_3 = T$$
$$Y_3 = -8Y_1^4 + M(S - T)$$
$$Z_3 = 2Y_1 Z_1$$
$$S = 4X_1 Y_1^2, M = 3X_1^2 + aZ_1^4, T = -2S + M^2$$

有限体における乗算, 2 乗，逆元をそれぞれ M, S, I で表現するものとし，以下に Affine 座標系, Projective 座標系，Jacobian 座標系における楕円曲線上の演算の計算コストを示す.

表 6.3: 楕円曲線上の演算の計算コスト

座標系	加算	2 倍算 ($a \neq 0, -3$)	2 倍算 ($a = 0$)	2 倍算 ($a \neq -3$)
Affine	$2M + 1S + I$	$2M + 2S + I$	$2M + 2S + I$	$2M + 2S + I$
Projective	$12M + 2S$	$7M + 5S$	$6M + 4S$	$7M + 3S$
Jacobian	$12M + 4S$	$4M + 6S$	$3M + 4S$	$4M + 4S$

$a = -3$ のとき，Projective 座標系では $aZ_1^2 + 3X_1^2 = 3(X_1 + Z_1)(X_1 - Z_1)$ と変形でき，2 回の 2 乗のところを 1 回の乗算で計算可能である．これは Jacobian 座標系でも成立する．有限体の演算における 1 回の逆元の計算コストは $8 \sim 30M$ と推定されており，また，演算アルゴリズムでは加算よりも 2 倍算の回数が多いため，本実装の楕円曲線の演算は Jacobian 座標系を採用する.

6.3.3 Miller Operation

Miller's Algorithm の主要な演算として楕円曲線上における演算と Miller's Formula によりペアリングの中間値 f_i を評価する演算がある．本稿では後者を Miller Operation と呼ぶこととする．楕円曲線における演算は Jacobian 座標系を採用しているため，Miller Operation で導出される直線式を Jacobian 座標系における直線式に変形する．以下に 2 点 $P_1 = (X_1 : Y_1 : Z_1), P_2(X_2 : Y_2 : Z_2)$ を通る直線式 g_1 及び P_1 における接線 g_2 を示す.

$$g_1(x, y) = \{(Z_1^3 y - Y_1)(Z_1^2 X_2 - Z_2^2 X_1)Z_2 - (Z_1^3 Y_2 - Z_2^3 Y_1)(Z_1^2 x - X_1)\}/(Z_1 Z_2)^3 Z_1^2$$
$$g_2(x, y) = \{Z_3 Z_1^2 y - 2Y_1^2 - (3X_1^2 + aZ_1^4)(xZ_1^2 - X_1)\}/(Z_1^6)$$

補題 4.1 により，埋め込み次数 k の因子を d として，$\mathbb{F}_{q^d}$ の元による乗算は最終べき乗により単位元になるので，上式における分母は省略可能である．また，直線式 g_i のいくつかの係数は楕円曲線の加算・2 倍算を計算する際に出現する値である．よって，加算・2 倍算を計算する際に値を保持しておき，それを直線式の計算に利用することにより，係数を再計算せず

に g_i を導出可能である．前小節の変数を利用すると，g_1, g_2 は次のようになる．

$$g_1(x,y) = (Z_1^3 y - Y_1)Z_2 H - (Z_1^2 x - X_1)r$$
$$g_2(x,y) = Z_3 Z_1^2 y - 2Y_1^2 - M(xZ_1^2 - X_1)$$

$\mathbb{G}_1 \times \mathbb{G}_2$ 型のペアリング (Tate, twisted Ate, optimized twisted Ate ペアリング) の場合，点 $P \in E(\mathbb{F}_q)$ に対して導出された直線式 $g_1, g_2 \in \mathbb{F}_q(E)$ に点 $\psi(Q') \in E(\mathbb{F}_{q^k})$ を代入，ペアリングの値 $f \in \mathbb{F}_{q^k}$ と計算する．点 $Q' \in E'(\mathbb{F}_{q^e})$ に対する点 $\psi(Q') \in E(\mathbb{F}_{q^k})$ は Sparce な構造を有しており，$\psi(Q')$ の成分 x, y と $\mathbb{F}_q$ の元の乗算には $\mathbb{F}_q$ における乗算が e 回必要になる．

