Computer Security Symposium 2019
21 - 24 October 2019

楕円曲線のMe演算の負演算とその応用

白勢 政明[1,a)]

概要：著者は，有限体上定義された楕円曲線にMe演算 $\oplus$ を定義し，暗号への応用を試みてきた．Me演算の大きな特徴は，$+$ との分配律 $(P_1 \oplus P_2)+Q = (P_1+Q) \oplus (P_2+Q), P+(Q_1 \oplus Q_2) = (P+Q_1) \oplus (P+Q_2)$ を満たすことと，結合律を満たさないことである．本報告は，$\oplus$ の負演算 $\ominus$ を定義し，$\ominus$ を使った応用例として疑似乱数生成を考察する．

キーワード：楕円曲線，疑似乱数，離散対数問題，Me演算

Negative operation of Me operation of elliptic curve and its application

Masaaki Shirase[1,a)]

Abstract: The authors defined Me operation $\oplus$ on elliptic curve defined over finite field, and have tried application to cryptography. The major features of the Me operation are to satisfy the distribution law with $+$, $(P_1 \oplus P_2)+Q = (P_1+Q) \oplus (P_2+Q)$ and $P+(Q_1 \oplus Q_2) = (P+Q_1) \oplus (P+Q_2)$, and not to satisfy the associative law. The authors define the negative operation $\ominus$ of oplus and consider pseudorandom number generation as an application using $\ominus$ in this report.

Keywords: Elliptic curve, pseudorandom number, Discrete logarithm problem, Me operation

1. はじめに

近年，SSL/TLS通信において楕円曲線Diffie-Hellman (ECDH) 鍵共有や楕円曲線署名の1つのECDSAが用いられることが多くなっており，BitCoinのような暗号通貨でもECDSA用いられる場合がある．また，欧米ではv2x通信にECDSAが用いられることが決定した [1]．このように，楕円曲線暗号系は耐量子性は有しないものの，当面の実際的な公開鍵暗号としてますます普及する勢いである．

p を $p \equiv 3 \pmod 4$ となる7以上の素数とし，$E/\mathbb{F}_p$ を $\#E(\mathbb{F}_p)$ が奇数となる楕円曲線とする．著者は，$P, Q \in E(\mathbb{F}_p)$ に対して，Me演算 $\mathrm{Me(P,Q)} = \mathrm{P} \oplus \mathrm{Q}$ を定義した [4], [6]．これは由良によって定義された $\mathbb{F}_p$ 上M演算 [10] の楕円曲線版である．Me演算の大きな特徴は，べき等律，可換律，$+$ との分配律を満たすが，一般に結合律を満たさないことである．べき等律によりMe演算の繰り返しは意味をなさないが，補助元 $Z \in E(\mathbb{F}_p)$ を用いることで，ベースポイント P と自然数 n に対するMeスカラー倍 $P_{n,Z}$ が定義される．ECDLPのMe演算版MeDLPは P, Z, Q から $Q = P_{n,Z}$ を満たす n を見つける問題である．[8] では $E(\mathbb{F}_p)$ が巡回群をなし $2Z$ か $-Z$ が $E(\mathbb{F}_p)$ の生成元になる時，MeDLPはECDLPと同等に困難かより困難であることを示した．これは P, Z, Q を公開鍵，n を秘密鍵とする公開鍵暗号プロトコルの構成が可能かもしれないことを意味している．また，ペアリング e の双線形性

$$e(P, Q_1+Q_2) = e(P, Q_1) \cdot e(P, Q_2)$$

とMe演算の分配律

$$P+(Q_1 \oplus Q_2) = (P+Q_1) \oplus (P+Q_2)$$

は類似な性質であることから，ペアリングの代替としてMe演算が使用できるか模索した [5]．

しかしながらMe版ECCDH問題は簡単に解けてしま

[1] 公立はこだて未来大学
Future Unoversity Hakodate
[a)] shirase@fun.ac.jp

い [4]，多くの暗号プロトコルは ECDLP の困難性ではなく ECCDH 問題の困難性を利用しているため，今の所 Me 演算を用いた暗号プロトコルの構成はほとんど成功していない[*1]．

本稿は，$p \equiv 3 \pmod 4$ となる 7 以上の素数 p と $\#E(\mathbb{F}_p) = 2\times$ 奇数となる楕円曲線 $E/\mathbb{F}_p$ に対して，集合

$$\mathcal{E}(\mathbb{F}_p) = E(\mathbb{F}_p) \cup \{\mathcal{Z}\}$$

に Me 演算を拡張する．ここで $\mathcal{Z}$ は特別な元である．そして，$\mathcal{E}(\mathbb{F}_p)$ 上の Me 演算 $\oplus$ では，$\mathcal{Z}$ が単位元となり，$\oplus$ の負演算 (negative operation)$\ominus$ が定義できることを示す．すると，有限体上の四則演算を用いるプロトコル (の一部) の楕円曲線版を考えることができる．その例として，疑似乱数生成を考察する．

付録に本稿とは直接は関係しない Me 演算と Me スカラー倍の性質をまとめておく．また, 先行研究では MeDLP'(Me 演算版 DLP の 1 つ) は ECDLP と同等に困難かより困難であることが示されているが，[7] で与えた証明に欠陥が見つかり [8] でその欠陥を取り除いたため，証明が見づらくなっていた．ここでこの証明を整理しておく．

