離散対数問題の困難性に関する調査
関数体篩法の近年の改良とその影響について

2014 年 2 月作成 (2015 年 2 月更新)

概 要

ペアリング暗号の安全性は, 楕円曲線上の離散対数問題と有限体上の離散対数問題を解く計算の困難性を基盤としている. 即ちそれらの離散対数問題の内で一つでも解くことができればペアリング暗号は解読されてしまう. 有限体上の離散対数問題を効率よく解く手法として数体篩法と関数体篩法が挙げられ, 前者は標数が大きい有限体に, 後者は標数の小さい有限体の場合に適している. 近年, 関数体篩法の改良で大きな進展があった. これまで関数体篩法の関係探索段階において, sieving (篩) と呼ばれる手法が採用されてきたが, 近年は pinpointing に代表される新たな手法 (Frobenius representation algorithm など) が提案され, さらに Kummer extension の性質などが利用できる有限体では計算量が大きく削減される. 一方で, 標数の大きい有限体上の離散対数問題に適した数体篩法の改良も進んではいるものの, 関数体篩法ほどの計算量の改善は現在まで報告されていない.

本稿では, ペアリング暗号に適した標数の小さい有限体上の離散対数問題において, 上記の新たな手法を導入した関数体篩法に関する近年の研究報告について簡単に説明する. 特に重要な事実として, Kummer extension などの性質の利用が有効でない, ペアリング暗号で利用される標数の小さな有限体上の離散対数問題に対しても, 新たな手法の有効性を示す研究報告を挙げる.

最後に, 関数体篩法や数体篩法を有効に適用するには, 拡大次数の大きさと部分体の大きさの比などが関係するため, ペアリング暗号の安全性は推奨された有限体ごとに評価される必要があることを注意として挙げる.

1 概説

有限体上の離散対数問題を解く計算の困難性はペアリング暗号の安全性の基盤となっており, 有限体はペアリング暗号の安全性を決定する重要な暗号パラメータとみなされる. さらに, 有限体はペアリング暗号の暗号処理速度にも影響を及ぼすため, 安全性と実用性の双方を考慮して有限体の設定を行う必要がある.

標数が大きい有限体上の離散対数問題を解くことに適したアルゴリズムとして数体篩法が知られており, 同様に標数が小さい場合については関数体篩法が適していることが知られている. 特に標数が小さい場合については下記の三種の有限体に関連付けられるペアリング暗号の研究が盛んに行われている: (i) 標数が 3 で拡大次数が 6ℓ (ℓ は素数, 以下同様) の有限体 $GF(3^{6\ell})$, (ii) 標数が 2 で拡大次数が 4ℓ の有限体 $GF(2^{4\ell})$, (iii) 標数が 2 で拡大次数が 12ℓ の有限体 $GF(2^{12\ell})$. これらの有限体を使用するペアリング暗号の安全性を評価するために, 各々の有限体に適した関数体篩法の研究が様々な組織によって行われている.

関数体篩法では関係探索段階において, sieving (篩) によって relation と呼ばれる, モニックで既約な次数の小さい多項式 (因子基底) の積で表される多項式を生成し収集する. この relation から各因子基底の離散対数を解とする線型方程式が得られ, この後の線型代数段階でその線型方程式を解く. 後述の新しい手法である pinpointing の戦略に沿った手法が登場するまではこの二つの段階の計算量が関数体篩法の計算量を決定していた [1]. Pinpointing は sieving に代わる手法として Joux によって 2012 年に提案された [14].

[1]関数体篩法の一種で, 漸近的な計算量が quasi-polynomial である Frobenius Representation algorithm [5] の計算量は, 関係探索段階や線型代数段階ではなく, 与えられた離散対数問題を解く段階である個別離散対数計算段階 (Individual Logarithm Phase) の計算量で見積もられる. しかし, Joux と Pierrot らの ASIACRYPT 2014 のスライドに書かれているように, Frobenius Representation algorithm においても, 実際の計算では線型代数段階の計算コストが最も大きい場合が多い.

