Dual Pairing Vector Spaceを用いた属性ベース暗号におけるマスター鍵更新

川合 豊[1]

概要：本稿では属性ベース暗号 (Attribute-based encryption, ABE) のマスター鍵更新に着目する．ABE では全ての暗号文や復号鍵を生成する鍵となるマスター鍵が存在する．通常の公開鍵暗号や電子署名で用いられる公開鍵が数年に一回更新されるのと同様に，ABE のマスター鍵に関しても同様に更新が必要になるケースがある．マスター鍵は全てのパラメータの基となっているため，マスター鍵を更新した場合，それまでに生成された暗号文も新しいマスター鍵と対応するよう更新する必要がある．最も素朴な更新方法は，一度すべての暗号文を復号し，再度暗号化する方法だが，一度平文に戻してしまうため安全性上の問題があり，クラウド上などで実行することはできない．そこで本稿では，マスター鍵を更新した場合でも，暗号文を復号することなく更新可能な暗号文ポリシー型 ABE (Ciphertext-Policy ABE, CP-ABE) 方式を岡本らによって提案された双対ベクトル空間（Dual Paring Vector Space，DPVS) を用いた CP-ABE を基に構成する．

キーワード：Dual Pairing Vector Space，属性ベース暗号，マスター鍵更新

Master Key Updatable Attribute-Based Encryption on the Dual Pairing Vector Space

Yutaka Kawai[1]

Abstract: In this paper, we focus on a “master key update” method for attribute-based encryption schemes. In ABE system, in order to generate ciphertexts and decryption keys, there is a master key which is a pair of a public key and a master secret key. The update of the master key of ABE (a public key and a master secret key) is necessary as similar as normal public key encryption. Since all ciphertexts are constructed from a master key, all ciphertexts also should be updated based on a new master key if the master key is updated. In previous works, in this situation, all ciphertexts must be decrypted and plaintexts are encrypted by using the new public key which is generated from the new master secret key. This method is called dec-then-enc methodology. Since in this method ciphertexts must be decrypted once, if all ciphertexts are stored an external storage, for example cloud storages, a user who uses the ABE system should download all ciphertexts and executes dec-then-enc method for all ciphertexts. In order to overcome this problem, we introduce new method that ciphertext can be updated without decryption. We propose the first ciphertext-policy ABE scheme with mater key update property based on the technique of the access structures of Okamoto-Takashima (CRYPTO 2010). The security is proven under Decisional Linear (DLIN) in the standard model as same as Okamoto-Takashima CP-ABE scheme.

Keywords: Dual Pairing Vector Space，Attribute-based encryption，master key update

1. はじめに

1.1 属性ベース暗号とマスター鍵更新

属性ベース暗号は Sahai らによって提案され，暗号

[1] 三菱電機株式会社
Mitsubishi Electric

化する際に通常の公開鍵暗号や ID ベース暗号に比べ柔軟な復号条件を設定することができる暗号技術である [2], [4], [5], [6], [8], [9], [10], [11], [12].

通常の PKI を用いた公開鍵暗号や電子署名で用いられる公開鍵は，鍵の危殆化などを考慮し数年に一回更新（再生成）される．これは鍵の経年劣化の恐れからであり，この問題は属性ベース暗号でも起こりうる問題であるため，これらの暗号技術でも鍵更新方法を考える必要がある．ABE では，公開しているすべてのユーザに共通の公開鍵，Private Key Generator（PKG）が持つユーザ秘密鍵を作成するためにマスター秘密鍵，そしてユーザ一人一人が持つユーザ秘密鍵，が存在する．ユーザ秘密鍵の更新は，通常の公開鍵暗号と同様に，PKG で再生成し配布すればよい．しかし，公開鍵とマスター秘密鍵（本稿では合わせてマスター鍵と呼ぶ）はユーザ秘密鍵や暗号文の基となるパラメータであるため，従来の方法だけでは対応することができない．最も素朴な方法は，マスター鍵生成，すなわち Setup を含めすべてをやり直す方法である．すなわち，ユーザ秘密鍵と暗号文を再生成することである．これにより，更新前に既に生成された暗号文については，一度古い鍵で復号し平文に戻し，新しい鍵で再度暗号化する必要がある．マスター鍵更新は数年に一回程度行うことを考えると，その期間中に生成された全ての暗号文について実行する必要があり現実的ではない．また，一度復号し平文に戻すため，クラウドのような第三者機関で実行することがセキュリティ上望ましくなく，すべてをローカルにダウンロードしての実行となるため，ユーザの負荷が膨大になる．これらのことから，暗号文を復号せずにマスター鍵更新を実行する技術が必要となる．

1.2 貢献

本稿では，マスター鍵更新を考慮に入れた CP-ABE を MKU-CP-ABE(Master Key Updatable CP-ABE) として定義をする．また，既存の岡本らによって提案されている双対ベクトル規定 (Dual pairing vector spaces: DPVS) を用いて構成されている CP-ABE [7] と DPVS の基底変換技法を組み合わせることで，マスター鍵を更新した場合でも暗号文を復号することなく更新可能な具体的方式を提案する．