2. 準備

2.1 有限体

素数 p に対して集合

$$\mathbb{F}_p = \{0, 1, 2, \cdots, p-1\}$$

は体をなすことが知られている．また，

$$\mathbb{F}_p^* = \{1, 2, \cdots, p-1\}$$

と表す．$\mathbb{F}_p^*$ は $\mathbb{F}_p$ の (乗法に関する) 正則元の集合である．$g, g^a \in \mathbb{F}_p^*$ から a を求める問題を離散対数問題 (DLP) という．$g, g^a, g^b \in \mathbb{F}_p^*$ から g^{ab} を計算する問題を CDH 問題という．DLP を解ければ CDH 問題も解けることが簡単に分かり，これは DLP は CDH 問題と同等に困難かより困難であることを意味する．しかし，DLP が CDH 問題より困難であるかどうかは未解決である．

p が十分に大きい (例えば，$p \approx 2^{2048}$) ならば，現在の計算環境では DLP を解くことは困難である (と信じられている)．DH 鍵共有などの公開鍵暗号系は，DLP や CDH 問題の困難性を安全性の根拠としている．

2.2 楕円曲線

ある体 $\mathbb{K}$ に対して，E を Weierstrass 標準形

$$y^2 = x^3 + ax + b,\ a, b \in \mathbb{K} \qquad (1)$$

で与えられる $\mathbb{K}$ 上楕円曲線とする．E の $\mathbb{K}$-有理点の集合 $E(\mathbb{K})$ は，

$$E(\mathbb{K}) = \{(x, y) \in \mathbb{K} \times \mathbb{K} : (x, y) \text{ は (1) を満たす }\} \cup \{\mathcal{O}\}$$

で定義され，ここで $\mathcal{O}$ は無限遠点である．任意の $P, Q \in E(\mathbb{K})$ に対して，$P + Q \in E(\mathbb{K})$ が定義され，$(E(\mathbb{K}), +)$ は $\mathcal{O}$ を単位元とするアーベル群をなすことが知られている [2]，[9]．特に，$\mathbb{K}$ が有限体ならば $(E(\mathbb{K}), +)$ は有限アーベル群をなす．また，自然数 n と $P \in E(\mathbb{K})$ からスカラー倍 $nP = P + P + \cdots + P$(n 個の和) が定義される．

$\mathbb{K} = \mathbb{F}_p$(有限体) の場合，$P, nP \in E(\mathbb{F}_p)$ から n を求める問題を楕円曲線離散対数問題 (ECDLP) という．P, aP, bP から abP を計算する問題を ECCDH 問題という．ECDL を解ければ ECCDH 問題も解けることが簡単に分かり，これは ECDLP は ECCDH 問題と同等に困難かより困難であることを意味する．しかし，ECDLP が ECCDH 問題より困難であるかどうかは未解決である．

p が十分に大きく (例えば，$p \approx 2^{256}$) かつ適切に楕円曲線の係数 a, b を選ぶならば，現在の計算環境では ECDLP を解くことは困難である (と信じられている)．楕円曲線暗号系は，ECDLP や ECCDH 問題の困難性を安全性の根拠としている．

2.3 楕円曲線上の Me 演算と Me スカラー倍

2.3.1 定義と性質

p を $p \equiv 3 \pmod 4$ を満たす 7 以上の素数とする．$E/\mathbb{F}_p$ を Weierstrass 標準形 $y^2 = x^3 + ax + b$ で与えられる楕円曲線とし，更に $\#E(\mathbb{F}_p)$ は奇数であるとする．すると，$(x_0, 0)$ の形の点は $E(\mathbb{F}_p)$ には存在しない[*2]．

関数 $\mathrm{sign} : E(\mathbb{F}_p) \setminus \{\mathcal{O}\} \to \{\pm 1\}$ を

$$\mathrm{sign}((x_0, y_0)) = \left(\frac{y_0}{p}\right)$$

と定義する．ここで，$\left(\frac{\cdot}{\cdot}\right)$ は Legendre 記号である．すると，$P \in E(\mathbb{F}_p) \setminus \{\mathcal{O}\}$ に対して $\mathrm{sign}(P)$ と $\mathrm{sign}(-P)$ は異符号である．

Me 演算 $\mathrm{Me} : E(\mathbb{F}_p) \times E(\mathbb{F}_p) \to E(\mathbb{F}_p)$ を $k \in \mathbb{N}$ を 1 つ固定して

$$\mathrm{Me}(P, Q) = \begin{cases} P & P = Q \text{ の時} \\ kP - (k-1)Q & \mathrm{sign}(P - Q) = 1 \text{ の時} \\ kQ - (k-1)P & \mathrm{sign}(P - Q) = -1 \text{ の時} \end{cases}$$

と定義する．$P \oplus Q = \mathrm{Me}(P, Q)$ と書くことにする．Me 演算は次の性質を持つ．

命題 1 ([4])
$P, Q, R \in E(\mathbb{F}_p)$ に対して，次が成り立つ．
(a) べき等律: $P \oplus P = P$.

[*1] 電子署名の場合 ECDLP の困難性をベースにしているものがあり，[7] で Me 演算を用いた電子署名を提案した．

[*2] $(x_0, 0) \in E(\mathbb{F}_p) \Leftrightarrow \#E(\mathbb{F}_p)$ は偶数，である．

(b) 可換律: $P \oplus Q = Q \oplus P$.
(c) $+$ との分配律: $(P \oplus Q) + R = (P + R) \oplus (Q + R)$,
$P + (Q \oplus R) = (P + Q) \oplus (P + R)$.

