ペアリング暗号解読の世界記録とその安全性評価

高木　剛[†]　下山　武司[††a)]　篠原　直行[†††]　林　卓也[†††]

World Record Cryptanalysis of a Pairing-Based Cryptography and Its Security Evaluation

Tsuyoshi TAKAGI[†], Takeshi SHIMOYAMA[††a)], Naoyuki SHINOHARA[†††], and Takuya HAYASHI[†††]

あらまし　ペアリング暗号の安全性は，有限体上の離散対数問題 (DLP) の困難さを根拠としている．本論文では，標数が小さい有限体を利用するペアリング暗号方式の安全性評価を目的として，標数が小さい有限体上の DLP の困難性を考察する．特に有限体 $\mathbb{F}_{3^{6\cdot 97}}$ は η_T ペアリングの実装ベンチマークで広く利用されていたものである．著者らは関数体篩法の改良アルゴリズムとその高速実装を提案し，2012 年 4 月に $\mathbb{F}_{3^{6\cdot 97}}$ 上の DLP を，252 CPU コアにより 148.2 日で解読することに成功した．この成果が発表された後，標数の小さい有限体上の DLP を解くアルゴリズムの研究で大きな進展があった．本論文ではこれらの進展についても解説する．

キーワード　ペアリング暗号，離散対数問題，関数体篩法，大規模並列計算

1. まえがき

1.1 ペアリング暗号

ペアリング暗号は，ペアリング写像という特殊な写像を用いた暗号方式の総称である．境–大岸–笠原によってペアリング写像が暗号方式の構築に初めて導入され [47]，それ以降，ペアリング写像を応用することで，従来では効率的な構成が難しいとされてきた高機能な暗号応用が様々に実現されている．代表的なものとして 3 者 Diffie-Hellman 鍵交換方式 [31] や ID ベース暗号 [16] などがある．例えば ID ベース暗号では，各個人に割り振られた識別子（例えばメールアドレス）を公開鍵として利用できる．公開鍵とその所有者が自明に紐付くため，証明書が不要になるという大きなメリットがある(注1)．

ペアリング写像は，同じ位数の群 $\mathbb{G}_1, \mathbb{G}_2$ において $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ となる写像 e である(注2)．この写像の特に重要な性質として双線形性がある．つまり，$p = |\mathbb{G}_1|$ とし，ある $a, b \in \mathbb{Z}_p, P, Q \in \mathbb{G}_1$ について，

$$e(aP, bQ) = e(bP, aQ) = e(P, Q)^{ab} \qquad (1)$$

が成り立つ．慣例的に $\mathbb{G}_1$ を加法群，$\mathbb{G}_2$ を乗法群として記述する．RSA 暗号などの従来の公開鍵暗号方式で扱う写像は双線形性を満たさないため，ペアリング暗号と従来の公開鍵暗号方式との違いは，双線形性を利用できるかの違いであると言える．

1.2 ペアリング暗号の安全性評価と離散対数問題

ペアリング写像の応用により新たな暗号方式の構成が様々に進展したが，それと同時にペアリング暗号の安全性の評価が必要となった．ペアリング暗号の安全性は，$\mathbb{G}_1, \mathbb{G}_2$ 上の離散対数問題 (DLP) の計算量的な困難性に支えられている．離散対数問題とは，巡回群 $\mathbb{G}$ において，その生成元を $g \in \mathbb{G}$ としたときに，$a \in \mathbb{G}$ について $a = g^x$ となる最小の整数 x を求める問題である．実際には，ペアリング暗号は双線形 DH 問題 (BDH) や決定的線形問題 (DLIN) などの数論問

† 九州大学マス・フォア・インダストリ研究所，福岡市
Kyushu University, Fukuoka-shi, 819–0395 Japan
†† （株）富士通研究所，川崎市
FUJITSU Laboratories LTD., Kawasaki-shi, 211–8588 Japan
††† 情報通信研究機構，小金井市
National Institute of Information and Communications Technology, Koganei-shi, 184–8795 Japan
a) E-mail: shimo-shimo@jp.fujitsu.com
DOI:10.14923/transcomj.2016SHI0003

(注1)：公開鍵と所有者の紐付けには証明書が不要という意味であり，より広い用途での証明書が不要という意味ではないことに注意．

(注2)：詳細に書くと，$\mathbb{G}_1, \mathbb{G}_1', \mathbb{G}_2$ という同じ位数の群において $\mathbb{G}_1 \times \mathbb{G}_1' \to \mathbb{G}_2$ となる写像であり，$\mathbb{G}_1$ と $\mathbb{G}_1'$ との間に多項式時間で行き来できる写像があるかどうかで分類される．本論文で扱うペアリング写像は，$\mathbb{G}_1$ と $\mathbb{G}_1'$ を同一視できるためこのように記述する．

題に安全性が帰着されるが，これらの問題は DLP の計算により容易に計算できることが知られているため，DLP はペアリング暗号の安全性を支える最も根本的な計算問題といえる．

DLP の困難性は $\mathbb{G}_1, \mathbb{G}_2$ の位数の大きさに比例するため，位数を十分に大きくすることで安全性を確保できる．しかし，ペアリング暗号の処理時間もまたこれらの位数の大きさに比例するため，必要以上に位数を大きくしてしまうと暗号の効率性が損なわれてしまう．このため，DLP の計算困難性を詳細に評価することは，ペアリング暗号の安全性と効率性を両立する上で重要な課題である．

DLP 計算アルゴリズムの計算量は漸近的に評価できるものの，定数倍や実装方法，計算環境による影響が無視されてしまうため，漸近的な計算量だけでは詳細な評価は困難である．計算量を詳細に評価する方法としては，実際に計算するという方法が最も単純かつ詳細に評価できるが，当然ながら暗号で利用されるサイズの DLP 計算は現実時間では困難である．このため実際には，十分に大きな DLP(世界記録など) を計算し，それに必要だった計算資源や計算時間から漸近計算量では無視される部分を評価し，DLP の計算量を詳細に評価する．

1.3 標数の小さい有限体を利用するペアリング暗号の安全性評価

ペアリング写像を効率的に計算するアルゴリズムとして，標数 3 の n 次拡大の有限体 $\mathbb{F}_{3^n}$ 上の超特異だ円曲線 E で定義される η_T ペアリングがある [9]．超特異だ円曲線 E の埋込次数は 6 であり，η_T ペアリングの安全性は有限体 $\mathbb{F}_{3^{6n}}$ の DLP に帰着される．CRYPTO 2002 において Barreto らは，曲線 E 上の Tate ペアリングを効率的に計算するアルゴリズムを発表し [11]，その後も曲線 E を利用した高速実装が多く提案されている [3], [12]～[14], [26], [27], [41]．これらの高速実装では拡大次数 $n = 97$ によるベンチマーク比較が実施されていたため，有限体 $\mathbb{F}_{3^{6\cdot 97}}$ 上の DLP の困難性の評価は特に重要な研究課題であった．

本論文では標数が小さい有限体上の DLP の困難性について述べる．特に前半では，2012 年に有限体 $\mathbb{F}_{3^{6\cdot 97}}$ 上の DLP を解いた成果 [28] について説明する．後半では，上記の成果以降の研究動向について解説する．

