数理解析研究所講究録
1514巻 2006年 39-45

$GF(3^m)$における Tate Pairing の計算および実装について

岩見 真希
Maki Iwami
筑波大学 システム情報工学研究科
Graduate School of Systems and Information Engineering, University of Tsukuba*

久保寺 範和
Norikazu Kubotera
日本電気株式会社 システム基盤ソフトウェア開発本部
System Platform Software Development Division, NEC Corporation†

側高 幸治
Koji Sobataka
日本電気株式会社 ユビキタスソフトウェア事業部
Ubiquitous Software Division, NEC Corporation‡

岡本 栄司
Eiji Okamoto
筑波大学 システム情報工学研究科
Graduate School of Systems and Information Engineering, University of Tsukuba§

1 はじめに

人とモノのＩＤ化が進むにつれ，プライバシ保護と信頼性確保の両立が課題となる．ユビキタス社会における快適な市民生活の実現，安心して経済活動が行える安全な社会の実現のために，情報セキュリティ対策として，匿名署名，分散認証，情報隔離などの技術を組み合わせた，プライバシ保護情報セキュリティシステムの醸成技術の開発が求められている．筆者らは，科学技術振興調整費 重要課題解決型研究等の推進 情報セキュリティに資する研究開発「セキュリティ情報の分析と共有システムの開発」において，匿名署名やグループ署名等の性能評価に関する研究として，特に楕円曲線上の pairing 計算のアルゴリズムとその理論的安全性の研究を行ってきた．楕円曲線上の pairing は，楕円曲線暗号の解読に応用されてきたという歴史をもつが，近年，その双線形性を ID ベース公開鍵暗号や Short Signature などに利用した暗号方式

*maki@risk.tsukuba.ac.jp (2006年4月より 大阪経済法科大学教養部 特別専任講師 maki@keiho-u.ac.jp)
†n-kubotera@bp.jp.nec.com
‡k-sobataka@bx.jp.nec.com
§okamoto@risk.tsukuba.ac.jp

が盛んに提案されている．一方，pairing 計算のアルゴリズムに関する論文も，例えば楕円曲線上のものだけでも，標数 p（p は大きな素数）では [3]，標数 3 では [2, 4, 5]，標数 2 では [2, 5] 等，様々な効率的なアルゴリズムが考案されてきている．ここでは，具体的には，Tate pairing について，各標数における拡大体での計算に着目し，それぞれ何次拡大まで計算すれば現実社会で求められている安全性の強度を満たすかを理論的に算出して比較する．また，安全性と効率性を考えて取り組んできた実装結果を報告する．

2 Tate pairing 写像について

楕円曲線上の点は，無限遠点 $\mathcal{O}$ を単位元として付加し，加法 "+" を次のように定義することで群をなす．

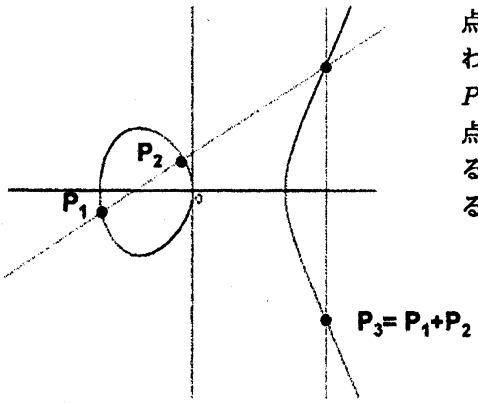

図 1: 楕円曲線上の加算

$y^2 = x^3 + ax + b$ (判別式 $D \neq 0$) (Weierstrass の標準形)，点 $P_1 = (x_1, y_1)$，点 $P_2 = (x_2, y_2)$ に対し，$P_1 + P_2$ であらわされる点 $P_3 = (x_3, y_3)$ を，図 1 でみられるように，直線 P_1P_2 と楕円曲線との交点を，x 軸に関して対称移動させた点で定義する．$P_1 = P_2$ のとき，直線 P_1P_2 は点 P_1 における接線と考えてよい（このとき，点 P_1 の 2 倍算を意味する）．P_3 の座標は，次の公式であらわすことができる．

