効率のトレードオフが直接的に実現可能かつ実用的な属性ベース暗号の提案

アッタラパドゥン　ナッタポン† 山田翔太† 照屋唯紀† 花岡悟一郎†
松本　勉‡

† 産業技術総合研究所
〒 135-0064 東京都江東区青海 2-4-7 臨海副都心センター別館（バイオ・IT 融合研究棟）
{n.attrapadung,yamada-shota,tadanori.teruya,hanaoka-goichiro}@aist.go.jp

‡ 横浜国立大学
〒 240-8501 横浜市保土ヶ谷区常盤台 79-7　環境情報 1 号棟 7 階
tsutomu@ynu.ac.jp

あらまし 本論文では，適応的安全性を持ち，鍵長と暗号文長の間の直接的なトレードオフが実現可能な新たな属性ベース暗号方式を提案する．我々の提案する鍵ポリシー属性ベース暗号方式は，方式のセットアップ時に設定可能な変数 d によってパラメータ付けされており，t を属性の集合のサイズ，m をポリシーのサイズとすると，提案方式の暗号文長と復号コストは $O(t/d)$，秘密鍵長は $O(md)$，公開鍵長は $O(d)$ である．本方式は，Eurocrypt 2014 で Attrapadung によって提案された，制限なし属性ベース暗号と，暗号文が定数長な属性ベース暗号の両方式の一般化と見ることができる．

Practical Attribute-Based Encryption with Performance Tradeoff

Nuttapong Attrapadung† Shota Yamada† Tadanori Teruya†
Goichiro Hanaoka† Tsutomu Matsumoto‡

†National Institute of Advanced Industrial Science and Technology (AIST)
2-4-7 Aomi, Koto-ku, Tokyo, 135-0064, Japan
{n.attrapadung,yamada-shota,tadanori.teruya,hanaoka-goichiro}@aist.go.jp

‡Yokohama National University
79-7 Tokiwadai, Hodogaya-ku, Yokohama-shi, Kanagawa 240-8501, JAPAN
tsutomu@ynu.ac.jp

Abstract We propose new fully-secure attribute-based encryption (ABE) schemes such that the key sizes and ciphertext sizes can be directly traded off. Our proposed schemes are parameterized by a positive integer d, which can be arbitrarily chosen at setup. In our key-policy ABE, the ciphertext size and the decryption time is $O(t/d)$, the private key size is $O(md)$, and the public key size is $O(d)$, where t, m are the sizes of attributes and policies corresponding to ciphertext and private key, respectively. Our scheme can be considered as a generalization of two ABE instantiations, namely, the unbounded ABE scheme, and the ABE scheme with constant-size ciphertexts, both proposed recently inside the framework by Attrapadung (Eurocrypt 2014).

1 はじめに

背景. 属性ベース暗号は，柔軟なアクセス制御を可能にする暗号技術である．属性ベース暗号では，暗号文と秘密鍵のそれぞれに属性が割り当てられ，それらがある条件を充たすときに限り復号が可能である．例えば，鍵ポリシー属性ベース暗号 (Key policy attribute-based encryption, KP-ABE)[10] においては，暗号文に属性の集合が，秘密鍵に属性の上で定義される論理式が対応し，その論理式をその集合が充足する時に限り復号が可能である．暗号文ポリシー属性ベース暗号 (Ciphertext policy attribute-based encryption, CP-ABE)[7, 14] は，暗号文と秘密鍵の役割を交換したものである．これら両方の一般化として，双

ポリシー属性ベース暗号 (Dual policy attribute-based encryption, DP-ABE) も提案されている [3]．理論的な興味と実用性から，属性ベース暗号の研究は，盛んに行われている [13, 10, 12, 1]．

本研究の貢献． 本研究では，Attrapadung[1] によって提案された以下の二つの方式に着目し，両者の一般化であるような KP-ABE を提案した．

- 一つ目の方式は，暗号文が短い KP-ABE である．既存の多くの KP-ABE では，暗号文長は付属する属性の個数に比例して長くなるが，この方式では暗号文は定数長である．また，この方式は適応的安全性という強い安全性を達成している．一方，欠点は，暗号文に付属できる属性の個数に上限があること，秘密鍵長が比較的長いことである．
- 二つ目の方式は，無制限 KP-ABE である．ここで，無制限というのは，暗号文に関連付けされる属性の個数や秘密鍵に付属するポリシーのサイズに，上限がないという意味である．この方式は，他にも，秘密鍵長が比較的短く，また，適応的安全性を達成しているという利点を持つ．一方，欠点は，暗号文長が付属する属性の個数に比例して大きくなることである．

提案方式は，無制限 KP-ABE であり，また，暗号文，公開鍵，秘密鍵の長さと暗号化，復号の演算の効率性は上述の二方式の中間である．より詳細には，提案方式は，方式のセットアップ時に設定可能な変数 d によってパラメータ付けされており，t を暗号文に付属させる属性の数，m をポリシーのサイズとすると，暗号文長と復号コストは $O(t/d)$，秘密鍵長は $O(md)$，公開鍵長は $O(d)$ である．t に上限を設定し，d をその上限値に一致させると提案方式は上述の一つ目の方式に一致し，$d=1$ とした場合，二つ目の方式に一致する．ここまでは，KP-ABE の場合に関して説明したが，CP-ABE と DP-ABE に関しても，類似のトレードオフを達成する方式の構成が可能である．

このような，柔軟な効率性のトレードオフが実現できることは，例えば属性ベース暗号をハードウェアトークンに実装する場合など，時間/サイズ的制約が予め正確に定まっている環境において有益であると考えられる．なぜなら，d をその制約範囲内で調整することで，利用可能なリソースを最大限有効活用できるからである．

2 準備

述語族． $\mathbb{X}_\kappa$ を “鍵属性”，$\mathbb{Y}_\kappa$ を “暗号文属性”とし，$R = \{ R_\kappa : \mathbb{X}_\kappa \times \mathbb{Y}_\kappa \to \{0,1\} \mid \kappa \in \mathbb{N}^c \}$ をその直積の上で定義される述語族とする．ここで，c は定数である．インデックス $\kappa = (n_1, n_2, \ldots, n_c)$ は，述語族に関連する各種パラメータの上限を指定するものとする．

属性ベース暗号． 述語族 R に対する属性ベース暗号は，以下のアルゴリズムから構成される:

- $\mathsf{Setup}(1^\lambda, \kappa) \to (\mathsf{PK}, \mathsf{MSK})$: セットアップアルゴリズムはセキュリティパラメータ 1^λ と，述語族 R に関連付けされたインデックス κ を入力とし，マスター公開鍵 PK とマスター秘密鍵 MSK を出力する．
- $\mathsf{Encrypt}(Y, M, \mathsf{PK}) \to \mathsf{CT}$: 暗号化アルゴリズムは，暗号文属性 $Y \in \mathbb{Y}_\kappa$，平文 $M \in \mathcal{M}$，マスター公開鍵 PK を入力とし，暗号文 CT を出力する．
- $\mathsf{KeyGen}(X, \mathsf{MSK}, \mathsf{PK}) \to \mathsf{SK}$: 鍵生成アルゴリズムは，鍵属性 $X \in \mathbb{X}_\kappa$ とマスター秘密鍵 MSK を入力とし，秘密鍵 SK を出力する．
- $\mathsf{Decrypt}(\mathsf{CT}, \mathsf{SK}) \to M$: 復号アルゴリズムは暗号文 CT と対応する暗号文属性 Y，秘密鍵 SK と対応する鍵属性 X を入力とし，平文 M または $\perp$ を出力する．