2. 準備

2.1 記法

A が分布であるときに $y \xleftarrow{\mathsf{R}} A$ は y を A からその分布に従ってランダムに選ぶことを指す．A が集合であるときに，$y \xleftarrow{\mathsf{U}} A$ は y を A から一様に選ぶことを指す．位数 q の有限体を $\mathbb{F}_q$ と表し，$\mathbb{F}_q \setminus \{0\}$ を $\mathbb{F}_q^\times$ と表す．$\mathbb{F}_q$ 上のベクトル $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$ を $\vec{x}$ と表記する．二つのベクトル $\vec{x}$ と $\vec{v}$ の内積 $\sum_{i=1}^n x_i v_i$ を $\vec{x} \cdot \vec{v}$ と表す．$\mathbb{F}_q^n$ での零ベクトルを $\mathbf{0}$ と表す．X^{T} は行列 X の転置行列を表し，I_ℓ と 0_ℓ はそれぞれ ℓ 行 ℓ 列の単位行列と零行列を指す．ベクトル空間 $\mathbb{V}$ の要素は $\boldsymbol{x} \in \mathbb{V}$ と表す．$\boldsymbol{b}_i \in \mathbb{V}\ (i = 1, \ldots, n)$ である時，$\boldsymbol{b}_i, \ldots, \boldsymbol{b}_n$ によって作られる部分空間は $\mathsf{span}\langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_n \rangle \subseteq \mathbb{V}$ と表される．また，$\mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ と $\mathbb{B}^* := (\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_n^*)$ に対して，$(x_1, \ldots, x_n)_{\mathbb{B}} := \sum_{i=1}^n x_i \boldsymbol{b}_i$，及び $(y_1, \ldots, y_n)_{\mathbb{B}^*} := \sum_{i=1}^n y_i \boldsymbol{b}_i^*$ と定義する．$\vec{e}_j$ は $(\overbrace{0 \cdots 0}^{j-1}, 1, \overbrace{0 \cdots 0}^{n-j}) \in \mathbb{F}_q^n$（$j = 1, \ldots, n_t$）を指す．また，$GL(n, \mathbb{F}_q)$ は次元 n の $\mathbb{F}_q$ 上の一般線形群を指す．

2.2 Dual Pairing Vector Spaces (DPVS)

定義 1 (対称ペアリング群)．: 対称ペアリング群 $(q, \mathbb{G}, \mathbb{G}_T, G, e)$ は素数 q，位数 q の加法的巡回群 $\mathbb{G}$ と乗法的巡回群 $\mathbb{G}_T$ 及び $G \neq 0 \in \mathbb{G}$ と多項式時間で計算可能な非退化性を持つ双線形写像 $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ からなる．セキュリティパラメータ 1^λ を入力として上記対象ペアリング群 $(q, \mathbb{G}, \mathbb{G}_T, G, e)$ を出力するアルゴリズムを $\mathcal{G}_{\mathsf{bpg}}$ と書く．

定義 2 (Dual pairing vector spaces (DPVS))．: *DPVS* は $(q, \mathbb{V}, \mathbb{G}_T, \mathbb{A}, e)$ は位数 q，$\mathbb{F}_q$ 上の N 次元ベクトル空間 $\mathbb{V} := \overbrace{\mathbb{G} \times \cdots \times \mathbb{G}}^{N}$，位数 q の巡回群 $\mathbb{G}_T$，$\mathbb{V}$ の標準基底 $\mathbb{A} := (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_N)$（但し $\boldsymbol{a}_i := (\overbrace{0, \ldots, 0}^{i-1}, G, \overbrace{0, \ldots, 0}^{N-i})$）とペアリング演算 $e : \mathbb{V} \times \mathbb{V} \to \mathbb{G}_T$ から構成される．

ここで，N 次元ベクトル $\boldsymbol{x} := (G_1, \ldots, G_N) \in \mathbb{V}$ と $\boldsymbol{y} := (H_1, \ldots, H_N) \in \mathbb{V}$ のペアリング演算 $e(\boldsymbol{x}, \boldsymbol{y})$ を $e(\boldsymbol{x}, \boldsymbol{y}) := \prod_{i=1}^N e(G_i, H_i) \in \mathbb{G}_T$ と定義する．また，上記演算は非退化性をもつ．$e(G, G) \neq 1 \in \mathbb{G}_T$ であれば任意の i と j に対して，$e(\boldsymbol{a}_i, \boldsymbol{a}_j) = e(G, G)^{\delta_{i,j}}$ である．ここで $\delta_{i.j}$ は $i = j$ の時に $\delta_{i.j} = 1$ であり，$i \neq j$ の時 $\delta_{i.j} = 0$ である．*DPVS* 生成アルゴリズム $\mathcal{G}_{\mathsf{dpvs}}$ は，セキュリティパラメータ $1^\lambda (\lambda \in \mathbb{N})$ と $\mathbb{V}$ の次元 $N \in \mathbb{N}$ を入力として，$\mathsf{param}'_{\mathbb{V}} := (q, \mathbb{V}, \mathbb{G}_T, \mathbb{A}, e)$ を出力する．このアルゴリズムは $\mathcal{G}_{\mathsf{bpg}}$ から構成することができる．

