Computer Security Symposium 2018
22 - 25 October 2018

有限体上楕円曲線の新しい演算に基づくDLPとECDLPの関係

白勢 政明[1]

概要：著者は，有限体上楕円曲線 $E/\mathbb{F}_p$ 及び $P, Z \in E(\mathbb{F}_p), n \in \mathbb{N}$ に対して P をベースポイント，Z を補助元とする Me スカラー倍 $P_{n,Z}$(Me は M operation for elliptic curve の意味) を定義し，$P, Z, Q \in E(\mathbb{F}_p)$ から $Q = P_{n,Z}$ となる n を見つける問題を MeDLP と定義した．更に，$z \in \mathbb{Z}$ に対して，P, z, Q から $Q = P_{n,zP}$ となる n を見つける問題を MeDLP' と定義した．著者は 2018 年 5 月の ISEC[5] にて，MeDLP' インスタンスが解を持つ場合，その MeDLP' インスタンスを解けるならば，対応する ECDLP インスタンスをその MeDLP' インスタンスの解を使って多項式時間で解けることを示した．しかし，いつ MeDLP' が解を持つかは不明であった．本稿は，$E(\mathbb{F}_p)$ が巡回群の時，$z \in \mathbb{Z}$ を適切に選べば MeDLP' インスタンスが解を持つことを示す．更に，ECDLP インスタンスを解いて解 m が得られるならば，m から簡単に計算できる $n \in \mathbb{Z}$ に対して，2^n はある MeDLP' インスタンスの解であることを示す．なお，2^n は $\log_2 n$ ビットではなく n ビットであることに注意されたい．

キーワード：楕円曲線，ECDLP，一方向性関数，Me 演算，Me スカラー倍，MeDLP

Relationship Between the DLP based on New Operation on Elliptic Curve over Finite Field and the ECDLP

Masaaki Shirase[1]

Abstract: The author defined the Me scalar multiplication $P_{n,Z}$ of the base point P and auxiliary Z for $P, Z \in E(\mathbb{F}_p)$ and $n \in \mathbb{N}$, where E is an elliptic curve over $\mathbb{F}_p$. Moreover, they defined Me version of DLPs. The MeDLP is: given $P, Z, Q \in E(\mathbb{F}_p)$, compute $n \in \mathbb{N}$ such that $Q = P_{n,Z}$. The MeDLP' is: given $P, z(\in \mathbb{Z}), Q$, compute $n \in \mathbb{N}$ such that $Q = P_{n,zZ}$. In ISEC in May 2018, they showed that in the case where the MeDLP' instance (P, z, Q) has a solution, if the MeDLP' instance can be solved, the corresponding ECDLP instance can be solved in polynomial time using the solution [5]. However, when MeDLP' had a solution was unknown. This report shows that when $E(\mathbb{F}_p)$ is a cyclic group, if $z \in \mathbb{Z}$ is properly chosen then MeDLP' instance has a solution. Furthermore, this report shows if a solution m of an ECDLP instance is obtained by solving the instance, then 2^n is a solution of a certain MeDLP' instance, where the n is an integer easily computed from m. Note that 2^n is n-bit instead of $\log_2 n$-bit.

Keywords: Elliptic Curve, ECDLP, One-way Function, Me operation, Me scalar multiplication, MeDLP

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，欧米では v2x 通信に ECDSA が用いられることが決定した [1]．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．

由良によって定義された $\mathbb{F}_p$ 上 M 演算はべき等律，可換律，$+$ との分配律を満たすが，結合律を満たさない [7]．従って，$a \in \mathbb{F}_p$ に対して，$(\cdots(a \oplus a) \oplus \cdots) \oplus a = a$ とな

[1] 公立はこだて未来大学
Future University Hakodate

© 2018 Information Processing Society of Japan

る．先行研究 [3] では，$a, z \in \mathbb{F}_p$ と $n \in \mathbb{N}$ に対して，a をベースとし z を補助元とする M スカラー倍 $a_{n,z}$ を定義した．また，$a, z, b \in \mathbb{F}_p$ から $b = a_{n,z}$ を満たす $n \in \mathbb{N}$ を求める問題を MDLP と定義した．