正当性． 全ての，κ，$M \in \mathcal{M}$，$R_\kappa(X,Y) = 1$ を満たす $X \in \mathbb{X}_\kappa$，$Y \in \mathbb{Y}_\kappa$，$\mathsf{Setup}(1^\lambda, \kappa)$ によって生成された鍵ペア $(\mathsf{PK}, \mathsf{MSK})$，正しく生成された暗号文 $\mathsf{CT} \leftarrow \mathsf{Encrypt}(Y, M, \mathsf{PK})$ に関して，$\mathsf{Decrypt}(\mathsf{CT}, \mathsf{SK}) \to M$ が成立することを要求する．

安全性． 属性ベース暗号の安全性の要求として，適応的安全性 (full/adaptive security) が標準的である．本稿で提案する方式は，全てこの安全性を達成している．適応的安全性の定義に関しては，[1] などを参照されたい．

(通常の)KP-ABE の述語． $\mathcal{U}$ を属性のユニバースとする．この述語では，鍵属性は，単調なスパンプログラム（あるいはアクセス構造）(A, π) で定められる．A は，$m \times k$ のサイズ $(m, k \in \mathbb{N})$ の整数成分の行列であり，$\pi : [1,m] \to \mathcal{U}$ は写像である．属性の集合 $S \subseteq \mathcal{U}$ に対して，$A|_S$ は，A の j 行目で $\pi(j) \in S$ であるものだけからなる A の部分行列である．$(1, 0, \ldots, 0) \in \mathsf{rspan}(A|_S)$ であるとき，(A, π) は $S \subseteq \mathcal{U}$ を受理するという．ここで，rspan() は，行列を入力とし，その行列の行ベクトルの張る空間を返す関数とする．単調なスパンプログラムを述語としてあつかえる属性ベース暗号は，単調な論理式も述語として扱うことができる [10]．

2.1 鍵ポリシー両空間暗号 (KP-DSE)

我々の，提案 KP-ABE 方式は，鍵ポリシー両空間暗号 (Key policiy over doubly spatial encryp-

tion, KP-DSE) からの変換によって得られる．この小節では KP-DSE を定義する．

アフィン空間の概念． N, n, d を，$0 \le d \le n$ を満たす自然数とする．また，$\boldsymbol{m}^\top$ を $\mathbb{Z}_N^n$ の縦ベクトルとする．また，$\boldsymbol{M} \in \mathbb{Z}_N^{n\times d}$ をフルランクな行列とする．$\mathbb{Z}_N^n$ のアフィン空間は，ベクトルと行列の組 $(\boldsymbol{m}, \boldsymbol{M})$ によって，

$$\boldsymbol{m}^\top + \mathsf{cspan}(\boldsymbol{M}) = \left\{ \boldsymbol{m}^\top + \boldsymbol{M}\boldsymbol{v}^\top \;\middle|\; \boldsymbol{v} \in \mathbb{Z}_N^d \right\}.$$

と定義される．cspan() は，行列の，列ベクトルの張る空間を返す関数である．

KP-DSE の述語． この述語は以下のように定義される．述語族は，$(N, n) \in \mathbb{N}^2$ によってインデックス付けされている．鍵属性のドメイン $\mathbb{X}_{(N,n)}$ は $A \in \mathbb{Z}_N^{m\times k}(m, k \in \mathbb{N}$ は多項式長) とラベル付け写像 π の組全体からなる．π は $[1, m]$（A の行に対応）から $\mathbb{Z}_N^n$ 内のアフィン空間への写像である．また，暗号文属性 $\mathbb{Y}_{(N,n)}$ のドメインは，$\mathbb{Z}_N^n$ 内のアフィン空間全体である．対応する述語 $R^{\mathsf{KP\text{-}DSE}}_{(N,n)} : \mathbb{X}_{(N,n)} \times \mathbb{Y}_{(N,n)} \to \{0,1\}$ は以下のように定義される．

$$R^{\mathsf{KP\text{-}DSE}}_{(N,n)}((A,\pi), S) = 1 \Leftrightarrow$$
$$(1, 0, \ldots, 0) \in \mathsf{span}\{A_i | \exists Y \in S \text{ s.t. } \pi(i) \cap Y \neq \emptyset\}$$

2.2 埋め込み補題

埋め込み補題 [8] は，ある述語に対する属性ベース暗号から，別の述語に対する属性ベース暗号への変換が可能であるための十分条件を与えるものである．以下の二つの述語族を考える．

$$R^{\mathsf{F}}_{\kappa} : A_\kappa \times B_\kappa \to \{0,1\},\ R^{\mathsf{F}'}_{\kappa'} : A'_{\kappa'} \times B'_{\kappa'} \to \{0,1\},$$

それぞれの述語族は，$\kappa \in \mathbb{N}^c$ と $\kappa' \in \mathbb{N}^{c'}$ によってパラメータ付けされている．また，以下のような三つの効率的に計算可能な写像を考える．

$$f_{\mathsf{p}} : \mathbb{Z}^{c'} \to \mathbb{Z}^c, f_{\mathsf{e}} : A'_{\kappa'} \to A_{f_{\mathsf{p}}(\kappa')}, f_{\mathsf{k}} : B'_{\kappa'} \to B_{f_{\mathsf{p}}(\kappa')}$$

それぞれ，パラメータ間の写像，暗号文属性間の写像，鍵属性間の写像であり，任意の $X' \in A'_{\kappa'}, Y' \in B'_{\kappa'}$ に対し，以下が成立するとする．

$$R^{\mathsf{F}'}_{\kappa'}(X', Y') = 1 \Leftrightarrow R^{\mathsf{F}}_{f_{\mathsf{p}}(\kappa')}(f_{\mathsf{e}}(X'), f_{\mathsf{k}}(Y')) = 1.$$

この時，次の補題が成り立つ．

Lemma 1 (埋め込み補題 [8])．上述の条件を満たす写像が存在する時，述語 $R^{\mathsf{F}'}_{\kappa'}$ に対応する属性ベース暗号 Π' を，述語 R^{F}_{κ} に対応する属性ベース暗号 Π に変換可能である．もし Π が正当性と選択的/適応的安全性を持てば，Π' も正当性と選択的/適応的安全性を持つ．

