# 暗号文分割型の ID ベース検索可能暗号の構成

冨田　幸嗣[†]　　土井　洋[‡]　　毛利　公美[††]　　白石　善明[‡‡]

† 名古屋工業大学
466-8555　愛知県名古屋市昭和区御器所町
tomida.koji@nitzlab.com

‡ 情報セキュリティ大学院大学
221-0835　神奈川県横浜市神奈川区鶴屋町 2-14-1
doi@iisec.ac.jp

†† 岐阜大学
501-1193　岐阜県岐阜市柳戸 1-1
mmohri@gifu-u.ac.jp

‡‡ 神戸大学
657-8501 兵庫県神戸市灘区六甲台町 1-1
zenmei@port.kobe-u.ac.jp

**あらまし** IDベース検索可能暗号（IBEKS）は暗号文の検索者をIDで指定できる検索可能暗号であり，匿名階層型IDベース暗号（匿名HIBE）から構成できることが知られている．アクセス制御が高機能でない分，計算コストが低いというIBEKSの特徴を活かせるよう，我々は計算コストの低い非匿名HIBEを基にIBEKSを構成することを考えた．非匿名HIBEの暗号文を分割し匿名HIBEとして扱えるように暗号文分割型HIBEを定義し，それを暗号文を分割したIBEKSへと変換する手法を提案する．本稿では非匿名HIBEであるBB1-HIBEを基に，暗号文分割型匿名HIBEと暗号文分割型IBEKSを構成し，その安全性と計算コストについて評価する．

# Construction of Ciphertext Divided Identity-Based Encryption with Keyword Search

Koji Tomida†　　Hiroshi Doi‡　　Masami Mohri[††]　　Yoshiaki Shiraishi[‡‡]

† Nagoya Institute of Technology
Gokiso-cho, Showa-ku, Nagoya, Aichi
466-8555, JAPAN
tomida.koji@nitzlab.com

‡ Institute of Information Security
2-14-1 Tsuruya-cho, Kanagawa, Yokohama
221-0835, JAPAN
doi@iisec.ac.jp

†† Gifu University
1-1 Yanagido, Gifu 501-1193, JAPAN
mmohri@gifu-u.ac.jp

‡‡ Kobe University
1-1 Rokkodai-cho, Nada-ku, Kobe, Hyogo
657-8501, JAPAN
zenmei@port.kobe-u.ac.jp

**Abstract** IBEKS is Identity-Based Encryption with Keyword Search which can be constructed from anonymous Hierarchical Identity-Based Encryption (A-HIBE). In IBEKS scheme, the searcher who can search ciphertext is determined by ID used for encryption. IBEKS does not have fine-grained access control, but it has the feature of low computational cost. On the other hand, anonymous HIBE (A-HIBE) is more complicated than non-anonymous HIBE (NA-HIBE). If we can construct IBEKS from NA-HIBE, we can reduce computational cost. In this paper, we define Ciphertext Divided HIBE (CD-HIBE) by dividing ciphertext of NA-HIBE for treating NA-HIBE as A-HIBE. Then, we propose a transformation to construct IBEKS from NA-HIBE. Finally we construct the concrete Ciphertext Divided IBEKS (CD-IBEKS) from BB1-HIBE (NA-HIBE) and discuss its security and computational cost.

# 1 導入

暗号文を復号することなく, 暗号文をキーワード検索できる暗号技術に検索可能暗号がある． 検索可能暗号を使えば, 第三者に機密性の高いデータを預けたとしても，検索時にデータの中身を知られる恐れがなく，情報漏えいのリスクを減らすことができる. 検索可能暗号の適用先としてパブリッククラウド上での機密性の高いデータの利活用が期待されている.

Boneh らによって最初の公開鍵系の検索可能暗号 PEKS（PEKS: Public Key Encryption with Keyword Search）[4]が提案された．Boneh らは ID ベース暗号（IBE）から PEKS を構成する手法(ibe-2-peks 変換)を提案しており， 自身らが提案した ID ベース暗号[5]を基にした PEKS の一構成を示している.

IBE では，メールアドレスなどの ID により受信者を指定して暗号文を作成する．IBE から PEKS を構成する際には，暗号化に使う“受信者の ID”を“検索キーワード”とみなして PEKS への変換を行っている．IBE では暗号文の受信者を ID で指定するが，PEKS でも検索者を ID で指定できれば, 検索者の ID による簡易なアクセス制御が実現できる.

Abdalla らによって PEKS と IBE のコンセプトを組み合わせた ID ベース検索可能暗号 IBEKS（IBEKS: Identity-Based Encryption with Keyword Search）[1]が提案された．IBEKS は，IBE 方式同様に暗号化に（公開パラメータと）受信者の ID を指定するということを除き PEKS と同様である. また文献[1]では階層型 IBE（HIBE: Hierarchical IBE）から， IBEKS を構成する手法(hibe-2-ibeks)が提案されている. 安全な IBEKS 方式を得るためには，変換元の HIBE 方式が level2-Anonymous という性質を持っている必要がある．匿名 HIBE（A-HIBE: Anonymous HIBE）方式は非匿名な HIBE（NA-HIBE: Non-Anonymous HIBE）方式に比べると一般に計算コストが高い．したがって IBEKS 方式は A-HIBE をベースとするためにコストが高くなっている.

