種数 2 の超楕円曲線上に定義された η_T ペアリングの実装と標数 2 の有限体における離散対数問題

石井 将大† 猪俣 敦夫‡ 藤川 和利‡

†奈良先端科学技術大学院大学
〒 630-0192 奈良県生駒市高山町 8916-5

‡奈良先端科学技術大学院大学総合情報基盤センター
〒 630-0192 奈良県生駒市高山町 8916-5

あらまし ペアリングを用いた暗号技術の研究において，標数 2,3 等の小標数の定義体におけるペアリングの開発，実装は盛んに成されてきた．しかし，最近 A. Joux [17], F. Göloğlu et al. [13, 14] により比較的小さな標数を持つ，ある有限体における離散対数問題に対する効率的なアルゴリズムが提案され数々の数値実験が行われてきた．更に，R. Barbulescu et al. [5] において，ある小標数の有限体の離散対数問題に対する quasi-polynomial 時間の新たなアルゴリズムが提案された．

有限体の離散対数問題に対する効果的なアルゴリズムは，ペアリング暗号のセキュリティ強度に直接影響を与える．本研究では，標数 2 の定義体と種数 2 の超楕円曲線上の η_T ペアリングについて，最近の新たな離散対数問題に対するアルゴリズム [14, 5, 17] についてセキュリティレベルの考察を与え，種数 2 の超楕円曲線上に定義された η_T ペアリングの実装について評価を行う．

An Efficient Implementation of η_T Pairing on Genus 2 Hyperelliptic Curve and Discrete Logarithms in Finite Fields of Characteristic 2

Masahiro ISHII† Atsuo INOMATA‡ Kazutoshi FUJIKAWA‡

†Nara Institute of Science and Technology
8916-5 Takayama, Ikoma, NARA 630-0192 JAPAN
‡Information Initiative Center, Nara Institute of Science and Technology
8916-5 Takayama, Ikoma, NARA 630-0192 JAPAN

Abstract There are many efforts to exploit efficient algorithms and implement of parings over finite fields of small characteristic in researches for pairing-based cryptosystems. In the recent research about discrete logarithm in finite field, A. Joux [17] and F. Göloğlu et al.[13, 14] presented a new DLP algorithm and experimented with solving DLP in finite fields of small characterisitc using the new algorithm. R. Barbulescu et al.[5] presented a new quasi-polynomial algorithm for DLP in finite fields of small characteristic.

In this study, we consider security level of the η_T pairing on the hyperelliptic curve of genus 2 over the field of characteristic 2 with the new DLP algorithm [14, 5, 17], and perform implementation of the η_T pairing in appropriate security level.

1 序論

ペアリングは楕円曲線上の点の集合，或いは，超楕円曲線の Jacobian 上の群構造を保つ双線形写像であり，その数学的性質を用いて ID ベース暗号やブロードキャスト暗号，関数型暗号等に応用されている．最も高速に実装出来るペアリングとして，小標数の有限体を定義体に持つ超特異曲線上の η_T ペアリング [6] が挙げられ，これまでに様々な高速実装が行われてきた [15, 9, 11, 7, 4, 1].

本研究では Barreto ら [6] による定義体 $\mathbb{F}_{2^m}$ 上の種数 2 の超楕円曲線

$$C\colon y^2 + y = x^5 + x^3$$

を用いた η_T ペアリングを対象とし，そのセキュリティレベルと実装について評価する．この η_T ペアリングは次数 12 の distortion map により，定義体の 12 次拡大体 $\mathbb{F}_{2^{12m}}$ にその値が埋め込まれる．従って，η_T ペアリングの安全性は Jacobian における離散対数問題の困難性と，有限体 $\mathbb{F}_{2^{12m}}$ 上の離散対数問題の困難性が保証している．本研究では，最近の有限体上の離散対数問題に対する効率的なアルゴリズムの提案に関して，$\mathbb{F}_{2^{12m}}$ におけるセキュリティレベルに注目する．以下，離散対数問題を DLP とかく．