先行研究 [4] では，M 演算，M スカラー倍，MDLP の有限体 $\mathbb{F}_p$ 上楕円曲線 E 版である Me 演算，Me スカラー倍，MeDLP を定義した．$P, Z \in E(\mathbb{F}_p)$, $n \in \mathbb{N}$ に対して，P をベースポイント，Z を補助元とする Me スカラー倍を $P_{n,Z}$ と表記する．MeDLP は $P, Z, Q \in E(\mathbb{F}_p)$ から $Q = P_{n,z}$ となる $n \in \mathbb{N}$ を見つける問題である．

2018 年 5 月の ISEC で発表した先行研究 [5] では，$z \in \mathbb{Z}$ に対して P, z, Q から $Q = P_{n,zP}$ となる n を見つける問題を MeDLP' と定義した．更に，MeDLP' インスタンスが解を持つ場合，その MeDLP' インスタンスを解けるならば，対応する ECDLP インスタンスをその MeDLP' インスタンスの解を使って多項式時間で解けることを示した．しかし，いつ MeDLP' インスタンスが解を持つかは不明であった．

本稿は，$E(\mathbb{F}_p)$ が巡回群をなす時，$z \in \mathbb{Z}$ を適切に選べば MeDLP' インスタンスが解を持つことを示す．先行研究 [5] の結果とこの結果より，MeDLP' は ECDLP と同等に困難かより困難であると言え，Me スカラー倍は一方向性関数に成り得る可能性がある．更に，ECDLP インスタンスを解いて解 m が得られるならば，m から簡単に計算できる $n \in \mathbb{Z}$ に対して，2^n はある MeDLP' インスタンスの解であることを示す．

2. 準備

2.1 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], [6]．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 が十分に大きい (例えば，$p \approx 2^{256}$) 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 の困難性を安全性の根拠としている．

2.2 有限体上楕円曲線上の Me 演算と Me スカラー倍

2.2.1 定義と性質

$p \equiv 3 \pmod 4$ を満たす 5 以上の素数 p のみを考える．$E/\mathbb{F}_p$ 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[*1]．$P = (x_0, y_0) \in E(\mathbb{F}_p)$ に対して，$-P = (x_0, -y_0) \in E(\mathbb{F}_p)$ であり，

$$\begin{cases} \left(\frac{y_0}{p}\right) = 1 \\ \left(\frac{-y_0}{p}\right) = -1 \end{cases} \quad \text{または} \quad \begin{cases} \left(\frac{y_0}{p}\right) = -1 \\ \left(\frac{-y_0}{p}\right) = 1 \end{cases} \qquad (2)$$

が成り立つ．ここで，$\left(\frac{\cdot}{p}\right)$ は Legendre 記号である．

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．すると，(2) より $P \in E(\mathbb{F}_p) \setminus \{\mathcal{O}\}$ に対して

$$\mathrm{sign}(P) \text{ と } \mathrm{sign}(-P) \text{ は異符号}$$

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．
(i) $P \oplus P = P$.
(ii) $P \oplus Q = Q \oplus P$.
(iii) $(P \oplus Q) + R = (P + R) \oplus (Q + R)$,
$P + (Q \oplus R) = (P + Q) \oplus (P + R)$.

$E(\mathbb{F}_p)$ に 2 つの演算 $+$ と $\oplus$ を持たせることができたが，一般に $\oplus$ は結合律を満たさない，つまり

$$(P \oplus Q) \oplus R = P \oplus (R \oplus Q) \text{ は成り立たない．}$$

これは，$(E(\mathbb{F}_p), \oplus)$ は群をなさないことを意味する．更に，$P \oplus P = P$ より

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

となる．従って，上記のような Me 演算 $\oplus$ の繰り返しは意

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

© 2018 Information Processing Society of Japan

アルゴリズム 1 (Me スカラー倍の計算)