検索可能暗号とアクセス制御を組み合わせようとしたときに，関数型暗号や述語型暗号，属性ベース暗号を使えば柔軟なアクセス制御ができるが, 高機能な検索を実現しようとすれば, それだけ方式の構成は複雑となり, 計算コストは高くなる．IBE はこれらの方式に比べると実現できる機能がシンプルな分, 比較的計算コストは低い. モバイルアプリなどで検索可能暗号を使い，単純なアクセス制御を実現したい状況があれば，低コストな IBE で検索可能暗号を実現する方が適していることがある．一方，企業などで機密情報をある条件をもつ特定のメンバーだけにアクセス可能にしたいというような場合には, 多少コストが高くても高機能な関数型暗号や属性ベース暗号を基にした検索可能暗号などの方式が向いていると言える．このように考えると，IBEKS は簡易的なアクセス制御で十分である，もしくは多少機能が簡素でも計算コストを低くしたい，というようなアプリケーションに向いていると考えられる．コストの低い IBE の特徴を活かして，簡易的なアクセス制御機能を実現するということを考えると IBEKS の計算コストはより低く実現することが望ましい.

そこで我々は， A-HIBE より計算コストの低い NA-HIBE を変換元にして，計算コストの増加を抑えた IBEKS を構成することを目指す．そのため，NA-HIBE を使っても，A-HIBE と同じ匿名性が得られるように，暗号文を 2 分割し, それぞれを 2 つのサーバに分けて保管する暗号文分割型の HIBE（CD-HIBE: Ciphertext Divided HIBE）を提案する．さらに HIBE から IBEKS を構成する方法（cd-hibe-2-cd-ibeks）を示し， 実際に NA-HIBE であることが知られている BB1-HIBE 方式[2]を使った CD-IBEKS 方式の構成を示す．また，構成された CD-IBEKS 方式が安全であることを証明する．なお, 暗号文分割型の先行研究[7]などでは, 鍵供託問題の解決が図られている．提案方式においても，鍵供託問題の解決を図ることができる.

最後に，他の IBEKS 方式と安全性・計算コストについて評価する.

# 2 準備

本稿では，いくつかの方式について述べるが，$pk$は システム共通のパラメータを，$msk$はシステムのマスター秘密鍵を，$MsgSp$は平文空間を意味する.

## 2.1 双線形性

$\mathbb{G}_1, \mathbb{G}_2$を同じ素数$p$を位数にもつ巡回群とする．写像 $e: \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$が次の性質を満たすとき，写像$e$は双線形写像であるという.

**双線形性：** 任意の整数$a, b \in \mathbb{Z}$と任意の$g, h \in \mathbb{G}_1$に対して$e(g^a, h^b) = e(g, h)^{ab}$ が成立する.

**非縮退性：** $\mathbb{G}_1$の生成元を$g$とするとき$\mathrm{e}(g, g)$が$\mathbb{G}_2$の生成元になる.

**計算可能性：** 任意の $g, h \in \mathbb{G}_1$ に対して$e(g, h)$ を計算する多項式時間アルゴリズムが存在する.

## 2.2 階層型 ID ベース暗号

ID ベース暗号では，単一の秘密鍵発行機関（PKG: Private Key Generator）が，ID に対する秘密鍵発行要求に応じて, 要求者の認証などを行った後に秘密鍵発行を行う.

これに対し，階層型 ID ベース暗号（以下，HIBE）は，ID に階層構造を取り入れることにより PKG の秘密鍵発行権限を委譲・分散できるようにした方式であり，文献[6]で提案された．

ID は文字列のベクトルで表現されており，階層が $l$ の場合，例えば $id = (id_1, \ldots, id_l)$ と表現される．$id|_i = (id_1, \ldots, id_i)$は$id$の$i$番目までの要素のベクトルである．$\mathrm{par}(id)$ は$id|_{|id|-1}$のことであり，$id$の親を表す．

このように ID は階層化されており，上位（親）の秘密鍵所有者は自身の秘密鍵を使い，下位（子）の秘密鍵の発行ができる．HIBE を用いることで 1 つの PKG に集中していた「ユーザの ID の認証」と「秘密鍵発行」を複数の PKG に分散処理させることができる．階層型 ID ベース暗号方式 $\mathcal{HIBE}$=（Setup, KeyDer, Enc, Dec）は 4 つのアルゴリズムで定義される[1]．なお，必要に応じてランダム関数 $H$を用いる．

**Setup**： $(pk, msk) \xleftarrow{\$} \mathrm{Setup}(1^k)$
**KeyDer**： $usk[id] \xleftarrow{\$} \mathrm{KeyDer}^H(usk[par(id)], id)$,
**Encrypt**： $C \xleftarrow{\$} \mathrm{Encrypt}^H(pk, id, M)$
**Decrypt**： $M \leftarrow \mathrm{Decrypt}^H(usk[id], C)$

ここで，$usk[id]$は$id$に対する秘密鍵である．

HIBE は守秘を実現する方式であるから，暗号文から平文に関する情報が漏れない性質（＝秘匿性）を達成しなければならない．この性質は通常の公開鍵暗号と同様に，識別不可能性（IND: Indistinguishability）のゲームを用いて証明される．

一方，文献[1]で述べられているように IBEKS を HIBE から構成する場合には，暗号文の匿名性（暗号文から，暗号化に用いた ID を知ることができないこと）が求められる．この性質も，匿名性(ANO: Anonymity)のゲームを用いて証明される．