2.3 スパンプログラムと非モノトーンアクセス構造

定義 3 (スパンプログラム [1])．$\{p_1, \ldots, p_n\}$ を変数の集合とする．$\hat{M} := (M, \rho)$ をラベル付された行列とする．ここで，行列 M は，$\mathbb{F}_q$ 上の $\ell \times r$ の行列である．また，ρ は，行列 M の各行に付加されたラベルであり，$\{p_1, \ldots, p_n, \neg p_1, \ldots, \neg p_n\}$ のいずれか *1* つのリテラルへ対応付けられる．なお M の全ての行に付加されたラベル $\rho_i (i = 1, \ldots, L)$ がいずれかが *1* つのリテラルへ対応付けられる．つまり，$\rho : \{1, \ldots, \ell\} \to \{p_1, \ldots, p_n, \neg p_1, \ldots, \neg p_n\}$ である．

全ての入力列 $\delta \in \{0,1\}^n$ に対して，行列 M の部分行列 M_δ は，入力列 δ によってラベル ρ に値 *1* が対応付けられた行列 M の行から構成される部分行列である．つまり M_δ は，$\delta_i = 1$ であるような p_i に対応付けられた行列 M

の行と，$\delta_i = 0$ であるような $\neg p_i$ に対応付けられた行列 M の行とからなる部分行列である．言い換えると，写像 $\gamma : \{1, \ldots, L\} \to \{0,1\}$ が，$[\rho(j) = p_i] \wedge [\delta_i = 1]$ もしくは $[\rho(j) = \neg p_i] \wedge [\delta_i = 0]$ である場合に $\gamma(j) = 1$ であり，他の場合 $\gamma(j) = 0$ であるとする．ここで M_j は，行列 M の j 番目の行である．

ここで，ラベル ρ が正のリテラル $\{p_1, \ldots, p_n\}$ にのみ対応づけらえれている場合，スパンプログラムはモノトーンと呼ばれる．一方，ラベル ρ がリテラル $\{p_1, \ldots, p_n m \neg p_1, \ldots, \neg p_n\}$ に対応付けられている場合，非モノトーンと呼ばれる．スパンログラム $\hat{M}$ は $\vec{1} \in \mathsf{span}\langle M_\delta \rangle$ である場合に限り入力列 δ を受理し，他の場合には拒絶する．即ち，入力列 δ によって，行列 $\hat{M}$ から得られる行列 M_δ の行を線形結合して $\vec{1}$（各要素の値が 1 であるような行ベクトル）が得られる場合に限りスパンプログラム $\hat{M}$ は δ を受理する．

定義 4 (属性情報の内積とアクセス構造). $\mathcal{U}_t$ *(*$t = 1, \ldots, d$ かつ $\mathcal{U}_t \subset \{0,1\}^*$*)* は，部分全集合であり，属性の集合である．そして，$\mathcal{U}_t$ は，それぞれの部分全集合の識別情報 $t \in \{1, \ldots, d\}$ と，n 次元ベクトル $\vec{v} \in \mathbb{F}_q^{n_t} \setminus \{\vec{0}\}$ を含む，つまり，$\mathcal{U}_t$ は $(t, \vec{v})$ である．$\mathcal{U}_t$ をスパンプログラム $\hat{M} := (M, \rho)$ における変数 p とする．つまり，$p := (t, \vec{v})$ とする．そして，変数 $p := (t, \vec{v}), p' := (t', \vec{v}'), \ldots,$ としたスパンプログラムをアクセス構造 $\mathbb{S} := (M, \rho)$ とする．

次に Γ を属性の集合とする．つまり，$\Gamma := \{(t, \vec{x}_t) \mid \vec{x}_t \in \mathbb{F}_q^{n_t} \setminus \{\vec{0}\}, 1 \leq t \leq d\}$ とする．アクセス構造 $\mathbb{S}$ に Γ が与えられた場合，スパンプログラム $\hat{M}$ に対する写像 $\gamma : \{1, \ldots, \ell\} \to \{0,1\}$ は以下のように定義される．$i = 1, \ldots, \ell$ の各整数 i に対して $[\rho(i) = (t, \vec{v}_i)] \wedge [(t, \vec{x}_t) \in \Gamma] \wedge [\vec{v}_i \cdot \vec{x}_t = 0]$ もしくは $[\rho(i) = \neg(t, \vec{v}_i)] \wedge [(t, \vec{x}_t) \in \Gamma] \wedge [\vec{v}_i \cdot \vec{x}_t \neq 0]$ である場合に $\gamma(i) = 1$ であり，他の場合 $\gamma(i) = 0$ とする．即ち，属性情報 $\vec{v}$ と $\vec{x}$ との内積により，行列 M のどの行を行列 M_δ に含めるかが決定され，アクセス構造 $\mathbb{S} := (M, \rho)$ は $\vec{1} \in \mathsf{span}\langle (M_i)_{\gamma(i)=1} \rangle$ である場合に限り Γ を受理する．本稿では，$\mathbb{S}$ が Γ を受理する場合 $R(\Gamma, \mathbb{S}) = 1$ と記述し，受理しない場合は $R(\Gamma, \mathbb{S}) = 0$ と記述する．