2.3 記法

指数部に行列を書く記法． ベクトルは，特に指定がないときは，行ベクトルとして扱うが，列ベクトルとして扱うこともある．また，$\mathbb{GL}_{p,n}$ によって，$\mathbb{Z}_p^{n\times n}$ 内の正則な行列全体のなす群（一般線形群）を表す．$\mathbb{G}$ を群とし，$\boldsymbol{a} = (a_1, \ldots, a_n) \in \mathbb{G}^n$ と $\boldsymbol{b} = (b_1, \ldots, b_n) \in \mathbb{G}^n$ をベクトルとする．このとき，$\boldsymbol{a} \cdot \boldsymbol{b}$ は $(a_1 \cdot b_1, \ldots, a_n \cdot b_n)$ をあらわすものとする．ここで，$\cdot$ は $\mathbb{G}$ 内での群演算を表す．$g \in \mathbb{G}$ と，$\boldsymbol{c} = (c_1, \ldots, c_n) \in \mathbb{Z}^n$ に対して，$g^{\boldsymbol{c}}$ によって $(g^{c_1}, \ldots, g^{c_n})$ を表すものとする．行列 $\boldsymbol{M} \in \mathbb{Z}_p^{d\times n}$ に関しても，$g^{\boldsymbol{M}}$ を同様に定義する．また，行列 $\boldsymbol{Q} \in \mathbb{Z}_p^{\ell\times d}$ に対し，$(g^{\boldsymbol{Q}})^{\boldsymbol{M}} = g^{\boldsymbol{QM}}$ のように表記する．$\boldsymbol{M}$ と $g^{\boldsymbol{Q}} \in \mathbb{G}^{\ell\times d}$ から，($\boldsymbol{Q}$ の値を知らずに) $g^{\boldsymbol{QM}}$ が効率的に計算可能である．実際，$g^{\boldsymbol{QM}}$ の (i,j) 成分は，$\prod_{k=1}^{d}(g^{\boldsymbol{Q}_{i,k}})^{\boldsymbol{M}_{k,j}}$ のように計算可能である．$g^{\boldsymbol{M}}$ と $\boldsymbol{Q}$ に関しても同様のことが言える．$\boldsymbol{X} \in \mathbb{Z}_p^{r\times c_1}$ と $\boldsymbol{Y} \in \mathbb{Z}_p^{r\times c_2}$ に対して，以下のような表記を用いる．

$$e(g_1^{\boldsymbol{X}}, g_2^{\boldsymbol{Y}}) = e(g_1, g_2)^{\boldsymbol{Y}^\top \boldsymbol{X}} \in \mathbb{G}_T^{c_2\times c_1}.$$

射影を表す行列． [2] と同様に，$\begin{pmatrix} \boldsymbol{I}_b \\ 0 \end{pmatrix}$ は最初の b 行が単位行列であり最後の行が零ベクトルであるような $(b+1)\times b$ サイズの行列を表す．この行列は，行列の左 b 列を取り出す射影の役割を持つ．実際，$X \begin{pmatrix} \boldsymbol{I}_b \\ 0 \end{pmatrix} \in \mathbb{Z}_p^{(b+1)\times b}$ は，X の最初の b 列からなる行列である．同様に，$\begin{pmatrix} \boldsymbol{0} \\ 1 \end{pmatrix}$ は，$(b+1)\times 1$ 行列で，最後の成分が 1 で，その他の成分は 0 である行列を表す．これは，行列の最後の列を取り出す射影の役割を持つ．

3 提案 KP-ABE 方式

この節では，1節で説明したような，効率性の柔軟なトレードオフが可能な KP-ABE 方式を提案する．設計においては，埋め込み補題 (Lemma 1) を利用し，KP-DSE から通常の KP-ABE への一般的変換を示し，その変換を [1, 2] で構成された KP-DSE に適用するという方針を採る．より詳細には，partitioned KP-ABE という KP-ABE のシンタックスを少し変更した概念を導入し，partitioned KP-ABE から通常の KP-ABE への変換と，KP-DSE から partitioned KP-ABE への変換を示す．これらの組み合わせで，KP-DSE から KP-ABE への一般的変換が得られる．

主となるアイデア． 我々の提案 KP-ABE 方式では，パラメータ d を導入し，属性の集合 S を，$|S_j| \le d$ を満たすような互いに素な $\ell(= \lceil |S|/d \rceil)$

個の集合に $S = S_1 \sqcup \cdots \sqcup S_\ell$ と分割する．さらに，それぞれの S_j を，[4, 1] と同様に，アフィン空間に埋め込む．これにより，$\mathbb{Z}_N^{d+1}$ 内の ℓ 個のアフィン空間に関連付けされる KP-DSE 方式を得る．[1] では，ℓ 個のアフィン空間を利用する際には，暗号文長は $O(\ell)$ であった．提案方式でも，同様に暗号文長は $O(\ell) = O(|S|/d)$ となる．

Partitioned KP-ABE. 中間的な述語族として，（単調なスパンプログラムを扱うことができる）“partitioned KP-ABE” を定義する．この述語族は，通常の KP-ABE を定義する述語族とほとんど同じであり，整数 N に加えて（N は $\mathbb{Z}_N$ を定める），変数 d にもインデックス付けされているところのみが異なる．つまり，述語族は，$(N, d) \in \mathbb{N}^2$ によって指定される．この新たな述語族を導入する目的は，述語族のシンタックスの都合上のものである．鍵属性の空間は通常の KP-ABE と同様である．暗号文属性の空間は，サイズが d 以下の $\mathcal{U}$ の部分集合の集合で，それぞれの部分集合が，互いに素であるようなもの全体とする．述語は，

$$\begin{aligned} & R^{\mathsf{Partition\text{-}KP\text{-}ABE}}_{(N,d)}((A,\pi),U) = 1 \\ \Leftrightarrow\ & (1,0,\ldots,0) \in \mathsf{span}\{A_i | \exists W \in U \ \text{ s.t. } \pi(i) \in W\}. \end{aligned}$$

と定義される．

Partitioned KP-ABE から通常の KP-ABE への変換. Partitioned KP-ABE は，暗号文属性を以下のように定めることによって，簡単に通常の KP-ABE に変換することができる．

$$S \mapsto \{S_1, \cdots S_\ell\}.$$

上式で，$\ell = \lceil |S|/d \rceil$ とし，全ての $j \in [1, \ell]$ に対して $|S_j| \leq d$ が成立し，また，$S = S_1 \sqcup \cdots \sqcup S_\ell$ であるとする．一意的に上記のような分割を得るため，S は $S = \{b_1, \ldots, b_{|S|}\}$ のように辞書式順序に並び替えられ，$j \in [1, \ell - 1]$ に対して，$S_j = \{b_{(j-1)d+1}, \ldots, b_{jd}\}$ と定義されるものとする．（したがって，$S_\ell = \{b_{(\ell-1)d+1}, \ldots, b_{|S|}\}$ である．）このとき，以下が成り立つ．

$$\begin{aligned} & R^{\mathsf{KP\text{-}ABE}}_{N}((A,\pi),S) = 1 \\ \Leftrightarrow\ & R^{\mathsf{Partition\text{-}KP\text{-}ABE}}_{(N,d)}((A,\pi),\{S_1, \cdots S_\ell\}) = 1. \end{aligned}$$