HIBE の IND（-CPA）安全や ANO（-CPA）安全の詳細な定義は文献[1]を参照のこと．

## 2.3 ID ベース検索可能暗号（IBEKS）

公開鍵系の検索可能暗号 PEKS（Public Key Encryption with Keyword Search）[4]は ID ベース暗号の受信者の ID を検索キーワードとみなすことで構成できることが知られている．IBE では ID で暗号化した暗号文を ID に対応する秘密鍵で復号したときに平文 M が正しく復号される．このことを利用して，PEKS ではトラップドアによる復号結果があらかじめ指定された平文 M となったときに，暗号文とトラップドアのキーワードが一致したと確認している．PEKS では ID をキーワードとして扱うため，暗号文の検索者を指定することができない．ID ベース暗号と PEKS の両方のコンセプトを組み合わせた ID ベース検索可能暗号（IBEKS： Identity-Based Encryption with Keyword Search）[1]では，暗号文とトラップドアに含まれるキーワードだけでなく，ID の一致も計算により確認できるようになり，暗号文の検索者を ID で指定できるようになった．ID ベース検索可能暗号方式 $\mathcal{IBEKS}$ =(Setup, KeyDer, Trapdoor, Encrypt, Test) は 5 つのアルゴリズムで定義される[1].

**Setup**： $(pk, msk) \xleftarrow{\$} \mathrm{Setup}(1^k)$
**KeyDer**： $usk[id] \xleftarrow{\$} \mathrm{KeyDer}^H(msk, id)$
**Trapdoor**： $T_w \xleftarrow{\$} \mathrm{Trapdoor}^H(usk[id], w)$
**IBEKS**： $C \xleftarrow{\$} \mathrm{IBEKS}^H(pk, id, w)$
**Test**： $b \xleftarrow{\$} \mathrm{Test}^H(T_w, C)$

ここで，暗号文を $C = \mathrm{IBEKS}^H(pk, id, w')$，トラップドアを$T_w = \mathrm{Trapdoor}^H(usk[id'], w')$とすると，$w = w'$かつ$id = id'$ときに 1 を，そうでなければ 0 を出力する．

なお，IBEKS は匿名性を有する（2 階層の）階層型 ID ベース暗号から構成できることが文献[1]で示されている．そこで，本稿では匿名性を有する階層型 ID ベース暗号の構成を目標とする．

# 3 暗号文分割型の HIBE

IBEKS は 2 階層の A-HIBE から構成可能だが，我々は NA-HIBE をベースにして IBEKS を構成することを考える．我々のアプローチは NA-HIBE の暗号文を分割し，それらを各々異なるサーバに送り，その部分復号結果を得ることで，NA-HIBE を A-HIBE として使えるようにすることにある．以下，暗号文分割型 HIBE（CD-HIBE: Ciphertext Divided HIBE）と呼ぶ．すると，暗号文分割型 HIBE を使い暗号文を分割した IBEKS を構成できる．この IBEKS のことを，以下，暗号文分割型 IBEKS（CD-IBEKS）と呼ぶ．本章では，暗号文を 2 分割した HIBE とその IBEKS への適用方法について説明する．次の 4 章で NA-HIBE である BB1-HIBE をもとに暗号文分割型 HIBE を構成し，具体的な暗号文分割型 IBEKS の構成について述べる．

暗号文分割型 HIBE では暗号文生成者が分割した 2 つの暗号文はそれぞれ別のサーバに送られる．しかし，分割した 2 つの暗号文の両方を攻撃者に入手されると，元の暗号文に戻されて匿名性を失うことになる．そこで，暗号文を保管する 2 つのサーバ同士は結託しないことを前提条件とする．また，提供者が暗号文をサーバに送るときに，攻撃者がその両方を入手可能であると，やはり匿名性を失うことになる．そのため暗号文の生成者とサーバ間の通信は HIBE 方式とは別種の公開鍵暗号方式により暗号化を行うものとする．これは，例えば，提供者は暗号文をそれぞれのサーバの公開鍵で二重に暗号化し各サーバへ送ることで実現できる．各サーバは受け

取った暗号文を自身の秘密鍵で復号して分割暗号文を入手する．暗号文の受信者は，秘密鍵をサーバに送り，暗号文を部分的に復号してもらう．その後，部分復号結果を受け取り，まとめることによって，最終的な復号結果を得る．公開鍵暗号で秘密鍵を第三者に渡すことは，通常考えないが，今回は検索可能暗号に変換することを見据えてこのようなモデルとした．

## 3.1 アルゴリズム

暗号文分散型 HIBE 方式 $\mathcal{CD\text{-}HIBE}=$（Setup, KeyDer, Encrypt, Divide, ShareDecrypt, Combine）は次の 6 つのアルゴリズムからなる．