定義 5. 次に，非モノトーンアクセス構造（もしくはスパンプログラム）における秘密分散について定義を行う．

(1) M を $\ell \times r$ の行列とし，$\vec{f}^{\mathrm{T}} := (f_1, \ldots, f_r)^{\mathrm{T}} \xleftarrow{\mathsf{U}} \mathbb{F}_q^r$ を列ベクトルとする．また，$s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}} = \sum_{k=1}^{r} f_k$ を共有される秘密情報とする．また，$\vec{s}^{\mathrm{T}} := (s_1, \ldots, s_\ell)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}$ を ℓ 個の s_0 に対する分散情報のベクトルとし，s_i を $\rho(i)$ に属するものとする．

(2) もしアクセス構造 $\mathbb{S} := (M, \rho)$ が Γ を受理する場合，つまり，$\gamma : \{1, \ldots, \ell\} \to \{0,1\}$ について $\vec{1} \in \mathsf{span}\langle (M_i)_{\gamma(i)=1} \rangle$ である場合，$I \subseteq \{i \in \{1, \ldots, \ell\} \mid \gamma(i) = 1\}$ である定数 $\{\alpha_i \in \mathbb{F}_q \mid i \in I\}$ が存在し $\sum_{i \in I} \alpha_i s_i = s_0$ となる．

2.4 Dual Orthonormal Basis Generator

以下に，本方式で用いる双対基底生成器 $\mathcal{G}_{\mathsf{ob}}$（dual orthonormal basis generator）を示す．

$\mathcal{G}_{\mathsf{ob}}(1^\lambda, \vec{n} = (d; n_1, \ldots, n_d))$:
$\mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, G, e) \leftarrow \mathcal{G}_{\mathsf{bpg}}(1^\lambda)$
$N_0 := 5$, $N_t := 3n_t + 1$ for $t = 1, \ldots, d$,
$\psi \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times, g_T := e(G, G)^\psi$,
For $t = 0, \ldots, d$
$\mathsf{param}'_t := (q, \mathbb{V}_t, \mathbb{G}_T, \mathbb{A}_t, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, N_t)$,

$$X_t := \begin{pmatrix} \vec{\chi}_{t,1} \\ \vdots \\ \vec{\chi}_{t,N_t} \end{pmatrix} := (\chi_{t,i,j})_{i,j},$$

$$\begin{pmatrix} \vec{\vartheta}_{t,1} \\ \vdots \\ \vec{\vartheta}_{t,N_t} \end{pmatrix} := \quad (\vartheta_{t,i,j})_{i,j} := \psi \cdot (X_t^{\mathrm{T}})^{-1},$$

where $(\chi_{t,i,j})_{i,j} \xleftarrow{\mathsf{U}} GL(N_t, \mathbb{F}_q)$,
$\mathsf{param}_{\vec{n}} := (\{\mathsf{param}_t\}_{t=0,\ldots,d}, g_T)$,
$\boldsymbol{b}_{t.i} := \sum_{j=1}^{N_t} \chi_{t,i,j} \boldsymbol{a}_{t,j}, \mathbb{B}_t := (\boldsymbol{b}_{t.1}, \ldots, \boldsymbol{b}_{t.N_t})$,
$\boldsymbol{b}^*_{t.i} := \sum_{j=1}^{N_t} \vartheta_{t,i,j} \boldsymbol{a}_{t,j}, \mathbb{B}^*_t := (\boldsymbol{b}^*_{t.1}, \ldots, \boldsymbol{b}^*_{t.N_t})$,
return $(\mathsf{param}_{\vec{n}}, \{\mathbb{B}_t, \mathbb{B}^*_t\}_{t=0,\ldots,d})$.

2.5 Decisional Linear (DLIN) Assumption

定義 6 (DLIN: Decisional Linear 仮定 [3]). DLIN 問題は $(\mathsf{param}_{\mathbb{G}}, G, \xi G, \kappa G, \delta\xi G, \sigma\kappa G, Y_\beta) \xleftarrow{\mathsf{R}} \mathcal{G}_\beta^{\mathsf{DLIN}}(1^\lambda)$ を入力として $\beta \in \{0,1\}$ を推定する問題であり，各パラメータは $\beta \xleftarrow{\mathsf{U}} \{0,1\}$ に対して以下のように決定される．

$$\mathcal{G}_\beta^{\mathsf{DLIN}}(1^\lambda) : \mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, G, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{bpg}}(1^\lambda),$$
$$\kappa, \delta, \xi, \sigma \xleftarrow{\mathsf{U}} \mathbb{F}_q,\ Y_0 := (\delta + \sigma)G, \quad Y_1 \xleftarrow{\mathsf{U}} \mathbb{G},$$
$$\text{return } (\mathsf{param}_{\mathbb{G}}, G, \xi G, \kappa G, \delta\xi G, \sigma\kappa G, Y_\beta)$$