2012 年当時，有限体上の DLP を効率良く解くアルゴリズムとして関数体篩法 (Function Field Sieve, 以後 FFS と略記) [1], [2] が挙げられた．特に小さな標数の有限体上の DLP については，Joux-Lercier により提案された FFS の改良版 (JL06-FFS) [39] が有効であった．そこで著者らは JL06-FFS に対する改良法を幾つか提案し解読実験を行った．FFS には大きく分けて四つのフェーズ (多項式選択，関係式探索，線形代数，個別離散対数) があり，最も計算量が多いフェーズが関係式探索と線形代数となる．関係式探索フェーズでは，JL06-FFS に対する格子篩法の適用，SIMD による格子篩法の実装，実装パラメータの最適化などにより，約 6 倍の高速化を行った．線形代数フェーズでは，$\mathbb{F}_{3^{6\cdot 97}}$ の Galois 群の作用による変数圧縮，Singleton-clique 及び Merge [19] による行列縮約により，Lanczos 法で用いる行列のサイズを元のサイズの約 4.5%に圧縮することが可能となった．JL06-FFS に対するこれらの改良法を実装することにより，923 ビットの有限体 $\mathbb{F}_{3^{6\cdot 97}}$ の DLP を，合計 252 CPU コア (Core2 quad, Xeon など) を用いて 148.2 日で解読することに成功した．関係探索フェーズは 53.1 日，線形代数フェーズは 80.1 日，個別離散対数フェーズは 15.0 日の計算時間となった．これらの詳細については **2.** で説明する．

2012 年 12 月，関係式探索フェーズにおいて pinpointing と呼ばれる，篩とは異なる新たな手法が提案され [32]，翌 2013 年に，pinpointing の方針に沿ったアルゴリズムの提案により，標数の小さな有限体 $\mathbb{F}_{q^k}$ 上の DLP を解くために必要な計算量が $L_{q^k}(1/3)$ から $L_{q^k}(1/4 + o(1))$ に削減された [33]．篩から pinpointing への方針転換の影響は大きく，その後，アルゴリズムの改良により，計算量が quasi-polynomial time にまで削減された [10]．これらのアルゴリズム [10], [33] が属するアルゴリズムは Frobenius representation algorithm (本論文では FRA と略記) と総称される [40]．これら最新の研究動向については **3.** で述べる．

2. $\mathbb{F}_{3^{97}}$ 上の η_T ペアリング暗号解読

本章では，2011 年から 2012 年にかけて実施した，$\mathbb{F}_{3^{97}}$ 上の η_T ペアリング暗号解読について述べる．$\mathbb{F}_{3^{97}}$ 上 η_T ペアリングの安全性は，有限体 $\mathbb{F}_{3^{6\cdot 97}}$ の離散対数問題 (DLP) に帰着されることから，以降，小標数上の DLP の解法として知られている，Joux-Lercier により提案された FFS の改良版 (JL06-FFS) [39] をベースとしたアルゴリズムを用いた計算機実験 [29], [48] について述べる．

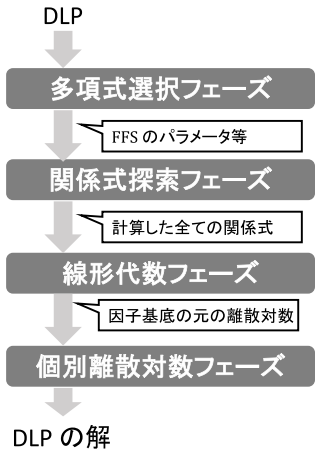


図 1　関数体篩法の概要
Fig. 1　Overview of function field sieve.

2.1　関数体篩法

関数体篩法 (FFS) は，小標数の拡大体における DLP の解法として，漸近的に最も効率的な手段として知られており，1994 年に Adleman [1] によって提案されて以来，幾つかの改良が提案されている [2], [38], [39]．本論文の実験では JL06-FFS [39] をベースに更に改良を加えたものを用いている．

関数体篩法は，多項式選択，関係式探索，線形代数，個別離散対数の四つのフェーズで構成される (図 1 参照)．最も計算量が必要となるフェーズは関係式探索と線形代数である．以下，それぞれのフェーズについて順に述べる．

2.1.1　多項式選択フェーズ

パラメータ $\kappa \in \{1,2,3,6\}$ 及び $d_H, d_m \in \mathbb{N}$ について，有限体 $\mathbb{F}_{3^\kappa}$ 上の二変数多項式 $H(x,y) \in \mathbb{F}_{3^\kappa}[x,y]$ 並びに既約多項式 $f(x)$ を次が成り立つように決める．

$$H(x,y) = x + y^{d_H} \tag{2}$$

$$H(x,m) \equiv 0 \pmod{f},\ \deg f = 6n/\kappa. \tag{3}$$

ただし，$m \in \mathbb{F}_{3^\kappa}[x]$ は，次数 $d_m (< 6n/\kappa)$ のランダムに選ばれたモニック既約多項式である．この多項式 $f(x)$ により，同型 $\mathbb{F}_{3^{6n}} \cong \mathbb{F}_{3^\kappa}[x]/(f)$ が定まる．二種類の集合 $F_A(B), F_R(B)$ を次のように定める．

$$F_R(B) = \{\mathfrak{p} \in \mathbb{F}_{3^\kappa}[x] \mid \deg(\mathfrak{p}) \le B, \mathfrak{p} \text{ はモニック既約}\} \tag{4}$$

$$F_A(B) = \{\langle \mathfrak{p}, y - t\rangle \in \mathrm{Div}(\mathbb{F}_{3^\kappa}[x,y]/(H)) \mid \mathfrak{p} \in F_R(B),\ H(x,t) \equiv 0 \bmod \mathfrak{p}\}, \tag{5}$$

ただし，$\mathrm{Div}(\mathbb{F}_{3^\kappa}[x,y]/(H))$ は，$\mathbb{F}_{3^\kappa}[x,y]/(H)$ の因子群，$\langle \mathfrak{p}, y-t\rangle$ は，$\mathfrak{p}$ と $y-t$ で生成される因子，B は，因子の次数の最大値を定める正の整数である．$F_R(B) \cup F_A(B)$ を因子基底と呼ぶ．

2.1.2　関係式探索フェーズ

次の性質を満たす組 $(r,s) \in (\mathbb{F}_{3^\kappa}[x])^2$ を関係式と呼ぶ．

$$\deg r \le R,\ \deg s \le S,\ \gcd(r,s) = 1, \tag{6}$$

$$rm + s = \prod_{\mathfrak{p}_i \in F_R(B)} \mathfrak{p}_i^{a_i}, \tag{7}$$

$$\langle ry + s\rangle = \sum_{\langle \mathfrak{p}_j, y - t_j\rangle \in F_A(B)} b_j \langle \mathfrak{p}_j, y - t_j\rangle. \tag{8}$$

ただし a_i, b_j は非負整数である．関係式探索フェーズの目標は，この関係式を因子基底の個数以上抽出することである．上記式を満たす組を具体的に求める際には次の式が用いられる．

$$(-r)^{d_H} H(x, -s/r) = \prod_{\langle \mathfrak{p}_j, y - t_j\rangle \in F_A(B)} \mathfrak{p}_j^{b_j}. \tag{9}$$