**Setup**： $(pk, msk) \xleftarrow{\$} \mathrm{Setup}(1^k)$

**KeyDer**： $usk[id] \xleftarrow{\$} \mathrm{KeyDer}^H(usk[par(id)], id)$

**Encrypt**： $C \xleftarrow{\$} \mathrm{Encrypt}^H(pk, id, M)$

**Divide**： $CT_1, CT_2 \xleftarrow{\$} \mathrm{Devide}(C)$

**ShareDecrypt**：

$PR_1 \xleftarrow{\$} \mathrm{ShareDecrypt}(usk[id], CT_1)$

$PR_2 \xleftarrow{\$} \mathrm{ShareDecrypt}(usk[id], CT_2)$

**Combine**： $R \xleftarrow{\$} \mathrm{Combine}(PR_1, PR_2)$

## 3.2 モデル

提案方式は，送信者，サーバ 1，サーバ 2，受信者および PKG の 4 エンティティからなる．

**送信者**： PKG から受け取った公開パラメータと受信者の ID から 2 階層の階層型 IBE の暗号文を生成する．生成した暗号文を 2 分割して，それぞれをサーバ 1，サーバ 2 の公開鍵で 2 重に暗号化して送る．

**サーバ 1・サーバ 2**： 送信者から暗号文を受け取り，自身の持つ秘密鍵で復号し，分割暗号文を得る．更に受信者から受け取った秘密鍵を用い，分割暗号文を部分的に復号する．部分復号結果を受信者に渡す．サーバ同士は結託しないものとする．

**PKG**： 受信者の ID を受け取り，それに対応する 1 階層目の秘密鍵を計算し，それを受信者に渡す．

**受信者**： PKG から受け取った秘密鍵を使い，サーバ 1 とサーバ 2 に部分復号をクエリする．この際，2 階層目の秘密鍵を作成し，各サーバに送る．更に，各サーバから部分復号結果を受け取り，それらの結果を統合し暗号文を最終的に復号する．

図 1 に CD-HIBE のシーケンス図を示す．

## 3.3 安全性

暗号文分割型 HIBE の秘匿性と匿名性については，図 2 に示すように片方のサーバ（サーバ 1）と PKG が結託する場合を考える．なお，サーバ 2 は攻撃には加わらない．一方，PKG が攻撃者と結託すると，すべての

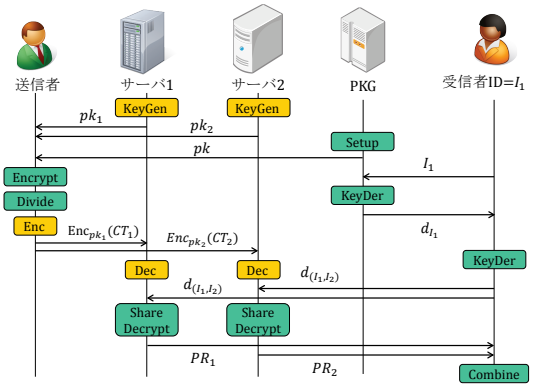


図 1　暗号文分割型 HIBE のシーケンス

秘密鍵を作ることができるので，ゲームにおける秘密鍵のクエリは不要となる．

本論文では文献[1]の秘匿性と匿名性の定義を基に，PKG の結託を考慮した秘匿性と匿名性を定義する．なお，IBEKS へ適用することを考慮し 2 階層に限定した定義とする．

### 3.3.1 秘匿性（IND）

暗号文分割型 HIBE の秘匿性を攻撃者 $\mathcal{A}$ と挑戦者 $C$ の間の実験（Experiment）として定式化する．

Experiment $\mathbf{Exp}^{\mathrm{CD-HIBE-IND-CPA-b}}_{\mathcal{CD\text{-}HIBE},\mathcal{A}}(k)$：

$(pk, msk) \xleftarrow{\$} \mathrm{Setup}(1^k)$

$pick\ random\ oracle\ H$

$((id_1, id_2), M_0, M_1, state) \xleftarrow{\$} \mathrm{A}^H(find, \{pk, msk\})$

If $|M_0| \neq |M_1|\ or\ M_0, M_1 \notin MsgSp$ then return 0

$CT \xleftarrow{\$} \mathrm{Encrypt}(pk, (id_1, id_2), M_b)$

$CT_1, CT_2 \xleftarrow{\$} \mathrm{Divide}(CT)$

$b' \xleftarrow{\$} \mathrm{A}^H(guess, CT_1, state)$

$return\ b'$

この実験の攻撃者 A の識別利得を次の様に定義する．

$\mathbf{Adv}^{\mathrm{CD-HIBE-IND-CPA}}_{\mathcal{CD\text{-}HIBE},\mathcal{A}}(k)$

$= \Pr\left[\mathbf{Exp}^{\mathrm{CD-HIBE-IND-CPA-1}}_{\mathcal{CD\text{-}HIBE},\mathcal{A}}(k) = 1\right]$

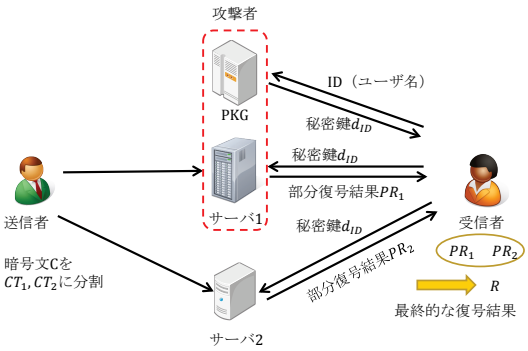


図 2　暗号文分割型 HIBE のモデル

$-\Pr\left[\mathbf{Exp}_{\mathcal{CD}\text{-}\mathcal{HIBE},\mathcal{A}}^{\mathrm{CD-HIBE-IND-CPA-0}}(k)=1\right]$

識別利得$\mathrm{Adv}_{\mathcal{CD}\text{-}\mathcal{HIBE},\mathcal{A}}^{\mathrm{CD-HIBE-IND-CPA}}$が無視可能であるときに, CD-HIBE 方式 $\mathcal{CD}\text{-}\mathcal{HIBE}$ は CD-HIBE-ANO-CPA 安全であるという.

