

y-座標復元を伴うモンゴメリ型 楕円曲線上のスカラー倍計算方法と 楕円曲線暗号における効率性の解析

桶屋 勝幸

(株)日立製作所

E-mail: okeya_k@itg.hitachi.co.jp

櫻井 幸一

九州大学



概要

- [LH00]: “Montgomery’s method **CAN’T** compute the y -coordinate of kP ”
- モンゴメリ法の y 座標復元 $\left\{ \begin{array}{l} P=2 \text{ 既知} \\ P>2 \text{ 未解決} \end{array} \right.$
- $P>2$ の場合の y 座標復元方法の提案
- 楕円ElGamal暗号の最高速実行が可能

[LH00] Lim, C.H., Hwang, H.S., Fast Implementation of Elliptic Curve Arithmetic in $GF(p^m)$, Proc. PKC’00, LNCS1751, (2000), 405-421



内容

はじめに

楕円曲線暗号における y 座標の必要性

y 座標復元

モンゴメリ型 **vs.**
ワイエルシュトラ
ス型



内容



はじめに

楕円曲線暗号における y 座標の必要性

y 座標復元

モンゴメリ型 **vs.**
ワイエルシュトラ
ス型



楕円曲線暗号

楕円曲線暗号：楕円曲線上の離散
対数問題の求解に対する困難性に基
づく公開鍵暗号

離散対数問題：楕円曲線上の点 P
とスカラー倍 $Q(=kP)$ とから、
スカラー値 k を求める問題



楕円曲線暗号

スカラー倍 : 楕円曲線上の点 P
に対して、スカラー値 k の回数だけ
その点を加える演算及びその結果
の点 $Q(=kP)$

今までのところ特別なクラスの楕円曲線
以外に対しては準指数時間による解法
は見つかっていない。



モンゴメリ型楕円曲線

[Mon87]

$$E^M : BY^2 = X^3 + AX^2 + X$$
$$\left(E : y^2 = x^3 + ax + b \right)$$

ワイエル
シュトラス
型

楕円曲線法による因数分解の高速化

y座標を
用いないので

高速なスカラー倍計算アルゴリズム

[Mon87] Montgomery, P.L., Speeding the Pollard and Elliptic Curve
Methods of Factorizations, Math. Comp. 48, (1987) 243-264



モンゴメリ型楕円曲線の研究

- 楕円曲線法による因数分解の高速化

- ・Montgomery(1987), 小山(1987)

高速演算可能

- 楕円曲線暗号への適用

- ・伊豆(1999), 竹内-小山(1999), 大岸-境-笠原

y座標を用いない

- ⁽¹⁹⁹⁹⁾ タイミング攻撃等への防御法

- ・Lopez-Dahab(1999), 桶屋-車谷-櫻井(2000),

- Lim-Hwang(2000), 桶屋-櫻井(2000)

耐タイミング攻撃

- y座標復元を伴うスカラー倍計算

- ・Lopez-Dahab(1999), 桶屋-櫻井(2001)[本発表]

y座標復元



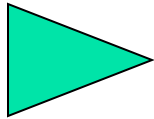
高速スカラー倍計算方法の研究

- **定義体**
 - ・ **素体** 標数2の有限体, OEF **ワイエルシュタス型**
- **座標系**
 - ・ Affine座標, **射影座標**, Jacobian座標, **混合座標系**
- **楕円曲線の式**
 - ・ **Weierstrass標準形** (標数2), Koblitz曲線,
Montgomery-form
- **スカラー値の表現**
 - ・ **binary**, 符号付, NAF, **Window法**
法



内容

はじめに



楕円曲線暗号における y 座標の必要性

y 座標復元

モンゴメリ型 **vs.**
ワイエルシュトラ
ス型



問題と要望

- モンゴメリ型は y 座標を計算できない
- でも楕円暗号には y 座標が必要



y座標を必要とするスキーム

y座標不必要

この違い
は？

y座標必要

ECES(暗号)
ECDSA-S(署名) ...

ECDSA-V (署名検証)
ECELGamal(暗号) ...

kP
の演算のみ必要

$kP + Q$
の演算が必要



大岸-境-笠原の署名法の問題点 IOSK99I

モンゴメリ型楕円曲線においてy座標を用いないECDSAの署名検証方法

ハッシュ値が異なるメッセージに対して同じ署名を受け入れる

ECDSA-V
実行の為の
一つの解決法

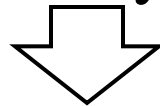
検証の為の計算式が2次式である為
別の解が存在することによる

**IOSK99I 大岸-境-笠原, y座標を必要としない楕円型署名の演算法,
Proc. SCIS'99, W4-1.3, (1999), 285-287**

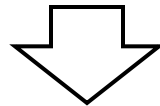


y座標復元

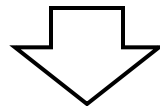
スカラー倍計算後のy座標を復元する



$kP + Q$ のような演算が可能



全ての楕円曲線スキームの実行が可能



モンゴメリ型の利点 (**高速性・安全性**)