近年において，有限体上の離散対数問題に対する新たなアルゴリズムが提案され，実際に数値実験により比較的大きなサイズの体における離散対数問題が破られ，進展が見られている．ペアリングや有限体上の DLP の困難性セキュリティレベルに対する評価に用いられてきた一般的な指標として，Coppersmith [10] による準指数時間のアルゴリズムや，L. Adleman ら [3] による関数体篩法が挙げられる．しかし，小標数や，ある特別な条件を満たす有限体に対する DLP の解法として，quasi-polynomial 時間等の本質的に効率的なアルゴリズムが提案された．先の Coppersmith 法, 或いは関数体篩法 [3] の計算量は，L 記法

$$L_Q(\alpha, c) = \exp((c + o(1))(\log Q)^{\alpha}(\log\log Q)^{1-\alpha})$$

を用いて $L(\frac{1}{3}, (32/9)^{1/3})$ と表される．ここで，$Q = q^n$（q は素数冪）とし有限体 $\mathbb{F}_Q$ 上の DLP について考えるものとする．更に，$o(1)$ は n が無限大の時 0 となる関数である．2006 年，A. Joux と R. Lercier [18] により標数（或いは部分体）のサイズが中程度の有限体上の DLP に対するアルゴリズムが提案され，更に Joux のその Joux-Lercier アルゴリズムを ‘pinpointing’ という技術を用いて改良したアルゴリズム [16] によって，ある体における DLP について大幅な計算量の削減に成功している．具体的な計算量は第 2 節で示す．

2013 年，Joux は更にアルゴリズムを進化させ，[17] により heurictic な計算量として $(L(1/4, o(1))$ で計算可能な高速なアルゴリズムを提案した．又，独立的に F. Göloğlu et al.[13] により，Joux-Lercier アルゴリズムの一種として，特に標数 2 のある有限体上の DLP を解く高速なアルゴリズムを示し，数値実験 [14] も行われた．更に R. Barbulescu et al.[5] により，[17] の関数体篩法における descent フェーズにおいて，heuristic に quasi-polynomial 時間で計算可能なアルゴリズムを開発し，ある有限体上の DLP に対する quasi-polynomial アルゴリズムとして提案した．この様にして，特に小標数，中程度のサイズの標数を持つ有限体上の DLP に対し，実験的，理論的にこの研究分野の進展が起こっている．

DLP アルゴリズムの進化により，ペアリングのセキュリティレベルや，安全なペアリングパラメタについての評価は欠かせないものとなっている．G. Adj et al.[2] により，標数 3 の定義体における楕円曲線上の η_T ペアリングに関するセキュリティレベルの低下が報告された．Adj らは $\mathbb{F}_{3^{6\cdot 509}}$ 上の DLP に対し Joux, R. Barbulescu らのアルゴリズム [17, 5] を適用した結果として，林ら [22] による鍵長の見積もり結果である 111 bit（実際には Adj らは関係式生成フェーズの並列計算により，線形代数フェーズをボトルネックと考えて 102 bit と見ている）に対し，実際には 73 bit でしかないことを示した．本研究では，主に [2] を参考にして $\mathbb{F}_{2^{12m}}$ における DLP の困難性について考察を与え，特定の拡大次数 m に対し η_T ペアリングを実装し，評価を与える．

第 2 節において，本節で述べた DLP アルゴリズムについて，計算量とそのアルゴリズムにより高速に計算される有限体の条件について簡潔に示す．第 3 節において，実際に $\mathbb{F}_{2^{12m}}$ 上の DLP によるセキュリティレベルに関して考察を与える．

その考察を基に第 4 節において，ある拡大次数 m を固定し η_T ペアリングの実装を行い，評価を与える．終わりに第 5 節において結論を述べる．

2 小標数の有限体の離散対数問題とそのアルゴリズム

本節では，最近提案されている有限体の DLP アルゴリズムに関して，主に [2] を参考にしてそれぞれアルゴリズムの特徴を述べる．特に断らない限り有限体 $\mathbb{F}_Q$, $Q = q^n$（q は p 冪）上の DLP について考えているものとする．

2.1 関数体篩法と Joux-Lercier アルゴリズム

関数体篩法は index calculus method の一つであり，数体篩法と同様の計算を行う．即ち $\mathbb{F}_Q$ 上の関数体で計算が行われ，多項式が m-smooth であるとは各既約因子が m を超えないことであり，因子基底を決定して乗法的な関係式を集め，それぞれの基底の元における離散対数を求めることから最終的に目的の離散対数を得るという流れである．この時，関数体を構成する多項式，又，付随するパラメタによりアルゴリズム全体の計算量が大きく変わる．更に，入力である有限体のパラメタ q, n の形に依り漸近的に得られる計算量の評価が行われる．