### 3.3.2 匿名性（ANO）

暗号文分割型 HIBE の匿名性を攻撃者 $\mathcal{A}$ と挑戦者 $\mathcal{C}$ の間の実験として定式化する.

Experiment $\mathbf{Exp}_{\mathcal{CD}\text{-}\mathcal{HIBE},\mathcal{A}}^{\mathrm{CD-HIBE-ANO-CPA-b}}(k)$ :

$(pk, msk) \xleftarrow{\$} \mathrm{Setup}(1^k)$

$pick\ random\ oracle\ H$

$\left((id_{0,1}, id_{0,2}),\ (id_{1,1}, id_{1,2}),\ M,\ state\right) \xleftarrow{\$} \mathrm{A}^H(find, \{pk, msk\})$

If $M \notin MsgSp$ then return 0

$CT \xleftarrow{\$} \mathrm{Encrypt}\left(pk, (id_{b,1}, id_{b,2}), M\right)$

$CT_1, CT_2 \xleftarrow{\$} \mathrm{Divide}(CT)$

$b' \xleftarrow{\$} A^H(guess, CT_1, state)$

If $\left(id_{0,1}, id_{0,2}\right) \neq \left(id_{1,1}, id_{1,2}\right)$

$then\ return\ \ b'\ else\ return\ 0$

この実験の攻撃者 $\mathcal{A}$ の識別利得を次の様に定義する.

$\mathbf{Adv}_{\mathcal{CD}\text{-}\mathcal{HIBE},\mathcal{A}}^{\mathrm{CD-HIBE-ANO-CPA}}(k)$

$= \Pr\left[\mathbf{Exp}_{\mathcal{CD}\text{-}\mathcal{HIBE},\mathcal{A}}^{\mathrm{CD-HIBE-ANO-CPA-1}}(k)=1\right]$

$-\Pr\left[\mathbf{Exp}_{\mathcal{CD}\text{-}\mathcal{HIBE},\mathcal{A}}^{\mathrm{CD-HIBE-ANO-CPA-0}}(k)=1\right]$

識別利得$\mathbf{Adv}_{\mathcal{CD}\text{-}\mathcal{HIBE},\mathcal{A}}^{\mathrm{CD-HIBE-ANO-CPA}}$が無視可能であるときに, CD-HIBE 方式 $\mathcal{CD}\text{-}\mathcal{HIBE}$ は CD-HIBE-ANO-CPA 安全であるという.

## 3.4 暗号文分割型の HIBE から IBEKS への変換

この節では 2 階層のあらゆる CD-HIBE 方式を, CD-IBEKS 方式へと変形する一般的な変換方法 cd-hibe-2-cd-ibeks 変換について説明する. 2 階層の CD-HIBE 方式 $\mathcal{CD}\text{-}\mathcal{HIBE}$=（Setup, KeyDer, Encrypt, Divide, ShareDec, Combine）が与えられたとき, cd-hibe-2-cd-ibeks 変換により, CD-IBEKS 方式 $\mathcal{CD}\text{-}\mathcal{IBEKS}$=（Setup, KeyDer, CD-IBEKS, Trapdoor, Divide, ShareSearch, ShareTest）は次の様に与えられる. Setup, KeyDer, Divide はそのまま共通して使える. また, 平文$M$ はあらかじめ固定されているものとする.

CD- IBEKS$(pk,\ id,\ w) = C$

$where\ C \xleftarrow{\$} \mathrm{Encrypt}(pk,\ (id, w),\ M)$

Trapdoor$(usk[id],\ w) = T_w$

$where\ T_w \xleftarrow{\$} \mathrm{KeyDer}\left(usk[id],\ (id, w)\right)$

ShareSearch$(T_w,\ CT_b) = PR_b$

$where\ PR_b \xleftarrow{\$} \mathrm{ShareDec}(T_w,\ CT_b),$

$b \in \{0,1\}$

ShareTest$(PR_1, PR_2)\ returns\ 1$

$if\ \ \mathrm{Combine}(PR_1, PR_2) = M\ else\ returns\ 0$

# 4 具体的構成

IBEKS への適用を目的として, 2 階層の HIBE に対する暗号文分割型 HIBE の具体的構成例と安全性について述べる. その後, 暗号文分割型 IBEKS の構成例を示す.

## 4.1 BB1-HIBE 方式

BB1-HIBE 方式は秘匿性について DBDH 仮定の下で IND-sID-CPA 安全であることが証明されている. 一方で BB1-HIBE 方式は匿名性を有していない NA-HIBE の 1 つである. これは暗号文に含まれている ID と, 暗号文に使われていると推測した ID が一致しているかどうかを暗号文のみから確かめることができるためである. 匿名性を有さない理由は文献[3]で詳しく説明されている.

本節では IBEKS へ適用することを考慮し, 2 階層に限定して BB1-HIBE 方式の構成を説明する.

以下, 公開鍵である階層 ID をベクトル表現で $ID = \left(I_1,\ I_2\right) \in {\mathbb{Z}_p}^2$ と表す.

**Setup:**

まず, ランダムな生成元$g \in {\mathbb{G}_1}^*$, ランダムな$\alpha \in \mathbb{Z}_p$ を選び, $g_1 = g^\alpha$ とする. そしてランダムな要素 $h_1, h_2, g_2 \in \mathbb{G}_1$ を選ぶ. このとき, 公開パラメータ$pk$とマスター秘密鍵$msk$ は次のように与えられる. $pk = (g, g_1, g_2, h_1, h_2),\ \ msk = g_2^\alpha$.