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda(x_1 - x_3) - y_1 \end{aligned}$$

$$\lambda = \begin{cases} \dfrac{y_1 - y_2}{x_1 - x_2} & (x_1 \neq x_2) \\ \dfrac{3x_1^2 + a}{2y_1} & (x_1 = x_2,\ y_1 + y_2 \neq 0) \end{cases}$$

$q = p^m$ (p は素数，m は自然数)，E を有限体 $\mathbb{F}_q$ 上の楕円曲線，$E(\mathbb{F}_q)$ を E 上の $\mathbb{F}_q$ 有理点全体に無限遠点 $\mathcal{O}$ を単位元として加えた群，$E[\ell]$ を $\ell P = \mathcal{O}$ を満たす $P \in E(\mathbb{F}_q)$ から構成される $E(\mathbb{F}_q)$ の部分群，K を $E[\ell](\mathbb{F}_q) \subset E(\mathbb{F}_{q^k})$ を満たす最小の拡大次数とする．以下，ℓ は q と互いに素で，かつ $E(\mathbb{F}_q)$ の位数を割り切る素数とする．

$P, Q \in E[\ell](\mathbb{F}_q)$ とするとき，Tate pairing $e_\ell(\ ,\ )$ は，次で定義される写像である．

$$e_\ell(\ ,\ ) : E[\ell](\mathbb{F}_q) \times E[\ell](\mathbb{F}_{q^k}) \to \{\zeta_\ell\}\ (\subset \mathbb{F}_{q^k}^*),\quad e_\ell(P, \phi(Q)) = f_P(\phi(Q))^{(q^k-1)/\ell}$$

ここで，f_P は $(f_P) = \ell(P) - \ell(\mathcal{O})$ を満たす有利関数で，$\phi(Q)$ は (f_P) と disjoint なサポートをもつような $(Q) - (\mathcal{O})$ と equivalent な zero divisor で，Q に distorsion map ϕ を施して得ることができる．ここで $\{\zeta_\ell\}$ は $\mathbb{F}_{q^k}^*$ における 1 の ℓ 乗根のなす群をあらわす．

Tate pairing は，次の 3 つの性質をもつ．特に bilinearity の性質が，各種暗号方式を可能にしている．

- bilinearity : 任意の $P, P_1, P_2 \in E[\ell](\mathbb{F}_q)$, $Q, Q_1, Q_2 \in E[\ell](\mathbb{F}_{q^k})$ に 対して，
  $e_\ell(P_1 + P_2, Q) = e_\ell(P_1, Q)e_\ell(P_2, Q)$ かつ $e_\ell(P, Q_1 + Q_2) = e_\ell(P, Q_1)e_\ell(P, Q_2)$.
  すなわち，任意の $a \in \mathbb{Z}$ に対して，$e_\ell(aP, Q) = e_\ell(P, aQ) = e_\ell(P, Q)^a$ が成り立つ．
- non-degeneracy : 任意の $Q \in E[\ell](\mathbb{F}_{q^k})$ に対して $e_\ell(P, Q) = 1$ であるならば，$P = \mathcal{O}$.
  すなわち，$P \neq \mathcal{O}$ に対して，$e_\ell(P, Q) \neq 1$ なる $Q \in E[\ell](\mathbb{F}_{q^k})$ が存在する．
- compatibility : $\ell = h\ell'$ とする．$P \in E(\mathbb{F}_q)[\ell]$, $Q \in E(\mathbb{F}_{q^k})[\ell']$ ならば $e_{\ell'}(hP, Q) = e_\ell(P, Q)^h$.