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

味をなさない．そこで先行研究 [4] 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．

Me スカラー倍は次のような性質を持つ．

命題 2 ([4])
$P, Q, Z \in E(\mathbb{F}_p), n \in \mathbb{N}$ に対して，

$$P_{n,Z} + Q = P + Q_{n,Z} = (P + Q)_{n,Z}$$

が成り立つ．

注意 3 ([4])
本稿とは直接関係しないが，Me スカラー倍の興味深い性質を紹介する．$P, Q, Z \in E(\mathbb{F}_p), n \in \mathbb{N}$ に対して，次が成り立つ．
(i) $P_{n,Z} \oplus Q_{n,Z} = (P \oplus Q)_{n,Z}$
(ii) $(P_{n,Z})_{m,Z} = (P_{m,Z})_{n,Z} = P_{n,Z} + P_{m,Z} - P$

定義 4
(i) $P, Z, Q \in E(\mathbb{F}_p)$ 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)** という．
(ii) $P, z(\in \mathbb{Z}), Q$ 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')** という．

2.2.2 2018 年 5 月 ISEC での先行研究の結果 [5]

先行研究研究 [5] で扱ったアルゴリズム 2 を紹介する．$l = \#E(\mathbb{F}_p)$ 及び $\mathcal{P} \in E(\mathbb{F}_p) \times \mathbb{Z}/l\mathbb{Z}$ 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．

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

アルゴリズム 2

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

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** $\mathcal{Y}$

第 1 成分のみに注目すれば $E(\mathbb{F}_p) \times \mathbb{Z}/l\mathbb{Z}$ 上の $\oplus$ と，$E(\mathbb{F}_p)$ 上の $\oplus$ は同じ演算であり，

$$(\mathcal{P} \oplus \mathcal{Q})[1] = \mathcal{P}[1] \oplus \mathcal{Q}[1] \tag{3}$$

であることが分かる．

アルゴリズム 2 に対して次が成り立つ．

補題 5
$P \in E(\mathbb{F}_p), z \in \mathbb{Z}/l\mathbb{Z}, n \in \mathbb{N}$ を入力した時のアルゴリズム 2 の出力を $\mathcal{Y}'$ とする．すると，次が成り立つ．
(i) $\mathcal{Y}'[1] = P_{n,zP}$
(ii) $\mathcal{Y}'[2]P = P_{n,zP}$
$\because$) (i) (3) より，$P \in E(\mathbb{F}_p), z \in \mathbb{F}_p, n \in \mathbb{N}$ を入力するときのアルゴリズム 2 の第 1 成分の処理と，$P, zP \in E(\mathbb{F}_p), n \in \mathbb{N}$ を入力するときのアルゴリズム 1 の処理は同一である．従って，(i) が成り立つ．
(ii) アルゴリズム 2 のすべてのステップにおいて，

$$\mathcal{Y}[1] = \mathcal{Y}[2]P$$

が成り立っている．よって，

$$\mathcal{Y}'[2]P = \mathcal{Y}'[1] = P_{n,zP}$$

となる．□

補題 5 から，次の命題が得られる．

命題 6
$l = \#E(\mathbb{F}_p)$ とする．すると，MeDLP' インスタンス $(P, z, Q) \in E(\mathbb{F}_p) \times \mathbb{Z} \times E(\mathbb{F}_p)$ の解が得られれば，この解を使って ECDLP インスタンス (P, Q) を多項式時間で解くことができる ($Q = tP$ となる $t \in \mathbb{Z}/l\mathbb{Z}$ を計算できる)．
$\because$) MeDLP' インスタンス (P, z, Q) を解くことができ，$Q = P_{n,zP}$ となる $n \in \mathbb{N}$ が得られたと仮定する．(P, z, n) を入力としてアルゴリズム 2 を実行すると，補題 5 の (ii) より，その出力の第 2 成分 t は $tP = Q$ を満たす．この t は ECDLP インスタンス (P, Q) の解である．□