$j = 1,2$に対し, 関数$F_j$: $\mathbb{Z}_p \to \mathbb{G}_1$ を$F_j(x) = g_1^x h_j$として定義する.

**KeyDer(1 階層目) :**

秘密鍵$msk$, 1 階層目の ID である$I_1 \in \mathbb{Z}_p$を入力とし, 乱数$r_1 \in \mathbb{Z}_p$を選び, 秘密鍵$d_{I_1} = (g_2^\alpha \cdot F_1(I_1)^{r_1},\ g^{r_1})$を出力する.

**KeyDer(2 階層目) :**

1 階層目の ID が$I_1$である秘密鍵$d_{I_1} = (d_0, d_1)$, 2 階層目の ID である$I_2 \in \mathbb{Z}_p$と入力とし, 乱数$r_2 \in \mathbb{Z}_p$を選び, 秘密鍵$d_{(I_1,I_2)} = (d_0 F_2(I_2)^{r_2}, d_1,\ g^{r_2})$を出力する.

**Encrypt :**

平文$M \in \mathbb{G}_2$と$ID = (I_1, I_2) \in \mathbb{Z}_p^2$, 乱数$s \in \mathbb{Z}_p$を使い暗号文 C を次のように求める. $C = (e(g_1, g_2)^s \cdot M, g^s, F_1(I_1)^s, F_2(I_2)^s)$

**Decrypt :**

暗号文$C = (A, B, C_1, C_2)$を秘密鍵$d_{ID} = (d_0, d_1, d_2)$で次のように復号する. $M' = A \cdot \frac{e(C_1,d_1)e(C_2,d_2)}{e(B,d_0)}$

## 4.2 BB1-HIBE ベースの暗号文分割型 HIBE

BB1-HIBE をもとに, 暗号文分割型 HIBE を構成する. なお, 2 階層に限定し, その階層ID は ID＝$(I_1, I_2) \in {\mathbb{Z}_p}^2$ とする.

**Setup, KeyDer(1 階層目), KeyDer(2 階層目), Encrypt**：

4.1 節の Setup, KeyDer(1 階層目), KeyDer(2 階層目), Encrypt と同一である.

**Divide**：

乱数$(t_{\mathrm{A}},\ t_B,\ t_1,\ t_2) \in \mathbb{Z}_p^4$ を選び, 暗号文 $C = (A, B, C_1, C_2)$を次のように$CT_1, CT_2$に分割する. $t'_j = 1 - t_j (j \in \{A, B, 1,2\})$ とおく.

$CT_1 = \left(A^{t_{\mathrm{A}}}, B^{t_B}, C_1^{t_1}, C_2^{t_2}\right)$, $CT_2 = \left(A^{t'_{\mathrm{A}}},\ B^{t'_B},\ C_1^{t'_1},\ C_2^{t'_2}\right)$.

**ShareDecrypt**：

分割暗号文$CT_i = \left(A_i, B_i, C_{i,1}, C_{i,2}\right)$に対し秘密鍵 $d_{(I_1,I_2)} = (d_0, d_1, d_2)$を使い部分復号結果$PR_i = A_i \cdot \frac{e(C_{i,1},d_1)e(C_{i,2},d_2)}{e(B_i,d_0)}$を求める. なお, この処理は BB1-HIBE の Decrypt と同一である.

**Combine**：

部分復号結果$PR_1, PR_2$に対し$PR_1 \cdot PR_2$を求める. $PR_1 \cdot PR_2$が復号結果となることは,

$$\mathrm{PR}_1 \cdot \mathrm{PR}_2 = A^{t_A} \cdot \frac{\prod_{i=1}^{2} e\left(C_i^{t_i}, d_i\right)}{e\left(B^{t_B}, d_0\right)} \cdot A^{t'_{\mathrm{A}}} \cdot \frac{\prod_{i=1}^{2} e\left(C_i^{t'_i}, d_i\right)}{e\left(B^{t'_B}, d_0\right)}$$

$$= A^{t_A + t'_A} \cdot \frac{\prod_{i=1}^{2} e\left(C_i^{(t_i + t'_i)}, d_i\right)}{e\left(B^{(t_B + t'_B)}, d_0\right)} = A \cdot \frac{\prod_{i=1}^{2} e(C_i, d_i)}{e(B, d_0)}$$

により確認できる. ここで最後の$A \cdot \frac{\prod_{i=1}^{2} e(C_i,d_i)}{e(B,d_0)}$は 4.1 節で述べた BB1-HIBE の Decrypt の出力そのものである.

## 4.3 安全性

BB1-HIBE ベースの暗号文分割型 HIBE の安全性について述べる.

### 4.3.1 識別不可能性

BB1-HIBE ベースの暗号文分割型 HIBE の $\mathbf{Exp}_{\mathcal{CD}\text{-}\mathcal{HIBE},\mathcal{A}}^{\mathrm{CD-HIBE-IND-CPA-b}}(k)$に関する実験を述べる. なお, 記述の簡略化のために, 攻撃者 $\mathcal{A}$はサーバ 1 とする.