一方，$\mathbb{G}_2 \times \mathbb{G}_1$ 型のペアリング (Ate, optimized Ate ペアリング) では，点 $\phi_d(Q') \in E(\mathbb{F}_{q^k})$ に対して導出された直線式 $g_1, g_2 \in \mathbb{F}_{q^k}(E)$ に点 $P \in E(\mathbb{F}_q)$ を代入し，ペアリングの値 $f \in \mathbb{F}_{q^k}$ を計算する．1 の原始 d 乗根を ζ とすると，twist の定義として与える $D \in \langle\zeta\rangle$ であるため，twist における同型写像は $\phi_d(x,y) = (\zeta^2 x, \zeta^3 y)$ で表記可能である．よって，2 点 $\phi_d(P_1) = (\zeta^2 X_1/Z_1^2, \zeta^3 Y_1/Z_1^3), \phi_d(P_2) = (\zeta^2 X_2/Z_2^2, \zeta^3 Y_2/Z_2^3)$ を通る直線式 g_1 及び P_1 における接線 g_2 を示す.

$$g_1(x,y) = \{(Z_1^3 y - \zeta^3 Y_1)(Z_1^2 X_2 - Z_2^2 X_1)Z_2 - \zeta(Z_1^3 Y_2 - Z_2^3 Y_1)(Z_1^2 x - \zeta^2 X_1)\}\zeta^2/(Z_1 Z_2)^3 Z_1^2$$
$$g_2(x,y) = \{\zeta^3 Z_3 Z_1^2 y - 2Y_1 - (3\zeta^4 X_1^2 + aZ_1^4)(xZ_1^2 - \zeta^2 X_1)\}/(Z_1^6)$$

よって，$g_1, g_2 \in \mathbb{F}_{q^i}(E)$ の計算コストは以下のように導出される．$\mathbb{F}_{q^i}$ における乗算 M_i を単位とし，推定した計算コストを以下に示す.

表 6.4: 直線式の計算コスト

直線式	$a = 0$	$a \neq 0, a = -3$
$g_1 \in \mathbb{F}_q(E)$	$(6+2e)M_1$	$(6+2e)M_1$
$g_2 \in \mathbb{F}_q(E)$	$(3+2e)M_1 + S_1$	$(3+2e)M_1$
$g_1 \in \mathbb{F}_{q^k}(E)$	$4M_e + 2eM_1$	$4M_1 + 2eM_1$
$g_2 \in \mathbb{F}_{q^k}(E)$	$3M_e + S_e + 2eM_1$	$2M_e + 2eM_1$

第7章　性能評価

楕円曲線における演算及び Miller Operation の計算コストからペアリング演算の計算コストを推定する．Optimized Ate ペアリング及び Optimized twisted Ate ペアリングの性能評価として従来のペアリング及び他の主要な暗号要素技術と計算コストの比較を行う．また，ソフトウェア実装による性能評価も併せて行う．

7.1　理論値による評価

7.1.1　計算コスト推定

$\mathbb{G}_1 \times \mathbb{G}_2$ 型のペアリング $f_{N,P}(\psi(Q))$ 及び $\mathbb{G}_2 \times \mathbb{G}_1$ 型のペアリング $f_{N,\psi(Q)}(P)$ における Miller's algorithm の 2 倍算，加算における演算は次のようになる．

$$f_{N,P}(\psi(Q)) \begin{cases} V \leftarrow P \\ f \leftarrow f^2 \cdot g_{V,V}(\psi(Q)), & V = 2V \\ f \leftarrow f \cdot g_{V,P}(\psi(Q)), & V = V + P \end{cases}$$

$$f_{N,\phi(Q')}(P) \begin{cases} V \leftarrow \psi(Q) \\ f \leftarrow f^2 \cdot g_{V,V}(P), & V = 2V \\ f \leftarrow f \cdot g_{V,\psi(Q)}(P), & V = V + \psi(Q) \end{cases}$$