Sieving では, 篩区間に対応する relation の候補である各多項式に対して, ある因子基底を因子として持つものを, その因子基底による割り算をほとんどすることなく, マーキングのみを行うことで収集していた. 即ち sieving の利点は, 多項式の割り算をマーキングで代用することで, relation の候補となる各多項式に対する計算コストを削減することである. しかし, 候補となる多項式の数は膨大である. Pinpointing では, 小さな次数の既約多項式の積で表される多項式を探し, その多項式から複数の同様な異なる多項式を大量に生成する. Pinpointing の狙いは, 一つの relation を得るために必要な候補の多項式の個数を少なくすることである. 有限体 $GF(q^n)$ 上の離散対数問題を解く場合に, $Q := q^n$ と書くことにして, 関数体篩法の計算量を表すために次の関数を用意する:

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

但し $0 < \alpha < 1$ で $c > 0$ とする.

以下で, 関数体篩法の計算量が改善される, 近年までの経緯について簡単に紹介する. (この部分については Adj, Menezes, Oliveira, Henríquez らの原稿に詳しく書かれている [2].) 2006 年に Joux と Lercier によって提案された関数体篩法の計算量は,

$$q = L_Q(1/3, 3^{-2/3}),\ n = 3^{2/3}(\log Q/\log\log Q)^{2/3}$$

の場合に $L_Q(1/3, 1.44)$ であったが, この関数体篩法に pinpointing を適用することにより, その計算量は $L_Q(1/3, 0.96)$ に削減された. その結果 Joux は 1425-bit の有限体 $GF(p^{57})$ ($p = 33341353$ とする) 上の離散対数問題を解くことに成功した.

2013 年, Joux は pinpointing の方針に沿って改良された手法を導入することによって,

$$q \approx n/2$$

の場合に $L_Q(1/4 + o(1), c)$ となるアルゴリズムを提案し, 6168-bit の有限体 $GF(2^{8\cdot 3\cdot 257})$ 上の離散対数問題を解いた [16]. さらに, 同年, Barbulescu, Gaudry, Joux と Thomé は [16] の最後の計算段階を改良することによって

$$q \approx n,\ n \leq q + 2$$

の場合に有限体 $GF(q^{2n}) = GF(Q)$ 上の離散対数問題を解く計算量を quasi-polynomial time

$$(\log Q)^{O(\log\log Q)}$$

に改良することに成功した [5]. 注意すべきはこの計算量が, 任意の $0 < \alpha < 1$ と $c > 0$ に対して, $L_Q(\alpha, c)$ より漸近的に小さいことである. これら [5, 16] の種の手法は Frobenius representation algorithm と呼ばれる [22].

最後に, 上述のように関数体篩法の計算量は適用する有限体の大きさだけではなく, 部分体の大きさと拡大次数の大きさの比などの影響も受ける. 従って, ペアリング暗号の安全性は, 推奨された暗号パラメータごとに評価される必要がある.

2 小さい標数の有限体を使用するペアリング暗号への影響

この節では, 小さい標数の有限体を使用するペアリング暗号への Frobenius representation algorithm が与える影響に関する研究成果について紹介する. 結論としては, 数値実験の報告においても理論値によるその安全性評価の報告においても, 小さい標数の有限体を使用するペアリング暗号の安全性がそれ以前の見積もりより低くなることを意味する結果が報告されている.

表 1: 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記録. 表中の * は Kummer extension または twisted Kummer extension の性質を適用されたことを意味する.

Date	Field	Bitsize	CPU-hours	Algorithm	Authors	Reference
1992	$GF(2^{401})$	401	114000	[6]	Gordon, McCurley	[11]
2001.09	$GF(2^{521})$	521	2000	[19]	Joux, Lercier	[19]
2001	$GF(2^{607})$	607	> 200000	[6]	Thomé	[24]
2005.09	$GF(2^{613})$	613	26000	[19]	Joux, Lercier	[21]
2012.06	$GF(3^{6\cdot 97})$	923	895000	[20]	Hayashi et al.	[13]
2013.02	$GF(2^{2\cdot 7\cdot 127})$	1778*	220	[16]	Joux	[15]
2013.02	$GF(2^{3^3\cdot 73})$	1971*	3132	[7]	Göloğlu et al.	[7]
2013.03	$GF(2^{2^4\cdot 3\cdot 5\cdot 17})$	4080*	14100	[16]	Joux	[17]
2013.04	$GF(2^{809})$	809	19300	[1, 20]	The Caramel Group	[4]
2013.04	$GF(2^{2^3\cdot 3^2\cdot 5\cdot 17})$	6120*	750	[7, 16]	Göloğlu et al.	[8]
2013.05	$GF(2^{2^3\cdot 3\cdot 257})$	6168*	550	[16]	Joux	[18]
2014.01	$GF(3^{6\cdot 137})$	1303	888	[16]	Adj et al.	[3]
2014.01	$GF(2^{2\cdot 3^5\cdot 19})$	9234*	398000	[16]	Granger et al.	[9]
2014.01	$GF(2^{2^2\cdot 3\cdot 367})$	4404	52000	[16]	Granger et al.	[10]
2014.09	$GF(3^{5\cdot 479})$	3796	8600	[16]	Joux, Pierrot	[22]
2014	$GF(3^{6\cdot 163})$	1551	1201	[16]	Adj et al.	[3]
2014.10	$GF(2^{1279})$	1279	35040	[16]	Kleinjung	[23]