2.4 DLP の困難性を利用した疑似乱数

[3] で紹介されている離散対数問題の困難性を利用した疑似乱数生成は，次のように行われる．
(1) $g \in \mathbb{F}_p^*$ を生成元とし，$a_0 \in \mathbb{N}$ を 1 つ選ぶ．
(2) 再帰的に

$$a_i = g^{a_{i-1}} - 1 \tag{2}$$

とし，LSB(a_i) の連結を疑似乱数とする．

この楕円曲線版を提案することが本稿の目的の 1 つである．

3. 本稿の寄与

本節では，p は 7 以上の $p \equiv 3 \pmod 4$ を満たす素数とする．$\#E(\mathbb{F}_p)$ が $2\times$ 奇数の場合に対して，$E(\mathbb{F}_p)$ に特別な元 $\mathcal{Z}$ を追加した集合 $\mathcal{E}(\mathbb{F}_p)$ に Me 演算を定義し，Me 演算の負演算が定義されることを示す．それから，Me 演算の負演算を利用するアプリケーション例として，ECDLP に困難性を利用した疑似乱数生成法を提案する．

3.1 Me 演算の負演算

p は $p \equiv 3 \pmod 4$ を満たす 7 以上の素数とし，$E/\mathbb{F}_p$ を Weierstrass 標準形 $y^2 = x^3 + ax + b$ で与えられる $\mathbb{F}_p$ 上楕円曲線とし，更に $\#E(\mathbb{F}_p)$ は $2\times$ 奇数であるとする[*3]．すると，$E(\mathbb{F}_p)$ には位数 2 の点 T が 1 つだけ存在する．T の y 座標は 0 であることに注意されたい．集合 $\mathcal{E}(\mathbb{F}_p)$ を

$$\mathcal{E}(\mathbb{F}_p) = E(\mathbb{F}_p) \cup \{\mathcal{Z}\}$$

と定義する．ここで，$\mathcal{Z}$ は特別な元である[*4]．$E(\mathbb{F}_p)$ 上の加算 $+$ を次のように $\mathcal{E}(\mathbb{F}_p)$ 上に拡張する．

$$\forall P \in E(\mathbb{F}_p) \text{ に対して } P + \mathcal{Z} = \mathcal{Z} + P = \mathcal{Z} \tag{3}$$

$$\mathcal{Z} + \mathcal{Z} = \mathcal{Z} \tag{4}$$

なお，次の命題より $-\mathcal{Z}$ は定義されない．

命題 2
$-\mathcal{Z} \in \mathcal{E}(\mathbb{F}_p)$ は存在しない．
$\because$) $P = -\mathcal{Z}$ となる $P \in \mathcal{E}(\mathbb{F}_p)$ が存在すると仮定する．すると，

$$P + \mathcal{Z} = \mathcal{O}$$

を満たす．しかしながら，(3) と (4) より $P + \mathcal{Z} = \mathcal{Z} \neq \mathcal{O}$ となり矛盾である．□

定義 3
演算 sign : $\mathcal{E}(\mathbb{F}_p) \setminus \{\mathcal{O}\} \to \{0, \pm 1\}$ をルジャンドル記号を用いて

$$\mathrm{sign}((x_0, y_0)) = \left(\frac{y_0}{p}\right)$$

と定義する．

定義 4
(a) 演算 Me : $\mathcal{E}(\mathbb{F}_p) \times \mathcal{E}(\mathbb{F}_p) \to \mathcal{E}(\mathbb{F}_p)$ を 2 以上の整数 k を 1 つ固定して次のように定義する．
(a)-(i) 任意の $P \in \mathcal{E}(\mathbb{F}_p)$ に対して

$$\mathrm{Me}(P, \mathcal{Z}) = \mathrm{Me}(\mathcal{Z}, P) = P$$

(a)-(ii) 共に $\mathcal{Z}$ でない P, Q に対して

$$\mathrm{Me}(P, Q) = \begin{cases} P & P = Q \text{ の時} \\ \mathcal{Z} & \mathrm{sign}(P - Q) = 0 \text{ の時} \\ kP - (k-1)Q & \mathrm{sign}(P - Q) = 1 \text{ の時} \\ kQ - (k-1)P & \mathrm{sign}(P - Q) = -1 \text{ の時} \end{cases}$$

と定義する．演算子 $\oplus$ を用いて

$$P \oplus Q = \mathrm{Me}(P, Q)$$

と書くことにする．
(b) $P \in \mathcal{E}(\mathbb{F}_p)$ に対して，$\ominus P$ を

$$\ominus P = P + T$$

と定義する．$P \oplus (\ominus Q)$ を $P \ominus Q$ と書くことにする．

命題 5
$\mathcal{Z} \in \mathcal{E}(\mathbb{F}_p)$ と任意の $P \in \mathcal{E}(\mathbb{F}_p)$ に対して
(a) $\ominus \mathcal{Z} = \mathcal{Z}$,
(b) $P \ominus P = \mathcal{Z}$,
(c) $\ominus \mathcal{O} = T$,
が成り立つ．
$\because$) (a) 次の計算による．

$$\begin{aligned} \ominus\mathcal{Z} &= \mathcal{Z} + T && \text{定義 4 の (b) より} \\ &= \mathcal{Z} && \text{(3) より} \end{aligned}$$

(b) $P = \mathcal{Z}$ の時，次の計算が得られる．

$$\begin{aligned} \mathcal{Z} \ominus \mathcal{Z} &= \mathcal{Z} \oplus (\ominus\mathcal{Z}) \\ &= \mathcal{Z} \oplus \mathcal{Z} && \text{(a) より} \\ &= \mathcal{Z} && \text{定義 4 の (a) より} \end{aligned}$$