Joux らは [18] において Adleman らのものとは違う形の関数体篩法を提案し，漸近的な計算量としてより良い結果を得た．即ち

$$q = \exp(3^{1/3}(\log Q)^{1/3}(\log\log Q)^{2/3}),$$
$$n = 3^{-1/3}\left(\frac{\log Q}{\log\log Q}\right)^{2/3}$$

とバランスがとれている時，

$$L_Q\left(\frac{1}{3}, 3^{1/3}\right) \approx L_Q(1/3, 1.442)$$

と出来る．これより，$\mathbb{F}_Q$ の形によっては，従来の Coppersmith method による計算量の見積もりは不正確なものになる．

関数体篩法に関し，因子基底の関係式生成における篩処理は計算量が大きな箇所であるが，Joux は [16] により pinpointing という技術によりこの篩処理の高速化に成功した．q と n が

$$q = \exp(3^{1/3}(\log Q)^{1/3}(\log\log Q)^{2/3}),$$
$$n = 3^{-1/3}\left(\frac{\log Q}{\log\log Q}\right)^{2/3}$$

の様な値を取る時，漸近的な計算量

$$L_Q\left(\frac{1}{3}, 2/3^{2/3}\right) \approx L_Q(1/3, 0.961)$$

が得られる．

2.2 小標数の有限体における DLP アルゴリズム

本節では，特に小標数の有限体上の DLP に有効なアルゴリズムについて，それらの最適なパラメタに対する漸近的計算量を述べる．Joux は [17] により有限体の構成法や Frobenius map による作用等を用いた効率的な関数体篩法の変形を提案し，アルゴリズムの計算量は

$$q \approx n,\ n = 2m$$

の時，

$$L_Q\left(\frac{1}{4}, 2/3^{2/3}\right) \approx L_Q(1/3, 0.961)$$

となる．因子基底の個別の離散対数を求める descent フェーズにおいて大幅な計算量の削減が達成されている．

Göloğlu は Joux とは独立に，binary field$q = 2\ell$ について拡大次数と ℓ に対してある条件を課し，Joux-Lercier アルゴリズムの変形として，効率的な DLP アルゴリズムを示した．[2] より，

$$n \approx 2^m d_1,\ d_1 \approx 2^m,\ m \mid \ell$$

の時，漸近的計算量は

$$L_Q\left(\frac{1}{3}, 2/3^{2/3}\right) \approx L_Q(1/3, 0.961)$$

となり，更に

$$n \approx 2^m d_1,\ 2^m \gg \ell,\ m \mid \ell$$

の時，漸近的計算量は

$$L_Q\left(\frac{1}{3},(2/3)^{2/3}\right)\approx L_Q(1/3,0.763)$$

から

$$L_Q\left(\frac{1}{3},1/2^{1/3}\right)\approx L_Q(1/3,0.794)$$

の間を取る．

3 $\mathbb{F}_{2^{12m}}$ における離散対数問題の困難性

本節では，binary field 上定義された種数 2 の超楕円曲線上の η_T ペアリングのセキュリティレベルに関して，12 次拡大体 $\mathbb{F}_{2^{12m}}$ の DLP に対する困難性について考察を与える．第 2 節において述べたそれぞれの DLP アルゴリズムと，漸近的計算量と関連する有限体の入力パラメタについて，その解読困難性を見積もる．

まず，$\mathbb{F}_{2^{12m}}$ においては，Coppersmith のアルゴリズムから 128 bit セキュリティレベルとして拡大次数 $m=367,439$ の場合のペアリングが実装されてきた．以下に Coppersmith のアルゴリズムと Joux-Lercier によるアルゴリズムの拡大次数 m に対する漸近的計算量の曲線のグラフを図 1 に示す．

