社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2006－CSEC－34 (16)
2006／7／20

効率的なグループ署名を実現する楕円曲線の構成方法

久保寺 範和* 古川 潤† 佐古 和恵†
E-mail:n-kubotera@bp.jp.nec.com, j-furukawa@ay.jp.nec.com, k-sako@ab.jp.nec.com
日本電気株式会社
*システム基盤ソフトウェア開発本部 †インターネットシステム研究所
〒108-8557 東京都港区芝浦 2-11-5 〒211-8666 神奈川県川崎市中原区下沼部 1753

概要：古川等はペアリングを用いたグループ署名方式（ACISP2005）で、従来の方式に比べて署名長と計算量が小さい方式を提案した。このグループ署名方式を実現するには、ペアリングを持つ楕円曲線と、この楕円曲線と同じ位数を持ちかつペアリングを持たない楕円曲線との対を構成する必要がある。しかし、このような楕円曲線の対を実際に構成した例は知られていなかった。本論文では、このような楕円曲線の対を実際に構成することで、効率的なグループ署名を実現可能であることを示す。

キーワード：グループ署名、楕円曲線、双線形写像

A Method for Generating Elliptic Curves suitable for Implementing an Efficient Group Signature scheme

Norikazu KUBOTERA* Jun FURUKAWA† Kazue SAKO†
E-mail:n-kubotera@bp.jp.nec.com, j-furukawa@ay.jp.nec.com, k-sako@ab.jp.nec.com
NEC Corporation
*System Platform Software Development Division
2-11-5 Shibaura, Minato-ku, Tokyo, 108-8557, Japan
†Internet Systems Research Laboratories
1753, Shimonumabu, Nakahara-ku, Kawasaki, 211-8666, Japan

Abstract : Furukawa et al. proposed in ACISP2005 an efficient group signature scheme from bilinear maps. The proposed scheme is most efficient among previously knwon group signature schemes in signature length and in computational complexity under q-strong Diffie-Hellman assumption. This group signature scheme requires a pair of elliptic curves of the same order such that one provides efficient bilinear maps but the other has no efficient bilinear map. However, a generation of such a pair has not been reported. In this paper, we generate such pair of elliptic curves for the first time, which demonstrates the feasibility of the efficient group signature scheme.

Keyword : Group Signature Scheme, elliptic curves, bilinear maps

1．はじめに

近年インターネットの普及により、オンラインショッピングといったWebサービスの利用者が増加している。現在では、サービスを受ける際、本人を確認するための個人認証が行われている。そのため、誰が、いつ、どのようなサービスを受けたかという情報がWebサービス事業者に渡ることになる。最近では、インターネット上での個人情報の流出が問題となっており、Webサービス利用者は、自分がいつどこで何をしていたかを知られることに不安を感じる。また、個人情報保護法により、企業での個人情報の取り扱いが法律で決められることになり、

Web サービス事業者は、プライバシを保護し、安全にインターネットを使用できる環境を構築する必要がある。

グループ署名を用いることにより以下のことを実現することができ、プライバシを保護することが可能となる。

(1) 個人名や ID といった個人を特定する情報を用いずに、認証対象があるグループに所属しているかどうか確認可能

(2) 特定の管理者のみが、認証された個人が誰であったかを認証記録から特定することが可能

グループ署名は様々な方式が提案されているが、署名長が長くなってしまうという課題がある。この課題に関して、近年、楕円曲線上の双線形写像（ペアリング）を用いたグループ署名方式により、より短い署名長でのグループ署名を実現可能としている。特に、古川等の提案したグループ署名方式（ACISP2005）[1] は、従来の方式と比較して署名長と計算量の小さい方式である。

2．楕円曲線構成課題点

ACISP2005 で提案されたグループ署名方式（以下、古川ー今井グループ署名方式と記す）は、同じ安全性をもつグループ署名方式と比較して効率的な方式である。古川ー今井グループ署名方式は、同じ素数位数 N を持つ群 G_1, G_2, G_T, G およびペアリング $e : G_1 \times G_2 \to G_T$ を用いている。また、G は Diffie-Hellman 判別問題が難しい群である。

ここでペアリングを持つ $\mathbf{F}_p$ 上楕円曲線を E_1 とし、E_2 をペアリングを持たない楕円曲線とする。ただし、E_1, E_2 は共に素数位数 N の点を持つとする。