関係式から，因子基底の対数値について $(3^{6n}-1)/(3^\kappa - 1)$ を法とした線形関係が導かれる．

$$\sum_{\mathfrak{p}_i \in F_R(B)} a_i \log_g \mathfrak{p}_i \equiv \sum_{\langle \mathfrak{p}_j, y - t_j\rangle \in F_A(B)} b_j \log_g \mathfrak{s}_j \tag{10}$$

ここで，$\mathfrak{s}_j$ は $\langle \mathfrak{p}_j, y - t_j\rangle$ の y に m を対応させた $\mathbb{F}_{3^\kappa}[x]/(f)$ の要素である．

2.1.3　線形代数フェーズ

線形代数フェーズでは，関係式探索フェーズで得られた関係式から，因子基底の対数値を解とする線形方程式を生成し，それを解く．

$$\log_g \mathfrak{p}_1, ..., \log_g \mathfrak{p}_{\#F_R(B)},\ \log_g \mathfrak{s}_1, ..., \log_g \mathfrak{s}_{\#F_A(B)}. \tag{11}$$

2.1.4　個別離散対数フェーズ

個別離散対数フェーズでは，最終目標であるターゲット T を special-Q decent 法 [39] を用いて因子基底の積として表す．それにより線形代数フェーズで求められた各因子基底に対する対数値を代入することで，ターゲットとなる対数値 $\log_g T$ を求めることができる．

$$\log_g T \equiv \sum_{\mathfrak{p}_i \in F_R(B)} a_i \log_g \mathfrak{p}_i + \sum_{\langle \mathfrak{p}_j, y - t_j\rangle \in F_A(B)} b_j \log_g \mathfrak{s}_j \tag{12}$$

2.2 ターゲットの選択

解読実験を行うにあたり，有限体 $\mathbb{F}_{3^{6\cdot 97}}$ 上のターゲットを決める必要がある．まず，$\mathbb{F}_{3^{97}}$ 上のペアリングとして $y^2 = x^3 - x + 1$ で定義される超特異だ円曲線 E を設定する．だ円曲線 E の位数は 151 ビットの素因子 $P_{151} = (3^{97} + 3^{49} + 1)/7$ を含む．だ円曲線 E においてこの P_{151} の位数をもつ部分群を $\mathbb{G}_1$ とする．

本実験では，ターゲットとして設定するパラメータの恣意性を排除するため，円周率 π 並びに自然対数の底 e を用いて次のように $\mathbb{G}_1$ 上の有理点 $\mathcal{Q}_\pi, \mathcal{Q}_e$ を設定する．同型写像 $\phi : \sum_{i=0}^{96} d_i x^i \mapsto \sum_{i=0}^{96} d_i 3^i \in \mathbb{Z}$ により 3^{97} 以下の自然数と $\mathbb{F}_3[x]/(x^{97} + x^{16} + 2)$ の要素への対応を用い，$x_\pi = \phi^{-1}(\lfloor \pi \cdot 3^{95} \rfloor + (11)_3)$，$x_e = \phi^{-1}(\lfloor e \cdot 3^{96} \rfloor + (120)_3)$ とする．これらの値から更に $y_\pi = (x_\pi^3 - x_\pi + 1)^{(3^{97}+1)/4}$，$y_e = (x_e^3 - x_e + 1)^{(3^{97}+1)/4}$ とし，だ円曲線上の有理点 $\mathcal{Q}_\pi = (x_\pi, y_\pi)$ と $\mathcal{Q}_e = (x_e, y_e) \in \mathbb{G}_1$ を抽出する．なお，x_π, x_e は，だ円曲線 E 上の有理点となるよう最小の補正を行っている．$\mathcal{Q}_\pi$, $\mathcal{Q}_e$ について，だ円曲線上の有理点のなす群における DLP (ECDLP (注3)) を以下のように設定する．

$$\mathcal{Q}_\pi = [s]\mathcal{Q}_e. \tag{13}$$

これは，η_T ペアリングの計算により，$\mathbb{F}_{3^{6\cdot 97}}$ 上の DLP に帰着される．

$$\begin{aligned} s &= \log_{\eta_T(\mathcal{Q}_\pi, \mathcal{Q}_e)} \eta_T(\mathcal{Q}_\pi, \mathcal{Q}_\pi) \qquad (14)\\ &= \log_g \eta_T(\mathcal{Q}_\pi, \mathcal{Q}_\pi) / \log_g \eta_T(\mathcal{Q}_\pi, \mathcal{Q}_e) \bmod P_{151} \end{aligned}$$

本実験では対数値 s を求めるために，$\log_g \eta_T(\mathcal{Q}_\pi, \mathcal{Q}_\pi)$, $\log_g \eta_T(\mathcal{Q}_\pi, \mathcal{Q}_e)$ を解読ターゲットとして $\mathbb{F}_{3^{6\cdot 97}}$ 上の DLP を解く．

次節以降，関係式探索と線形代数フェーズについて，JL06-FFS に対する改良点を中心に，計算機による解読実験で得られた結果を含めて述べる．

2.3 関係式探索フェーズの改良

標数 3 の拡大体 $\mathbb{F}_{3^{6\cdot 97}}$ 上の要素を計算機上で表現する際，$\mathbb{F}_{3^\kappa}[x]/(f)$ ($\kappa \in \{1, 2, 3, 6\}$) の 4 種類の表現方法が考えられる．これらの中から，関係式の抽出確率から算出される計算量並びに線形代数部の計算量を見積もった．全体として $\kappa = 3$ が最も効率的に解読できる値であったため，$\kappa = 3$ として選択する．これにより $d_H = 6, d_m = 33$ が決まる．更に $B = 6$ とする．

(注3)：EC は elliptic curve（だ円曲線）の略．

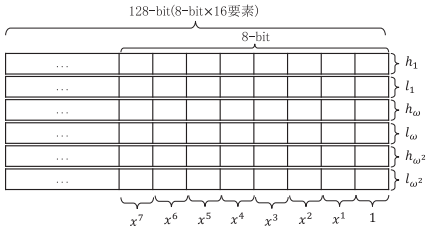


図 2　基礎体 $\mathbb{F}_{3^3}$ の表現方法
Fig. 2　Data structure of elements in $\mathbb{F}_{3^3}$.