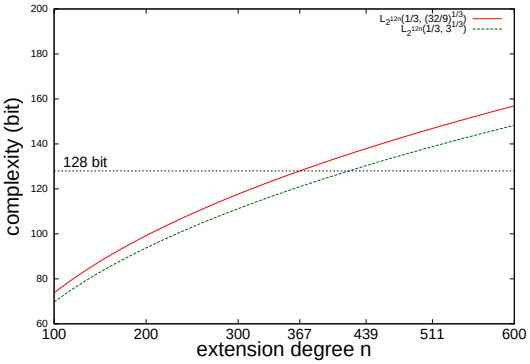

図 1: Coppersmith アルゴリズムと Joux-Lercier [18] の計算困難性

Joux-Lercier アルゴリズムに関しては q,n のバランスが取れているときは $n=367,439,511$ のときはそれぞれ $120.97, 130.32, 138.78$ bit セキュリティレベルとなるが，第 2 節で述べた q,n の関係を満たすには $\mathbb{F}_{2^{12m}}$ をある拡大体に埋め込まなければならない．従って，一概にどこまでセキュリティレベルが低下するかは実際に [22] にある様に厳密に計算して見積もる必要がある．これは Joux の pinpointing を用いた DLP アルゴリズム [16] についても同様で，関数体篩法の各段階で計算量の見積もりが必要だが，漸近的計算量が等しい Göloğlu [14] のアルゴリズムに関しセキュリティレベルの考察を与える．本研究ではセキュリティレベルの低下を見積もるため，拡大次数を大きめに取り $m=511$ の場合を考察する．この時，$\mathbb{F}_{2^{12m}}$ の n 拡大体を考えて，$2^{12n\cdot 511}=2^{12n\cdot(2^9-1)}$ から最低 $n=3$ でなければ条件

$$n\approx 2^m d_1,\ d_1\approx 2^m,\ m\mid \ell$$

を満たさない．よって $\mathbb{F}_{2^{12m}}$ の三次拡大体に対し，漸近的計算量は図 2 の様に表される．

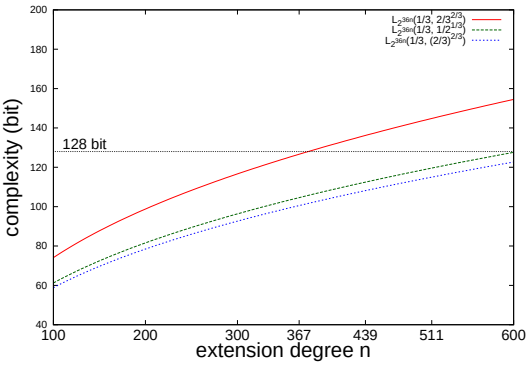

図 2: Göloğlu ら [13] による DLP アルゴリズムの計算困難性

少なくとも $m=511$ の時，Joux の pinpointing のアルゴリズムに対して n,q が釣り合うためには 10 次拡大を行う必要があり，128 bit セキュリティレベルを保っている様に見えるが，実際にアルゴリズムに各箇所の計算量をを厳密に見積もらなければならない．

最後に，[5, 17] の quasi-polynomial 時間の DLP アルゴリズムに関しては，[2, §5] の最後に標数 2 の場合の注意書きがあり，$m=367,439$ に対しては関数体篩法の関係式生成フェーズを 2^{40} プロセッサを用意したと仮定して並列計算することにより，初めて Joux-Lercier に優位性を持つとあり，

有効的ではなさそうである．$m = 511$ の時は明らかではないので，他のパラメタも合わせ今後正確に調べて行きたい．

4 種数 2 の超楕円曲線上の η_T ペアリングの実装と評価

本節では，$\mathbb{F}_{2^{12m}}$ に対する DLP の計算困難性についてセキュリティレベルの低下を考慮し，128 bit セキュリティレベルを仮定して $m = 511$ の場合の η_T ペアリングの評価を行う．η_T ペアリングはソフトウェア，ハードウェア上に高速に実装され [8, 12, 7, 4, 1]，数々の研究が行われてきた．FPGA 等，ハードウェア実装においては 128 bit セキュリティレベルのパラメタを取っても数 μ 秒オーダの高速化が成されている．本研究では開発環境 VC++により SIMD 実装を行った．開発環境の詳細を表 1 に表す．