© 2018 Information Processing Society of Japan

2.2.3 2018年5月ISECでの先行研究[5]の主張の不備

先行研究[5]では，命題6から

$$\text{MeDLP' の困難さ} \geq \text{ECDLP の困難さ} \tag{4}$$

であると主張した．しかしながら，命題6から言えることは，

MeDLP' インスタンス (P, z, Q) が解を持つならば，
MeDLP' の困難さ $\geq$ ECDLP の困難さ

である．従って，$P_0, Q_0 \in E(\mathbb{F}_p)$ はある $z \in \mathbb{Z}$ に対してMeDLP' インスタンス (P_0, z, Q_0) は解を持ち，$P_1, Q_1 \in E(\mathbb{F}_p)$ はどの $z \in \mathbb{Z}$ に対してもMeDLP' インスタンス (P_1, z, Q_1) は解を持たないとすると，

ECDLP インスタンス (P_0, Q_0) の困難さ
$\leq$ MeDLP' インスタンス (P_0, z, Q_0) の困難さ
$<$ ECDLP インスタンス (P_1, Q_1) の困難さ

かもしれず，一般に(4)を主張することはできない．従って，いつMeDLP' インスタンスが解を持つかを考察する必要がある．

3. 本稿の寄与

3.1節は，$E(\mathbb{F}_p)$ が巡回群をなす時，$z \in \mathbb{Z}$ を適切に選べばMeDLP' インスタンスが解を持つことを示す．更に，ECDLP インスタンスを解いて解 m が得られるならば，2^m はあるMeDLP' インスタンスの解であることを示す．3.2節は，MeDLP' の困難さとECDLP の困難さを考察する．

3.1 MeDLP' とECDLP の関係

本節では，$k = 2$ の場合のMe演算

$$\mathrm{Me}(P, Q) = P \oplus Q = \begin{cases} P & P = Q \text{ の時} \\ 2P - Q & \mathrm{sign}(P - Q) = 1 \text{ の時} \\ 2Q - P & \mathrm{sign}(P - Q) = -1 \text{ の時} \end{cases} \tag{5}$$

のみを考える．

まず，3つの補題を与える．

補題7 $P, Z \in E(\mathbb{F}_p)$，$n \in \mathbb{N}$ に対して

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

である．

$\because$) n の2進数表現を $(1n_{l-2}n_{l-3}\cdots n_0)_2$ とすると，$2n$ の2進数表現は $(1n_{l-2}n_{l-3}\cdots n_00)_2$ である．アルゴリズム1を使って $P_{2n,Z}$ を計算する時，最後のラウンドのステップ3の右辺の Y は $P_{n,Z}$ と同一である．よって，ステップ3では $(Z + P_{n,Z}) \oplus P_{n,Z}$ が計算され，ステップ4のif文はfalseのため実行されず，ステップ6で $(Z + P_{n,Z}) \oplus P_{n,Z}$ が返される．よって，$P_{2n,Z} = (Z + P_{n,Z}) \oplus P_{n,Z}$ である．□

補題8 任意の $Z \in E(\mathbb{F}_p), Z \neq \mathcal{O}, n \in \mathbb{N}$ に対して，

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

が成り立つ．

$\because$) $\mathrm{sign}(Z) = 1$ の時，

$$\mathcal{O}_{2^n,Z} = 2nZ \tag{6}$$

が成り立つことを数学的帰納法により示す．

$n = 1$ の時，Me スカラー倍の定義より

$$\mathcal{O}_{2,Z} = (Z + \mathcal{O}) \oplus \mathcal{O} = Z \oplus \mathcal{O}$$

となり

$$\mathrm{sign}(Z - \mathcal{O}) = \mathrm{sign}(Z) = 1$$

が得られる．よって(5)で $P = Z$，$Q = \mathcal{O}$ とすることにより

$$Z \oplus \mathcal{O} = 2Z - \mathcal{O} = 2Z$$

が得られる．

$n = k$ で(6)が成り立つ，つまり，

$$\mathcal{O}_{2^k,Z} = 2kZ \tag{7}$$

が成り立つと仮定する．すると，

$$\begin{aligned} \mathcal{O}_{2^{k+1},Z} &= (Z + \mathcal{O}_{2^k,Z}) \oplus \mathcal{O}_{2^k,Z} && \text{補題7より} \\ &= (Z + 2kZ) \oplus 2kZ && \text{仮定(7)より} \\ &= (2k+1)Z \oplus 2kZ \end{aligned}$$