上式は，$\pi(i) \in S$ であることと，$\pi(i) \in S_j$ であるような $j \in [1, \ell]$ が存在することが等価であることからしたがう．

3.1 KP-DSE から Partitioned KP-ABE への変換

この小節では，KP-DSE が KP-ABE に変換可能であることを示す．変換は以下の通りである．

- **パラメータ間の写像.** 写像 f_{p} を $f_{\mathsf{p}} : (N, d) \mapsto (N, d+1)$ のように定める．すなわち，（KP-DSE であつかえる）アフィン空間の次元の最大値は $n = d + 1$ である．
- **鍵属性間の写像.** アクセス構造 $\mathbb{A} = (A, \pi)$ を考える．m を，アクセス行列 A の行の数とする．写像 f_{k} は

  $$f_{\mathsf{k}} : \mathbb{A} = (A, \pi) \mapsto \mathbb{A}' = (A, \pi')$$

  のように定義される．上式で，$i = 1, \ldots, m$ に関して，$\pi'(i)$ は，$\pi'(i) = \mathsf{cspan}(\boldsymbol{X}^{(i)})$ と定義される．ここで，

  $$\boldsymbol{X}^{(i)} := \begin{pmatrix} -\pi(i) & -\pi(i)^2 & \cdots & -\pi(i)^d \\ 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}.$$

  である．特に，$\pi'(i)$ は，原点 $\mathbf{0}^\top$ を通過するようなアフィン空間である．（すなわち，ベクトル空間である．）
- **暗号文属性間の写像.** 互いに素な集合の集合 $\{S_1, \ldots, S_\ell\}$ で，全ての $j \in [1, \ell]$ に関して $|S_j| \leq d$ が成り立つものを考える．写像 f_{c} は，以下のように定義される．

  $$f_{\mathsf{c}} : \{S_1, \ldots, S_\ell\} \mapsto \{\boldsymbol{y}^{(1)}, \ldots, \boldsymbol{y}^{(\ell)}\}$$

  上式で，$\boldsymbol{y}^{(i)}$ は，下記のような 0 次元アフィン空間（すなわち点）として定義される．

  $$\boldsymbol{y}^{(j)} := (a_{j,0}, a_{j,1}, \ldots, a_{j,d})^\top.$$

  ここで，$a_{j,\iota}$ は，多項式 $p_j(z) := \prod_{y \in S_j}(z - y) = a_{j,0} + a_{j,1}z + \cdots + a_{j,d}z^d$ の z^ι の係数である．

次に以下の補題を示す．この補題と，埋め込み補題 (Lemma 1) を組み合わせることにより，上記の方法で，KP-DSE を KP-ABE に変換できることがわかる．

Lemma 2. 任意のアクセス構造 $\mathbb{A} = (A, \pi)$ と，任意の属性の集合 S に関して，

$$\begin{aligned} & R^{\mathsf{Partition\text{-}KP\text{-}ABE}}_{d}(\mathbb{A}, \{S_1, \ldots, S_\ell\}) = 1 \\ \Leftrightarrow\ & R^{\mathsf{KP\text{-}DSE}}_{f_{\mathsf{p}}(d)}(f_{\mathsf{k}}(\mathbb{A}), f_{\mathsf{c}}(\{S_1, \ldots, S_\ell\})) = 1. \end{aligned}$$

が成立する．

Proof. KP-DSE の述語族の定義から，定理を証明するには，任意の $i \in [1,m], j \in [1,\ell]$ に関して，以下が成り立つことを示せば十分である：

$$\pi(i) \in S_j \quad \Longleftrightarrow \quad \boldsymbol{y}^{(j)} \in \mathsf{cspan}(\boldsymbol{X}^{(i)}). \quad (1)$$

式 (1) を，順方向と逆方向に分けて証明する．

順方向の証明 ($\Rightarrow$). $\pi(i) \in S_j$ と仮定する．すると，p_j の定義から，$p_j(\pi(i)) = 0$ が成り立つ．したがって，

$$\begin{aligned}\boldsymbol{X}^{(i)}(\boldsymbol{a}^{(j)})^\top &= \big(-(a_{j,1}\pi(i) + \cdots + a_{j,d}\pi(i)^d), \\ &\qquad a_{j,1}, \ldots, a_{j,d}\big)^\top \\ &= (a_{j,0}, a_{j,1}, \ldots, a_{j,d})^\top = \boldsymbol{y}^{(j)},\end{aligned}$$

が成立する．上式の二番目の等号では，$p_j(\pi(i)) = a_{j,0} + a_{j,1}\pi(i) + \cdots + a_{j,d}\pi(i)^d = 0$ であることを使っている．これによって，$\boldsymbol{y}^{(j)} \in \mathsf{cspan}(\boldsymbol{X}^{(i)})$ を得る．したがって，順方向の証明が完了した．

逆方向の証明 ($\Leftarrow$). 対偶を証明する．$\pi(i) \notin S$ と仮定すると，$p_j(\pi(i)) \neq 0$ が成立する．以下，$\boldsymbol{y}^{(j)} \in \mathsf{cspan}(\boldsymbol{X}^{(i)})$ であると仮定して矛盾を導く．条件より，ある $\boldsymbol{v}^\top = (v_1, \ldots, v_d)^\top$ が存在して，

$$\boldsymbol{X}^{(i)}\boldsymbol{v}^\top = \boldsymbol{y}^{(j)}.$$

が成り立つ．したがって，$\boldsymbol{X}^{(i)}, \boldsymbol{y}^{(j)}$ の定義より，

$$\begin{aligned}&\big(-(v_1\pi(i) + \cdots + v_d\pi(i)^d), v_1, \ldots, v_d\big)^\top \\ &\qquad = (a_{j,0}, a_{j,1}, \ldots, a_{j,d})^\top\end{aligned}$$

が成立する．これにより，$p_j(\pi(i)) = 0$ を得るが，これは最初の仮定に矛盾する．したがって，$\boldsymbol{y}^{(j)} \notin \mathsf{cspan}(\boldsymbol{X}^{(i)})$ を得る． □

3.2 提案 KP-ABE 方式の具体的な記述（合成数位数群上）

この小節では，我々の示した KP-DSE から KP-ABE への変換法を，[1] で提案されている，合成数位数群上での KP-DSE 方式に適用して得られる方式の具体的記述を示す．(ただし，[1] では対称ペアリング群上で方式は記述されているが，本稿では非対称ペアリング群上で記述する．) 提案方式では，合成数位数の非対称ペアリング群の生成アルゴリズム $\mathcal{G}_{\mathsf{composite}}$ を用いる．$\mathsf{composite}(\lambda)$ は，$(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, N, p_1, p_2, p_3) \xleftarrow{\$} \mathcal{G}_{\mathsf{composite}}(\lambda)$ を出力する．ここで，$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ は，位数が $N = p_1p_2p_3$ であるような 3 つの群であり，これらの群上で双線形写像 $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ が定義される．以下，$\mathbb{G}_{1,p_i}, \mathbb{G}_{2,p_i}$ を，それぞれ，位数が p_i であるような，$\mathbb{G}_1, \mathbb{G}_2$ の部分群とする．方式の記述は以下の通りである．