$\mathbb{G}_1 \times \mathbb{G}_2$ 型のペアリング $f_{N,P}(\psi(Q))$ に関する処理を "Miller lite" と呼び，$\mathbb{G}_2 \times \mathbb{G}_1$ 型のペアリング $f_{N,\psi(Q')}(P)$ に関する処理を "Full Miller" と呼ぶ [24]．それぞれの計算コストを C_{Lite},C_{Full} と表記する．ここで，ある $N \in \mathbb{Z}$ の Hamming Weight を $\mathrm{wt}(N)$ とすれば，前章で導出した楕円曲線における演算及び Miller operation の計算コストに f の乗算コストを加えて C_{Lite}, C_{Full} は次のようになる．ここでは，性能評価に必要となる $A = 0, -3$ の場合のみ扱う．
When $A = -3$:

$$C_{\mathrm{Lite}} = (4S_1 + (2e+7)M_1 + S_k + M_k)\log_2 N + (4S_1 + (2e+18)M_1 + M_k)\mathrm{wt}(N)$$
$$C_{\mathrm{Full}} = (4S_e + 6M_e + 2eM_1 + S_k + M_k)\log_2 N + (4S_e + 16M_e + 2eM_1 + M_k)\mathrm{wt}(N)$$

When $A = 0$:

$$C_{\mathrm{Lite}} = (5S_1 + (2e+6)M_1 + S_k + M_k)\log_2 N + (4S_1 + (2e+18)M_1 + M_k)\mathrm{wt}(N)$$
$$C_{\mathrm{Full}} = (5S_e + 6M_e + 2eM_1 + S_k + M_k)\log_2 N + (4S_e + 16M_e + 2eM_1 + M_k)\mathrm{wt}(N)$$

7.1.2 性能評価

$P \in E(\mathbb{F}_q)[r], Q \in E'(\mathbb{F}_{q^e})[r]$ として以下の 5 つの Modified ペアリングによる性能評価を行う．ただし，最終べき乗の処理は含めず，$T = t - 1, S = q \bmod r, S_e = q^e \mod r$ とする．

1. Tate ペアリング: $f_{r,P}(\psi(Q))$
2. Ate ペアリング: $f_{T,\psi(Q)}(P)$
3. Twisted Ate ペアリング: $f_{T^e,P}(\psi(Q))$
4. Optimized Ate ペアリング: $f_{S,\psi(Q)}(P)$
5. Optimized twisted Ate ペアリング: $f_{S_e,P}(\psi(Q))$

1,3,5 の計算コストは C_{Lite}，2,4 の計算コストは C_{Full} で算出する．$k = 4, 8$ のとき $A = 0$, $k = 6, 12$ のとき $A = -3$ とする．また，$k = 4$ のとき，MOV security $\sim$ 1280, $k = 6, 8, 12$ のとき，MOV security $\sim$ 3072 となるように設定する．$f_{N,P}(\psi(Q)), f_{N,\psi(Q)}(P)$ における N として §6.2.2 で示した T, S, S_e を利用して性能評価を行う．埋め込み次数 $k = 2^i 3^j$ となる有限体 $\mathbb{F}_{p^k}$ の乗算コストを $M_k = 3^i 5^j M_1, S_k = 3^i 5^j S_1$ とする．Pairing-friendly Field における 2 乗と乗算のコスト比はほぼ $S/M = 0.7 \sim 0.8$ であるため [13]，$S_k = 0.8 M_k$ とする．以下に算出したペアリングの計算コストを示す.

表 7.1: ペアリングの計算コスト

パラメータ	ペアリング	$\mathrm{wt}(N) \sim 0$		$\mathrm{wt}(N) \sim (1/2)\log_2 N$	
		Standard	Optimized	Standard	Optimized
$k = 4, d = 4$	Tate	4544		6240	
$\log_2 q \sim 320$	Ate	4384	2192	6800	3400
$\log_2 r \sim 160$	twisted Ate	4544	2272	6240	3120
$k = 6, d = 6$	Tate	9984		14874	
$\log_2 q \sim 512$	Ate	9984	4992	14618	7309
$\log_2 r \sim 256$	twisted Ate	9984	4992	14874	7437
$k = 8, d = 4$	Tate	16077		21351	
$\log_2 q \sim 384$	Ate	15399	15399	23904	23904
$\log_2 r \sim 256$	twisted Ate	24116	12058	32026	16013
$k = 12, d = 6$	Tate	24320		33306	
$\log_2 q \sim 256$	Ate	14720	14720	21543	21543
$\log_2 r \sim 256$	twisted Ate	24320	18240	33306	24980