$P \neq \mathcal{Z}$ の時，定義 4 の (b) より $\ominus P = P + T$ なので，

$$P \ominus P = P \oplus (P + T)$$

となるが，$\mathrm{sign}(P - (P + T)) = \mathrm{sign}(-T) = 0$ なので，定義 4 の (a) より $P \ominus P = \mathcal{Z}$ である．

[*3] 2.3 節や Me 演算の先行研究では，$\#E(\mathbb{F}_p)$ は奇数であることに注意されたい．
[*4] 無限遠点 $\mathcal{O}$ は $E(\mathbb{F}_p)$ の特別な元であるとよく言われるが，射影座標系では $\mathcal{O}$ は (∞ を用いず) 表現できる．これに対して $\mathcal{Z}$ は全くの (記号的な) 特別な元である．
後に示すように $\mathcal{Z}$ は体の加法の単位元 0 に対応するため，zero の頭文字から記号 $\mathcal{Z}$ を採用した．

(c) $\ominus\mathcal{O} = \mathcal{O} + T = T$. □

定義 4 の (a) は $\mathcal{Z}$ が単位元となるように (やや強引に) $\mathcal{E}(\mathbb{F}_p)$ 上に $\oplus$ を定義した．定義 4 の (b) のように $\ominus$ を定義すると，命題 5 の (b) より $\ominus$ は $\oplus$ の負演算となることが分かる．

$\mathcal{E}(\mathbb{F}_p)$ 上 Me 演算に対して次が得られる．

命題 6

$P, Q, R \in \mathcal{E}(\mathbb{F}_p)$ に対して，次が成り立つ．

(a) $P \oplus P = P$.

(b) $P \oplus Q = Q \oplus P$.

(c) $(P \oplus Q) + R = (P + R) \oplus (Q + R)$,
$P + (Q \oplus R) = (P + Q) \oplus (P + R)$.

(d) 一般に $(P \oplus Q) \oplus R \neq P \oplus (Q \oplus R)$.

∵) $P, Q, R \in E(\mathbb{F}_p)$ の場合は命題 1 に依る．

(a) $P = \mathcal{Z}$ の時，定義 4 の (a) より $\mathcal{Z} \oplus \mathcal{Z} = \mathcal{Z}$ となる．

(b) $P = \mathcal{Z}$ の時，定義 4 の (a) より

$$\mathcal{Z} \oplus Q = Q \oplus \mathcal{Z} = Q$$

となる．$Q = \mathcal{Z}$ の時も同様.

(c) $P = \mathcal{Z}$ とする．すると次が得られる．

$$\begin{aligned} (\mathcal{Z} \oplus Q) + R &= Q + R \\ (\mathcal{Z} + R) \oplus (Q + R) &= \mathcal{Z} \oplus (Q + R) \\ &= Q + R \end{aligned}$$

よって，$(\mathcal{Z} \oplus Q) + R = (\mathcal{Z} + R) \oplus (Q + R)$ である．更に，

$$\begin{aligned} \mathcal{Z} + (Q \oplus R) &= \mathcal{Z} \\ (\mathcal{Z} + Q) \oplus (\mathcal{Z} + R) &= \mathcal{Z} \oplus \mathcal{Z} \\ &= \mathcal{Z} \end{aligned}$$

より，$\mathcal{Z} + (Q \oplus R) = (\mathcal{Z} + Q) \oplus (\mathcal{Z} + R)$ である．$Q = \mathcal{Z}$ や $R = \mathcal{Z}$ の時も同様.

(d) 命題 1 より．□

以上より，$(\mathcal{E}(\mathbb{F}_p), \oplus, +)$ は次の性質を持つことが分かる．

(a) 命題 5 より，$\mathcal{Z}$ は $\oplus$ に関する単位元であり，$\forall P \in \mathcal{E}(\mathbb{F}_p)$ に対して $\oplus$ に関する逆元 $\ominus P \in \mathcal{E}(\mathbb{F}_p)$ が存在する．

(b) $(\mathcal{E}(\mathbb{F}_p) \setminus \{\mathcal{Z}\}, +) = (E(\mathbb{F}_p), +)$ は $\mathcal{O}$ を単位元とする群をなす．(これは楕円曲線の一般的な性質である．)

(c) 命題 6 より，$\oplus$ と $+$ は分配律を満たす．

これらは体 $(K, +, \cdot)$ の定義に類似している．

(a) $(K, +)$ は 0 を単位元とする群をなす．つまり，$+$ に関して分配律を満たし，$+$ に関する単位元 $0 \in K$ が存在し，$\forall a \in K$ に対して $+$ に関する逆元 $-a \in K$ が存在する．

(b) $(K \setminus \{0\}, \cdot)$ は 1 を単位元とする群をなす．

(c) $+$ と $\cdot$ は分配律を満たす．

つまり，$(\mathcal{E}(\mathbb{F}_p), +, \oplus)$ は，$\oplus$ が結合律を満たさないこと以外は体と同じ性質を持つ．従って，有限体の四則演算を利用するアプリケーションに対して，その楕円曲線版を構成できるかもしれない．

3.2 ECDLP の困難性を利用した疑似乱数生成

2.4 節で紹介した疑似乱数生成の楕円曲線版を構成できる．p は $p \equiv 3 \pmod 4$ を満たす 7 以上の素数とし，$E/\mathbb{F}_p$ を Weierstrass 標準形 $y^2 = x^3 + ax + b$ で与えられる $\mathbb{F}_p$ 上楕円曲線とし，更に $\#E(\mathbb{F}_p)$ は $2 \times l$ (l は素数) であるとする．次のように疑似乱数を生成する．

(1) $G \in E(\mathbb{F}_p)$ を位数 $2l$ の点とし (つまり G は $E(\mathbb{F}_p)$ の生成元)，$a_0 \in \mathbb{N}$ を 1 つ選ぶ.