まず数値実験に関してであるが, 表 1 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 [2]. 表 1 が示すように, Frobenius representation algorithm ([7, 16]) において Kummer extension または twisted Kummer extension 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る (i) $GF(3^{6\ell})$ (ℓ は素数とする) に分類される有限体については, 素数次拡大の有限体に次いで計算コストの高い有限体に分類でき, $GF(3^{6\cdot 137})$ や $GF(3^{6\cdot 163})$ の場合が解かれている. 従って $\ell \leq 163$ である有限体 $GF(3^{6\ell})$ 上の離散対数問題が現実的な時間内で解かれることが見込まれる. また, (iii) $GF(2^{12\ell})$ (ℓ は素数とする) の場合については, 128-bit 安全性が見込まれていた有限体 $GF(2^{12\cdot 367})$ の場合が解かれている. 従って, その部分体である $GF(2^{4\cdot 367})$ 上の離散対数問題も解くことが可能であるため, $\ell \leq 367$ である有限体 $GF(2^{12\ell})$ と 有限体 $GF(2^{4\ell})$ 上の離散対数問題は現実的な時間内で解かれることが見込まれる.

理論的な安全性評価については, Adj, Menezes, Oliveira, Henríquez らは, Frobenius representation algorithm ([5]) を用いた場合, 特に 128-bit 安全性が見込まれていた有限体 $GF(3^{6\cdot 509})$ の場合は 73.7-bit 安全性と見積もっている [2]. また, Granger, Kleinjung, Zumbrägel らは体の表現を工夫することにより, 同じく 128-bit 安全性が見込まれていた有限体 $GF(2^{4\cdot 1223})$ を使用した場合は 59-bit 安全性と見積もっている [10].

[2] 表 1 は, Joux らがまとめた離散対数問題に関するサーベイ集 “The Past, evolving Present and Future of Discrete Logarithm” [21] の Table 1 を編集し 2014 年 1 月以降の結果などを追記したものである.

3 Pinpointing を用いた関数体篩法の概要

表 1 が示すように, Frobenius representation algorithm は, 標数が小さい有限体上の離散対数問題を現時点で最も効率よく解く手法である. Frobenius representation algorithm の新たな方針は, 関係探索段階において sieving とは異なる手法で relation を効率よく生成することである. この方針が最初に採用されたのは関数体篩法 JL06-FFS [20] の 関係探索段階において pinpointing を導入した手法である [14]. この節では pinpointing 用いた関数体篩法について簡単に説明する. Frobenius representation algorithm [16, 5] については Hayashi が参考文献 [12] で簡明に説明している.

3.1 標数が小さい場合の関数体篩法の例

まず, 関数体篩法 JL06-FFS [20] について簡単に説明する. 有限体 $\mathbb{F}_{q^n}$ 上の DLP を JL06-FFS で解く場合, 二つの多項式 $f_1(x,y) = x - g_1(y), f_2(x,y) = -g_2(x) + y \in \mathbb{F}_q[x,y]$ を用意する. 但し g_1 と g_2 の次数をそれぞれ d_1, d_2 とし, $-g_2(g_1(y)) + y$ は $\mathbb{F}_q$ 上で既約な n 次多項式 $f(y)$ を因子として持つとする. さらに次数 d_1, d_2 と因子基底の最大次数 D は, $d_1 \approx \sqrt{Dn}$ と $d_2 \approx \sqrt{n/D}$ が成り立つように設定される.