$\mathbf{Exp}_{\mathcal{CD}\text{-}\mathcal{HIBE},\mathcal{A}}^{\mathrm{CD-HIBE-IND-CPA-0}}(k)$の場合, 攻撃者 $\mathcal{A}$ に, $pk = (g, g_1, g_2, h_1, h_2), msk = g_2^{\alpha}$が与えられ, $\mathcal{A}$ は $\left((I_1, I_2), M_0,\ M_1,\ state\right)$を出力する.

これに対し, 挑戦者 $\mathcal{C}$はあらかじめ定められた$b = 0$に対し, $CT = (A, B, C_1, C_2) = (e(g_1, g_2)^s \cdot M_0, g^s, F_1(I_1)^s, F_2(I_2)^s)$を作成し, さらに乱数 $(t_{\mathrm{A}},\ t_B,\ t_1,\ t_2) \in \mathbb{Z}_p^4$ を選び $CT_1 = \left(A^{t_{\mathrm{A}}}, B^{t_B}, C_1^{t_1}, C_2^{t_2}\right)$を $\mathcal{A}$ に渡す.

最後に, $\mathcal{A}$は$b'$を出力する.

一方, $\mathbf{Exp}_{\mathcal{CD}\text{-}\mathcal{HIBE},\mathcal{A}}^{\mathrm{CD-HIBE-IND-CPA-1}}(k)$の場合についても同様にゲームを構成できるが, 群$\mathbb{G}_1, \mathbb{G}_2$が素数$p$を位数に持つ巡回群であることから, 乱数$(t_{\mathrm{A}},\ t_B,\ t_1,\ t_2) \in \mathbb{Z}_p^4$の選び方によっては, $b = 0$の場合の出力$CT_1$が $\mathcal{A}$ に渡される可能性もある.

実際, $CT_1$が攻撃者 $\mathcal{A}$ に渡される確率は, $b = 0$の場合も, $b = 1$の場合も, 乱数$t_{\mathrm{A}},\ t_B,\ t_1,\ t_2$ の選択に依存し$1/p^4$である. このため, 攻撃者は$CT_1$を得ても, $b$が 0 であるか 1 であるかを識別できない. よって, BB1-HIBE ベースの暗号文分割型 HIBE の識別不可能性に関する識別利得は 0 となる.

### 4.3.2 匿名性

4.3.1 節と同様に, BB1-HIBE ベースの暗号文分割型 HIBE の$\mathbf{Exp}_{\mathcal{CD}\text{-}\mathcal{HIBE},\mathcal{A}}^{\mathrm{CD-HIBE-ANO-CPA-b}}(k)$に関するゲームを構成できる. $b = 0$および$b = 1$の場合のいずれにおいても, 4.3.1 節と同様に, 同一の$CT_1$が渡される可能性があり, その確率はやはり, $1/p^4$である. このため, 攻撃者は$CT_1$を得ても, $b$が 0 であるか 1 であるかを識別できない. よって, BB1-HIBE ベースの暗号文分割型 HIBE の匿名性に関する識別利得は 0 となる.

## 4.4 BB1-HIBE ベースの暗号文分割型 IBEKS

2 階層の A-HIBE から IBEKS への変換は, 文献[1]に示されている. IBEKS における ID として$I_1$, キーワードとして$w$を指定する暗号化は, 階層 ID を$(I_1, w)$とする A-HIBE の暗号化で実現される.

一方, KeyDer（1 階層目）を用いて, 検索者の ID である$I_1$に対応する 1 階層の秘密鍵$d_{I_1}$を生成する. 検索者は秘密鍵$d_{I_1}$と検索キーワード$w$を入力とし, トラップドア$T_w = d_{(I_1,w)}$を生成する. これは階層 ID を$(I_1, w)$とする KeyDer (2 階層目)として実現される. 図 3 にシーケンス図を示す.

暗号文分割型 BB1-HIBE をベースとした IBEKS の構成について述べる. ベースとする暗号文分割型の

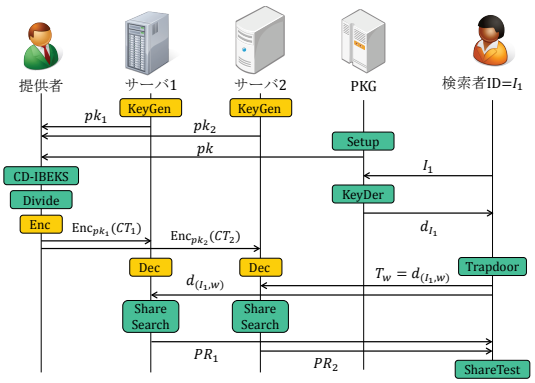


図 3　暗号文分割型 IBEKS のシーケンス

BB1-HIBE 方式は 2 階層のものを用いる．階層 ID は$ID = (I_1, w) \in \mathbb{Z}_p^2$であり，$I_1$は検索者の ID を，$w$は検索キーワードをそれぞれ表す．また平文$M = 1 \in \mathbb{G}_2$とする．この 1 は群$\mathbb{G}_2$の乗法単位元を表す．

**Setup：**

4.2 節の Setup と同一である．

**KeyDer：**

4.2 節の KeyDer（1 階層目）と同一であり，1 階層目の ID が$I_1$である鍵を出力する．

**CD-IBEKS：**

ID を$I_1$とし，キーワードを$w$とする場合は，階層 ID を$(I_1, w)$，平文$M$を$1 \in \mathbb{G}_2$として，4.2 節の Encrypt を行う．