関係式の抽出には格子篩 [37], [38], [42], [45] を用いている．格子篩は，関係式の探索空間 $(r, s) \in (\mathbb{F}_{3^3}[x])^2$ において，ある特定の因子基底 Q で割れるものだけを集めた空間 (この Q を special-Q，より簡単に sp-Q と呼ぶ) を利用する．Q に対応して決まる格子基底 $(r_1, s_1), (r_2, s_2)$ で張られる格子空間 $(r, s) = c(r_1, s_1) + d(r_2, s_2)$ 上では，因子基底の存在確率が上がることを利用した改良方式である．格子篩法では，(r, s) の代わりに，各 sp-Q に対し上記の (c, d) を探索する．この探索空間は c-d 空間と呼ぶ．なお，各 sp-Q から格子基底の選び方には任意性があるが，ここで，r_1, r_2 の選択方法として，$r_1 \equiv 0, r_2 \equiv 1 \pmod{x}$ と設定することで，c-d 空間における d の値を $d \equiv 1 \pmod{x}$ に限定することができ，c-d 空間における関係式の探索範囲を通常の方法に比べて 1/27 に削減できる．

解読実験では格子篩の実装プログラムの処理性能が，効率に大きく影響する．そのため，本実験では格子篩の実装で，数々の実装上の工夫を適用している．その幾つかを述べる．

基礎体 $\mathbb{F}_{3^3}$ の表現方法として，多項式剰余 $\mathbb{F}_3[\omega]/(\omega^3 - \omega - 1)$ を用いているが，本実装においては，その各要素を 6 ビットの値 $(h_1, \ell_1, h_\omega, \ell_\omega, h_{\omega^2}, \ell_{\omega^2}) \in \mathbb{F}_2^6$ として表現する．これにより基礎体上の演算をレジスター 6 個を用いて統一的に行うことができる (図 2 参照)．また，関係式探索フェーズでは，因子基底として 6 次式以下 (7 ビットで表現) を扱うため，各々を 8 ビットに割り当てることで，128 ビットのレジスタに 16 個の要素を収めることができる．これにより計算機がもつレジスタサイズを最大限利用し，並列度を上げることが可能となり，処理性能を大きく向上させることができる．これらの改良により，オリジナルと比較して約 6 倍の処理性能向上が達成されている．

実際の解読実験では，この格子篩プログラムを 47

台の PC (計 212 CPU コア) で並列に計算させ，関係式探索を行った．実験は 2011 年 5 月 14 日に開始し，同年 9 月 9 日に終了した．人為的ミスによる時間的ロスを含め，計 118 日かかっている．実際の計算機の稼働率から，計算に必要な実質的な計算機時間を算出すると，212 CPU コア (Xeon E5440) で，53.1 日と算出される．表 1 は，関係式探索フェーズのデータの詳細である．

2.4 線形代数フェーズの改良と実験結果

得られた関係式から，因子基底の対数値に関する線形方程式が生成されるが，そのままでは線形方程式が大きすぎるため，線形方程式を解く計算量が，必要以上に非常に大きくなってしまう．よって効率的に解を求めるためには，できる限り事前に線形方程式を圧縮しておく必要がある．そのために，Galois action, Singleton-clique, 更に Merge の技術等を適用し，圧縮を行っている．

Galois action は，Galois 群の作用により，空間 $\mathbb{F}_{3^{6\cdot 97}}/\mathbb{F}_{3^{3\cdot 97}}$ における自己同型写像を利用した方法である [29], [39]．この自己同型写像を用いることで，次の線形関係式が導かれる．$\log(\mathfrak{p}') = \tau\log(\mathfrak{p})$, $\log(\mathfrak{p}'') = \tau^2\log(\mathfrak{p})$, $\tau = 3^{97^2} \bmod P_{151}$．ただし，$\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$ は，次数が等しい因子基底である．ほとんど全ての因子基底で上記を満たす 3 個の組が存在することから，この線形式を用いることで，解くべき線形方程式に現れる因子基底の個数を 1/3 に減らすことができる．ただし上記線形式を用いる際，そのまま代入するのでは，線形式の係数が 151 ビットに増えてしまうため，その後の処理の計算量が著しく増加してしまう．そこで，方程式の係数を τ 進数に変換して保持することで，Galois action 適用後の線形方程式の係数を 24 ビットに抑えて処理を行える工夫を行っている．

更に，方程式に重要度に応じた重みづけを行った上で，冗長な方程式を削除することで扱われる線形方程式の個数を削減する手順 (Singleton-clique), 並びにガウス消去法の一部を先行して実施することで，線形方程式の対象となる行列のサイズを削減する手順 (Merge) により，続く Lanczos 処理に関わる計算量を削減している．表 2 に行列圧縮の効果をまとめた．

得られた行列に対し，P_{151} を法とする Parallel Lanczos 法により，解を求める．各々12 CPU, 2 NIC をもつ 21 台の計算機を 7×3 に分割し，48 ポートの Gbit HUB に接続した環境に実装して計算を実施した．151 ビット整数の乗算剰余については，ASM 言語で最適化された Montgomery 乗算を実装した．計算は 2012 年 1 月 16 日に開始し，90 日後の同年 4 月 14 日に終了した．計算機の停止時間等を除くことで，実質的に 80.1 日必要であったと見積もられる (詳細については表 3 参照)．

表 1 関係式探索フェーズで収集された関係式の個数
Table 1 Number of collected relations in collecting relations phase.

格子篩	159032292 関係式 (2500000 sp-Q) (64.91 関係式/sp-Q, 389 秒/sp-Q)
	153815493 関係式（重複除去後） (2449991 sp-Q)
自明な関係式	33786299
計	187602242 (因子基底 134697663)

表 2 Galois action, Singleton-clique, Merge による行列圧縮
Table 2 Compressing matrix using Galois action, Singleton-clique and Merge.

手法	行列サイズ (#式 ×#変数)
入力	187602242 × 134697663
Galois action	159394665 × 45049572
Singleton-clique	14060794 × 14040791
Merge	6141443 × 6121440

表 3 Parallel Lanczos 法の計算時間
Table 3 Computational time of parallel Lanczos method.

計算時間/ループ	626.3 ミリ秒
同期時間/ループ	46.5 ミリ秒
通信時間/ループ	457.3 ミリ秒
合計時間/ループ	1130.1 ミリ秒
ループ回数	6121438
合計時間	80.1 日

2.5 最終ステップ並びに解読世界記録

最終ステップとして，**2.2** で示した解読ターゲット $\log_g \eta_T(\mathcal{Q}_\pi, \mathcal{Q}_e)$, $\log_g \eta_T(\mathcal{Q}_\pi, \mathcal{Q}_\pi)$ の値を求める．なお g としては，多項式 $t^3 - t - 1$ の根を ω としたとき $g = (x+\omega)^{(3^{6\cdot 97}-1)/P_{151}}$ と決める．ターゲットとなる対数値を有理化法並びに special-Q decent 法によって，因子基底の対数値の和の形で表現し，得られた式に因子基底の対数値を代入することで求める対数値が得られる．この計算には，168 CPU コアを用いて一つにつき 7.5 日間を必要とした．

$$\log_g \eta_T(\mathcal{Q}_\pi, \mathcal{Q}_e) \tag{15}$$
$$= 154096662595700795834782326842395703646965637 0$$
$$\log_g \eta_T(\mathcal{Q}_\pi, \mathcal{Q}_\pi) \tag{16}$$
$$= 163028195063550729566380917121783309697044989 4$$
$$s = \log_{\eta_T(\mathcal{Q}_\pi, \mathcal{Q}_e)} \eta_T(\mathcal{Q}_\pi, \mathcal{Q}_\pi) \tag{17}$$

表 4　$\mathbb{F}_{3^{6\cdot 97}}$ 上の DLP 計算時間
Table 4　Summary of time data for solving DLP over $\mathbb{F}_{3^{6\cdot 97}}$.