- $\mathsf{Setup}(1^\lambda, d)$: セットアップアルゴリズムは，合成数位数の群 $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, N, p_1, p_2, p_3) \xleftarrow{\$} \mathcal{G}_{\mathsf{composite}}(\lambda)$ を選び，部分群の生成元 $g_1 \xleftarrow{\$} \mathbb{G}_{1,p_1}$，$g_2 \in \mathbb{G}_{2,p_1}$，$Z_3 \xleftarrow{\$} \mathbb{G}_{2,p_3}$ を選ぶ．また，$\boldsymbol{h} = (h_0, h_1, \ldots, h_{d+1}, \phi_1, \phi_2, \phi_3, \eta) \xleftarrow{\$} \mathbb{Z}_N^{d+6}$ と $\alpha \xleftarrow{\$} \mathbb{Z}_N$ を選ぶ．公開鍵は，$\mathsf{PK} = (g_1, g_2, e(g_1,g_2)^\alpha, g_1^{\boldsymbol{h}}, Z_3)$ で，マスター秘密鍵は $\mathsf{MSK} = \alpha$ である．
- $\mathsf{Encrypt}(S, M, \mathsf{PK})$: 暗号化アルゴリズムは，$S \subseteq \mathbb{Z}_N$ を入力とし，以下のように動作する．
  1. ℓ を $\ell = \lceil |S|/d \rceil$ と設定し，S を全ての $j \in [1,\ell]$ に関して $|S_j| \leq d$ が成り立つように $S = S_1 \sqcup \cdots \sqcup S_\ell$，$|S_j| \leq d$ と分割する．また，$j \in [1,\ell]$ に関して，多項式 $p_j(z) := \prod_{y \in S_j}(z - y)$ の z^ι の係数 $a_{j,\iota}$ を計算する．
  2. $s, w, s_1, \ldots, s_\ell \xleftarrow{\$} \mathbb{Z}_N$ をサンプルし，暗号文 $\mathsf{CT} = (C_0, C_1, C_2, C_3, C_4, \{C_{5,j}, C_{6,j}\}_{j \in [1,\ell]})$ を出力する．ここで，$C_0 = (e(g_1,g_2)^\alpha)^s M \in \mathbb{G}_T$ であり，
$$\begin{aligned}C_1 &= g_1^s, & C_2 &= g_1^{s\eta}, \\ C_3 &= g_1^{s\phi_1 + w\phi_2}, & C_4 &= g_1^w, \\ C_{5,j} &= g_1^{w\phi_3 + s_j(h_0 + h_1 a_{j,0} + \cdots + h_{d+1}a_{j,d})} \\ C_{6,j} &= g_1^{s_j}\end{aligned}$$
  である．
- $\mathsf{KeyGen}((A,\pi), \mathsf{MSK}, \mathsf{PK})$: $A \in \mathbb{Z}_N^{m \times k}$，$\pi : [1,m] \to \mathbb{Z}_N$ であるようなアクセス構造を表す組 (A,π) を入力とし，以下のように動作する．ここで，$m, k \in \mathbb{N}$ とする．まず，$r, u, r_1, \ldots, r_m, v_2, \ldots, v_k \xleftarrow{\$} \mathbb{Z}_N$ をサンプルし，$v_1 = r\phi_2$，$\boldsymbol{v} = (v_1, \ldots, v_k)$ とする．$\boldsymbol{K} = (K_1, K_2, K_3, \{K_{4,i}, K_{5,i}, \boldsymbol{K}_{6,i}\}_{i \in [1,m]})$ を，
$$\begin{aligned}K_1 &= g_2^{\alpha + r\phi_1 + u\eta}, & K_2 &= g_2^u, \\ K_3 &= g_2^r, & K_{4,i} &= g_2^{A_i\boldsymbol{v}^\top + r_i\phi_3}, \\ K_{5,i} &= g_2^{r_i}, \\ \boldsymbol{K}_{6,i} &= \Big(K_{6,i,0} = g_2^{r_i h_0}, \\ &\qquad \Big\{K_{6,i,j} = g_2^{r_i\left(h_{j+1} - h_1\pi(i)^j\right)}\Big\}_{j=1}^{d}\Big).\end{aligned}$$
  のように計算する．また，ランダムな群の元 $\boldsymbol{R} \xleftarrow{\$} \mathbb{G}_{2,p_3}^{3+(d+3)m}$ をサンプルし（$\boldsymbol{R}$ の群の元の個数は，$\boldsymbol{K}$ と同じである），秘密鍵 $\mathsf{SK} = \boldsymbol{K} \cdot \boldsymbol{R}$ を出力する．

- $\mathsf{Decrypt}(\mathsf{CT}, \mathsf{SK})$: まず，$\mathsf{CT}, \mathsf{SK}$ から $(S, (A, \pi))$ を取り出す．以下，暗号文の復号が可能であるために，(A, π) は S を受理するものと仮定する．集合 I を $I := \{\, i \in [1, m] \mid \pi(i) \in S \,\}$ と定義する．LSSS の性質から，秘密情報の復元のための係数 $\{\mu_i\}_{i \in I}$ が存在し，$\sum_{i \in I} \mu_i A_i \boldsymbol{v}^\top = v_1 (= r\phi_2)$ が成立する．復号アルゴリズムは，次のように動作する．

  1. 全ての $i \in I$ に対して，以下を行う．まず，j_i を，$\pi(i) \in S_{j_i}$ を満たすインデックスとする．(全ての $i \in I$ に関して $\pi(i) \in S$ が成り立ち，かつ，$\{S_1, \ldots, S_\ell\}$ が互いに素なので，そのようなインデックスは必ず一意的に存在する．) 秘密鍵から，$\boldsymbol{K}_{6,i} = (K_{6,i,0}, \ldots, K_{6,i,d})$ を取り出し，
  $$D_{6,i} := K_{6,i,0} \cdot K_{6,i,1}^{a_{j_1}} \cdots K_{6,i,d}^{a_{j_d}}.$$
  を計算する．
  2. 次に，以下を計算する：
  $$\begin{aligned} &e(C_1, K_1) e(C_2, K_2)^{-1} e(C_3, K_3)^{-1} \\ &\cdot \prod_{i \in I} \left(e(C_4, K_{4,i}) e(C_{5,j_i}, K_{5,i})^{-1} e(C_{6,j_i}, D_{6,i}) \right)^{\mu_i} \\ &= e(g_1, g_2)^{\alpha s}. \end{aligned}$$
  3. 最後に $M \leftarrow C_0 / e(g_1, g_2)^{\alpha s}$ を計算し，出力する．