(2) 再帰的に

$$a_i = x(a_{i-1}G \oplus T) \tag{5}$$

とし，$\mathrm{LSB}(a_i)$ の連結を疑似乱数とする．

2.4 節の DLP を困難性を利用した疑似乱数生成とこの疑似乱数生成を比較する．(2) の g^{a_0} は g の乗算 $\cdot$ の a_0 回の繰り返しであり，(5) の a_0G は G の加算 $+$ の a_0 回の繰り返しである．$g^{a_0} - 1$ は g^{a_0} に乗法単位元 1 の加法逆元 -1 を $+$ しており，$a_0G + T$ は a_0G に加法単位元 $\mathcal{O}$ の Me 演算 $\oplus$ の逆元 T を $\oplus$ している．

4. まとめと今後の課題

本稿は，$\#E(\mathbb{F}_p) = 2\times$ 奇数となる楕円曲線 $E/\mathbb{F}_p$ に対して，$\mathcal{E}(\mathbb{F}_p) = E(\mathbb{F}_p) \cup \{\mathcal{Z}\}$ 上に Me 演算 $\oplus$ を定義した．$\mathcal{E}(\mathbb{F}_p)$ 上 Me 演算には $\oplus$ の負演算 $\ominus$ が定義でき，$(\mathcal{E}(\mathbb{F}_p), \oplus, +)$ は $\oplus$ が結合律を満たさないこと以外は体と同じ性質を持つことを示した．それから，本稿は $\ominus$ を用いる疑似乱数生成を提案した．

今後の課題として，$(\mathcal{E}(\mathbb{F}_p), \oplus, +)$ の体の類似性を利用した暗号プロトコルを提案していきたい．

謝辞

本研究は，JSPS 科研費 19K11966 の助成を受けたものです．

参考文献

[1] 一般財団法人日本自動車研究所：平成 27 年度戦略的イノベーション創造プログラム (自動走行システム)：v2x 等車外情報の活用にかかるセキュリティ技術の研究・開発プロジェクト, 2016. http://www.meti.go.jp/meti_lib/report/2016fy/000459.pdf.

[2] 宮地充子：代数学から学ぶ暗号理論, 日本評論社, 2012.

[3] 岡本栄司：暗号理論入門第 2 版, 共立出版, 2002.

[4] 白勢政明： 有限体上 M 関数の有限体上楕円曲線への拡張とその応用, *CSS2017*, 2017.

[5] 白勢政明. 新しい暗号演算を用いたキーワード検索暗号, *SCIS2018*, 2018.

[6] M. Shirase： New operation and problems on elliptic curve and their application, *ICCE-TE2018*, 2018.

[7] 白勢政明：有限体上楕円曲線の新しい演算に基づく離散対数問題の困難性とディジタル署名, *ISEC2018-1*, 2018.

[8] 白勢政明：有限体上楕円曲線の新しい演算に基づく DLP と ECDLP の関係, *CSS2018*, 2018.

[9] J. H. Silverman： *The arithmetic of elliptic curves*, Springer-Verlag New York, 1985.

[10] F. Yura : Solitons with nested structure over finite fields, *Journal of Physics A: Mathematical and Theoretical*, Vol. 47, pp. 1–23, 2014.

付　　録

A.1 $\#E(\mathbb{F}_p)$ = 奇数の場合の Me 演算

先行研究では $\#E(\mathbb{F}_p)$ = 奇数となる楕円曲線 $E(\mathbb{F}_p)$ 上の Me 演算を扱ってきた．ここではその性質をいくつか紹介する．

A.1.1 Me スカラー倍

Me 演算 $\oplus$ のべき等律より

$$(\cdots(((P\oplus P)\oplus P)\oplus P)\oplus\cdots P)\oplus P = P$$

となり，$\oplus$ の繰り返しは意味をなさない．先行研究 [4], [6] では，$P, Z \in E(\mathbb{F}_p)$ に対してアルゴリズム 1 の出力により，**P をベースポイント，Z を補助元とする Me スカラー倍**を定義した．

アルゴリズム 1 (Me スカラー倍の計算)

入力: $P, Z \in E(\mathbb{F}_p), n = (1\, n_{l-2} n_{l-3} \cdots n_0)_2 \in \mathbb{N}$
出力: $P_{n,Z} \in E(\mathbb{F}_p)$

1. $Y = P$
2. **for** $i = l-2$ **down to** 0
3. $\quad Y = (Z+Y)\oplus Y$
4. $\quad$ **if** $n_i = 1$ **then** $Y = Y \oplus P$
5. **end for**
6. **return** Y

Me スカラー倍は次のような性質を持つ．

命題 7 ([4], [6])
$P, Q, Z \in E(\mathbb{F}_p), n \in \mathbb{N}$ に対して，次が成り立つ．
(a) $P_{n,Z} + Q = P + Q_{n,Z} = (P+Q)_{n,Z}$
(b) $P_{n,Z} \oplus Q_{n,Z} = (P \oplus Q)_{n,Z}$
(c) $(P_{n,Z})_{m,Z} = (P_{m,Z})_{n,Z} = P_{n,Z} + P_{m,Z} - P$

$P, Q \in E(\mathbb{F}_p)$ から $Q = nP$ を満たす $n \in \mathbb{N}$ を求める問題を ECDLP と言い，その具体例を ECDLP インスタンス (P, Q) と言うように，Me スカラー倍に関する問題を次のように定義する．