この関数体篩法の関係探索段階では,

$$\mathcal{A}(y)g_1(y) + \mathcal{B}(y) = \mathcal{A}(g_2(x))x + \mathcal{B}(g_2(x))$$

の両辺が D-smooth となる一変数の $\mathbb{F}_q$ 係数多項式の組 $(\mathcal{A}(z), \mathcal{B}(z))$ を集める. 但し, $\mathcal{A}(z), \mathcal{B}(z)$ の次数は D 以下とし, さらに $\mathcal{A}(z)$ はモニックとする.

JL06-FFS の計算量は, $q = L_{q^n}(1/3, \alpha D)$ のとき, 関係探索段階の計算量は $L_{q^n}(1/3, c_1)$, 線型代数段階のそれは $L_{q^n}(1/3, c_2)$ となる. ただし

$$c_1 = \frac{2}{3\sqrt{\alpha D}} + \alpha D,\ c_2 = 2\alpha D$$

で, 次の条件が成り立つとする：

$$(D+1)\alpha \geq \frac{2}{3\sqrt{\alpha D}}.$$

3.2 Pinpointing

簡単な例として, 関数体篩法 JL06-FFS において $D = 1$ とした場合で, pinpointing について説明する. まず, $g_1(y) = y^{d_1}$ と設定し, $D = 1$ より $\mathcal{A}(z) = z + a$, $\mathcal{B}(z) = bz + c$ であることから, 次の形の relation の候補について考える:

$$y^{d_1+1} + ay^{d_1} + by + c = xg_2(x) + ax + bg_2(x) + c. \tag{1}$$

この両辺が 1 次多項式の積に分解できる (1-smooth である) 場合に relation が得られる.

3.2.1 One-sided pinpointing

式 (1) の左辺が 1-smooth であることと, $y = au$ とした場合に, 多項式 $u^{d_1+1} + u^{d_1} + ba^{-d_1}u + ca^{-d_1-1}$ が 1-smooth であることは同値である. 従って, $u^{d_1+1} + u^{d_1} + Bu + C \in \mathbb{F}_q$ の形の多項式に注目して, これが 1-smooth となる (B, C) が得られれば, その一つの (B, C) から $q - 1$ 個の 1-smooth な多項式 $y^{d_1+1} + ay^{d_1} + by + c$ が得られる. ($a \in \mathbb{F}_q^*$ に対して $b = Ba^{d_1}, c = Ca^{d_1+1}$ とする.)

一つの 1-smooth な $u^{d_1+1}+u^{d_1}+Bu+C$ を得るために, 漸近的に $(d_1+1)!$ 個の候補が必要である. 従って (1) の左辺については $(d_1+1)!+(q-1)$ 個の候補が存在する. またそのときの $q-1$ 個の $a\in\mathbb{F}_q^*$ に対して, (1) の右辺が 1-smooth になる個数の期待値は $(q-1)/(d_2+1)!$ であることから, 一つの relation を得るために必要な候補の期待値は

$$\frac{(d_1+1)!+(q-1)}{(q-1)/(d_2+1)!}=\frac{(d_1+1)!(d_2+1)!}{q-1}+(d_2+1)!$$

となり, sieving の場合の $(d_1+1)!(d_2+1)!$ 個に比べてずっと小さい.

3.2.2 Kummer extensions, Frobenius and advanced pinpointing

拡大次数 n が d_1d_2-1 である Kummer extension の場合に, 式 (1) の両辺に pinpointing を行うことができる. さらに線型方程式の変数を実質的に $1/n$ 倍に減らすことができる.

有限体 $\mathbb{F}_q$ は 1 の原始 n 乗根 μ を含むとする. このとき $\mathbb{F}_q$ 上の n 次の Kummer extension は $P(x)=x^n-K$ で定義される. (K の設定に注意.) K の n 乗根 κ で $\kappa^q=\mu\kappa$ となるものが存在し,

$$P(x)=\prod_{i=0}^{n-1}(x-\mu^i\kappa)$$

とかける. そのような Kummer extension において, $g_1(y),g_2(x)$ を次のように定義する:

$$g_1(y)=y^{d_1}/K,\ g_2(x)=x^{d_2}. \tag{2}$$

このとき $x=g_1(y)$, $y=g_2(x)$ であることから, $x^{d_1d_2}-Kx=0$ となり両辺を x で割ることで $P(x)$ を得る.