$\mathrm{wt}(N) \sim (1/2)\log_2 N$ において従来のペアリングと比較すると，$k = 4, 6$ のとき約 2.00 倍，$k = 8$ のとき約 1.33 倍の高速化を実現可能であると予想される．また，$k = 12$ のとき Optimized twisted Ate ペアリングは Tate ペアリングより約 1.33 倍高速である．Ate ペアリングに対して $\deg(t-1) \geq \deg(r)$，あるいは Twisted Ate ペアリングに対して $\deg((t-1)^e - 1) \geq \deg(r)$ の条件を満足するとき，提案したペアリングのループ回数は $(\deg(r) - 1)/\deg(r)\lfloor \log_2 r \rfloor$ となり，最小で Tate ペアリングの約半分のループ長で計算可能である．

7.1.3 各演算の計算コスト

楕円曲線におけるスカラー倍算及び有限体におけるべき乗剰余計算の計算コストを算出する．どちらも演算アルゴリズムとして最も一般的な 2 進展開法を採用するものとする．楕円曲線における 2 倍算，加算を D, A, 有限体における乗算，2 乗算を M, S とすると，スカラー倍の計算コスト C_S，べき乗剰余の計算コスト C_{EXP} は一般に次のようになる．

$$C_S = (\log_2 N)D + \frac{1}{2}(\log_2 N)A = (10M + 8S)\log_2 N$$
$$C_{EXP} = (\log_2 N)S + \frac{1}{2}(\log_2 N)M = (\frac{1}{2}M + S)\log_2 N$$

前述したように，スカラー倍算に適した楕円曲線とペアリング演算に適した楕円曲線は異なり，それに伴ってべき乗剰余のコストも変動する．ここでは，ペアリング演算に適した楕円曲線を採用する．MOV security $\sim$ 1280, 3072 における計算コストを算出し，ペアリングの性能評価に用いたパラメータを利用する．部分群の位数 r となる生成元 $P \in E(\mathbb{F}_q), g \in \mathbb{F}_q^*$ に対してスカラー倍算を $sP \in E(\mathbb{F}_q), s \in \mathbb{Z}_r$，べき乗剰余を $g^l \in \mathbb{F}_{q^k}, l \in \mathbb{Z}_r$ とする．最終べき乗は §4.3.1 で述べた高速化手法を適用することにより，計算コストは $(\Phi_k(q)/r)$ 乗のコストとほぼ同等となり，そのビット長は $\log_2 \frac{\Phi_k(q)}{r} = \frac{\varphi(k)}{k}\log_2(q^k) - \log_2(r)$ である．有限体 $\mathbb{F}_q$ における乗算 M によるコスト算出のため，同一行における相対評価となる. 以下に各演算の計算コストを示す.

表 7.2: 各演算の計算コスト

MOV security	k	$\log_2 q$	$\log_2 r$	ペアリング	スカラー倍算	べき乗剰余	最終べき乗
1280	4	320	160	2192	2624	1872	5616
3072	6	512	256	4992	4199	4992	14976
3072	8	384	256	12058	4199	8986	44928
3072	12	256	256	14720	4199	14976	44928

スカラー倍算の計算コストは群位数にのみ依存しており，定義体に対して一定である．ペアリング及びべき乗は埋め込み次数の増加によって多項式演算の計算コストが急激に増大する傾向があり，Shortsignature など定義体のサイズが署名長となる場合を除いて，できる限り小さい埋め込み次数を選択する方が望ましい．また，ペアリング及びべき乗剰余の計算コスト比は $k = 8$ を除いてほぼ等しいが，Reduced ペアリングに必要となる最終べき乗はペアリングの約 3 倍程度の計算コストを要する．すなわち，一般的にプロトコルで用いられる Reduced ペアリングの計算量の約 4 分の 3 はべき乗剰余の処理になる．

7.2 実測値による評価

7.2.1 実測環境

以下に実測環境を示す．多倍長演算ライブラリとして GNU MP [54] を利用する．

表 7.3: 実測環境

OS	Linux Fedora core version 2.6
CPU	AMD Opteron$^{\mathrm{TM}}$ Processor 246 (2.0GHz)
Memory	1.0GHz
Language	C++
Compiler	gcc version 3.4.4

7.2.2 実測結果

前章に基づいてペアリングのソフトウェア実装し，$k = 6, 8, 12$ において，§6.2 で示したパラメータを用いて $\mathbb{G}_1 \times \mathbb{G}_2$ 型のペアリングの実測実験を行った．ペアリングの演算時間は 10 回試行させた平均値とする．ただし，最終べき乗の処理は含めない．実測値を下表に示す．