$G_1 = E_1(\mathbf{F}_p)[N], G_2 = (E_1(\mathbb{F}_{p^m})/NE_1(\mathbf{F}_{p^m})), G_T = \mathbb{F}_{p^m}^{\times}/(\mathbb{F}_{p^m}^{\times})^N$ とし、ペアリング e は Tate ペアリングであるとする。（ただし、m は埋め込み次数）

$$e : E_1(\mathbf{F}_p)[N] \times (E_1(\mathbb{F}_{p^m})/NE_1(\mathbf{F}_{p^m})) \longrightarrow \mathbb{F}_{p^m}^{\times}/(\mathbb{F}_{p^m}^{\times})^N$$

上記のように、古川ー今井グループ署名方式を実現するには以下の条件を満たす楕円曲線の対 E_1, E_2 での演算を実行する必要がある。

(1) 大きな素数位数の点を持ち、かつ、ペアリングを持つ楕円曲線 E_1

(2) 楕円曲線 E_1 と同じ位数の点を持ち、かつペアリングを持たない楕円曲線 E_2

(3) 楕円曲線 E_1, E_2 は共にセキュリティ上安全と思われる楕円曲線であること

しかし、上記の条件を満たす楕円曲線の対を構成した例は知られておらず、条件 (1)(2)(3) を満たす楕円曲線の対を生成可能か否かは疑問視されていた。

本論文では、上記の条件 (1)(2)(3) を満たす楕円曲線の構成に成功したことを示す。

3．楕円曲線の構成方法

3．1．楕円曲線構成方法概要

ペアリングを持つ楕円曲線とその位数と等しい位数を持つ楕円曲線でペアリングを持たない楕円曲線の対を以下の手順で構成した。

手順 1: ペアリングを持つ素数位数の安全な楕円曲線を 1 つ選択する。

手順 2: 手順 1 で検索した楕円曲線の位数と同じ楕円曲線を複数構成する。

手順 3: 手順 2 で構成した楕円曲線で、ペアリングを持つものを除外した上で安全性を満たすものを選択する。

手順 3 で安全性を満たすものがなかった場合、手順 1 に戻る。

3．2．手順 1: ペアリングを持つ楕円曲線の検索

ペアリングを持つ楕円曲線 E_1 を検索する。E_1 の位数を N（素数）とする。ペアリング e は

$$e : E_1(\mathbb{F}_p)[N] \times (E_1(\mathbb{F}_{p^m})/NE_1(\mathbf{F}_{p^m})) \longrightarrow \mathbb{F}_{p^m}^{\times}/(\mathbb{F}_{p^m}^{\times})^N$$

であり、有限体 $\mathbb{F}_{p^m}$ の離散対数問題を解くことを困難とする為に

$$(p\text{ の bit 数})\times m \geq 1024$$

となる必要がある。また、楕円曲線の離散対数問題を解くことを困難にする為に、楕円曲線の定義体の標数 p は160bit 以上の素数である必要がある。その一方、ペアリングの演算速度の高速化を考慮した場合、p のビット数は小さいほうが好ましいため、埋め込み次数 m を大きくしたほうがよい。埋め込み次数が 2、3、6 の楕円曲線はよく知られているので、本論文では、埋め込み次数 6 の楕円曲線を選択することにした。ペアリングを持つ楕円曲線は、MNT 曲線 [2][3] から構成できることが知られている。具体的な楕円曲線は [3] の 4.1 Extending the search に記載されている。本論文ではそのうち下記の楕円曲線を選択することにした。

$E_1/\mathbb{F}_p : y^2 = x^3 + ax + b$

標数 p : 150 28799 61398 50344 65755 50645 07715 65229 28283 22178 60390 15599 64838 40017 (224bit 素数)

位数 N : 150 28799 61398 50344 65755 50645 07715 61352 58325 47441 25520 63929 65411 95021 (素数)

a : -3

b : 3 45630 27717 27404 21841 09525 86178 73363 85553 84721 22976 05300 75211 56770