フェーズ	主な手法	時間 (日数)
関係式探索	格子篩	53.1
線形代数	parallel Lanczos 法	80.1
個別離散対数	有理化及び special-Q descent	15.0
合計		148.2

計算機環境：252 CPU コア

$$= 1752799584850668137730207306198131424550967300$$

最後に，この値が ECDLP の解 $\mathcal{Q}_\pi = [s]\mathcal{Q}_e$ となっていることを確認し，2012 年 4 月 24 日，ペアリング暗号解読の世界記録を達成した．今回の解読実験で必要となった計算量を表 4 に記載している．

3. 最新の評価結果

2012 年 12 月，関係式探索フェーズにおいて pinpointing と呼ばれる，篩とは異なる新たな手法が Joux によって提案され，関数体篩法 JL06-FFS に導入された [32]．更に 2013 年，Joux は pinpointing の方針に沿ったアルゴリズム [33] を提案することで，標数の小さい有限体 $\mathbb{F}_{q^k}$ 上の離散対数問題を解くために必要な計算量を $L_{q^k}(1/3)$ から $L_{q^k}(1/4+o(1))$ に削減することに成功した．このアルゴリズムを改良することで Barbulescu らは計算量が quasi-polynomial time となるアルゴリズムを提案した [10]．これらのアルゴリズム [10], [33] が属するアルゴリズムは Frobenius representation algorithm (FRA と略記) とよばれる [40].

FRA と篩の方針の違いを以下に説明する．双方とも関係式探索フェーズの計算コストを削減することが主な目的である．篩の狙いは多項式の割り算をマーキングで代行することで計算量を削減し，次数の小さい既約多項式の積で表される多項式 (B-smooth な多項式) を効率的に収集することである．FRA の方針は，次数の小さい既約多項式の積で表される多項式，例えば次のような多項式

$$\prod_{\beta\in\mathbb{F}_q}(y-\beta) = y^q - y. \tag{18}$$

に変数変換を施して B-smooth な多項式を効率良く収集することである．B-smooth となる確率の高い多項式をマーキングにより調べる篩とは異なり，変数変換により直接収集することができるため，関係式探索フェーズの計算量を大幅に削減でき，結果として全体の計算量を削減することに成功している．

3.1 Frobenius representation algorithm

この節では FRA に属するアルゴリズム [10], [33] の要点について簡潔に説明する．特に FRA のキーポイントは関係探索フェーズに適した拡大体の構成方法であり，Frobenius 写像の性質による式 (18) を利用することに注意されたい．(更に Barbulescu らはこの性質を Joux のアルゴリズム [33] の個別離散対数フェーズに適用することで，計算量を quasi-polynomial time に削減することに成功している [10]．) また，FRA におけるクンマー拡大の利点についても説明する．

3.1.1 多項式選択フェーズ

有限体 $\mathbb{F}_{q^k}$ 上の離散対数問題を解くために，技術的な理由から，位数がより大きい有限体 $\mathbb{F}_{q^{2k}}$ 上の離散対数問題を解く(注4)．小さい次数の多項式 $h_0, h_1 \in \mathbb{F}_{q^2}[x]$ と $h_1x^q - h_0$ の k 次の既約因子である $f \in \mathbb{F}_{q^2}[x]$ によって，有限体 $\mathbb{F}_{q^{2k}}$ を $\mathbb{F}_{q^2}[x]/(f)$ で表現する．ここで重要な性質として次が成り立つことに注意する：

$$x^q \equiv h_0 \cdot h_1^{-1} \pmod{f}. \tag{19}$$

また，有限体 $\mathbb{F}_{q^{2k}}$ の元は $k-1$ 次以下の $\mathbb{F}_{q^2}$ 係数の多項式で表されるため，この節での因子基底は全ての B 次以下で既約な $\mathbb{F}_{q^2}$ 係数の多項式と h_1 からなる集合とする．

3.1.2 関係式探索フェーズ

関係式探索フェーズにおいて一次多項式の離散対数を求めるために式 (18) の左辺が一次多項式の積で表される性質を利用する．また，$ad \neq bc$ なる $a, b, c, d \in \mathbb{F}_{q^2}$ に対して $y = (ax+b)/(cx+d)$ の変数変換を行うことで，一つの 1-smooth な多項式から複数の 1-smooth な多項式を生成する．すなわち，式 (18) から次の式を得る：

$$\begin{aligned}(cx+d)&\prod_{\beta\in\mathbb{F}_q}((a-\beta c)x+(b-\beta d))\\ &= (cx+d)(ax+b)^q - (ax+b)(cx+d)^q\\ &\equiv (cx+d)(a^qx^q+b^q)\\ &\quad -(ax+b)(c^qx^q+d^q) \pmod{f}.\end{aligned} \tag{20}$$

更に，式 (20) に式 (19) の性質を利用することで次の式を得る：

(注4)：$\mathbb{F}_{q^{2k}}$ 上の離散対数問題が解けることは，その部分体である $\mathbb{F}_{q^k}$ 上の離散対数問題も解けることを意味することに注意.

$$h_1(cx+d)\prod_{\beta\in\mathbb{F}_q}((a-\beta c)x+(b-\beta d)) \quad (21)$$
$$\equiv (cx+d)(a^q h_0+b^q h_1) -(ax+b)(c^q h_0+d^q h_1) \pmod f. \quad (22)$$

多項式 (22) の次数は $\max\{\deg h_0, \deg h_1\}+1$ であり，この値は h_0, h_1 の設定から小さいため，この多項式は高い確率で小さい次数の多項式の積に因子分解されることが見込まれる．多項式 (21) は h_1 と一次多項式の積であることから，多項式 (22) が一次の多項式の積に因子分解されれば，h_1 と一次多項式の離散対数を解とする線形方程式が得られる．このような線形方程式を q^2 個以上集めて連立線形方程式を生成する．二次以上の既約多項式も因子基底の元として利用する場合は，例えば B 次の既約多項式については $y=(ax^B+bx^{B-1}+\cdots+c)/(dx^B+ex^{B-1}+\cdots+f)$ のような変数変換を利用することで対応できる．

3.1.3 線形代数フェーズ

関数体篩法の場合と同様に関係探索フェーズで生成した線形方程式を線形代数フェーズで解く．この計算によって h_1 と因子基底の元の離散対数を得る．

3.1.4 個別離散対数フェーズ

個別離散対数フェーズでは与えられた元 $P(x)\in\mathbb{F}_{q^2}[x]$ の離散対数を $P(x)$ より次数の低い多項式の離散対数で表現する．これを再帰的に行うことで，$P(x)$ の離散対数を因子基底の離散対数で表すことができる．文献 [10] において，**3.1.2** で述べた方針が個別離散対数フェーズにも導入された．以下でその計算について説明する．