安全性． 上記の提案方式の適応的安全性は，[2] の KP-DSE 方式の適応的安全性と，3.1節の議論と，埋め込み補題 (Lemma 1) からただちに従う．より詳しくは，以下の定理が成り立つ．

Theorem 3. 上記の提案方式は，非対称合成数位数ペアリング群上での *Subgroup Decision* 仮定 *1,2,3*, $(d+1, \ell)$-EDHE3 仮定，$(d+1, m, k)$-EDHE4 仮定の下で，適応的安全である．ここで，d は方式内で設定する変数で，$\ell = \lceil |S| / d \rceil$ であり，S はチャレンジ暗号文に付属する暗号文属性のサイズで，m, k は秘密鍵に関連付けされるアクセス行列のサイズの最大値である．

3.3 提案 KP-ABE 方式の具体的な記述（素数位数群上）

この小節では，3.1節で示した KP-DSE から KP-ABE への変換方法を，[2] で提案された素数位数群上の KP-DSE 方式に適用して得られる方式を示す．提案方式では，素数位数の非対称ペアリング群の生成アルゴリズム $\mathcal{G}_{\mathsf{prime}}$ を用いる．$\mathcal{G}_{\mathsf{prime}}(\lambda)$ は，$(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, p) \xleftarrow{\$} \mathcal{G}_{\mathsf{prime}}(\lambda)$ を出力する．ここで，$\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ は，位数が p であるような 3 つの群であり，これらの群上で双線形写像 $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ が定義される．方式の記述は以下の通りである．

- $\mathsf{Setup}(1^\lambda, d)$: セットアップアルゴリズムは，$(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, p) \xleftarrow{\$} \mathcal{G}_{\mathsf{prime}}(\lambda)$ を選び，群の生成元 $g_1 \xleftarrow{\$} \mathbb{G}_1$, $g_2 \xleftarrow{\$} \mathbb{G}_2$ を選ぶ．また，$\boldsymbol{H}_0, \boldsymbol{H}_1, \ldots, \boldsymbol{H}_{d+5}, \xleftarrow{\$} \mathbb{Z}_p^{(b+1)\times(b+1)}$, $\boldsymbol{B} \xleftarrow{\$} \mathbb{GL}_{p,b+1} \subset \mathbb{Z}_p^{(b+1)\times(b+1)}$, $\tilde{\boldsymbol{D}} \xleftarrow{\$} \mathbb{GL}_{p,b}$ を選び，$\boldsymbol{D} := \begin{pmatrix} \tilde{\boldsymbol{D}} & \boldsymbol{0} \\ \boldsymbol{0} & 1 \end{pmatrix} \in \mathbb{GL}_{p,b+1}$ と $\boldsymbol{Z} := \boldsymbol{B}^{-\top} \boldsymbol{D}$. を計算する．さらに，$\boldsymbol{\alpha} \xleftarrow{\$} \mathbb{Z}_p^{(b+1)\times 1}$ を選び，
  $$\mathsf{PK} = \left(e(g_1, g_2)^{\boldsymbol{\alpha}^\top \boldsymbol{B} \begin{pmatrix} \boldsymbol{I}_b \\ 0 \end{pmatrix}}, g_1^{\boldsymbol{B} \begin{pmatrix} \boldsymbol{I}_b \\ 0 \end{pmatrix}}, \left\{ g_1^{\boldsymbol{H}_i \boldsymbol{B} \begin{pmatrix} \boldsymbol{I}_b \\ 0 \end{pmatrix}} \right\}_{i=0}^{d+5} \right),$$
  $$\mathsf{MSK} = \left(g_2^{\boldsymbol{\alpha}}, g_2^{\boldsymbol{Z} \begin{pmatrix} \boldsymbol{I}_b \\ 0 \end{pmatrix}}, \left\{ g_2^{\boldsymbol{H}_i^\top \boldsymbol{Z} \begin{pmatrix} \boldsymbol{I}_b \\ 0 \end{pmatrix}} \right\}_{i=0}^{d+5} \right).$$
  を出力する．
- $\mathsf{Encrypt}(S \subset \mathbb{Z}_p, M, \mathsf{PK})$: 暗号化アルゴリズムは，$S \subseteq \mathbb{Z}_p$ を入力とし，以下のように動作する．

  1. ℓ を $\ell = \lceil |S| / d \rceil$ と設定し，S を全ての $j \in [1, \ell]$ に関して $|S_j| \le d$ が成り立つように $S = S_1 \sqcup \cdots \sqcup S_\ell$, $|S_j| \le d$ と分割する．また，$j \in [1, \ell]$ に関して，多項式 $p_j(z) := \prod_{y \in S_j} (z - y)$ の z^ι の係数 $a_{j,\iota}$ を計算する．
  2. $\boldsymbol{s}_0, \boldsymbol{w}, \boldsymbol{s}_1, \ldots, \boldsymbol{s}_\ell \xleftarrow{\$} \mathbb{Z}_p^{b \times 1}$ をサンプルし，暗号文 $\mathsf{CT} = (\boldsymbol{C}_1, \boldsymbol{C}_2, \boldsymbol{C}_3, \boldsymbol{C}_4, \{\boldsymbol{C}_{5,j}, \boldsymbol{C}_{6,j}\}_{j \in [1,\ell]}, C_0)$ を出力する．ここで，
  $$\begin{aligned} \boldsymbol{C}_1 &= g_1^{\boldsymbol{B} \begin{pmatrix} \boldsymbol{s}_0 \\ 0 \end{pmatrix}}, \quad \boldsymbol{C}_2 = g_1^{\boldsymbol{H}_{d+5} \boldsymbol{B} \begin{pmatrix} \boldsymbol{s}_0 \\ 0 \end{pmatrix}}, \\ \boldsymbol{C}_3 &= g_1^{\boldsymbol{H}_{d+2} \boldsymbol{B} \begin{pmatrix} \boldsymbol{s}_0 \\ 0 \end{pmatrix} + \boldsymbol{H}_{d+3} \boldsymbol{B} \begin{pmatrix} \boldsymbol{w} \\ 0 \end{pmatrix}}, \\ \boldsymbol{C}_4 &= g_1^{\boldsymbol{B} \begin{pmatrix} \boldsymbol{w} \\ 0 \end{pmatrix}}, \quad \boldsymbol{C}_{6,j} = g_1^{\boldsymbol{B} \begin{pmatrix} \boldsymbol{s}_j \\ 0 \end{pmatrix}}, \\ \boldsymbol{C}_{5,j} &= g_1^{\boldsymbol{H}_{d+4} \boldsymbol{B} \begin{pmatrix} \boldsymbol{w} \\ 0 \end{pmatrix} + \left(\boldsymbol{H}_0 \boldsymbol{B} + \sum_{k \in [0,d]} a_{j,k} \boldsymbol{H}_{k+1} \boldsymbol{B} \right) \begin{pmatrix} \boldsymbol{s}_j \\ 0 \end{pmatrix}} \end{aligned}$$
  かつ，$C_0 = e(g_1, g_2)^{\boldsymbol{\alpha}^\top \boldsymbol{B} \begin{pmatrix} \boldsymbol{s}_0 \\ 0 \end{pmatrix}} \cdot M \in \mathbb{G}_T$ である．