定義 8
(a) $P, Z, Q \in E(\mathbb{F}_p)$ から $Q = P_{n,Z}$ を満たす $n \in \mathbb{N}$ を求める問題を **Me スカラー倍の離散対数問題 (MeDLP)** といい，その具体例を MeDLP インスタンス (P, Z, Q) という．
(b) $P, z(\in \mathbb{Z}), Q$ から $Q = P_{n,zP}$ を満たす $n \in \mathbb{N}$ を求める問題を **Me スカラー倍の改良版離散対数問題 (MeDLP')** といい，その具体例を MeDLP' インスタンス (P, z, Q) という．
(c) $P, Z, P_{n,Z}, P_{m,Z} \in E(\mathbb{F}_p)$ から $(P_{n,Z})_{m,Z} = (P_{m,Z})_{n,Z}$ を計算する問題を **Me スカラー倍の CDH 問題 (MeCDH)** といい，その具体例を MeCDH インスタンス $(P, Z, P_{n,Z}, P_{m,Z})$ という．

命題 7 の (c) より MeCDH 問題は簡単に解けてしまう．しかしながら，MeDLP' は困難問題である．

A.1.2 MeDLP' の困難性

A.1.2 節では Me 演算の定義の k は $k = 2$ に限定する．

条件 9
$E(\mathbb{F}_p)$ と $P \in E(\mathbb{F}_p)$，$z \in \mathbb{Z}$ は次の (a) または (b) を満たす．
(a) $E(\mathbb{F}_p)$ は巡回群をなし，$Z = zP$ は

$$\mathrm{sign}(Z) = 1 \text{ かつ } 2Z \text{ は } E(\mathbb{F}_p) \text{ の生成元}$$

または

$$\mathrm{sign}(Z) = -1 \text{ かつ } -Z \text{ は } E(\mathbb{F}_p) \text{ の生成元}$$

である．
(b) $\#E(\mathbb{F}_p)$ は 3 以上の素数で，$P \neq \mathcal{O}, z \neq 0$.

条件 9 の (a) は (b) を含むことに注意されたい．

定理 10
$E(\mathbb{F}_p)$，$P \in E(\mathbb{F}_p)$，$z \in \mathbb{Z}$ は条件 9 を満たすとする．$l = \#E(\mathbb{F}_p)$ とする．$E(\mathbb{F}_p)$ と Z は条件 9 を満たすと仮定する．すると，$\forall Q \in E(\mathbb{F}_p)$ に対して MeDLP' インスタンス (P, z, Q) に解が存在し，その解を使って ECDLP インスタンス (P, Q) の解を多項式時間で構成できる．

$E(\mathbb{F}_p)$ は巡回群をなすとする．$P \in E(\mathbb{F}_p)$ を生成元，$l = \#E(\mathbb{F}_p)$ とする．MeDLP' インスタンス (P, z, Q) を解くオラクル $\mathcal{A}$ が存在すると仮定する．すると，ECDLP インスタンス (P, Q) を $\mathcal{A}$ を使って次のようにして解くことができる．
(i) $Z = zP$ が条件 9 を満たすように $z \in \mathbb{Z}$ を選ぶ．
(ii) $\mathcal{A}$ を使って MeDLP' インスタンス (P, z, Q) の解 n を得る．
(iii) 定理 10 より多項式時間で ECDLP インスタンス (P, Q) の解を構成できる．

これは，

$$\text{MeDLP' の困難さ} \geq \text{ECDLP の困難さ}$$

であることを意味する．

この定理の証明は，MeDLP' インスタンスの解の存在性を示すことと，MeDLP' インスタンスの解を入力すると ECDLP インスタンスの解を出力するアルゴリズムの構成からなる．

A.1.2.1 MeDLP' インスタンスの解の存在

A.1.2.1 節の主結果は命題 14 である．まず，命題 14 の証明に必要な 3 つの補題を与える．命題 12 は A.1.3 節でも用いられる．

補題 11

$P, Z \in E(\mathbb{F}_p), n \in \mathbb{N}$ に対して

$$P_{2n,Z} = (Z + P_{n,Z}) \oplus P_{n,Z}$$

である．

∵) [8] を参照．□

補題 12

任意の $Z \in E(\mathbb{F}_p), Z \neq \mathcal{O}, n \in \mathbb{N}$ に対して，

$$\mathcal{O}_{2^n,Z} = \begin{cases} 2nZ & \text{sign}(Z) = 1 \text{ の時} \\ -nZ & \text{sign}(Z) = -1 \text{ の時} \end{cases}$$

成り立つ．

∵) 補題 11 と n に関する数学的帰納法を用いる．詳細は [8] を参照.

補題 13

$E(\mathbb{F}_p)$ と $Z \in E(\mathbb{F}_p)$ は条件 9 を満たすと仮定する．すると，任意の $P \in E(\mathbb{F}_p)$ に対して，

$$\{P_{n,Z} \ : \ n = 1, 2, 3, \cdots\} = E(\mathbb{F}_p)$$

となる．

∵) 補題 12 を用いる．詳細は [8] を参照．□

命題 14

(a) $P \in E(\mathbb{F}_p)$ を生成元，$z \in \mathbb{Z}$ に対して $Z = zP$ とする．$E(\mathbb{F}_p)$ と Z は条件 9 を満たすと仮定する．すると，任意の $Q \in E(\mathbb{F}_p)$ に対して MeDLP' インスタンス (P, z, Q) は解を持つ．