$D=1$ で考えていることから因子基底は, $w\in\mathbb{F}_q$ に対して $x+w$ や $y+w$ の形をしている. これらの多項式は Frobenius map によって,

$$\begin{aligned}(x+w)^q &= x^q+w=\mu x+w=\mu(x+w/\mu),\\ (y+w)^q &= y^q+w=\mu y+w=\mu(y+w/\mu)\end{aligned}$$

となる. 従って, $\mathbb{F}_{q^n}^*/\mathbb{F}_q^*$ において,

$$\log(x+w/\mu)=q\log(x+q),\ \log(y+w/\mu)=q\log(y+q)$$

が成り立ち, 線型方程式の変数を減らすことができる.

One-side pinpointing のとき, 即ち式 (1) の場合と同様にして,

$$x^{d_2+1}+bx^{d_2}+ax+c=y^{d_1+1}/K+ay^{d_1}/K+by+c \tag{3}$$

について考える. 式 (3) の右辺が 1-smooth であることと, $u^{d_2+1}+u^{d_2}+ab^{-d_2}u+cb^{-d_2-1}$ が 1-smooth であることは同値であり, 同様に左辺については $v^{d_1+1}/K+v^{d_1}/K+ab^{-d_1}v+cb^{-d_1-1}$ が対応する. さらに $\lambda=c/(ab)$ とすることで, u,v を変数とするこれらの多項式はそれぞれ次のように書くことができる:

$$u^{d_2+1}+u^{d_2}+ab^{-d_2}(u+\lambda),\ (v^{d_1+1}+v^{d_1})/K+ab^{-d_1}(v+\lambda).$$

逆に (A,B,λ) を, $A\neq0$, $B\neq0$, AB^{d_2} が $\mathbb{F}_q$ において n 冪となり (Kummer extension を使用している), さらに

$$u^{d_2+1}+u^{d_2}+A(u+\lambda),\ (v^{d_1+1}+v^{d_1})/K+B(v+\lambda)$$

がそれぞれ 1-smooth となるように選ぶ. このとき, $A = ab^{-d_2}$, $B = ba^{-d_1}$ とすることで, $AB^{d_2} = a^{1-d_1 d_2} = a^{-n}$ から a を定めることができ, さらにその選び方は n とおりである. 各 a に対して $b = Ba^{d_1}$, $c = \lambda ab$ と定める.

最終的に relation 一つ当たりのコストは

$$O\left(\frac{n(d_1+1)!(d_2+1)!}{q-1}\right)+1$$

となるが, Frobenius map の効果で n を相殺できる.

3.3 計算量

$\mathbb{F}_{q^n}$ 上の離散対数問題を, pinpointing を導入した JL06-FFS で解くことを考える. ここで $Q = q^n$ とし, α は次を満たすとする:

$$\alpha = \frac{1}{n}\left(\frac{\log Q}{\log\log Q}\right)^{2/3}.$$

$D = 1$ とした場合に linear algebra step の計算量は $L_Q(1/3, 2\alpha)$ となる. $\alpha \geq 3^{-2/3}$ に対して, このコストは (双方の) pinpointing のコストより大きいため, 総計算量は $L_Q(1/3, 2\alpha)$ となる. $\alpha \in [3^{-2/3}, 2^{2/3})$ に対しては JL06-FFS よりも総計算量は小さくなり, とくに $\alpha = 3^{-2/3}$ のとき, 総計算量は $L_Q(1/3, 1.44)$ から $L_Q(1/3, 0.96)$ に減少する.

3.4 数値実験

まず, $p_1 = 33553771$, $p_2 = 33341353$ とする. このとき有限体 $\mathbb{F}_{p_1^{47}}$ と $\mathbb{F}_{p_2^{57}}$ の大きさはそれぞれ 1175-bit と 1425-bit となる. これらの有限体上の離散対数問題を Advanced pinpointing を使用して解く数値実験を行った場合, 双方とも 32000 CPU-hours を必要としたとの報告がある.