埋め込み次数 : 6

E_1 を構成するのに使用した虚二次体の判別式 $-D$: $D = 496659$

3．3．手順 2: 位数の等しい楕円曲線の構成

一般的に、大きな素体上の楕円曲線を構成する方法は知られている（参照 [4]）。虚数乗法という方法（CM 法）と呼ばれる手法であり、以下にその方法を記す。

【1】虚 2 次体 $K = \mathbb{Q}(\sqrt{-D})$ で、その類数 h_D の小さいものを選ぶ。

【2】ディオファントス方程式

$$4p = x^2 + Dy^2$$

が解を持つように素数 p を選択する。ただし、この素数は、得られる楕円曲線の定義体の標数となるため、p の bit 数は安全性を考慮する必要がある。

【3】$K = \mathbb{Q}(\sqrt{-D})$ に関するヒルベルト類多項式 H_D を求める。

【4】H_D の $\mathbb{Z}/p\mathbb{Z}$ での解を計算する。

【5】【4】の解を j 不変量に持つ楕円曲線を求める。

【6】【5】の楕円曲線の位数は

$$p + 1 \pm x$$

となる。

本論文では、与えられた素数位数 N を持つ楕円曲線を構成するのであるため、上記【2】【6】の式を変形し、以下の 2 式を満たす素数 p を求める。

$$4N = (x \pm 2)^2 + Dy^2 \quad (1)$$

$$p = N - 1 \pm x \quad (2)$$

上記 (1) の x が整数となるように D を正の整数の範囲で動かすが、(1) で x が整数解をもつためには、$-D \equiv 5 \bmod 8$ の条件が必要である。この条件の下で D を 1〜1,000,000 まで動かし、解 x を求める。解 x から (2) によって素数 p を求める。

(1) の解を求めた後の楕円曲線の構成方法は、従来の方法【3】〜【6】を同じである。

(1) の解を求めるアルゴリズムは以下である。

$N \leftarrow$ 150 28799 61398 50344 65755 50645 07715 61352 58325 47441 25520 63929 65411 95021

for $D \leftarrow 1$ **to** 1000000 **do**

if $-D \equiv 5 \bmod 8$ **then**

```
if 4N = X^2 + Dy^2 が解を持つ then
  x_1 ← X + 2
  x_2 ← X − 2
  x_3 ← −X + 2
  x_4 ← −X − 2
    for i ← 1 to 4
      if p ← N − 1 + x_i が素数 then
        output x_i, y, p
      end if
    end for
  end if
 end if
end for
```

このようにして条件を満たす D で $1 \leq D \leq 1,000,000$ のものは 17 個存在した。以下に記す。

D = (1)33307, (2)33459, (3)121283, (4)251187, (5)261539, (6)299763, (7)301131, (8)451627, (9)474523, (10)476315, (11)496659, (12)581755, (13)759035, (14)788971, (15)836475, (16)895955, (17)899987

上記の D から得られた標数 p は、本論文の最後に表にまとめた。上記の括弧の数字は、表での番号である。

一般に虚数乗法を用いて楕円曲線を構成する場合、類数が小さくなるように虚二次体 $K = \mathbb{Q}(\sqrt{-D})$ を選択する。なぜなら、【3】において、大きい類数のヒルベルト類多項式 H_D の計算が、現実的な時間で終了するか否かわからないからである。今回、求めた判別式 $-D$ の類数は、最小で 28 ($(1)D = 33307$)、最大で 286 ($(17)D = 899987$) であった。しかし、今回計算ソフトウェア MAGMA[5] を用いることにより、最大でも 2,3 分 (CPU:Pentium4 3.4GHz、メモリ:2GB) でヒルベルト類多項式を算出した。

このようにして、位数が与えられた N = 150 28799 61398 50344 65755 50645 07715 61352 58325 47441 25520 63929 65411 95021 (素数) である楕円曲線を構成することができた。構成例を以下に記す。

例 1 : $(1)D = 33307$ (類数 28)

$E_{2,1}/\mathbb{F}_p$: $y^2 = x^3 + ax + b$

標数 p : 150 28799 61398 50344 65755 50645 07715 57277 92058 25402 26013 31944 23846 29791

a : 48 07863 67817 76315 34209 90349 05960 38497 37860 63119 32775 89157 90124 83613

b : 54 13072 25762 97713 97335 69946 95794 80283 16336 99163 60461 53628 43596 62565