表 7.4: ペアリングの演算時間

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

Optimized twisted Ate ペアリングは Tate ペアリングと比較して $k = 6$ のとき 1.99 倍，$k = 8$ のとき 1.33 倍，$k = 12$ のとき 1.43 倍の高速化を実際に達成しており，理論値による性能評価とほぼ同様の結果を得たことが分かる．$k = 12$ のにおける理論値による評価との誤差は $(t-1)^2$ と r の Hamming Weight の差によって生じたものであると考えられる．

なお，$\mathbb{G}_2 \times \mathbb{G}_1$ 型のペアリングも同一のアルゴリズム構造を有するため，同様の結果を得ることが予想される．

第8章　結論

本稿では Ordinary Curve における Ate ペアリング及び Twisted Ate ペアリングに対して，Supersingular Curve における Eta ペアリングのループ削減手法を適用し，ループ長を短縮した Optimized Ate ペアリング及び Optimized twisted Ate ペアリングを提案した．$t-1, (t-1)^e$ に対して部分群 r を法とする剰余を計算しているため，常に Tate ペアリングよりも計算コストは小さくなる．さらに，Ate ペアリングにおいては $\deg(t-1) \geq \deg(r)$，Twisted Ate ペアリングにおいては $\deg((t-1)^e) \geq \deg(r)$ を満足するとき，提案したペアリングのループ回数は $(\deg(r)-1)/\deg(r)\lfloor \log_2 r \rfloor$ となり，最小で Tate ペアリングの約半分のループ長で計算可能である．

性能評価としてペアリング演算コストを理論的に算出し，$k = 4, 6$ のとき約 2 倍，$k = 8$ のとき約 1.32 倍の高速化が可能であることを示した．さらに，$\mathbb{G}_1 \times \mathbb{G}_2$ 型のペアリングをソフトウェア実装し，実際に理論値通りの高速化を達成可能であることを実証した．なお，$\mathbb{G}_2 \times \mathbb{G}_1$ 型のペアリングも同一のアルゴリズム構造を有するため，同様の結果を得ると予想される．

謝辞

本研究を遂行するにあたり，終始懇切な御指導，御鞭撻を賜った筑波大学大学院システム情報工学研究科 岡本栄司教授に心より感謝致します．御多忙の中，御指導頂きました筑波大学大学院システム情報工学研究科 岡本健講師に深く感謝致します．日頃から本研究に多くの議論を頂いた筑波大学大学院システム情報工学研究科 金山直樹研究員に厚く御礼申し上げます．本提案手法に関して御助言を頂いたベルリン工科大学 Florian Hess 教授に心より感謝致します．論文投稿・論文執筆にあたり，多大な御助言を頂いた独立行政法人科学技術振興機構 猪俣敦夫研究員に深く感謝の意を表します．

最後に，本研究への御助言を頂いた暗号・情報セキュリティ研究室の皆様方に感謝致します．

参考文献

[1] P.S.L.M. Barreto, S. Galbraith, C. Ó hÉigeartaigh, and M. Scott, "Efficient pairing computation on supersingular abelian varieties," *Cryptology ePrint Archive*, Report 2004/375, 2004. Available: http://eprint.iacr.org/2004/375.pdf

[2] P.S.L.M. Barreto, H.Y. Kim, B. Lynn, and M. Scott, "Efficient algorithms for pairing-based cryptosystems," *Advances in Cryptology–CRYPTO 2002*, LNCS 2442, pp.354-368, Springer-Verlag, 2002.

[3] P.S.L.M. Barreto, B. Lynn, and M. Scott, "Efficient implementation of pairing-based cryptosystem," *Journal of Cryptology*, 17(4):321–334, 2004.

[4] P.S.L.M. Barreto, B. Lynn, and M. Scott, "On the Selection of Pairing-Friendly Groups," *Selected Areas in Cryptography–SAC 2003*, LNCS 3006, pp.17-25, Springer-Verlag, 2003.

[5] P.S.L.M. Barreto and M. Naehrig, "Pairing-Friendly Elliptic Curve of Prime Order," *Selected Areas in Cryptography–SAC 2005*, LNCS 3897, pp.319-331, Springer-Verlag, 2006.

[6] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil pairing," *Advances in Cryptology–CRYPTO 2001*, LNCS 2139, pp.213-229, Springer-Verlag, 2001.

[7] D. Boneh, C. Gentry, and B. Waters, "Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys," *Advances in Cryptology–CRYPTO 2005*, LNCS 3621, pp.258–275, Springer-Verlag, 2006.