3 安全性に関する各標数での理論計算

社会で求められている強度，1024-bit RSA と同等の安全性をもつためには，拡大次数は何次必要なのだろうか．ここでは，supersingular な楕円曲線について，埋め込み次数をそれぞれ，標数 2 では 4 次，標数 3 では 6 次，標数 p では 2 次にとり（こうすれば安全な曲線の生成について考えなくてよい），それぞれに必要な拡大次数を導出する．表 3 のように，標数 2 での拡大次数を m_1，標数 3 での拡大次数を m_2 とする．ここで，標数 p での pairing 計算のアルゴリズムでは，素数 p の値自体を大きくとり，埋め込み次数 2 次以外の拡大は行わないため 1 とおいた．ここで m_1 と m_2 は安全性の観点から素数とする．ここで，complexity の計算公式 $\mathrm{L}_{p^M}[a,c] := \mathrm{Exp}[(c+o(1))\mathrm{Log}[p^M]^a\mathrm{Log}[\mathrm{Log}[p^M]]^{1-a}]$ を用いる．a の値は，数体ふるい（標数が大きな素数 p のとき），および関数体ふるい（標数が 2 または 3）が使えることから 1/3 となる [26, 19]．また，c の値は，標数 p が大きいときは $(64/9)^{1/3} \fallingdotseq 1.923$，標数が 2 や 3 のように小さいときには $(32/9)^{1/3} \fallingdotseq 1.526$ となる [15, 24]．標数 2 のとき，[16, 17] を根拠に，c の値として 1.526 ではなく 1.351 を用いるのは，ありがちな間違いである．1.351 がみられるのは，式変形した別表現の公式の中である．後述の Appendix A を参照されたい．したがって，

$$\mathrm{L}_{2^{4m_1}}[1/3, 1.526] \fallingdotseq \mathrm{L}_{3^{6m_2}}[1/3, 1.526] \fallingdotseq \mathrm{L}_{2^{1024}}[1/3, 1.923]$$

を解くことで，標数 p における 1024-bit RSA の安全性を基準としたとき，標数 2 および 3 で同等の安全性をもつためには，拡大次数 m_1 および m_2 はそれぞれどの程度必要か，また，そのとき何 bit 必要になるのかを，次のように求めることができる．$o(1)$ は微小ゆえ，0 とみなして解いた．

まず，標数 p における 1024-bit の complexity の値 $\mathrm{L}_{2^{1024}}[1/3, 1.923] = 1.31587 \times 10^{26}$ を基準とする．標数 2 のとき，$\mathrm{L}_{2^{4m_1}}[1/3, 1.526]$ の値は，$m_1 = 437$ では 1.25566×10^{26} で足りず，$m_1 = 438$ では 1.33159×10^{26} だが 438 は素数ではないので不適，よって素数である $m_1 = 439$（このとき 1.41199×10^{26}）を得る．また，このとき $4 \times 439 = 1756$-bit 必要であることもわかる．同様に，標数 3 のとき，$\mathrm{L}_{3^{6m_2}}[1/3, 1.526]$ の値は，$m_2 = 184$ では 1.28926×10^{26} で足りず，$m_2 = 185$ では 1.48206×10^{26} であるが，185 は素数ではないので不適，よって条件を満たす最小の素数として $m_2 = 191$（このとき 3.38793×10^{26}）を得る．また，このとき $3^{6\times 191} = 2^x$ を解いて $x = 1816.37$ であるから，1817-bit 必要であることもわかる．

表 1: 安全性：拡大次数の計算 (supersingular な曲線の場合)

標数 p	2	3	p (大きな素数)
拡大次数 m	439 (素数)	191 (素数)	1
埋め込み次数 k	4	6	2
complexity $\mathrm{L}_{p^M}[a,c]$	$\mathrm{L}_{2^{4m}}[1/3, 1.526]$	$\mathrm{L}_{3^{6m}}[1/3, 1.526]$	$\mathrm{L}_{p^{2m}}[1/3, 1.923]$
security（必要となる bit）	1756bit	1817bit	1024bit

次章で述べるスカラー倍算の公式によるメリットや数学的な興味深さ，工夫による計算速度向上の可能性，署名長が短いことによる short signature への応用，標数 2 に特化した攻撃法があらわれたときのこと等を考慮し，ここでは，標数 3 に注目することにする．

4 $GF(3^m)$ における pairing の計算について

$GF(3^m)$ における楕円曲線上の点の 3 倍算は，$P = (x, y)$ に対し，$3P = 3(x, y) = ((x^3)^3 - 1, -(y^3)^3)$ のように簡単な形になる．さらに，$GF(3^m)$ での 3 乗は速く計算できるため，点の 3 倍算が非常に効率よく

計算できる．したがって，スカラー倍算は3進表現することで，より高速に計算できる．また，標数3のsupersingularな楕円曲線の埋め込み次数は6であり，他の標数より大きくとれることに注目されたい．これにより署名長の方を短くとることができるので，short signatureへの応用に非常に適しているといえる．