例 2 : $(2)D = 33459$ (類数 68)

$E_{2,2}/\mathbb{F}_p$: $y^2 = x^3 + ax + b$

標数 p : 150 28799 61398 50344 65755 50645 07715 67158 60292 65203 12568 57925 87043 90969

a : 30 06068 72498 90395 23247 45755 91737 62516 44432 09463 45080 01969 32922 18542

b : 90 16662 16400 69554 19260 59133 24240 42125 71428 46276 22408 53987 21199 53885

3．4．手順 3：セキュリティ上の考慮

手順 2 により、与えられた位数を持つ楕円曲線を複数構成することができた。しかし、このように構成した楕円曲線で Diffie-Hellman 判別問題が容易に解ける可能性がある。

Diffie-Hellman 判別問題

G を群とする。$g, g^a, h, h^b \in G$ (ただし、$a, b \in \mathbb{Z}$) が与えられたとき、$a = b$ か否か判別できる。

この問題を回避するために構成した曲線が以下の性質を満たさないようにする。

(1)supersingular 曲線

$N = p + 1$ を満たす曲線 (標数 $p \neq 2, 3$ のため)

(2)anomalous 曲線

$N = p$ を満たす曲線

(3)MNT 曲線

ordinary かつ埋め込み次数が 6 以下の曲線

条件 (1)supersingular、(2)anomalous については、構成した楕円曲線全て該当しない。しかし、(3) に関して、(11)$D = 496659$ で得られた標数

150 28799 61398 50344 65755 50645 07715 65229 28283 22178 60390 15599 64838 40017

については埋め込み次数が 6 となるため、除外する。また、この楕円曲線は、手順 1 で検索した楕円曲線と同じ判別式を持つものである。

また、本論文で構成した楕円曲線は、特別な方法 [2][3] で生成されていないので、ペアリングを持たない楕円曲線となっている。

3．7．構成した楕円曲線例

セキュリティを考慮した結果、以下の D に対して構成した楕円曲線をグループ署名に使用する楕円曲線として選択した。また、構成した楕円曲線の例をいくつか示す。

D = (1)33307, (2)33459, (3)121283, (4)251187, (5)261539, (6)299763, (7)301131, (8)451627, (9)474523, (10)476315, (12)581755, (13)759035, (14)788971, (15)836475, (16)895955, (17)899987

例 3：(6)$D = 299763$（類数 112）

$E_{2,3}/\mathbb{F}_p$: $y^2 = x^3 + ax + b$

標数 p : 150 28799 61398 50344 65755 50645 07715 57277 92058 25402 26013 31944 23846 29791

a : 58 53539 66059 31952 48541 77645 20698 83576 74163 26854 85801 43440 41260 09581

b : 33 21720 29279 86439 68671 95354 66317 90124 43731 71692 54410 45063 41326 10629

例 4：(7)$D = 301131$（類数 204）

$E_{2,4}/\mathbb{F}_p$: $y^2 = x^3 + ax + b$

標数 p : 150 28799 61398 50344 65755 50645 07715 67158 60292 65203 12568 57925 87043 90969

a : 53 84257 37955 06720 94919 38755 59690 30784 42700 17496 29128 49560 23469 04774

b : 42 60284 85488 36902 75916 73133 88335 05589 74892 30210 54311 58805 40105 81421

例 5：(17)$D = 899987$（類数 286）

$E_{2,4}/\mathbb{F}_p$: $y^2 = x^3 + ax + b$

標数 p : 150 28799 61398 50344 65755 50645 07715 54048 26282 35130 40549 15633 63099 63551

a : 27 74959 35703 43901 74707 81043 14131 52487 32867 10286 72497 71538 09772 54599

b : 94 78880 89991 62541 16339 88558 79452 49073 60548 14556 95553 72557 43554 54353