(b) $E(\mathbb{F}_p)$ と $Z \in E(\mathbb{F}_p)$ は条件 9 を満たすと仮定する．すると，任意の $P, Q \in E(\mathbb{F}_p)$ に対して MeDLP インスタンス (P, Z, Q) は解を持つ．

∵) (a) 補題 13 より $E(\mathbb{F}_p) = \{P_{n,Z} \ : \ n = 1, 2, 3, \cdots\}$ であるから，$Q = P_{n',Z}$ と書ける $n' \in \mathbb{N}$ が存在する．この n' は MeDLP' インスタンス (P, z, Q) の解である．

(b) (a) と同様．□

A.1.2.2 MeDLP' の解を用いる ECDLP の解法

$l = \#E(\mathbb{F}_p)$ とする．$\mathcal{P} \in E(\mathbb{F}_p) \times \mathbb{Z}/l\mathbb{Z}$ に対して，$\mathcal{P}[1]$ は $\mathcal{P}$ の第 1 成分を，$\mathcal{P}[2]$ は $\mathcal{P}$ の第 2 成分を表すとする．$E(\mathbb{F}_p) \times \mathbb{Z}/l\mathbb{Z}$ 上の演算 $+$ を次のように定義する．

$$\mathcal{P} + \mathcal{Q} = (\mathcal{P}[1] + \mathcal{Q}[1], \mathcal{P}[2] + \mathcal{Q}[2])$$

$\mathcal{P}, \mathcal{Q} \in E(\mathbb{F}_p) \times \mathbb{Z}/l\mathbb{Z}$ に対して，$k \in \mathbb{N}$ を 1 つ固定して，$\mathcal{P} \oplus \mathcal{Q}$ を次のように定義する．

$$\mathcal{P} \oplus \mathcal{Q} = \begin{cases} (\mathcal{P}[1], \mathcal{P}[2]) & \text{if } \mathcal{P}[1] = \mathcal{Q}[1] \\ (k\mathcal{P}[1] - (k-1)\mathcal{Q}[1], k\mathcal{P}[2] - (k-1)\mathcal{Q}[2]) & \text{if sign}(\mathcal{P}[1] - \mathcal{Q}[1]) = 1 \\ (k\mathcal{Q}[1] - (k-1)\mathcal{P}[1], k\mathcal{Q}[2] - (k-1)\mathcal{P}[2]) & \text{if sign}(\mathcal{P}[1] - \mathcal{Q})[1] = -1 \end{cases}$$

これは $E(\mathbb{F}_p)$ 上 Me 演算の $E(\mathbb{F}_p) \times \mathbb{Z}/l\mathbb{Z}$ への拡張である．$E(\mathbb{F}_p)$ 上の $\oplus$ の定義と $E(\mathbb{F}_p) \times \mathbb{Z}/l\mathbb{Z}$ 上の $\oplus$ の定義より

$$(\mathcal{P} \oplus \mathcal{Q})[1] = \mathcal{P}[1] \oplus \mathcal{Q}[1]$$

であることが簡単に分かる．

アルゴリズム 1 に類似した次のアルゴリズム 2 を考える．

アルゴリズム 2

入力: $P \in E(\mathbb{F}_p), z \in \mathbb{Z}/l\mathbb{Z}, n = (1\, n_{l-2} n_{l-3} \cdots n_0)_2 \in \mathbb{N}$
出力: $\mathcal{Y} \in E(\mathbb{F}_p) \times \mathbb{Z}/l\mathbb{Z}$

1. $\mathcal{P} = (P, 1)$
2. $\mathcal{Z} = (zP, z)$
3. $\mathcal{Y} = \mathcal{P}$
4. **for** $i = l - 2$ **down to** 0
5. $\quad \mathcal{Y} = (\mathcal{Z} + \mathcal{Y}) \oplus \mathcal{Y}$
6. $\quad$ **if** $n_i = 1$ **then** $\mathcal{Y} = \mathcal{Y} \oplus \mathcal{P}$
7. **end for**
8. **return** $\mathcal{Y}$

このアルゴリズムの出力に対して，次が成り立つ．

命題 15

$P \in E(\mathbb{F}_p), z \in \mathbb{Z}/l\mathbb{Z}, n \in \mathbb{N}$ を入力した時のアルゴリズム 4 の出力を $\mathcal{Y}'$ とする．

(a) $\mathcal{Y}'[1] = P_{n,zP}$

(b) $\mathcal{Y}'[2]P = P_{n,zP}$

∵) [7] を参照．□

A.1.2.3 定理 10 の証明

命題 14 より MeDLP' インスタンス (P, z, Q) の解 $n \in \mathbb{N}$ が存在する．(P, z, n) を入力としてアルゴリズム 2 を実行すると，補題 15 の (b) よりその出力の第 2 成分 t は $tP = Q$ を満たす．よって，この t は ECDLP インスタンス (P, Q) の解である．

A.1.3 その他の性質

定理 10 とは逆に，ECDLP インスタンスの解を使って MeDLP' インスタンスの解は得られないだろうか? 次の命題はこの問の答えである．

命題 16

Me 演算の定義の k は $k = 2$ に限定する．$(\mathcal{O} \neq) P \in E(\mathbb{F}_p), l = \#E(\mathbb{F}_p), z \in \mathbb{Z}, z \neq 0$ に対して，$Z = zP$ とす

る．ECDLP インスタンス $(Z, Q-P)$ は解 m を持つとする．(つまり $Q-P=mZ$．) n を次のように定義する．

$$n = \begin{cases} m/2 \bmod l & \mathrm{sign}(Z)=1 \text{ の時} \\ -m \bmod l & \mathrm{sign}(Z)=-1 \text{ の時} \end{cases} \quad \text{(A.1)}$$