$GF(3^m)$でのTate pairingは次のように計算できる．まず，$\mathbb{F}_3$上約なsupersingularな楕円曲線として$E/\mathbb{F}_{3^m} : y^2 = x^3 - x + 1$を考える．$P, Q \in E[\ell](\mathbb{F}_{3^m})$とするとき，Tate pairing $e_\ell(\ ,\ )$は，$\gcd(\ell, 3) = 1$, $\ell | (3^{6m} - 1)$を満たす次の写像である．

$$e_\ell(\ ,\ ) : E[\ell](\mathbb{F}_{3^m}) \times E[\ell](\mathbb{F}_{3^{6m}}) \to \{\zeta_\ell\}\ (\subset \mathbb{F}^*_{3^{6m}}),\quad e_\ell(P, \phi(Q)) = f_P(\phi(Q))^{3^{3m}-1}$$

ここで，第2引数の6次拡大体の元は，$Q = (x, y) \in E[\ell](\mathbb{F}_{3^m})$に対し，$\phi(x, y) = (\rho - x, \sigma y)$, where $\sigma^2 + 1 = 0$, $\rho^3 - \rho - 1 = 0$ （すなわち$\mathbb{F}_3(\sigma) = \mathbb{F}_{3^2}$, $\mathbb{F}_3(\rho) = \mathbb{F}_{3^3}$）なるdistorsion map ϕ (nontrivial automorphism)を用いて構成する．$\{\zeta_\ell\}$は$\mathbb{F}^*_{3^6m}$における1のℓ乗根のなす群である．べき乗部分が$3^{3m} - 1$となることにも注意されたい．

標数3における楕円曲線上のpairing計算として，超楕円曲線$y^2 = x^p - x + 1$にも適用可能なDuursma-Leeのアルゴリズム[4]で$p = 3$としたものがある．ここで計算コストのかかる$\mathbb{F}_{3^m}$での3乗根の計算が必要となり，すでに計算してあるテーブルを利用する方法，[1]の3乗根の計算公式を用いる方法等がある．また，標数2での効率的なTate pairingアルゴリズムとして考案されたKwonのアルゴリズム[5]は，標数3でも同様に計算でき，3乗根の計算を必要としない効率的なアルゴリズムである．これらのアルゴリズムでは，楕円曲線$E(\mathbb{F}_{3^m})$: $y^2 = x^3 - x \pm 1$上の点の個数$\#E(\mathbb{F}_q) = 3^m \pm 3^{(m+1)/2} + 1$に対して，曲線上の点の位数は$3^m$であるが，超楕円曲線用に考案された$\eta_T$ pairing [2]を標数3の楕円曲線上に適用すると，位数が$\mp 3^{(m+1)/2} + 1$となり，より高速に計算できることがわかっている．ただし，η_T pairingでは，degenerate divisorを用いなければならないため，点の選び方に制限が加わることになる．

アルゴリズム 1 (Duursma-Lee [4])

INPUT : $P = (\alpha, \beta)$, $Q = (x, y)$
OUTPUT : $C = f_P(\phi(Q))$
$C \leftarrow 1$
for $(i = 1$ to $m;\ i{+}{+})$
$\alpha \leftarrow \alpha^3$, $\beta \leftarrow \beta^3$
$\mu = \alpha + x + b$, $\lambda = -\sigma\beta y - \mu^2$
$C \leftarrow C \cdot (\lambda - \mu\rho - \rho^2)$
$x \leftarrow x^{1/3}$, $y \leftarrow y^{1/3}$
end for

アルゴリズム 2 (Kwon [5])

INPUT : $P = (\alpha, \beta)$, $Q = (x, y)$
OUTPUT : $C = f_P(\phi(Q))$
$C \leftarrow 1$
$x \leftarrow x^3$, $y \leftarrow y^3$, $d \leftarrow mb$
for $(i = 1$ to $m;\ i{+}{+})$
$\alpha \leftarrow \alpha^9$, $\beta \leftarrow \beta^9$
$\mu = \alpha + x + b$, $\lambda = \sigma\beta y - \mu^2$
$C \leftarrow C^3 \cdot (\lambda - \mu\rho - \rho^2)$
$y \leftarrow -y$, $d \leftarrow d - b$
end for