であり，また

$$\mathrm{sign}((2k+1)Z - 2kZ) = \mathrm{sign}(Z) = 1$$

である．よって，(5)で $P = (2k+1)Z$，$Q = 2kZ$ とすることにより

$$\begin{aligned} (2k+1)Z \oplus 2kZ &= 2(2k+1)Z - 2kZ \\ &= 2(k+1)Z \end{aligned}$$

が得られ，$n = k + 1$ で(6)が成り立つ．

$\mathrm{sign}(Z) = -1$ の時，

$$\mathcal{O}_{2^n,Z} = -nZ \tag{8}$$

が成り立つことを数学的帰納法により示す．

$n = 1$ の時，Me スカラー倍の定義より

$$\mathcal{O}_{2,Z} = (Z + \mathcal{O}) \oplus \mathcal{O} = Z \oplus \mathcal{O}$$

となり

$$\mathrm{sign}(Z - \mathcal{O}) = \mathrm{sign}(Z) = -1$$

が得られる．よって，(5)で $P = Z$，$Q = \mathcal{O}$ とすることにより

© 2018 Information Processing Society of Japan

$$Z \oplus \mathcal{O} = 2\mathcal{O} - Z = -Z$$

が得られる．

$n = k$ で (8) が成り立つ，つまり，

$$\mathcal{O}_{2^k,Z} = -kZ \tag{9}$$

が成り立つと仮定する．すると，

$$\begin{aligned} \mathcal{O}_{2^{k+1},Z} &= (Z + \mathcal{O}_{2^k,Z}) \oplus \mathcal{O}_{2^k,Z} && \text{補題 7 より} \\ &= (Z - kZ) \oplus \mathcal{O}_{2^k,Z} && \text{仮定 (9) より} \\ &= (-(k-1)Z) \oplus (-kZ) \end{aligned}$$

であり，また

$$\mathrm{sign}(-(k-1)Z) - (-kZ) = \mathrm{sign}(Z) = -1$$

である．よって，(5) で $P = -(k-1)Z$，$Q = -kZ$ とすることにより

$$\begin{aligned} (-(k-1)Z) \oplus (-kZ) &= 2(-kZ) - ((-(k+1)Z) \\ &= (-k-1)Z \end{aligned}$$

が得られ，$n = k+1$ で (8) が成り立つ．□

補題 9　$E(\mathbb{F}_p)$ は巡回群をなすとする．補助元 $Z \in E(\mathbb{F}_p)$ は

$$\mathrm{sign}(Z) = 1 \text{ かつ } 2Z \text{ は } E(\mathbb{F}_p) \text{ の生成元} \tag{10}$$

または

$$\mathrm{sign}(Z) = -1 \text{ かつ } -Z \text{ は } E(\mathbb{F}_p) \text{ の生成元} \tag{11}$$

であるとする．すると，任意の $P \in E(\mathbb{F}_p)$ に対して，

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

となる．

∵) 任意の $P \in E(\mathbb{F}_p)$ に対して，

$$\{P_{n,Z} : n = 1, 2, 3, ...\} \subset E(\mathbb{F}_p) \tag{12}$$

は明らかである．

$Z \in E(\mathbb{F}_p)$ が (10) を満たすと仮定する．$2Z$ が $E(\mathbb{F}_p)$ の生成元なので

$$E(\mathbb{F}_p) = \{2nZ : n = 1, 2, 3, ...\} \tag{13}$$

である．補題 8 より

$$\begin{aligned} &\{2nZ : n = 1, 2, 3, ...\} \\ &\quad = \{\mathcal{O}_{2^n,Z} : n = 1, 2, 3, ...\} \\ &\quad = \{\mathcal{O}_{2^n,Z} + P : n = 1, 2, 3, ...\} \end{aligned} \tag{14}$$