任意の確率的アルゴリズム $\mathcal{E}$ に対して，$\mathsf{Adv}_{\mathcal{E}}^{\mathsf{DLIN}}(\lambda) := \left| \mathsf{Pr}\left[\mathcal{E}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_0^{\mathsf{DLIN}}(1^\lambda)\right] - \mathsf{Pr}\left[\mathcal{E}(1^\lambda, \varrho) \to 1 \,\middle|\, \varrho \xleftarrow{\mathsf{R}} \mathcal{G}_1^{\mathsf{DLIN}}(1^\lambda)\right] \right|$ を $\mathcal{E}$ のアドバンテージとして定義する．DLIN 仮定とは，任意の確率的多項式時間攻撃者 $\mathcal{E}$ に対し，上記のアドバンテージ $\mathsf{Adv}_{\mathcal{E}}^{\mathsf{DLIN}}(\lambda)$ がセキュリティパラメータ λ に対し無視できることと定義する．

3. Master Key Updatable CP-ABE (MKU-CP-ABE) Scheme

3.1 モデル

本節では，提案するマスター鍵更新可能な CP-ABE（MKU-CP-ABE）のモデルを示す．

定義 7. *MKU-CP-ABE* は以下の 7 つのアルゴリズムから

なる．

- Setup*:* セキュリティパラメータ 1^λ とフォーマット $\vec{n} := (d; n_1, \ldots, n_d)$ を受け取り，公開鍵 pk とマスター秘密鍵 msk，を出力する確率的アルゴリズム
- KG*:* 公開鍵 pk，マスター鍵 msk，属性の集合 $\Gamma := \{(t, \vec{x}_t) | \vec{x}_t \in \mathbb{F}_q^{n_t}, 1 \leq t \leq d\}$, を入力として，復号鍵 sk_Γ を出力する確率的アルゴリズム．
- Enc*:* 公開鍵 pk，アクセス構造 $\mathbb{S} := (M, \rho)$，平文 m を入力として，暗号文 $\mathsf{ct}_\mathbb{S}$ を出力する確率的アルゴリズム．
- Dec*:* 公開鍵 pk，復号鍵 sk_Γ，オリジナル暗号文 $\mathsf{ct}_\mathbb{S}$ を入力として，平文 m もしくは，復号失敗を表す記号 $\perp$ を出力する確定的アルゴリズム．
- MKU*:* 公開鍵 pk，マスター鍵 msk を入力として，更新された公開鍵 pk'，更新されたマスター鍵 msk'，更新情報 upk を出力するような確率的アルゴリズム．
- UpdCT*:* 更新情報 upk と，暗号文 $\mathsf{ct}_\mathbb{S}$ を入力とし，更新された暗号文 $\mathsf{ct}'_\mathbb{S}$ を出力するアルゴリズム．
- UpdDK*:* 更新情報 upk と，ユーザ秘密鍵 sk_Γ を入力とし，更新された暗号文 sk'_Γ を出力するアルゴリズム．

完全性は以下の通り

(1) 任意の $(\mathsf{pk}, \mathsf{msk}) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^\lambda)$，任意のアクセス構造 $\mathbb{S}$，任意の属性集合 Γ，任意の復号鍵 $\mathsf{sk}_\Gamma \xleftarrow{\mathsf{R}} \mathsf{KG}(\mathsf{pk}, \mathsf{msk}, \Gamma)$，および $\mathsf{ct}_\mathbb{S} \xleftarrow{\mathsf{R}} \mathsf{Enc}(\mathsf{pk}, \mathbb{S}, m)$ に対して $R(\Gamma, \mathbb{S}) = 1$ ならば $m = \mathsf{Dec}(\mathsf{pk}, \mathsf{sk}_\Gamma, \mathsf{ct}_\mathbb{S})$ が圧倒的確率で成り立つ．

(2) 任意の $(\mathsf{pk}, \mathsf{msk}) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^\lambda)$，任意のアクセス構造 $\mathbb{S}$，任意の属性集合 Γ，任意の復号鍵と暗号文 $\mathsf{sk}_\Gamma \xleftarrow{\mathsf{R}} \mathsf{KG}(\mathsf{pk}, \mathsf{msk}, \Gamma)$，$\mathsf{ct}_\mathbb{S} \xleftarrow{\mathsf{R}} \mathsf{Enc}(\mathsf{pk}, \mathbb{S}, m)$，及び任意の更新されたマスター鍵と更新情報 $(\mathsf{pk}', \mathsf{msk}', \mathsf{upk}) \xleftarrow{\mathsf{R}} \mathsf{MKU}(1^\lambda)$ に対して $R(\Gamma, \mathbb{S}) = 1$ ならば $m = \mathsf{Dec}(\mathsf{pk}, \mathsf{UpdDK}(\mathsf{sk}_\Gamma, \mathsf{upk}), \mathsf{UpdCT}(\mathsf{ct}_\mathbb{S}, \mathsf{upk}))$ が圧倒的確率で成り立つ．

3.2 安全性定義

本節では，MKU-CP-ABE の安全性 (Payload-Hiding security) を定義する．通常の Payload-Hiding と異なり，攻撃者は古いマスター秘密鍵 msk，公開鍵 pk，そして pk が MKU によって更新された pk' を持ち，pk' によって生成されたチャレンジ暗号文を受け取る．

定義 8 (Payload-Hiding 安全)**.**
MKU-CP-ABE が選択暗号文攻撃の下での *Payload-Hiding* 安全とは以下のような攻撃者とチャレンジャーとのゲームによって定義される．