与えられた $P(x)\in\mathbb{F}_{q^2}[x]$ の次数を D とする．まず最初の目的として $m:=\lceil D/2\rceil$ 次以下の多項式と，$P(x)$ を含む $P(x)$ を変形した多項式の積で表される関係式を生成する．**3.1.2** と同様にして，式 (18) に対して $y=(aP(x)+b)/(cP(x)+d)$ の変数変換を行い，式 (19) を適用することで

$$(cP(x)+d)\prod_{\beta\in\mathbb{F}_q}((a-\beta c)P(x)+(b-\beta d)) \quad (23)$$
$$\equiv (cP(x)+d)(a^q\overline{P}(x^q)+b^q) -(aP(x)+b)(c^q\overline{P}(x^q)+d^q)$$
$$\equiv (cP(x)+d)(a^q\overline{P}(h_0/h_1)+b^q) -(aP(x)+b)(c^q\overline{P}(h_0/h_1)+d^q) \pmod f$$

を得る．ただし $\overline{P}(x)$ は $P(x)$ の係数を q 乗したものとする．式 (23) の両辺に h_1^D をかけて，更に $\tilde{P}(x):=h_1^D\overline{P}(h_0/h_1)$ とすることで次の合同式を得る：

$$h_1^D(cP(x)+d)\prod_{\beta\in\mathbb{F}_q}((a-\beta c)P(x)+(b-\beta d))$$
$$\equiv (cP(x)+d)(a^q\tilde{P}(x)+b^q h_1^D) -(aP(x)+b)(c^q\tilde{P}(x)+d^q h_1^D) \pmod f. \quad (24)$$

多項式 (24) の次数は高々$(\max\{\deg h_0, \deg h_1\}+1)D$ である．この多項式が m 次以下の多項式の積に因子分解されるときに目的の関係式が得られる．このような関係式で与えられる線形方程式を十分集めて連立線形方程式を生成し，$P(x)$ を除く $P(x)$ を変形した多項式に対応する変数を行列の操作などによって消去することで，$P(x)$ の離散対数を m 次の多項式の離散対数で表すことができる．

3.2 クンマー拡大の効果

クンマー拡大の性質を利用することができれば，線形代数フェーズで扱う連立代数方程式の変数の個数を減らすことができる．たとえば [33] の手法では，有限体 $\mathbb{F}_{q^k}$ において $k=q-1$ ならば，乗法群 $\mathbb{F}_q^*$ の生成元 g に対して $f(x)=x^{q-1}-g$, $h_0=gx$, $h_1=1$ とすることで有限体 $\mathbb{F}_{q^k}$ を表現する．このとき

$$(x+\theta)^q=x^q+\theta^q=g(x+\theta^q/g) \quad (25)$$

が成り立ち，$x+\theta^q/g$ の離散対数を $x+\theta$ の離散対数で表現できる．その結果，線形代数フェーズで扱う変数の個数を削減することができる．

3.3 標数が 2 または 3 の有限体における記録

この節では，標数が 2 または 3 である有限体上の離散対数問題に対する FRA の効率性に関する研究成果について報告する．まず数値実験に関してであるが，表 5 は標数が 2 または 3 である有限体上の離散対数問題に関する主な記録をまとめたものである(注5)．表 5 が示すように，FRA [21], [33] においてクンマー拡大，またはねじれクンマー拡大の性質などを適用できる場合は，9234-bit 長の離散対数問題の記録のように，大きな bit 長の離散対数問題が解かれている．それに比べて素数次拡大の場合の最高記録は 1279-bit 長の離散対数問題となっている．ペアリング暗号で利用され

(注5)：表 5 は，Joux らがまとめた離散対数問題に関するサーベイ論文 “The Past, evolving Present and Future of Discrete Logarithm” [30] の Table1 を編集し 2014 年 1 月以降の結果を追記したものである．

表 5　標数 2 または 3 の有限体における離散対数問題計算記録．表中の * の計算記録では (ねじれ) クンマー拡大による高速化を利用している．
Table 5　The history of records of solving discrete logarithm problems over finite fields of characteristic two or three. The symbol * means that the property of (twisted) Kummer extension is used for the computation.

日付	有限体の位数	ビット長	CPU 時間	アルゴリズム	著者	文献
1992	2^{401}	401	114000	[20]	Gordon, McCurley	[25]
2001.09	2^{521}	521	2000	[38]	Joux, Lercier	[38]
2001	2^{607}	607	>200000	[20]	Thomé	[49]
2005.09	2^{613}	613	26000	[38]	Joux, Lercier	[30]
2012.06	$3^{6\cdot 97}$	923	895000	[39]	Hayashi et al.	[28]
2013.02	$2^{2\cdot 7\cdot 127}$	1778*	220	[33]	Joux	[34]
2013.02	$2^{3^3\cdot 73}$	1971*	3132	[21]	Göloğlu et al.	[21]
2013.03	$2^{2^4\cdot 3\cdot 5\cdot 17}$	4080*	14100	[33]	Joux	[35]
2013.04	2^{809}	809	19300	[2], [39]	The Caramel Group	[8]
2013.04	$2^{2^3\cdot 3^2\cdot 5\cdot 17}$	6120*	750	[21], [33]	Göloğlu et al.	[22]
2013.05	$2^{2^3\cdot 3\cdot 257}$	6168*	550	[33]	Joux	[36]
2014.01	$3^{6\cdot 137}$	1303	888	[33]	Adj et al.	[6]
2014.01	$2^{2\cdot 3^5\cdot 19}$	9234*	398000	[33]	Granger et al.	[24]
2014.01	$2^{2^2\cdot 3\cdot 367}$	4404	52000	[33]	Granger et al.	[23]
2014.09	$3^{5\cdot 479}$	3796	8600	[33]	Joux, Pierrot	[40]
2014	$3^{6\cdot 163}$	1551	1201	[33]	Adj et al.	[6]
2014.10	2^{1279}	1279	35040	[33]	Kleinjung	[43]
2016.07	$3^{6\cdot 509}$	4841	1752000	[33], [40]	Adj et al.	[4]

る $\mathbb{F}_{3^{6\ell}}$ (ℓ は素数とする) に分類される有限体については，128-bit 安全性が見込まれていた有限体 $\mathbb{F}_{3^{6\cdot 509}}$ が 2016 年 7 月に解かれている．また，$\mathbb{F}_{2^{12\ell}}$ (ℓ は素数とする) の場合についても，128-bit 安全性が見込まれていた有限体 $\mathbb{F}_{2^{12\cdot 367}}$ が 2014 年 1 月に解かれている．

理論的な計算コストの評価では，192-bit 安全性が見込まれていた有限体 $\mathbb{F}_{3^{6\cdot 1429}}$ 及び $\mathbb{F}_{2^{4\cdot 3041}}$ における離散対数問題を解くことに必要な計算時間は，FRA [10] を用いることで，それぞれ $1/2^{96}$ 倍，$1/2^{63}$ 倍に削減できると Adj, Menezes, Oliveira, Henríquez らは見積もっている [7]．

4. むすび

ペアリング暗号の安全性は，有限体上の離散対数問題 (DLP) の困難性を根拠としている．本論文では，標数が小さい有限体を利用するペアリング暗号方式の安全性評価を目的として，標数が小さい有限体上の DLP の困難性について議論した．特に，η_T ペアリングの実装ベンチマークで広く利用されていた有限体 $\mathbb{F}_{3^{6\cdot 97}}$ 上の DLP を著者らが解いた成果について解説した．