が得られる．命題 2 より

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

であるから

$$\begin{aligned} &\{\mathcal{O}_{2^n,Z} + P : n = 1, 2, 3, ...\} \\ &\quad = \{\mathcal{P}_{2^n,Z} : n = 1, 2, 3, ...\} \end{aligned} \tag{15}$$

である．$\{2^n : n = 1, 2, 3, ...\} \subset \{n = 1, 2, 3, ...\}$ より

$$\{P_{2^n,Z} : n = 1, 2, 3, ...\} \subset \{P_{n,Z} : n = 1, 2, 3, ...\} \tag{16}$$

が分かる．従って，(13)，(14)，(15)，(16) より

$$E(\mathbb{F}_p) \subset \{P_{n,Z} : n = 1, 2, 3, ...\} \tag{17}$$

が示された．(12) と (17) より，

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

が言える．

$Z \in E(\mathbb{F}_p)$ が (11) を満たす時も同等に

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

が示される．□

次の定理は本稿の主結果である．

定理 10

(i) $P \in E(\mathbb{F}_p)$ と $z \in \mathbb{Z}$ に対して，$Z = zP$ は (10) か (11) を満たすとする．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．

(ii) $Z \in E(\mathbb{F}_p)$ は (10) か (11) を満たすとする．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．

∵) (i) 補題 9 より $E(\mathbb{F}_p) = \{P_{n,Z} : n = 1, 2, 3, ...\}$ 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．

(ii) (i) と同様．□

系 11　$\#E(\mathbb{F}_p)$ は 3 以上の素数とする．

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

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

となる．

(ii) 任意の $P, Q \in E(\mathbb{F}_p), P \neq \mathcal{O}$ に対して MeDLP' インスタンス (P, z, Q) は解を持つ．

(iii) 任意の $P, Q, Z \in E(\mathbb{F}_p), Z \neq \mathcal{O}$ に対して MeDLP インスタンス (P, Z, Q) は解を持つ．

∵) (i) 一般に，位数が素数の有限アーベル群は巡回群であり，単位元以外は生成元に成り得る．よって，$-Z \neq \mathcal{O}$，$2Z \neq \mathcal{O}$ であるので，$-Z$ や $2Z$ は $E(\mathbb{F}_p)$ の生成元である．よって，$\mathrm{sign}(Z) = 1$ ならば (10) を，$\mathrm{sign}(Z) = -1$ ならば (11) を満たすので，補題 9 が適用できる．

(ii) (i) と定理 10 の (i) による．

(iii) (i) と定理 10 の (ii) による．□

© 2018 Information Processing Society of Japan

命題 12 $(\mathcal{O} \neq)P \in E(\mathbb{F}_p), l = \#E(\mathbb{F}_p), z \in \mathbb{Z}, z \neq 0$ 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．

$$n = \begin{cases} m/2 \bmod l & \mathrm{sign}(Z) = 1 \text{ の時} \\ -m \bmod l & \mathrm{sign}(Z) = -1 \text{ の時} \end{cases} \tag{18}$$

すると，2^n は MeDLP' インスタンス (P, z, Q) の解である．

∵) 補題 8 より $Q - P = mZ = \mathcal{O}_{2^n,Z}$ が成り立ち，命題 2 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．□

3.2 MeDLP' の困難さと ECDLP の困難さ

$E(\mathbb{F}_p)$，$P \in E(\mathbb{F}_p)$，$z \in \mathbb{Z}$ は次の条件を満たすとする．

条件 13
(i) $E(\mathbb{F}_p)$ は巡回群をなし，$Z = zP$ は (10) か (11) を満たす，
または，
(ii) $\#E(\mathbb{F}_p)$ は 3 以上の素数で，$P \neq \mathcal{O}$，$z \neq 0$.