- セットアップ． チャレンジャーはセットアップアルゴリズム $(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\mathsf{R}} \mathsf{Setup}(1^\lambda, n)$，および鍵更新アルゴリズム $(\mathsf{pk}', \mathsf{msk}', \mathsf{upk}) \xleftarrow{\mathsf{R}} \mathsf{MKU}(\mathsf{pk}, \mathsf{msk})$ を動作させ，攻撃者 $\mathcal{A}$ に λ，pk, msk, および pk' を与える．
- フェイズ *1*． 攻撃者は以下の多項式回の以下のクエリが許される．
  - 復号鍵クエリ． 攻撃者が Γ および $\beta \in \{0, 1\}$ をクエリ下ならば，チャレンジャーは $\beta = 0$ ならば $\mathsf{sk}_\Gamma \xleftarrow{\mathsf{R}} \mathsf{KG}(\mathsf{pk}, \mathsf{msk}, \Gamma)$ を，それ以外であれば $\mathsf{sk}'_\Gamma \xleftarrow{\mathsf{R}} \mathsf{KG}(\mathsf{pk}', \mathsf{msk}', \Gamma)$ を攻撃者 $\mathcal{A}$ に返す．
- チャレンジフェイズ． チャレンジクエリ $(m^{(0)}, m^{(1)}, \mathbb{S})$ は以下の制限がある．
  – いかなる復号鍵クエリ Γ に対しても $\mathbb{S}$ は Γ を受理してはいけない．

  チャレンジャーはランダムに $b \in \{0, 1\}$ を選択し，$\mathsf{ct}_\mathbb{S}^{(b)} \xleftarrow{\mathsf{R}} \mathsf{Enc}(\mathsf{pk}', \mathbb{S}, m^{(b)})$ を攻撃者 $\mathcal{A}$ に返す．
- フェイズ *2*． 攻撃者 $\mathcal{A}$ はフェイズ *1* と同様に復号鍵クエリを実行できるが，チャレンジフェイズでクエリした $\mathbb{S}$ が受理するような属性集合 Γ をクエリすることはできない．
- 出力． 攻撃者 $\mathcal{A}$ は推測値 $b' \in \{0, 1\}$ を出力し，$b = b'$ ならば攻撃者の勝ちとなる．

攻撃者の優位度を $\mathsf{Adv}_\mathcal{A}^{\mathsf{PH}}(\lambda) := \Pr[b = b'] - \frac{1}{2}$ と定義し，*MKU-CP-ABE* 方式が *Payload-Hiding* 安全であるとは，すべての多項式時間で動作する攻撃者に対して，この優位度がセキュリティパラメータに対して無視できる値であることとする．

4. 提案方式

4.1 構成のアイデア

DPVS を用いた CP-ABE 方式 [7] をベースに構成する．我々の構成では公開鍵 pk 及びマスター秘密鍵 msk はそれぞれランダム基底 $\mathbb{B}$ 及びその双対基底 $\mathbb{B}^*$ 上に構成されている．MKU アルゴリズムでは，ランダムな行列 $W \in \mathbb{F}_q^{N \times N}$ を選び，新たな基底 $\mathbb{B}' = \mathbb{B} \cdot W$ 及び $\mathbb{B}'^* = \mathbb{B} \cdot (W^{\mathrm{T}})^{-1}$ を生成する．ここで行列 W は更新情報 upk となる．W を用いることで，基底 $(\mathbb{B}, \mathbb{B}^*)$ から $(\mathbb{B}', \mathbb{B}'^*)$ へ変換することが可能なため，復号することなく $\mathbb{B}$ 上に構成された暗号文を $\mathbb{B}'$ の基底の暗号文へと変換することが可能となる．一方で，W を知らない攻撃者にとっては，基底 $(\mathbb{B}, \mathbb{B}^*)$ から $(\mathbb{B}', \mathbb{B}'^*)$ へ変換できず，加えて W はランダムに選んでいるため，それぞれの基底をランダムに選んだ場合と攻撃者が得られる情報は同じとなる．

4.2 提案 MKU-CP-ABE 方式

- $\mathsf{Setup}(1^\lambda, \vec{n} = (d; n_1, \ldots, n_d))$:
  $(\mathsf{param}_{\vec{n}}, \{\mathbb{B}_t, \mathbb{B}_t^*\}_{t=0,\ldots,d}) \leftarrow \mathcal{G}_{\mathsf{ob}}(1^\lambda, \vec{n})$
  $\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,2}, \boldsymbol{b}_{0,5})$,
  $\widehat{\mathbb{B}}_t := (\boldsymbol{b}_{t,1}, \ldots, \boldsymbol{b}_{t,n_t}, \boldsymbol{b}_{t,N_t})$ for $t = 1, \ldots, d$,
  $\widehat{\mathbb{B}}_0^* := (\boldsymbol{b}_{0,1}^*, \boldsymbol{b}_{0,2}^*, \boldsymbol{b}_{0,4}^*)$,
  $\widehat{\mathbb{B}}_t^* := (\boldsymbol{b}_{t,1}^*, \ldots, \boldsymbol{b}_{t,n_t}^*, \boldsymbol{b}_{t,2n_t+1}^*, \ldots, \boldsymbol{b}_{t,3n_t}^*)$ for $t = 1, \ldots, d$,

$\mathsf{pk} = (1^\lambda, \mathsf{param}_{\vec{n}}, \{\widehat{\mathbb{B}}_t\}_{t=0,\ldots,d})$, $\mathsf{msk} = (\{\widehat{\mathbb{B}}^*_t\}_{t=0,\ldots,d})$.