4．本構成方法の考察

本論文では、楕円曲線上のペアリングを用いたグループ署名方式で、署名長が短く、計算量の少ない方式[1]に使用する楕円曲線の対の構成に成功した。

構成する楕円曲線の対は、ペアリングを持つ楕円曲線と、その楕円曲線と位数の等しい楕円曲線でペアリングを持たない楕円曲線である。ペアリングを持つ楕円曲線は既知の楕円曲線（224bit）を用いた。この楕円曲線と位数が等しい楕円曲線を17個構成することができた。構成した17個の楕円曲線のうちで、セキュリティ上安全と思われる楕円曲線は16個存在した。楕円曲線構成に最も時間を要したのが、ディオファントス方程式$4N = (x \pm 2)^2 + Dy^2$の解法であり、Dの値を1～1,000,000まで動かし、解を探索するのに要した時間は約5時間ほどであった（CPU:Pentium4 3.4GHz, メモリ:2GByte, ソフトウェア:Magma)。よって、効率的なグループ署名実現に必要な楕円曲線の構成は数時間間程度で完了するため、上記のグループ署名方式は実現可能な方式であることが判明した。

本論文では、ペアリングを持つ楕円曲線として既知の224bitのMNT曲線を使用した。224bitというbit数は、楕円曲線のセキュリティ上問題ない値であるが、演算速度を考慮した場合、短いbit数（171bit程度）のほうが適している。また、グループ署名に高度なセキュリティが要求された場合、224bitよりも長いbit長が必要になる可能性もあるので、今後は、様々なbit数の楕円曲線の対を構成していくことを検討している。

5．おわりに

本論文では、効率的なグループ署名を実現するための楕円曲線の対を構成することに成功し、上記グループ署名方式を実現可能であることが判明した。今後は、今回構成した楕円曲線の対を基に効率的なグループ署名を実装し、評価を行っていく。

参考文献

[1] J.Furukawa, and H.Imai, "An Efficient Group Signature Scheme from Bilinear Maps", ACISP 2005, LNCS 3574, Springer Verlag, pp. 455-467, July 2005.

[2] 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.

[3] M.Scott and P.S.L.M.Barreto, "Generating more MNT elliptic curves", Cryptology ePrint Archive, Report 2004/058, 2004.

[4] イアン・F・ブラケ他, "楕円曲線暗号", ピアソン・エデュケーション

[5] MAGMA, The Magma Computational Algebra System for Algebra, Number Theory and Geometry, http://magma.maths.usyd.edu.au/magma/

付表：ディオファントス方程式の解から得られた標数

No.	D(判別式-D)	類数	標数
(1)	33307	28	150 28799 61398 50344 65755 50645 07715 57277 92058 25402 26013 31944 23846 29791
(2)	33459	68	150 28799 61398 50344 65755 50645 07715 67158 60292 65203 12568 57925 87043 90969
(3)	121283	81	150 28799 61398 50344 65755 50645 07715 54088 47220 64230 65817 40605 45557 96911
(4)	251187	88	150 28799 61398 50344 65755 50645 07715 65559 28543 10604 91308 96765 66673 37201
(5)	261539	170	150 28799 61398 50344 65755 50645 07715 56853 66793 20192 48765 70963 90417 85969
(6)	299763	112	150 28799 61398 50344 65755 50645 07715 57277 92058 25402 26013 31944 23846 29791
(7)	301131	204	150 28799 61398 50344 65755 50645 07715 67158 60292 65203 12568 57925 87043 90969
(8)	451627	56	150 28799 61398 50344 65755 50645 07715 54508 03242 60261 38413 64678 76673 11281
(9)	474523	104	150 28799 61398 50344 65755 50645 07715 59491 95390 95184 71112 38678 26057 46481
(10)	476315	192	150 28799 61398 50344 65755 50645 07715 67829 64354 65206 45851 67935 67899 03179
(11)	496659	160	150 28799 61398 50344 65755 50645 07715 65229 28283 22178 60390 15599 64838 40017
(12)	581755	124	150 28799 61398 50344 65755 50645 07715 53846 26122 91103 07623 35284 54436 92999
(13)	759035	272	150 28799 61398 50344 65755 50645 07715 66624 51136 32391 80624 88772 89397 69069
(14)	788971	219	150 28799 61398 50344 65755 50645 07715 68376 71299 33711 68321 58312 20102 33719
(15)	836475	272	150 28799 61398 50344 65755 50645 07715 67158 60292 65203 12568 57925 87043 90969
(16)	895955	280	150 28799 61398 50344 65755 50645 07715 68801 98183 71172 46728 85217 17575 26239
(17)	899987	286	150 28799 61398 50344 65755 50645 07715 54048 26282 35130 40549 15633 63099 63551