を享受できる

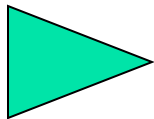
耐タイミング
攻撃など



内容

はじめに

楕円曲線暗号における y 座標の必要性



y 座標復元

モンゴメリ型 **vs.**
ワイエルシュトラ
ス型



要望と課題

- 楕円暗号に y 座標は必要
- でも平方根は計算したくない

y 座標復元を
行なう時に

スカラー倍計算
と比べて計算量
が大きい

従来法

y座標復元(P=2)[加算点利用法] [LD99]

$$P_2 = P_1 + P$$

$$P = (x, y)$$

$$P_1 = (x_1, y_1)$$

$$P_2 = (x_2, y_2)$$

スカラー倍点

$$P = (x, y)$$

$$P_1 = (x_1, ?)$$

$$P_2 = (x_2, ?)$$

モンゴメリ法による
スカラー倍計算後の状態

この関係より
方程式を立て、求解

四則演算のみ

y_1

$$y_1 = (x_1 + x) \left\{ (x_1 + x)(x_2 + x) + x^2 + y \right\} / x + y$$

[LD99] Lopes, J., Dahab, R., Fast Multiplication on Elliptic Curves over $GF(2^m)$
without Precomputation, CHES'99, LNCS1717, (1999) 316-327

提案法

y座標復元($P > 2$)[加算点利用法]

$$P_2 = P_1 + P$$

$$P = (x, y)$$

$$P_1 = (x_1, y_1)$$

$$P_2 = (x_2, y_2)$$

スカラー倍点

$$P = (x, y)$$

$$P_1 = (x_1, ?)$$

$$P_2 = (x_2, ?)$$

モンゴメリ法による
スカラー倍計算後の状態
一般に y_1 の2次式となってしまう
 y_1 の2次式は消去できる

四則演算のみ

$$y_1 = \frac{(x_1 x + 1)(x_1 + x + 2A) - 2A - (x_1 - x)^2 x_2}{2By}$$

y座標復元(P>2)[差分点利用法]

$$P_2 = P_1 + P$$

$$P_3 = P_1 - P$$

$$P = (x, y)$$

$$P_1 = (x_1, y_1)$$

$$P_2 = (x_2, y_2)$$

$$P_3 = (x_3, y_3)$$

スカラー倍点

この関係を
新たに追加

$$P = (x, y)$$

$$P_1 = (x_1, ?)$$

$$P_2 = (x_2, ?)$$

$$P_3 = (x_3, ?)$$

差分点のx座標も
既知の場合

方程式の差を取り
y₁の2次式を消去する

四則演算のみ

$$y_1 = \frac{(x_3 - x_2)(x_1 - x)^2}{4By}$$

y₁

モンゴメリ型楕円のスカラー倍において
差分点は与えられない

y座標復元($P > 2$)[差分点利用法]

$$P_2 = P_1 + P$$

$$P_3 = P_1 - P$$

$$P = (x, y)$$

$$P_1 = (x_1, y_1)$$

$$P_2 = (x_2, y_2)$$

$$P_3 = (x_3, y_3)$$

スカラー倍点

$$P = (x, y)$$

$$P_1 = (x_1, ?)$$

$$P_2 = (x_2, ?)$$

モンゴメリ法による
スカラー倍計算後の状態

差分点のx座標

x_3 の計算[四則演算のみ]
モンゴメリの加算公式を利用

x_3

y座標復元
[差分点利用法]

$$P_1 = (x_1, y_1)$$



y座標復元($P > 2$)の計算量

射影座標での計算量

加算点利用法

12M+S

差分点利用法

〔差分点を与えられた場合〕

10M+S

差分点利用法

〔差分点も計算〕

13M+2S

M: 乗算の計算量

S: 2乗算の計算量

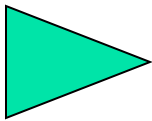


内容

はじめに

楕円曲線暗号における y 座標の必要性

y 座標復元



モンゴメリ型 **vs.**
ワイエルシュトラ
ス型



γ 座標復元とその効率性

- γ 座標復元は構成できたけど...
- でも他の方法と比べて効率的なの？



モンゴメリ型とワイエルシュトラス型との 高速性に関する比較

〔スカラー倍計算方法〕

〔S/M〕=0.8, 〔I/M〕=30

	ビット数			
	～ 295	～ 391	～ 481	～
ワイエルシュトラス型(w=4)	2 nd	3 rd	3 rd	2 nd
ワイエルシュトラス型(w=5)	3 rd	2 nd	1st	1st
モンゴメリ型	1st	1st	2 nd	3 rd

モンゴメリ型は391ビット未満のサイズでは最高速

w : window size

各数字は高速性に関する順番を表す

各種スキームにおける高速計算方法

(160ビット)

ECES ECElGamal ECDSA-V

Simultaneous-multi

不必要

不必要

1st

Montgomery with y

2nd

1st

2nd*

Montgomery without y

1st

計算不可

計算不可

Window-Method

3rd

2nd

3rd*

y 座標復元はこういった演算を要するスキームに有効

$$kP$$

$$kP + Q$$

$$kP + lQ$$

* : with comb method

各数字は高速性に関する順番を表す



結論

- [IOS01]: “Montgomery’s method **CAN** compute the y -coordinate of kP ”
- モンゴメリ法 $P > 2$ の y 座標復元方法の提案
- 楕円 ElGamal 暗号の最高速実行が可能
($kP + Q$ の演算を含むスキーム)

IOS01 桶屋-櫻井, y -座標復元を伴うモンゴメリ型楕円曲線上の
スカラー倍計算アルゴリズム, CHES2001, (2001)