最後に$3^{3m} - 1$乗して，Tate pairingの値を得る．

$\mathbb{F}_{3^m}$の演算で，各mにおける効率的な既約reduction trinomialはどのようなものなのだろうか．よく引用されている[11]で用いられている次の候補について考える．$m = 79$のとき，$x^{79} + x^{21} - 1$とあるが，これは$\mathbb{F}_3$上既約ではないので，既約なもの，特に[12]で議論されている既約trinomial $x^{79} \pm x^{26} \mp 1$とすべきであろう．$m = 97$のとき$x^{97} + x^{12} - 1$. $m = 163$のとき$x^{163} + x^{80} - 1$. $m = 167$のとき$x^{167} + x^{97} - 1$とあるが，これも$\mathbb{F}_3$上既約ではないので，既約なもの，特に[12]の$x^{167} - x^{71} - 1$とすべきであろう．$m = 173$のとき$x^{173} + x^{166} - 1$とあるが，第2項目の次数が低い方が速いことを考えると[12]から選んで$x^{173} - x^7 - 1$とすべきであろう．$m = 239$のとき$x^{239} + x^{24} - 1$とあるが，これも第2項目の次数を考えると$x^{239} - x^5 - 1$とすべきであろう．メールで問い合わせた返事によると，条件を満たす既約trinomialを見つけ，それで十分速いので最良のものまで追求しようとは考えなかったらしい．筆者らも，簡単のた

め，拡大次数 m の値ごとにそれぞれ reduction trinomial を固定して実装しているが，今後，より効率的な reduction trinomial を探すことも重要であるといえる．

5 測定結果

標数 3 における pairing の実装に利用可能な，フリーで使える $GF(3^m)$ での楕円曲線上での演算ライブラリやコードの調査および実装比較結果は次のとおり．

- **LiDIA[7] の楕円曲線上の演算ライブラリ**．今回，LiDIA の楕円曲線上の演算ライブラリを使用し，Kwon のアルゴリズムを実装したが，標数 3 では遅いことが判明した．実装は NEC が行った．
- **Paulo Barreto による 一部 MIRACL[8] のライブラリを使用したコード**．これを用いて，情報セキュリティ大学院大学の土井洋先生によるグループ署名ライブラリから呼び出し可能となるように，"NEC+LiDIA"で提供している I/F への変換を行った．
- **David Reis Jr. によるコード** [9]

表 2: 性能測定結果

プログラム	アルゴリズム	繰り返し回数	処理時間平均
NEC+LiDIA	Kwon	100	1.74s
Barreto+MIRACL	η_T	1000	3.91ms
David	BKLS [3]	500	9.87ms
	Duursma-Lee [4] (事前に 3 乗根計算あり)	500	3.95ms
	Kwon [5]	500	4.34ms
	Duursma-Lee [4] (事前に 3 乗根計算なし)	500	4.74ms

マシン環境 CPU: PentiumIV 3.4GHz, メモリ: 1GB

6 まとめ

標数 $2, 3, p$ についてそれぞれ調査した結果，特に標数 3 に注目してきた．計算コストから考えると標数 2 が速いと考えられるが，標数 3 における各演算の高速化の可能性および各標数に特化した攻撃法があらわれたときの対策，そして何より short signature への利用には標数 3 が最適であることが，今回，標数 3 に注目した理由である．今後は，標数 2 での実装も進めると同時に，現時点では，各標数及び体のサイズを固定した実装となっているが，上位アプリから指定できるような実装内容を検討中である．また，[14] 等のバッチ検証機能も付加していく．

謝辞

多大なるご助言を下さった，はこだて未来大学の高木剛先生，そして，情報セキュリティ大学院大学の土井洋先生，ＮＥＣの小松文子技術主管，筑波大学の岡本健先生，修士課程の松田誠一君をはじめ，「セキュリティ情報の分析と共有システムの開発」プロジェクトの皆様に感謝の意を表する．

A 暗号技術評価報告書 (2002年度版) CRYPTREC Report 2002, 2.4.2.2 攻撃法におけるデータの誤りに関する指摘と原因の考察 [13]