[8] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from Weil pairing," *Advances in Cryptology–ASIACRYPT 2001*, LNCS 2248, pp.514–532, Springer-Verlag, 2001.

[9] Jung Hee Cheon, Yongdae Kim, and Hyo Jin Yoon, "A New ID-based Signature with Batch Verification," *Cryptology ePrint Archive*, Report 2004/131, 2004. Available: http://eprint.iacr.org/2004/131.pdf

[10] Henri Cohen, Atsuko Miyaji, and Takatoshi Ono, "Efficient Elliptic Curve Exponentiation," *Advances in Cryptology–ASIACRYPT 1998*, LNCS 1514, pp.51–65, Springer-Verlag, 1998.

[11] S. A. Cook, "On the Minimum Computaion Time of Functions," PhD Thesis, Harvard University Department of Mathematics, 1966.

[12] Don Coppersmith, "Fast Evaluation of Logarithms in Fields of Characteristic Two," *IEEE Transaction on Information Theory*, Vol. IT-30, No. 4, July 1984.

[13] Ricardo Dahab, Augusto Jun Devegili, Colm Ó hÉigeartaigh, and Michael Scott, "Multiplication and Squaring on Pairing-Friendly Fields," *Cryptology ePrint Archive*, Report 2006/471, 2006. Available: http://eprint.iacr.org/2006/.pdf

[14] Pu Duan, Shi Cui, and Choong Wah Chan, "Effective Polynomial Families for Generating More Pairing-friendly Elliptic Curve", *Cryptology ePrint Archive*, Report 2005/236, 2005. Available: http://eprint.iacr.org/2005/236.pdf

[15] Iwan Duursma and Hyang-Sook Lee, "Tate Pairing Implementation for Hyperelliptic Cruves $y^2 = x^p - x + d$," *Advances in Cryptology–ASIACRYPT 2003*, LNCS 2894, pp.111-123, Springer-Verlag, 2003.

[16] David Freeman, M. Scott, and Edlyn Teske, "A taxonomy of pairing-friendly elliptic curves," *Cryptology ePrint Archive*, Report 2006/372, 2006. Available: http://eprint.iacr.org/2005/372.pdf

[17] S. Galbraith, K. Harrison, and S. Soldera, "Implementing the Tate pairing," *Algorithmic Number Theory Symposium–ANTS V*, LNCS 2369, pp.324–337, Springer-Verlag, 2002.

[18] R. Granger, D. Page, and M. Stam, "On small characteristic algebraic tori in pairing-based cryptography," *Cryptology ePrint Archive*, Report 2004/132, 2004. Available: http://eprint.iacr.org/2004/132.pdf

[19] F. Hess, "Efficient Identity Based Signature Schemes Based on Pairings," *Selected Areas in Cryptography–SAC 2002*, LNCS 2595, pp.310–324, 2003.

[20] F. Hess, N.P. Smart, and F. Vercauteren, "The Eta Pairing Revisited," *IEEE Transaction on Information Theory*, Vol.52, pp.4595-4602, no.10, October 2006.

[21] Antoine Joux, "A One Round Protocol for Tripartite Diffie-Hellman," *Algorithmic Number Theory Symposium–ANTS IV*, LNCS 1838, pp.385–394, Springer-Verlag, 2000.

[22] Antoine Joux, "Discrete logarithms in GF(p) — 130 digits," *NMBRTHRY Mailing List*, 18 June 2005.

[23] A. A. Karatsuba and Y. Ofman, "Multiplication of Multidigit Numbers on Automata," *Soviet Physics Doklady*, 7:595–596, 1963.

[24] N. Koblitz and A. Menezes, "Pairing-based cryptography at high security levels," *Cryptography and Coding: 10th IMA International Conference*, LNCS 3796, pp.13-36, Springer-Verlag, 2005.

[25] Arjen K. Lenstra, "Selecting Cryptographic Key Sizes," *Journal of CRYPTOLOGY*, vol.14, No.4, pp.255-293, December, 2001.

[26] Martijn Maas, "Pairing-Based Cryptography," Master's Thesis, Technische Universiteit Eindhoven, 2004.