- KeyGen$((A,\pi),\mathsf{MSK})$: $A \in \mathbb{Z}_p^{m\times k}$, $\pi:[1,m]\to\mathbb{Z}_p$ であるようなアクセス構造を表す組 (A,π) を入力とし，以下のように動作する．ここで，$m,k\in\mathbb{N}$ とする．まず，入力から $\mathsf{MSK}=\alpha$ を取り出す．次に，$\boldsymbol{r},\boldsymbol{u},\boldsymbol{r}_1,\ldots,\boldsymbol{r}_m,\boldsymbol{v}_2,\ldots,\boldsymbol{v}_k \xleftarrow{\$} \mathbb{Z}_p^{b\times 1}$ をサンプルする．最後に，$\mathsf{SK}=(\boldsymbol{K}_1,\boldsymbol{K}_2,\boldsymbol{K}_3,\{\boldsymbol{K}_{4,i},\boldsymbol{K}_{5,i},\boldsymbol{K}_{6,i,j}\}_{i\in[1,m],j\in[0,d]})$ を出力する．ここで，

$$\begin{aligned}
\boldsymbol{K}_1 &= g_2^{\boldsymbol{\alpha}+\boldsymbol{H}_{d+2}^\top \boldsymbol{Z}\binom{\boldsymbol{r}}{0}+\boldsymbol{H}_{d+5}^\top \boldsymbol{Z}\binom{\boldsymbol{u}}{0}},\\
\boldsymbol{K}_2 &= g_2^{\boldsymbol{Z}\binom{\boldsymbol{u}}{0}}, \qquad \boldsymbol{K}_3 = g_2^{\boldsymbol{Z}\binom{\boldsymbol{r}}{0}},\\
\boldsymbol{K}_{4,i} &= g_2^{A_{i,1}\boldsymbol{H}_{d+3}^\top \boldsymbol{Z}\binom{\boldsymbol{r}}{0}+\sum_{j=2}^{k} A_{i,j}\boldsymbol{Z}\binom{\boldsymbol{v}_j}{0}}\\
&\quad \cdot g_2^{\boldsymbol{H}_{d+4}^\top \boldsymbol{Z}\binom{\boldsymbol{r}_i}{0}},\\
\boldsymbol{K}_{5,i} &= g_2^{\boldsymbol{Z}\binom{\boldsymbol{r}_i}{0}}, \qquad \boldsymbol{K}_{6,i,0} = g_2^{\boldsymbol{H}_0^\top \boldsymbol{Z}\binom{\boldsymbol{r}_i}{0}},\\
\boldsymbol{K}_{6,i,j} &= g_2^{(\boldsymbol{H}_{j+1}^\top-\pi(i)^j\boldsymbol{H}_1^\top)\boldsymbol{Z}\binom{\boldsymbol{r}_i}{0}} \ \forall_{j\in[1,d]}
\end{aligned}$$

である．

- Decrypt$(\mathsf{CT},\mathsf{SK})$: (A,π) は S を受理すると仮定する．また，$I=\{\,i\in[1,m]\mid\pi(i)\in S\,\}$ とする．$\sum_{i\in I}\mu_i A_i=(1,0,\ldots,0)$ を満たすような，秘密復元のための係数 $\{\mu_i\}_{i\in I}$ を計算する．さらに，以下のように動作する．

  1. 全ての $i\in I$ に対して，以下を行う．j_i を，$\pi(i)\in S_{j_i}$ であるようなインデックスであるとする．(全ての $i\in I$ に関して $\pi(i)\in S$ が成り立ち，かつ，$\{S_1,\ldots,S_\ell\}$ が互いに素なので，そのようなインデックスは必ず一意的に存在する．) 次に，

  $$\boldsymbol{D}_{6,i} := \boldsymbol{K}_{6,i,0}\cdot \boldsymbol{K}_{6,i,1}^{a_{j_1}}\cdots \boldsymbol{K}_{6,i,d}^{a_{j_d}}.$$

  を計算する．

  2. 次に，$e(g_1,g_2)^{\boldsymbol{\alpha}^\top \boldsymbol{B}\binom{\boldsymbol{s}_0}{0}} = L_1\cdot L_2$ を計算する．ここで，

  $$\begin{aligned}
  L_1 &:= e(\boldsymbol{C}_1,\boldsymbol{K}_1)e(\boldsymbol{C}_2,\boldsymbol{K}_2)^{-1}e(\boldsymbol{C}_3,\boldsymbol{K}_3)^{-1},\\
  L_2 &:= \prod_{i\in I}\Big(e(\boldsymbol{C}_4,\boldsymbol{K}_{4,i})e(\boldsymbol{C}_{5,\pi(i)},\boldsymbol{K}_{5,i})^{-1}\\
  &\qquad \cdot e(\boldsymbol{C}_{6,\pi(i)},\boldsymbol{D}_{6,i})\Big)^{\mu_i},
  \end{aligned}$$

  である．

  3. 最後に，$M\leftarrow C_0/e(g_1,g_2)^{\boldsymbol{\alpha}^\top \boldsymbol{B}\binom{\boldsymbol{s}_0}{0}}$ を計算する．

安全性． 安全性に関して，以下の定理が成り立つ．

Theorem 4. 上記の *KP-ABE* 方式は，非対称素数位数群上の $\mathcal{D}_b$-*Matrix-DH* 仮定，$(d+1,\ell)$-EDHE3p 仮定，$(d+1,m,k)$-EDHE4p 仮定の下で，適応的安全である．ここで，d は方式内で設定する変数で，$\ell=\lceil|S|/d\rceil$ であり，S はチャレンジ暗号文に付属する暗号文属性のサイズで，m,k は秘密鍵に関連付けされるアクセス行列のサイズの最大値である．

なお，$\mathcal{D}_b$-Matrix-DH 仮定は，$b=1$ のとき SXDH 仮定より弱い仮定であり，$b=2$ のとき DLIN 仮定よりも弱い仮定である [9].