OS	Windows 8
CPU	Intel Core i7-3520M, 2.90GHz, 2 Cores
Memory	DDR3-1333, 5.60 GB
Compiler	Visual C++ 2013 Preview
SIMD 命令セット	SSE2, 4.1, 4.2

表 1: 実装環境

この η_T ペアリングは 12 次拡大体が 6 次拡大を始めに行い，その上に二次拡大を行って構成されているが，我々はこの構成を変更し 3 次拡大の後に 2 次拡大を逐次的に行うことにより，特に Miller loop 内で行われるある計算（乗算 $\alpha\beta$）のコストを削減することにより高速化を行った．実装結果は表 2 の通りである，

拡大体の構成	実行時間
$\mathbb{F}_{2^{12m}}/\mathbb{F}_{2^{6m}}$	354.9
$\mathbb{F}_{2^{12m}}/\mathbb{F}_{2^{6m}}/\mathbb{F}_{2^{3m}}$	207.6

表 2: $\mathbb{F}_{2^{12\cdot 511}}$ 上の η_T ペアリングの実行時間 (ms)

SIMD 実装において，レジスタ幅は 128 として計算を行い，拡大体の乗算は Karatsuba 法，基礎体の乗算は事前計算無しの Comb method によるものである．実行時間から見ても，高速化の余地は大きくあり，ペアリングの高速化と，ペアリング暗号のパラメタにかんして，そのセキュリティレベルの厳密案評価は今後の課題とし早急に取り組みたい．

5 結論

本研究では，近年進展のある有限体の離散対数問題に対する効率的なアルゴリズムの研究に関し，binary field を定義体に持つ，種数 2 の超楕円曲線上の η_T ペアリングのセキュリティレベルについて，一考察を与え，又，実際にペアリングの実装評価を与えた．厳密に，新たな DLP アルゴリズムに対し，セキュリティレベルがどの程度低下するのかを見積もることは容易ではなく，本稿においても詳しい結果が得られるものでは無かった．今後の課題として，DLP アルゴリズムの詳細な振る舞いに対し詳細に計算量の見積もりを与えること，更に，それによりどの様な有限体のパラメタ，関連してペアリングのセキュリティパラメタとして不適切，或いは現在のところ安全といえるものをより正確に分類したい．

参考文献

[1] J. Adikari, M. A. Hasan, and C. Negre: Towards Faster and Greener Cryptoprocessor for eta Pairing on Supersingular Elliptic Curve Over $\mathbb{F}_2^{1223}$, *Selected Areas in Cryptography SAC 2012, Lecture Notes in Computer Science*, **7707**, pp. 166–183, Springer-Verlag, 2013.

[2] G. Adj, A. Menezes, T. Oliveira, and F. Rodríguez-Henríquez: Weakness of $\mathbb{F}_{3^{6\cdot 509}}$ for Discrete Logarithm Cryptography, Cryptology ePrint Archive, Report 2013/446, Available: `http://eprint.iacr.org/2013/446`, 2013.

[3] L. Adleman and M.-D. Huang: Function field sieve method for discrete logarithms over finite fields, *Information and Computation*, **151**, pp. 5–16, 1999.

[4] D. Aranha, J. Beuchat, J. Detrey, and N. Estibals: Optimal eta pairing on supersingular genus-2 binary hyperelliptic curves, *Topics in Cryptology CT-RSA 2012, Lecture Notes in Computer Science*, **7178**, pp. 98–115, Springer-Verlag, 2012.

[5] R. Barbulescu, P. Gaudry, A. Joux, and E. Thomé: A Quasi-polynomial Algorithm for Discrete Logarithm in Finite Fields of Small Characteristic, Cryptology ePrint Archive, Report 2013/400, Available: `http://eprint.iacr.org/2013/400`, 2013.

[6] P. S. L. M. Barreto, S. Galbraith, C. Ó hÉigeartaigh, and M. Scott: Efficient Pairing Computation on Supersingular Abelian Varieties, *Designs, Codes and Cryptography*, **42**, pp. 239–271, 2007.

[7] J. Beuchat, J. Detrey, N. Estibals, E. Okamoto, and F. Rodríguez-Henríquez: Fast Architectures for the η_T Pairing over Small-Characteristic Supersingular Elliptic Curves, *IEEE Transactions on Computers*, **60**(2), pp. 266–281, 2011.