[27] Benoit Chevallier-Mames, Jean-Sebastien Coron, Noel McCullagh, David Naccache, and Michael Scott, "Secure Delegation of Elliptic-Curve Pairing," *Cryptology ePrint Archive*, Report 2005/150, 2005. Available: http://eprint.iacr.org/2005/150.pdf

[28] V. Miller, "Short Programs for Functions on Curves," Unpubliched manuscript, 1986.

[29] V. S. Miller, "The Weil Pairing, and Its Efficient Calculation," *Journal of CRYPTOLOGY*, vol.17, No.4, pp.235–261, September, 2004.

[30] A. Miyaji, M. Nakabayashi, and S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction," *IEICE Transactions on Fundamentals*, E84-A(5):1234–1243, 2001.

[31] A. Menezes, T. Okamoto, S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," *IEEE Transactions on Information Theory*, 39:1639–1646, 1993.

[32] J. Robertson, "Solving the generalized Pell equation," Unpubliched manuscript, 2004. Available: hht://hometown.aol.com/jpr2718/pell.pdf

[33] R. Sakai, K. Ohgishi, and M. Kasahara, "Cryptosystems based on pairing," *Symposium on Cryptography and Information Security–SCIS 2000*, C20,2000.

[34] M. Scott, "Scaling security in pairing-based protocols," *Cryptology ePrint Archive*, Report 2005/139, 2005. Available: http://eprint.iacr.org/2005/139.pdf

[35] M. Scott and P.S.L.M. Barreto, "Compressed pairings," *Advances in Cryptology–CRYPTO 2004*, LNCS 3152, pp.140–156, 2004.

[36] M. Scott and P.S.L.M. Barreto, "Generating more MNT elliptic curves," *Designs, Codes and Cryptography*, 38:209–217, 2006.

[37] Michael Scott, Neil Costigan, and Wesam Abdulwahab, "Implementing Cryptographic Pairings on Smartcards," *Cryptology ePrint Archive*, Report 2006/144, 2006. Available: http://eprint.iacr.org/2006/144.pdf

[38] Seiichi Matsuda, Naoki Kanayama, Florian Hess, and Eiji Okamoto," "Optimized versions of the Ate pairing and twisted Ate pairing," *Cryptology ePrint Archive*, Report 2007/013, 2007. Available: http://eprint.iacr.org/2007/013.pdf

[39] J. Solinas, “Generalized Mersenne numbers,” *technical report CORR-39*, Departmentof C&O, University of Waterloo, 1999. Available: http://www.cacr.math.uwaterloo.ca/

[40] Emmanuel Thomé, “Computation of Discrete Logarithms in $\mathbb{F}_{2^{607}}$,” *Advances in Cryptology–ASIACRYPT 2001*, LNCS 2248, pp.107–124, 2001.

[41] A. L. Toom, “The Complexity of a Scheme of Functional Elements realizing the Multiplication of Integers,” *Soviet Mathematics*, 4(3):714–716, 1963.

[42] André Weimerskirch and Christof Paar, “Generalizations of the Karatsuba Algorithm for Efficient Implementations,” *Cryptology ePrint Archive*, Report 2006/224, 2006. Available: http://eprint.iacr.org/2006/224.pdf

[43] 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,” 電子情報通信学会, ISEC 研究会, 2006.

[44] 松田誠一, 金山直樹, 猪俣敦夫, 岡本健, 岡本栄司, “ペアリングパラメータ設定に関する考察,” *DICOMO2006*, 3E2, 2006.

[45] J. A. Buchmann, “Introduction to Cryptography,” Springer-Verlag, 2000.

[46] A. Menezes, “Elliptic Curve Public Key Cryptosystems,” Kluwer Academic Publishers, 1993.

[47] J. H. Silverman, “The Arithmetic of Elliptic Curves,” New York, Springer-Verlag, 1986.

[48] Lawrence C. Washington, “Elliptic Curves,” Crc Pr I Llc, 2003.

[49] 岡本栄司「暗号理論入門」共立出版 2002.

[50] 岡本龍明　山本博資「現代暗号」産業図書出版 1997.

[51] 山本芳彦「数論入門」岩波図書 2003.

[52] 電子情報処理学会 編「情報セキュリティハンドブック」オーム社 2004.

[53] 情報処理振興事業協会　通信・放送機構「暗号技術評価報告書 (2002 年度)」(CRYPTREC Report 2002) 情報処理推進機構 2002.

[54] GNU MP, http://www.swox.com/gmp/ (2007.1.29)

[55] Voltage Security, http://www.voltage.com/ (2007.1.29)