4 性能評価

漸近的な性能評価． 提案する ABE 方式の漸近的な性能評価を表 1に示す．適応的安全性を達成，無制限か暗号文が定数長かのどちらかの方式のみを比較対象にしている．そのような方式として，それぞれ無制限 ABE 方式 [1, 2] と定数長暗号文方式 [1, 2] が提案されている．これら以外の方式はどれも選択的安全か，制限されているかのどちらかである．

性能の見積り． 素数位数群を用いた KP-ABE 方式の性能を見積もる．性能を最大化するために，$b=1$ として方式を具体化する．従って，この方式は SXDH 仮定に基づき構成される．具体例として $m=40,k=20,t=60$ と固定し，d を $d=1,4,20$ といくつかの値で固定した場合の群要素数と演算回数による計算コストを表 2に示す．より具体的に性能を見積るために，Zavattoni らのソフトウェア実装報告 [15] で使用されている 254-bit Barreto–Naehrig (BN) 曲線で実装することを想定した場合のビット長と計算時間の見積りを表 3に示す．この曲線では，圧縮表現 [6, 11] を使用することで各群における 1 つの要素をそれぞれ $|\mathbb{G}_1|=255$，$|\mathbb{G}_2|=509$，そして $|\mathbb{G}_T|=2032$ ビットで表現できる．また，Zavattoni らのソフトウェア実装報告 [15] を参考に，各群 $\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T$ のスカラー倍演算とペアリング演算 1 回の計算にかかる時間をそれぞれ 57, 104, 164, 342 マイクロ秒とした．d の値を調整することで，サイズと計算速度について次のようなトレードオフを確認した: d を大きくすると公開鍵長と秘密鍵長が長くなるが，暗号文長は小さくなり，暗号化の計算速度は速くなる．また，復号の計算速度は用いた値の最大でも最小でもない $d=4$ で最も速くなっている．

表 1: KP-ABE の漸近的性能評価

Scheme	$\|\mathsf{PK}\|$	$\|\mathsf{SK}\|$	$\|\mathsf{CT}\|$	暗号化の計算時間	復号の計算時間 expo.	復号の計算時間 pair.	無制限か？
無制限 ABE [1, 2]	$O(1)$	$O(m)$	$O(t)$	$O(t)$	$O(m)$	$O(m)$	yes
定数長暗号文 ABE [1, 2]	$O(T)$	$O(mT)$	$O(1)$	$O(T)$	$O(mT)$	$O(1)$	no, $T = \max t$
提案方式	$O(d)$	$O(md)$	$O(t/d)$	$O(t)$	$O(md)$	$O(\min\{m, t/d\})$	yes

表 2: 提案する $b = 1$ とした場合の素数位数群 KP-ABE 方式における計算コストと，いくつかの d の値について $m = 40, k = 20, t = 60$ と固定した場合の計算コスト．

d の値	$\|\mathsf{PK}\|$ (# of $\|\mathbb{G}_1\|$)	$\|\mathsf{SK}\|$ (# of $\|\mathbb{G}_2\|$)	$\|\mathsf{CT}\|$ (# of $\|\mathbb{G}_1\|$)	暗号化に要する演算回数 expo($\mathbb{G}_1$)	暗号化に要する演算回数 expo($\mathbb{G}_T$)	復号に要する演算回数 expo($\mathbb{G}_2$)	復号に要する演算回数 pair.
General	$2d + 12$	$2md + 6m + 6$	$4t/d + 8$	$2t + 6t/d$	1	$2md + 2m$	$\min\{4m + 8, 4t/d + 8\}$
$d = 1$	14	326	248	480	1	160	168
$d = 4$	20	566	68	210	1	400	68
$d = 20$	52	1846	20	138	1	1680	20

表 3: 表 2に基づき，提案する KP-ABE 方式を BN 曲線で実装すると想定した場合の性能の見積り

d の値	$\|\mathsf{PK}\|$ (bits)	$\|\mathsf{SK}\|$ (bits)	$\|\mathsf{CT}\|$ (bits)	暗号化の計算時間 expo($\mathbb{G}_1$)	暗号化の計算時間 expo($\mathbb{G}_T$)	復号の計算時間 expo($\mathbb{G}_2$)	復号の計算時間 pair.
$d = 1$	3,570	165,934	63,240	27.3 ms	164 μs	16.6 ms	57.4 ms
$d = 4$	5,100	288,094	17,340	11 ms	164 μs	41.6 ms	23.2 ms
$d = 20$	13,260	929,434	5,100	7.8 ms	164 μs	174.7 ms	6.8 ms

5 拡張

トレードオフ可能な CP/DP-ABE. [5] の一般的変換法を用いることによって，提案 KP-ABE 方式と類似のトレードオフを実現可能な CP-ABE 方式を得ることが可能である．さらに，[5] の双ポリシーへの変換法を利用することにより，類似のトレードオフを実現可能な DP-ABE 方式 [3] を得ることが可能である．詳細についてはフルヴァージョンを参照されたい．

謝辞. 本研究の一部分はセコム科学技術振興財団からの研究助成による．同財団の支援に謝意を表する．

参考文献

[1] N. Attrapadung. Dual System Encryption via Doubly Selective Security: Framework, Fully-secure Functional Encryption for Regular Languages, and More. In *Eurocrypt 2014*, pp. 557–577, 2014.

[2] N. Attrapadung. Dual System Encryption Framework in Prime-Order Groups. *IACR Cryptology ePrint Archive*, 2015:390, 2015.

[3] N. Attrapadung, H. Imai. Dual-Policy Attribute Based Encryption. In *ACNS'09*, pp. 168–185, 2009.

[4] N. Attrapadung, B. Libert, E. Panafieu. Expressive Key-Policy Attribute-Based Encryption with Constant-Size Ciphertexts In *PKC 2011*, pp. 90–108, 2010.

[5] N. Attrapadung, S. Yamada. Duality in ABE: Converting Attribute Based Encryption for Dual Predicate and Dual Policy via Computational Encodings. In *CT-RSA 2015*, pp. 87–105, 2015.

[6] R.M. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, F. Vercauteren. Handbook of Elliptic and Hyperelliptic Curve Cryptography. Discrete Mathemtics and Its Applications. Chapman & Hall/CRC, 2005.

[7] J. Bethencourt, A. Sahai, B. Waters. Ciphertext-Policy Attribute-Based Encryption. IEEE Symposium on Security and Privacy (S&P), pp. 321–334, 2007.

[8] D. Boneh, M. Hamburg. Generalized Identity Based and Broadcast Encryption Schemes. In *Asiacrypt 2008*, *LNCS* 5350, pp. 455–470, 2008.

[9] A. Escala, G. Herold, E. Kiltz, C. Rafols, J. L. Villar. An Algebraic Framework for Diffie-Hellman Assumptions. In *Crypto'13*, pp. 129–147, 2013.

[10] V. Goyal, O. Pandey, A. Sahai, B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *ACM CCS'06*, pp. 89–98, 2006.

[11] K. Karabina. Squaring in cyclotomic subgroups. In *Math. Comp.*, 82(281), pp. 555–579, 2012.

[12] T. Okamoto, K. Takashima, Fully secure functional encryption with general relations from the decisional linear assumption.In *Crypto 2010*, *LNCS* 6223, pp. 191–208, 2010.

[13] A. Sahai, B. Waters. Fuzzy Identity-Based Encryption In *Eurocrypt 2005*, *LNCS* 3494, pp. 457–473, 2005.

[14] B. Waters. Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization. In *PKC 2011*. pp. 53-70, 2011.

[15] E. Zavattoni, L. Dominguez Perez, S. Mitsunari, A. Sanchez-Ramirez, T. Teruya, F. Rodriguez-Henriquez. Software Implementation of an Attribute-Based Encryption Scheme. In *IEEE Trans. Computers* 64(5), pp. 1429–1441, 2015.