暗号技術評価報告書 (2002年度版) CRYPTREC Report 2002 [22] の 2.4.2. 離散対数問題 において，離散対数問題に対する攻撃法，および離散対数問題の困難性に安全性の根拠を置く暗号プリミティブでの安全な鍵サイズの調査報告がなされている．ここで，2.4.2.2 攻撃法 で，q を有限体の位数，計算量を $L_q[a,b] = e^{b(\log q)^a(\log\log q)^{1-a}}$ としたとき，表中で，標数 2 の拡大体の乗法群に対する Coppersmith の指数計算法 [17] による攻撃の計算量は $L_q[1/3, c+o(1)], c \approx 1.4$ で，その解読記録は $\mathbb{F}_{2^{607}}$ の 183 桁 [20, 21] であると記されている．しかし，ここで c の値は $(32/9)^{1/3}(=1.526\cdots)$ にすべきである．この誤りの原因は，根拠として挙げられている論文 [20] の 1 章の $c \approx 1.4$ によるものであると考えられる．しかしながら，論文 [20] は正しい．というのは，[20] で用いている計算量の式は $e^{(c+o(1))n^{1/3}\log^{2/3}n}$ (ここで n は拡大次数，すなわち $q=2^n$ をあらわす) であり，$e^{(c+0(1))(\log q)^{1/3}(\log\log q)^{2/3}}$ ではないからである．すなわち，これら異なる 2 つの公式を，$\log q = n$ と解釈して同一視してしまったことが誤りの原因であると考えられる．ここでの対数の底が 2 ではなく自然対数 e である (よって $\log q \neq n$ となる) ことは，Coppersmith の指数計算法のオリジナルの論文 [17] で確認されたい．なお，[17] IX 章 Table I によると，より正確な c の値としては，(四捨五入すると 1.4 ではあるが) best case として記されている 1.351 を用いるべきである．

上述のように，計算量の公式 $L_q[a,b] = e^{b(\log q)^a(\log\log q)^{1-a}}$ を用いたとき $L_{2^n}[1/3, c+o(1)]$ における c の値は $(32/9)^{1/3}(=1.526\cdots)$，公式 $e^{(c+o(1))n^{1/3}\log^{2/3}n}$ を用いたとき c の値は 1.4(正確には $1.351\cdots$) である．**計算確認：** $L_q[a,b] = e^{b(\log q)^a(\log\log q)^{1-a}}$ に $a=1/3, b=c+o(1), c=(32/9)^{1/3}(\approx 1.526), q=2^m$ を代入することで，次のように $e^{(\tilde{c}+o(1))n^{1/3}\log^{2/3}n}$, $\tilde{c}=1.351$ を導くことができる．

$$
\begin{aligned}
L_{2^n}[1/3, (32/9)^{1/3}+o(1)] &= e^{((32/9)^{1/3}+o(1))(\log 2^n)^{1/3}(\log\log 2^n)^{2/3}} \\
&= e^{((32/9)^{1/3}+o(1))n^{1/3}(\log 2)^{1/3}(\log n+\log\log 2)^{2/3}} \\
&= e^{((32/9)^{1/3}(\log 2)^{1/3}+o(1)(\log 2)^{1/3})n^{1/3}(\log n+\log\log 2)^{2/3}} \\
&\approx e^{(1.351+o(1))n^{1/3}(\log n)^{2/3}}
\end{aligned}
$$

参 考 文 献

[1] Paulo S. L. M. Barreto "A note on efficient computation of cube roots in characteristic 3" http://eprint.iacr.org/2004/305 (Cryptology ePrint Archive)

[2] Paulo S. L. M. Barreto, Steven Galbraith, Colm OhEigeartaigh, Michael Scott "Efficient Pairing Computation on Supersingular Abelian Varieties" http://eprint.iacr.org/2004/375 (Cryptology ePrint Archive)

[3] Paulo S. L. M. Barreto, Hae Y. Kim, Ben Lynn, Michael Scott "Efficient Algorithms for Pairing-Based Cryptosystems" Crypto 2002 Proc, LNCS 2442, Springer-Verlag, pp. 354 - 368 (2002).