また，この成果が発表された後，標数の小さい有限体上の DLP を解くアルゴリズムの研究で大きな進展があり，小さな標数の有限体上の DLP の計算可能な範囲が飛躍的に向上した（表 5）．本論文ではこれらの進展並びにその後の計算記録についても述べた．これらの結果から，小さな標数の有限体を用いたペアリング暗号方式を安全に運用するには，有限体の位数を従来よりもかなり大きくする必要があるため，実用上問題があると考えられている．最近のペアリング暗号の実装では，上記の結果の影響がない大きな標数の有限体を用いたペアリング写像が用いられている．

将来の展望: 情報技術の発展が進むにつれ利用される暗号は多岐にわたり，またそれらを安全に運用するために必要とされる安全性評価技術（関数体篩法など）も多種多様になっている．しかし，評価の対象が異なる安全性評価技術であっても，共通若しくは亜種にあたる部分的な計算アルゴリズム（格子篩，多項式を表現するデータ構造など）を使用することは多い．したがって，安全性評価の研究における長期的な観点によれば，一つの暗号の安全性評価技術の構築は他の暗号の安全性評価にも繋がっている．例えば，著者らは η_T ペアリング暗号の安全性を評価するために，関数体篩法の中で利用される格子篩法の改良を行った．この格子篩法は，RSA 暗号や素体を扱うペアリング暗号の安全性評価技術として利用される数体篩法でも利用されている．また著者らの研究で得られた，多項式演算に関する技術（多項式を表現するデータ構造）の知見も他の評価技術に広く応用されることが期待される．このように様々な暗号の安全性評価技術の知見の蓄積

によって，実際に使用されている暗号及び将来的に使用が見込まれる暗号の安全性評価技術が構築され，暗号の安全な運用が可能となっている．

文　献

[1] L.M. Adleman, “The function field sieve,” ANTS-I, LNCS 877, pp.108–121, 1994.

[2] L.M. Adleman and M.-D.A. Huang, “Function field sieve method for discrete logarithms over finite fields,” Inform. and Comput., vol.151, pp.5–16, 1999.

[3] O. Ahmadi, D. Hankerson, and A. Menezes, “Software implementation of arithmetic in F_{3^m},” WAIFI 2007, LNCS 4547, pp.85–102, 2007.

[4] G. Adj, I.C. Martinez, N.C. Cortes, A. Menezes, T. Oliveira, F.R. Henríquez, and L.R. Zamarripa, “Discrete Logarithms in GF(3^{6*509}),” https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;65bedfc8.1607.

[5] G. Adj, A. Menezes, T. Oliveira, and F.R. Henríquez, “Weakness of $\mathbb{F}_{3^{6\cdot 509}}$ for Discrete Logarithm Cryptography,” Pairing 2013, LNCS 8365, pp.20–44, 2013.

[6] G. Adj, A. Menezes, T. Oliveira, and F.R. Henríquez, “Computing Discrete Logarithms in $\mathbb{F}_{3^{6\cdot 137}}$ and $\mathbb{F}_{3^{6\cdot 163}}$ using Magma,” WAIFI 2014, LNCS 9061, pp.3–22, 2015.

[7] G. Adj, A. Menezes, T. Oliveira, and F.R. Henríquez, “Weakness of $\mathbb{F}_{3^{6\cdot 1429}}$ and $\mathbb{F}_{2^{4\cdot 3041}}$ for discrete logarithm cryptography,” Finite Fields and Their Applications, vol.32, pp.148–170, 2015.

[8] R. Barbulescu, C. Bouvier, J. Detrey, P. Gaudry, H. Jeljeli, E. Thomé, M. Videau, and P. Zimmermann, “Discrete Logarithm in GF(2^{809}) with FFS, PKC 2014, LNCS 8383, pp.221–238, 2014.

[9] P.S.L.M. Barreto, S. Galbraith, C. Ó hÉigeartaigh, and M. Scott, “Efficient pairing computation on supersingular Abelian varieties,” Des., Codes Cryptogr., vol.42, no.3, pp.239–271, 2007.

[10] R. Barbulescu, P. Gaudry, A. Joux, and E. Thomé, “A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic,” EUROCRYPT 2014, LNCS 8441, pp.1–16, 2014.

[11] P.S.L.M. Barreto, H.Y. Kim, B. Lynn, and M. Scott, “Efficient algorithms for pairing-based cryptosystems,” CRYPTO 2002, LNCS 2442, pp.354–368, 2002.

[12] J.-L. Beuchat, N. Brisebarre, J. Detrey, and E. Okamoto, “Arithmetic operators for pairing-based cryptography,” CHES 2007, LNCS 4727, pp.239–255, 2007.

[13] J.-L. Beuchat, N. Brisebarre, J. Detrey, E. Okamoto, M. Shirase, and T. Takagi, “Algorithms and arithmetic operators for computing the η_T pairing in characteristic three,” IEEE Trans. Comput., vol.57, no.11, pp.1454–1468, 2008.

[14] J.-L. Beuchat, N. Brisebarre, M. Shirase, T. Takagi, and E. Okamoto, “A coprocessor for the final exponentiation of the η_T pairing in characteristic three,” WAIFI 2007, LNCS 4547, pp.25–39, 2007.

[15] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” EUROCRYPT 2004, LNCS 3027, pp.506–522, 2004.

[16] D. Boneh and M. Franklin, “Identity-based encryption from the Weil pairing,” CRYPTO 2001, LNCS 2139, pp.213–229, 2001.

[17] D. Boneh, C. Gentry, and B. Waters, “Collusion resistant broadcast encryption with short ciphertexts and private keys,” CRYPTO 2005, LNCS 3621, pp.258–275, 2005.

[18] D. Boneh, B. Lynn, and H. Shacham, “Short signatures from the Weil pairing,” ASIACRYPT 2001, LNCS 2248, pp.514–532, 2001.

[19] S. Cavallar, “Strategies in filtering in the number field sieve,” ANTS-IV, LNCS 1838, pp.209–231, 2000.

[20] D. Coppersmith, “Fast evaluation of logarithms in fields of characteristic two,” IEEE Trans. Inf. Theory, vol.30, no.4, pp.587–593, 1984.

[21] F. Göloğlu, R. Granger, G. McGuire, and J. Zumbrägel, “On the function field sieve and the impact of higher splitting probabilities - Application to discrete logarithms in $\mathbb{F}_{2^{1971}}$ and $\mathbb{F}_{2^{3164}}$,” CRYPTO 2013, LNCS 8043, pp.109–128, 2013.

[22] F. Göloğlu, R. Granger, G. McGuire, and J. Zumbrägel, “Solving a 6120 -bit DLP on a desktop computer,” SAC 2013, LNCS 8282, pp.136–152, 2013.

[23] R. Granger, T. Kleinjung, and J. Zumbrägel, “Breaking ‘128-bit secure’ supersingular binary curves (or how to solve discrete logarithms in $\mathbb{F}_{2^{4\cdot 1223}}$ and $\mathbb{F}_{2^{12\cdot 367}}$),” CRYPTO 2014, LNCS 8617, pp.126–145, 2014.