表 2: 文献 [14] の実験結果

Bitsize	Total time (CPU-hours)	Relation construction (CPU-hours)	Linear algebra (CPU-hours)	Indiv. Log. (CPU-hours)
1175	約 32000	3	32000	4
1425	約 32000	6	32000	< 12

4 更新履歴

更新日時	主な更新内容
2015 年 2 月	•概要を追加. •2 節. 表 1 とその解説を加筆.

参考文献

[1] L. M. Adleman, M-D. A. Huang, “Function field sieve method for discrete logarithms over finite fields,” Inf. Comput., 151 (1999), 5-16.

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

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

[4] R. Barbulescu, C. Bouvier, J. Detrey, P. Gaudry, H. Jeljeli, E. Thomé, M. Videau, P. Zimmermann, “Discrete Logarithm in $GF(2^{809})$ with FFS,” Proc. of Public Key Cryptography 2014, LNCS 8383 (2014), 221-238.

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

[6] D. Coppersmith, “Fast evaluation of logarithms in fields of characteristic two,” IEEE Transactions on Information Theory, 30/4 (1984), 587-593.

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

[8] F. Göloğlu, R. Granger, G. McGuire, J. Zumbrägel, “Solving a 6120-bit DLP on a Desktop Computer,” Proc. of SAC 2013, LNCS 8282 (2013), 136-152.

[9] R. Granger, T. Kleinjung, J. Zumbrägel, “Discrete Logarithms in GF(2^9234),” `https://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind1401&L=NMBRTHRY&F=&S=&P=8736`.

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

[11] D. M. Gordon, K. S. McCurley, “Massively Parallel Computation of Discrete Logarithms,” Proc. of CRYPTO 1992, LNCS 740 (1992), 312-323.

[12] T. Hayashi, “Cryptanalysis of Pairing-based Cryptosystems Over Small Characteristic Fields,” Proc. of the Forum of Mathematics for Industry 2013, 1 (2013), 167-176.

[13] T. Hayashi, T. Shimoyama, N. Shinohara, T. Takagi, “Breaking Pairing-Based Cryptosystems Using η_T Pairing over $GF(3^{97})$,” Proc. of ASIACRYPT 2012, LNCS 7658 (2012), 43-60.

[14] A. Joux, “Faster index calculus for the medium prime case. Application to 1175-bit and 1425-bit finite fields,” Proc. of EUROCRYPT 2013, LNCS 7881 (2013), 177-193.

[15] A. Joux, “Discrete Logarithms in GF(2^1778),” `https://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind1302&L=NMBRTHRY&F=&S=&P=2317`.

[16] A. Joux, "A new index calculus algorithm with complexity $L(1/4 + o(1))$ in small characteristic," Proc. of SAC 2013, LNCS 8282 (2013), 355-379.

[17] A. Joux, "Discrete Logarithms in GF(2^4080)," https://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind1303&L=NMBRTHRY&F=&S=&P=13682.

[18] A. Joux, "Discrete Logarithms in GF(2^6168) [=GF((2^257)^24)]," https://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind1305&L=NMBRTHRY&F=&S=&P=3034.

[19] A. Joux and R. Lercier, "The function field sieve is quite special," Proc. of ANTS 2002, LNCS 2369 (2002), 431-445.

[20] A. Joux and R. Lercier, "The function field sieve in the medium prime case," Proc. of EUROCRYPT 2006, LNCS 4004 (2006), 254-270.

[21] A. Joux, A. Odlyzko, C. Pierrot, "The Past, evolving Present and Future of Discrete Logarithm," Open Problems in Mathematical and Computational Science, Springer (2014), 5-36.

[22] A. Joux, C. Pierrot, "Improving the Polynomial time Precomputation of Frobenius Representation Discrete Logarithm Algorithms - Simplified Setting for Small Characteristic Finite Fields," Proc. of ASIACRYPT 2014, LNCS 8873 (2014), 378-397.

[23] Kleinjung, "Discrete Logarithms in GF(2^1279)," https://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind1410&L=NMBRTHRY&F=&S=&P=1170.

[24] E. Thomé, "Computation of Discrete Logarithms in $\mathbb{F}_{2^{607}}$," Proc. of ASIACRYPT 2001, LNCS 2248 (2001), 107-124.