[4] Iwan Duursma, Hyang-Sook Lee "Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$" Asiacrypt 2003 Proc, LNCS 2894, Springer-Velag, pp. 111-123 (2003).

[5] Soonhak Kwon "Efficient Tate pairing Computation for Supersingular Elliptic Curves over Binary Fields" ACISP 2005 Proc, LNCS 3574, Springer-Verlag, pp.134 - 145 (2005)

[6] "The Pairing-Based Crypto Lounge" http://paginas.terra.com.br/informatica/paulobarreto/pblounge.html

[7] "LiDIA" http://www.informatik.tu-darmstadt.de/TI/LiDIA/

[8] "MIRACL" http://indigo.ie/mscott/

[9] David Reis Jr. "Efficient Implementation of Pairing Based Cryptosystems over $GF(3^m)$" http://www.fun.ac.jp/takagi/takagi/thesis/WS0405_David_Reis.pdf, 2005

[10] D. Page and N. Smart "Hardware implementation of finite fields of characteristic three" CHES2002, LNCS 2523, pp.529-539, 2002.

[11] K. Harrison, D. Page, and N. Smart "Software implementation of finite fields of characteristic three" LMSJ Comput. Math., vol.5, pp.181-193, 2002.

[12] Jorge Guajado Merchan "Arithmetic Architectures for Finite Fields $GF(p^m)$ with Cryptographic Applications" dissertation, Ruhr-Universitat Bochum, Universitatsbibliothek, Fakultat fur Elektrotechnik und Informationstechnik, 2004 http://deposit.ddb.de/cgi-bin/dokserv?idn=976951193

[13] 岩見真希 "暗号技術評価報告書 (2002 年度版) CRYPTREC Report 2002, 2.4.2.2 攻撃法におけるデータの誤りに関する指摘と考察" CRYPTREC 事務局に提出, 2006.

[14] 岩見真希, 高木剛, 岡本健, 岡本栄司 "楕円曲線上のペアリング計算におけるバッチ検証" 暗号と情報セキュリティシンポジウム (SCIS2006) 予稿集 CD-ROM 4C2-5(論文), 概要集 pp.315(概要), 2006.

[15] A.K. Lenstra, E.R. Verheul "The XTR public key system" Proceedings of Crypto 2000, LNCS 1880, Springer-Verlag 2000, pp.1-19.

[16] D. Coppersmith "Evaluating logarithms in $GF(2^n)$". 16th ACM Symp. Theory of Computing, pp.201-207, 1984.

[17] D. Coppersmith "Fast evaluation of logarithms in fields of characteristic two". IEEE Transactions in Information Theory, 30, pp.587-594, 1984.

[18] L. M. Adleman "The function field sieve" Proc. of the 1st International Symposium on Algorithmic Number Theory, Springer-Verlag LNCS 877, pp.108-121, 1994.

[19] L. M. Adleman and M. A. Huang "Function Field Sieve Method for Discrete Logarithms over Finite Fields". Inform. and Comput., 151, pp.5-16, 1999.

[20] E.Thomé "Computation of discrete logarithms in $GF(2^{607})$." Proc. of ASIACRYPT 2001, LNCS 2248, pp. 107-124, 2001.

[21] E.Thomé "Discrete Logarithms in $GF(2^{607})$." Available at http://www.lix.polytechnique.fr/Labo/Emmanuel.Thome/announcement/announcement.html

[22] "暗号技術評価報告書 (2002 年度版) CRYPTREC Report 2002" http://www2.nict.go.jp/tao/kenkyu/CRYPTREC/PDF/c02_report.pdf

[23] Antoine Joux, Reynald Lercier "The Function Field Sieve Is Quite Special" Proc. of the 5th International Symposium on Algorithmic Number Theory, Springer-Verlag LNCS 2369, 431-445, 2002.

[24] R. Granger, A.J. Holt, D. Page, N.P. Smart, and F. Vercauteren "Function Field Sieve in Characteristic Three" ANTS 2004: pp.223-234.

[25] 電子情報通信学会 "情報セキュリティハンドブック", 2004

[26] 岡本龍明, 太田和夫 "暗号・ゼロ知識証明・数論" 共立出版 1995.