[24] R. Granger, T. Kleinjung, and J. Zumbrägel, “Discrete logarithms in GF(2^9234),” https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;9aa2b043.1401, 2014.

[25] D.M. Gordon and K.S. McCurley, “Massively parallel computation of discrete logarithms,” CRYPTO’92, LNCS 740, pp.312–323, 1992.

[26] R. Granger, D. Page, and M. Stam, “Hardware and software normal basis arithmetic for pairing-based cryptography in characteristic three,” IEEE Trans. Comput., vol.54, no.7, pp.852–860, 2005.

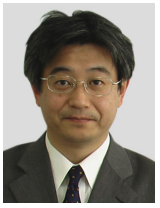
[27] D. Hankerson, A. Menezes, and M. Scott, “Software implementation of pairings,” Identity-Based Cryptography, pp.188–206, 2009.

[28] T. Hayashi, T. Shimoyama, N. Shinohara, and T. Takagi, “Breaking pairing-based cryptosystems using η_T pairing over $GF(3^{97})$,” ASIACRYPT 2012, LNCS 7658, pp.43–60, 2012.

[29] T. Hayashi, N. Shinohara, L. Wang, S. Matsuo, M. Shirase, and T. Takagi, “Solving a 676-bit discrete

logarithm problem in GF(3^{6n}),” PKC 2010, LNCS 6056, pp.351–367, 2010.
[30] A. Joux, A. Odlyzko, and C. Pierrot, “The past, evolving present and future of discrete logarithm,” Open Problems in Mathematical and Computational Science Book, Springer, 2014.
[31] A. Joux, “A one round protocol for tripartite Diffie-Hellman,” ANTS-IV, LNCS 1838, pp.385–394, 2000.
[32] A. Joux, “Faster index calculus for the medium prime case, Application to 1175-bit and 1425-bit Finite Fields,” EUROCRYPT 2013, LNCS 7881, pp.177–193, 2013.
[33] A. Joux, “A new index calculus algorithm with complexity $L(1/4 + o(1))$ in small characteristic,” SAC 2013, LNCS 8282, pp.355–379, 2013.
[34] A. Joux, “Discrete Logarithms in GF(2^1778),” https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;7d4dd9a6.1302, 2013.
[35] A. Joux, “Discrete Logarithms in GF(2^4080),” https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;71e65785.1303, 2013.
[36] A. Joux, “Discrete Logarithms in GF(2^6168) [=GF((2^257)^24)],” https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;49bb494e.1305, 2013.
[37] A. Joux et al., “Discrete logarithms in $GF(2^{607})$ and $GF(2^{613})$,” https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;48e40c30.0509, 2005.
[38] A. Joux and R. Lercier, “The function field sieve is quite special,” ANTS-V, LNCS 2369, pp.431–445, 2002.
[39] A. Joux and R. Lercier, “The function field sieve in the medium prime case,” EUROCRYPT 2006, LNCS 4004, pp.254–270, 2006.
[40] A. Joux and C. Pierrot, “Improving the polynomial time precomputation of frobenius representation discrete logarithm algorithms - Simplified setting for small characteristic finite fields,” ASIACRYPT 2014, LNCS 8873, pp.378–397, 2014.
[41] Y. Kawahara, K. Aoki, and T. Takagi, “Faster implementation of η_T pairing over $GF(3^m)$ using minimum number of logical instructions for $GF(3)$-addition,” Pairing 2008, LNCS 5209, pp.282–296, 2008.
[42] T. Kleinjung, K. Aoki, J. Franke, A.K. Lenstra, E. Thomé, J.W. Bos, P. Gaudry, A. Kruppa, P.L. Montgomery, D.A. Osvik, H.J.J. te Riele, A. Timofeev, and P. Zimmermann, “Factorization of a 768-Bit RSA modulus,” CRYPTO 2010, LNCS 6223, pp.333–350, 2010.
[43] Kleinjung, “Discrete Logarithms in GF(2^1279),” https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;256db68e.1410, 2014.
[44] T. Okamoto and K. Takashima, “Fully secure functional encryption with general relations from the decisional linear assumption,” CRYPTO 2010, LNCS 6223, pp.191–208, 2010.
[45] J.M. Pollard, “The lattice sieve,” The development of the number field sieve, LNIM 1554, pp.43–49, 1993.
[46] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” EUROCRYPT 2005, LNCS 3494, pp.457–473, 2005.
[47] 境　隆一，大岸聖史，笠原正雄，“Cryptosystems Based on Pairing,” 暗号と情報セキュリティシンポジウム予稿集，SCIS2000, 2000.
[48] N. Shinohara, T. Shimoyama, T. Hayashi, and T. Takagi, “Key length estimation of pairing-based cryptosystems using η_T pairing over $GF(3^n)$,” IEICE Trans. Fundamentals, vol.E97-A, no.1, pp.236–244, 2014.
[49] E. Thomé, “Computation of discrete logarithms in $\mathbb{F}_{2^{607}}$,” ASIACRYPT 2001, LNCS 2248, pp.107–124, 2001.

（平成 28 年 12 月 8 日受付，29 年 3 月 30 日再受付，
6 月 7 日早期公開）



高木　剛　（正員）

平 7 名古屋大学大学院理学研究科修士課程修了．同年日本電信電話株式会社入社．以降暗号理論の研究に従事．平 13 Dr.rer.nat．平 14 ダルムシュタット工科大学情報科学部助教授，平 17 公立はこだて未来大学システム情報科学部准教授，平 23 九州大学マス・フォア・インダストリ研究所教授．平 24 情報処理学会喜安記念業績賞，平 25 ドコモ・モバイル・サイエンス賞，平 26 本会業績賞，平 27 日本学術振興会賞各受賞．

下山　武司　（正員）

平 3 横浜市立大大学院修士課程了．同年 (株) 富士通研究所入社．以降暗号技術の研究に従事．H12 中央大学にて博士（工学）取得．平 9 SCIS 論文賞，平 24 同イノベーション論文賞，平 19 電気科学技術奨励賞，平 19 情報処理学会喜安記念業績賞，平 24 同賞，平 25 ドコモ・モバイル・サイエンス賞，平 26 本会業績賞各受賞．著書「気付力が夢を叶える！」など．

篠原　直行　（正員）

平 19 九州大学大学院博士課程了．同年科学技術振興機構研究員．博士（数理学）．平 21 立教大学博士研究員．同年情報通信研究機構入所．以来，計算数論・計算代数学の研究に従事．平 21 日本数式処理学会奨励賞，平 24 情報処理学会喜安記念業績賞，平 25 ドコモ・モバイル・サイエンス賞，平 26 本会業績賞各受賞．

林　　卓也　（正員）

平 22 公立はこだて未来大学大学院博士（前期）課程了．平 25 九州大学大学院博士後期課程了．同年九州大学マス・フォア・インダストリ研究所博士研究員．平 26 情報通信研究機構入所，現在に至る．公開鍵暗号の安全性に関する研究に従事．博士（機能数理学）．平 22 SCIS 論文賞，平 24 情報処理学会喜安記念業績賞，平 25 ドコモ・モバイル・サイエンス賞，平 28 CSS 最優秀論文賞各受賞．