[8] J. Beuchat, J. E. González-Díaz, S. Mitsunari, E. Okamoto, F. Rodríguez-Henríquez, and T. Teruya: High-Speed Software Implementation of the Optimal Ate Pairing over Barreto-Naehrig Curves, *Pairing 2010, Lecture Notes in Computer Science*, **6487**, pp. 21–39, Springer-Verlag, 2010.

[9] J. Beuchat, E. López-Trejo, L. Martínez-Ramos, S. Mitsunari, and F. Rodríguez-Henríquez: Multi-core Implementation of the Tate Pairing over Supersingular Elliptic Curves, *Proceedings of the 8th International Conference on Cryptology and Network Security, CANS '09, Lecture Notes in Computer Science*, **5888**, pp. 413–432, Springer-Verlag, Berlin, Heidelberg, 2009.

[10] D. Coppersmith: Fast Evaluation of Logarithms in Fields of Characteristic Two, *IEEE Transactions on Information Theory*, **30**, pp. 587–594, 1984.

[11] N. Estibals: Compact hardware for computing the Tate pairing over 128-bit-security supersingular curves, *Pairing-Based Cryptography Pairing 2010, Lecture Notes in Computer Science*, **6487**, pp. 397–416, Springer-Verlag, 2010.

[12] S. Ghosh, Dipanwita, R. Chowdhury, and A. Das: High Speed Cryptoprocessor for η_T Pairing on 128-bit Secure Supersingular Elliptic Curves over Characteristic Two Fields, *CHES'11, Lecture Notes in Computer Science*, **6917**, pp. 442–458, Springer-Verlag, Berlin, Heidelberg, 2011.

[13] 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 $\mathbb{F}_{2^{3164}}$, Cryptology ePrint Archive, Report 2013/074, Available: `http://eprint.iacr.org/2013/074`, 2013.

[14] F. Göloğlu, R. Granger, G. McGuire, and J. Zumbrägel: Solving a 6120-bit DLP on a Desktop Computer, Cryptology ePrint Archive, Report 2013/306, Available: `http://eprint.iacr.org/2013/306`, 2013.

[15] D. Hankerson, A. Menezes, and M. Scott: Software implementation of pairings, *Identity-Based Cryptography*, **7881**, pp. 177–193, IOS Press, 2008.

[16] A. Joux: Faster Index Calculus for the Medium Prime Case Application to 1175-bit and 1425-bit Finite Fields, *Advances in Cryptology EUROCRYPT 2013, Lecture*

Notes in Computer Science, **7881**, pp. 177–193, Springer-Verlag, 2013.

[17] A. Joux: A New Index Calculus Algorithm with Complexity $L(1/4 + o(1))$ in Very Small Characteristic, Cryptology ePrint Archive, Report 2013/095, Available: `http://eprint.iacr.org/2013/095`, 2013.

[18] A. Joux and R. Lercier: The Function Field Sieve in the Medium Prime Case, *EUROCRYPT 2006, Lecture Notes in Computer Science*, **4004**, pp. 254–270, 2006.

[19] A. Joux, R. Lercier, Nigel P. Smart, and Frederik Vercauteren: The Number Field Sieve in the Medium Prime Case, *CRYPTO 2006, Lecture Notes in Computer Science*, **4117**, pp. 326–344, Springer-Verlag, 2006.

[20] Y. Katoh, C. Cheng Y. Huang, and T. Takagi: Efficient Implementation of the EtaT Pairing on GPU, In *9th International Conference on Applied Cryptography and Network Security, ACNS 2011, Industrial Track*, pp. 119–133, 2011.

[21] A. K. Lenstra: Unbelievable Security. Matching AES Security Using Public Key Systems, *ASIACRYPT 2001, Lecture Notes in Computer Science*, **2248**, pp. 67–86, Springer-Verlag, 2001.

[22] N. Shinohara, T. Shimoyama, T. Hayashi, and T. Takagi: Key Length Estimation of Pairing-Based Cryptosystems Using η_T Pairing, *Information Security Practice and Experience - ISPEC 2012, Lecture Notes in Computer Science*, **7232**, pp. 228–244, Springer-Verlag, 2012.