- $\mathsf{KG}(\mathsf{pk}, \mathsf{msk}, \Gamma = (\{(t, \vec{x}_t) | \vec{x}_t \in \mathbb{F}_q^{n_t} \setminus \{\vec{0}\}, 1 \le t \le d\})$:
  $\delta, \varphi_0 \xleftarrow{\cup} \mathbb{F}_q$, $\vec{\varphi}_t \xleftarrow{\cup} \mathbb{F}_q^{n_t}$ for $(t, \vec{x}_t) \in \Gamma$,

$$\boldsymbol{k}^*_0 := \big(\overbrace{1}^{} , \overbrace{\delta, \ldots, 0}^{n_t}, \overbrace{\varphi_0, \ldots, 0}^{n_t}, \overbrace{0}^{1} \big)_{\mathbb{B}^*_0},$$

$$\boldsymbol{k}^*_t := \big(\overbrace{\delta\vec{x}_t, \ldots}^{n_t}, \overbrace{\vec{\varphi}_t, \ldots}^{n_t}, \overbrace{0}^{1} \big)_{\mathbb{B}^*_t}$$

  return $\mathsf{sk}_\Gamma := (\Gamma, \boldsymbol{k}^*_0, \{\boldsymbol{k}^*_t\}_{(t,\vec{x}_t)\in\Gamma})$.

- $\mathsf{Enc}(\mathsf{pk}, m, \mathbb{S} = (M, \rho))$:
  $\vec{f} \xleftarrow{\cup} \mathbb{F}_q^r$, $\vec{s}^{\mathrm{T}} := (s_1, \ldots, s_l)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}, s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}}$, $\eta_0, \zeta, \xleftarrow{\cup} \mathbb{F}_q$
  $\boldsymbol{c}_0 := (\ \zeta,\ -s_0,\ 0,\ 0,\ \eta_0\ )_{\mathbb{B}_0}$ $\quad c_{d+1} := m \cdot g_T^\zeta$,
  For $i = 1, \ldots, l$
  if $\rho(i) = (t, \vec{v}_i := (v_{i.1}, \ldots, v_{i.n_t}) \in \mathbb{F}_q^{n_t} \setminus \{\vec{0}\})(v_{i,n_t} \neq 0)$,

$$\boldsymbol{c}_i := \big(\overbrace{s_i\vec{e}_{t,1} + \theta_i\vec{v}_i, \ldots}^{n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{\eta_i}^{1} \big)_{\mathbb{B}_t},$$

  where $\theta_i, \eta_i \xleftarrow{\cup} \mathbb{F}_q$.
  if $\rho(i) = \neg(t, \vec{v}_i)$,

$$\boldsymbol{c}_i := \big(\overbrace{s_i\vec{v}_i, \ldots}^{n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{0^{n_t}}^{n_t}, \overbrace{\eta_i}^{1} \big)_{\mathbb{B}_t},$$

  where $\eta_i \xleftarrow{\cup} \mathbb{F}_q$.
  return $\mathsf{ct}_\mathbb{S} := (\mathbb{S}, \{\boldsymbol{c}_i\}_{i=0,\ldots,l}, c_{d+1})$.

- $\mathsf{Dec}(\mathsf{pk}, \mathsf{sk}_\Gamma := (\Gamma, \boldsymbol{k}^*_0, \{\boldsymbol{k}^*_t\}_{(t,\vec{x}_t)\in\Gamma}),$
  $\mathsf{ct}_\mathbb{S} := (\mathbb{S}, \{\boldsymbol{c}_i\}_{i=0,\ldots,l}, c_{d+1}))$:
  If $\mathbb{S} = (M, \rho)$ accepts $\Gamma := \{(t, \vec{x}_t)\}$, then compute I and $\{\alpha_i\}_{i\in I}$ such that $\vec{1} = \sum_{i\in I} \alpha_i M_i$ where M_i is the i-th row of M, and
  $I \subseteq \{i \in \{1, .., l\} \,|\, [\rho(i) = (t, \vec{v}_i) \wedge (t, \vec{x}_t) \in \Gamma \wedge \vec{v}_i \cdot \vec{x}_t = 0] \vee [\rho(i) = \neg(t, \vec{v}_i) \wedge (t, \vec{x}_t) \in \Gamma \wedge \vec{v}_i \cdot \vec{x}_t \neq 0]\}$,

$$K := e(\boldsymbol{c}_0, \boldsymbol{k}^*_0) \prod_{i\in I \wedge \rho(i)=(t,\vec{v}_i)} e(\boldsymbol{c}_i, \boldsymbol{k}^*_t)^{\alpha_i} \prod_{i\in I \wedge \rho(i)=\neg(t,\vec{v}_i)} e(\boldsymbol{c}_i, \boldsymbol{k}^*_t)^{\alpha_i/(\vec{v}_i\cdot\vec{x}_t)}$$

  return $m := c_{d+1}/K$.