すると，定理 10 や系 11 から，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．この時，先行研究 [5] の結果である命題 6 を適用できる．

条件 13 を満たすような $E(\mathbb{F}_p)$，$P \in E(\mathbb{F}_p)$，$z \in \mathbb{Z}$ 及び任意の $Q \in E(\mathbb{F}_p)$ に対して，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 (10) か (11) を満たすように $z \in Z$ を選ぶ．
(ii) (P, z, Q) を $\mathcal{A}$ へ入力し，$\mathcal{A}$ からの出力 n を得る．
(iii) (P, z, n) をアルゴリズム 2 へ入力し，その出力 $\mathcal{Y}$ を得る．
(iv) $m = \mathcal{Y}[2]$ は ECDLP インスタンス (P, Q) の解である．

これは，$E(\mathbb{F}_p)$，$P \in E(\mathbb{F}_p)$ に対して条件 13 を満たすような $z \in \mathbb{Z}$ が存在するならば

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

であることを意味する．

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 (18) 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．

しかしながら，このことから

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

を言えるのだろうか? MeDLP' インスタンスの解が秘密鍵となるような公開鍵暗号において秘密鍵 2^n が得られても，復号には指数時間を要することとなる．

$E(\mathbb{F}_p)$，$P \in E(\mathbb{F}_p)$ が条件 13 を満たすならば，少なくとも MeDLP' の困難性は ECDLP の困難性と同等である．従って，Me スカラー倍は暗号学的一方向性関数になり得る可能性はある．

4. まとめと今後の課題

本稿は，$E(\mathbb{F}_p)$，$P \in E(\mathbb{F}_p)$，$z \in \mathbb{Z}$ が条件 13 を満たす時，MeDLP' インスタンス (P, z, Q) の解 n に対して，次のようにして ECDLP インスタンス (P, Q) の解が得られること示した．

MeDLP' インスタンス (P, z, Q) の解 n
⇓：入力 (P, z, n)
アルゴリズム 2
⇓：出力 $\mathcal{Y}$
$m = \mathcal{Y}[2]$ は ECDLP インスタンス (P, z, Q) の解
$(|m| \approx |n|)$

この結果，条件 13 を満たす $E(\mathbb{F}_p)$，$P \in E(\mathbb{F}_p)$ に対して，

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

が言える．なお，楕円曲線暗号系で用いられる $E(\mathbb{F}_p)$ は条件 13 を満たすことは多い．以上より，Me スカラー倍は暗号学的一方向性関数になり得る可能性はある．

本稿は更に，ECDLP インスタンス $(zP, Q - P)$ の解 m に対して，次のようにして ECDLP インスタンス (P, z, Q) の解が得られること示した．

ECDLP インスタンス (P, Q) の解 m
⇓
(18) により n を計算
⇓
2^n は MeDLP' インスタンス $(Z, Q - P)$ の解
2^n は n ビット

この結果は

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

を意味するようにも見えるが，2^n は n ビットであるため，このような MeDLP' の解が得られても何かに使えるかは不明である．

先行研究 [4] では，Me スカラー倍を用いる ElGamal 暗号系の構成は課題が多いことを指摘した．本稿の結果 Me スカラー倍は暗号学的一方向性関数に成り得る可能性が高

© 2018 Information Processing Society of Japan

いことが判明したため，Me スカラー倍を用いる公開鍵暗号系の構成を考察したい．Me 演算と Me スカラー倍の性質の発見も暗号系構成に役立つかもしれない．$k = 2$ 以外の k による Me 演算の場合や，条件 13 を緩めた場合，本稿と同様の結果が得られるかを今後の課題として確かめたい．

謝辞

本研究は，JSPS 科研費 16K00188 の助成を受けたものです．公立はこだて未来大学の由良文孝氏からは，$\mathcal{O}_{n,Z}$ を考察することや補題 8 について助言を頂きました．感謝申し上げます．

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] 白勢政明. 有限体上 M 関数を用いた M-スカラー倍算の提案とその性質及び応用. 応用数理学会 2017 年度会, 2017.

[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. 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. 2018 年 5 月 ISEC, 2018.

[6] J. H. Silverman. *The arithmetic of elliptic curves*. Springer-Verlag New York, 1985. doi:10.1007/978-0-387-09494-6.

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

© 2018 Information Processing Society of Japan