すると，2^n は MeDLP' インスタンス (P, z, Q) の解である．
∵) 補題 12 より $Q-P=mZ=\mathcal{O}_{2^n,Z}$ が成り立ち，命題 7 の (c) より

$$Q = \mathcal{O}_{2^n,Z} + P = P_{2^n,Z}$$

となる．よって，2^n は MeDLP' インスタンス (P, z, Q) の解である．□

ECDLP インスタンスを解くオラクル $\mathcal{B}$ が存在すると仮定する．すると，MeDLP' インスタンス (P, z, Q) を $\mathcal{B}$ を使って次のようにして解くことができる．
(i) $(zP, Q-P)$ を $\mathcal{B}$ へ入力し，$\mathcal{B}$ からの出力 m を得る．
(ii) 式 (A.1) により n を計算する．
(iii) 2^n は MeDLP' インスタンス (P, z, Q) の解である．

ECC で用いる $E(\mathbb{F}_p)$ を対象とする．$p \approx 2^{256}(\approx \#E(\mathbb{F}_p))$ であるため，上記で得られる n は (p の約半分として)$n \approx 2^{255}$ となる．よって，上記で得られる MeDLP' インスタンスの解 2^n は (255 ビットでなく)2^{255} ビットである．従って，MeDLP' インスタンスの解 2^n を使って $R_{2^n,Z}$ を計算するには ECDLP の解のサイズの指数時間を要する．よって，

$$\text{MeDLP' の困難さ} \leq \text{ECDLP の困難さ}$$

は言えるかもしれないが，

MeDLP' の困難さを根拠とする公開鍵暗号の安全性
$\leq$ ECDLP の困難さを根拠とする公開鍵暗号の安全性

と言えるか不明である．

次の命題は，[7] で提案したディジタル署名の署名生成・検証で必要な Me スカラー倍の性質である．

命題 17
$n \in \mathbb{N}, Z, Q \in E(\mathbb{F}_p)$ から $Q = P_{n,Z}$ となる $P \in E(\mathbb{F}_p)$ を求めることができる．実際にランダムに $R \in E(\mathbb{F}_p)$ を選び，

$$P = Q - R_{n,Z} + R$$

とすれば良い．
∵) 次の計算による．

$$\begin{aligned} P_{n,Z} &= (Q - R_{n,Z} + R)_{n,Z} \\ &= ((Q - R_{n,Z}) + R)_{n,Z} \\ &= (Q - R_{n,Z}) + R_{n,Z} \quad \text{命題 7 の (c) より} \\ &= Q \quad \square \end{aligned}$$

A.1.4 注意

A.1.2 節 (特に定理 10) や命題 16 では Me 演算の定義に必要な k を $k=2$ に限定しているが，これは $k \neq 2$ では定理や命題，補題が成り立たないということではなく，まだ調べていないということである．おそらく他の k でもこれらの定理と命題，補題は (少し形を変えて) 成り立つと思われる．

A.1.5 MeDLP' の困難性を利用した暗号プロトコル

定理 10 より MeDLP' は ECDLP と同等に困難かより困難であるため，$Q = P_{s,zP}$ を満たす $P, Q, \in E(\mathbb{F}_p), z \in \mathbb{Z}, s \in \mathbb{N}$ に対して，(P, z, Q) を公開鍵，s を秘密鍵とするような暗号プロトコルを構成できるかもしれない．例えば，既存の ECC のプロセスでのスカラー倍を Me スカラー倍に置き換えると新しい暗号プロトコルが得られる．ECDH 鍵共有の Me 版は次のようになる．

(1) $P \in E(\mathbb{F}_p), z \in \mathbb{Z}$ をシステムパラメータとする．
(2) ユーザ A はランダムに $a \in \mathbb{Z}$ を選び $P_A = P_{a,zP}$ を計算し，P_A をユーザ B に送る．
(3) ユーザ B はランダムに $b \in \mathbb{Z}$ を選び $P_B = P_{b,zP}$ を計算し，P_B をユーザ A に送る．
(4) ユーザ A は，P_B の受信後 $K_A = (P_B)_{a,zP}$ を計算する．
(5) ユーザ B は，P_A の受信後 $K_B = (P_A)_{b,zP}$ を計算する．

命題 7 の (c) より $K_A = K_B$ となる．しかしながら，a, b を知らない第三者でも P, P_A, P_B を入手すると，$K_A = P_A + P_B - P$ により K_A を入手できてしまう．これは (MeDLP' は困難であるが)MeCDH 問題が困難でないためである．つまり，ECCDH 問題の困難性を利用している ECC に対して Me スカラー倍への置き換えで得られる暗号プロトコルは安全でない．

Me 演算を暗号プロトコルに用いるには次の 3 つが考えられる．

(1) 置き換え以外の処理を追加する．
→ 著者はこの方法を試みてきたが，今の所成功していない．
(2) ECDLP の困難性を利用している暗号プロトコルを対象とする．
→ 例えば Schnorr 署名は (ECCDH でなく)ECDLP の困難性を利用している．著者は Me 演算を用いる電子署名を [7] で提案しているが，同じ $E(\mathbb{F}_p)$ を用いる楕円曲線署名より署名長が長く計算コストも大きくなってしまう．
(3) 別の鍵共有法を探す．
→$(a, P_{a,Z})$ と $(b, P_{b,Z})$ から，$(P_{a,Z})_{b,Z}$ 以外に共有鍵があるだろうか? 見つかったとして安全であるか?