- $\mathsf{MKU}(\mathsf{pk}, \mathsf{msk} = (\{\widehat{\mathbb{B}}^*_t\}_{t=0,\ldots,d}))$:

$$W_0 \xleftarrow{\cup} GL(N_0, \mathbb{F}_q) \quad W_t \xleftarrow{\cup} GL(N_t, \mathbb{F}_q) \quad t = 1 \ldots, d$$

  For $t = 0, \ldots, d$

$$\widehat{\mathbb{B}}'_t := \widehat{\mathbb{B}}_t W_t$$

  For $t = 0, \ldots, d$

$$\widehat{\mathbb{B}}'^*_t := \widehat{\mathbb{B}}^*_t (W_t^{\mathrm{T}})^{-1}$$

  return
  $\mathsf{pk}' = (1^\lambda, \mathsf{param}_{\vec{n}}, g_t, \{\widehat{\mathbb{B}}'_t\}_{t=0,\ldots,d})$,
  $\mathsf{msk}' = (\{\widehat{\mathbb{B}}'^*_t\}_{t=0,\ldots,d}, \mathsf{upk} = \{W_t\}_{t=0,\ldots,d})$.

- $\mathsf{UpdCT}(\mathsf{upk} = \{W_t\}_{t=0,\ldots,d},$
  $\mathsf{ct}_\mathbb{S} := (\mathbb{S}, \{\boldsymbol{c}_i\}_{i=0,\ldots,l}, c_{d+1}))$:

$$\boldsymbol{c}'_0 := \boldsymbol{c}_0 W_0$$

$$\boldsymbol{c}'_i := \boldsymbol{c}_i W_t \quad \rho(i) = (t, \vec{v}_i) \text{ or } \rho(i) = \neg(t, \vec{v}_i)$$

  for $i = 0, \ldots, \ell$.
  return $\mathsf{ct}_\mathbb{S} := (\mathbb{S}, \{\boldsymbol{c}'_i\}_{i=0,\ldots,l}, c_{d+1})$.

- UpdDK $(\mathsf{upk} = \{W_t\}_{t=0,\ldots,d},$
  $\mathsf{sk}_\Gamma := (\Gamma, \boldsymbol{k}^*_0, \{\boldsymbol{k}^*_t\}_{(t,\vec{x}_t)\in\Gamma}))$:

$$\boldsymbol{k}'^*_0 := \boldsymbol{k}^*_0 (W_0^{\mathrm{T}})^{-1}$$

$$\boldsymbol{k}'^*_t := \boldsymbol{k}^*_t (W_t^{\mathrm{T}})^{-1} \quad (t, \vec{x}_t) \in \Gamma$$

  return $\mathsf{sk}'_\Gamma := (\Gamma, \boldsymbol{k}'^*_0, \{\boldsymbol{k}'^*_t\}_{(t,\vec{x}_t)\in\Gamma})$.

4.3 安全性

本提案方式は以下の定理が成り立つ

定理 9. 提案方式は *DLIN* 仮定の下で *payload-hiding* 安全を満たす.

証明のアイデア. 攻撃者は変換情報を入手することができないため，新たなマスター鍵も，古いマスター鍵もランダムに生成された場合と同じ情報しか得られることができない. そのため本定理の証明は，ベースとしている CP-ABE と同様の証明が可能となり，dual system encryption (DSE) 技法を用い，復号鍵を一つ一つ semi-functional 鍵へと変換していくことで達成される.

参考文献

[1] A. Beimel. Secure schemes for secret sharing and key distribution. *PhD Thesis, Israel Institute of Technology, Technion, Haifa*, 1996.

[2] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In *IEEE Symposium on Security and Privacy*, pages 321–334, 2007.

[3] D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In *Advances in Cryptology - CRYPTO 2004*, volume 3152 of *LNCS*, pages 41–55, 2004.

[4] D. Boneh and M. Hamburg. Generalized identity based and broadcast encryption schemes. In *ASIACRYPT 2008*, pages 455–470, 2008.

[5] D. Boneh and B. Waters. Conjunctive, subset, and range queries on encrypted data. In *TCC 2007*, pages 535–554, 2007.

[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM*

conference on Computer and communications security - ACM CCS 2006, pages 89–98, 2006.

[7] T. Okamoto and K. Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In *Advances in Cryptology - CRYPTO 2010*, volume 6223 of *LNCS*, pages 191–208, 2010. Full version is available at http://eprint.iacr.org/2010/563.

[8] R. Ostrovsky, A. Sahai, and B. Waters. Attribute-based encryption with non-monotonic access structures. In *ACM CCS 2007*, pages 195–203, 2007.

[9] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. Secure attribute-based systems. In *ACM CCS 2006*, pages 99–112, 2006.

[10] A. Sahai and B. Waters. Fuzzy identity-based encryption. In *Advances in Cryptology - EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 457–473, 2005.

[11] E. Shi and B. Waters. Delegating capabilities in predicate encryption systems. In *ICALP (2) 2008*, pages 560–578, 2008.

[12] B. Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In *PKC 2011*, pages 53–70, 2011.