**Divide：**

4.2 節の Divide と同一である．

**Trapdoor：**

ID を$I_1$とし，キーワードを$w$とする場合は，階層 ID を$(I_1, w)$として，4.2 節の KeyDer（2 階層目）を行う．

**ShareSearch：**

4.1 節の ShareDecrypt と同一である．

**ShareTest：**

4.1 節の Combine を実行し$R = PR_1 \cdot PR_2$を求める．$R$が$1 (= M)$のときに限り 1 を，そうでなければ 0 を出力する．

IBEKS の安全性についてインフォーマルではあるが，簡単に述べる．検索可能暗号で秘匿すべき情報は暗号化に使ったキーワードのことであり，IBEKS においては階層 ID がこれに当たる．本節で提案した IBEKS は暗号文分割型 HIBE のアルゴリズムを変更したものではなく，その入出力を少し工夫しただけのものである．そのため暗号文分割型 HIBE が匿名性を有していれば，その変換によって得られる IBEKS でも暗号文から階層 ID の情報が漏れないという同様の性質が得られる．フォーマルな安全性証明は今後の課題とする．

# 5　計算コスト評価

1 章で述べたように，IBEKS は簡易的なアクセス制御で十分である，もしくは多少機能が簡素でも計算コストを低くしたい，というようなアプリケーションに向いていると考えられる．その 1 例として，計算資源が少ないモバイル端末上で簡易なアクセス制御を実現する場合を想定し，4 章で提案した BB1-HIBE ベースの暗号文分割型 IBEKS 方式（以下，提案方式）の計算コストについて評価する．

表 1 に BB1-HIBE から構成した CD-IBEKS の計算コストを示す．exp は群$\mathbb{G}_1$上のべき乗演算，e はペアリング（e 関数）演算，$\mathrm{exp}_2$は群$\mathbb{G}_2$上のべき乗演算をそれぞれ表す．

モバイルアプリで計算コストの低さが求められる部分は，提供者，検索者が実行する部分のアルゴリズムである．IBEKS では提供者が IBEKS で暗号化を，検索者は Trapdoor で検索クエリを作成する．一方，CD-IBEKS では提供者が CD-IBEKS と Divide で暗号化と暗号文の分割を，検索者が Trapdoor と ShareTest で検索クエリの作成と部分検索結果から最終的な検索結果の計算を行う．ShareTest は単なる乗算の計算であり，他のアルゴリズムの計算と比べると無視できる．

本稿では，提供者の作成した暗号文をサーバに送るまでの総計算コスト（A）と，検索者の検索クエリの作成と検索結果を得るまでの総計算コスト（B）に着目し

表 1　IBEKS 方式の計算コスト

| | IBEKS (BW06-HIBE) | IBEKS (RS13-HIBE) | 提案方式 (BB1-CD-HIBE) | |
|---|---|---|---|---|
| 提供者の総計算量(A) | $25\mathrm{exp}+\mathrm{exp}_2$ | $5\mathrm{exp}+\mathrm{exp}_2$ | CD-IBEKS | 6exp+e |
| | | | Divide | $3\mathrm{exp}+\mathrm{exp}_2$ |
| 検索者の総計算量(B) | 61exp | 20exp | Trapdoor | 3exp |
| | | | ShareTest | negligible |

て計算コストの評価を行うものとする. IBEKS では（A）は IBEKS,（B）は Trapdoor に要する計算コストである．一方 CD-IBEKS では（A）は IBEKS と Divide の計算コストの和,（B）は Trapdoor に要する計算コストである．なお，CD-IBEKS では，(A)において更に二重暗号化のコストを必要とする．しかし，SSL の代用なども考えられるので，今回の評価では割愛した．

一方，IBEKS 方式は level-2 Anonymous という性質を持つ BW06-HIBE 方式[3]の提案により初めて安全に構成できるようになった．その後，安全な IBEKS を構成できる A-HIBE がいくつか提案されているが，提案方式と同様に素数位数のペアリングを使う方式の１つとして RS13-HIBE[8]がある．そこで，本論文では，提案方式と BW06-HIBE，RS13-HIBE を各々基にした IBEKS 方式の比較を行うこととした．BW06-HIBE 方式と RS13-HIBE の計算コストは文献[8]を参照している．結果を表１に示す.

まず，提案方式と BW06-HIBE を基に構成した IBEKS 方式の計算コストを比較する．表１によると，提案方式の計算コストは（A）でおよそ 1/2，（B）でおよそ 1/20 である．このように提案方式は BW06-HIBE ベースの IBEKS に比べ大幅に計算コストを削減できている．

次に，提案方式と RS13-HIBE を基に構成した IBEKS 方式の計算コストを比較する．表１によると，提案方式の計算コストは（A）で4exp + eだけ多くなるが，（B）ではおよそ 1/6 である．このことから，暗号文を検索するときには, A-HIBE を基に構成した IBEKS よりも提案方式のほうが，計算コストが少ないことが分かる．

提案方式は, 特に検索者の計算量を少なくできることが確認できた. 表 1 で評価していない提案方式の Setup, KeyDer は，ベースとなる方式(BB1-HIBE)における計算量と同一である．なお，提案方式は 2 サーバを必要とするため, 暗号文作成や二重暗号化のコストは少なくない. ただし，2 サーバを用いるため，文献[7]と同様に鍵供託問題を解決している．

# 6　まとめ

本稿では, 暗号文を分割し別サーバに保管する暗号文分割型 HIBE（CD-HIBE）を考案し，その安全性(IND, ANO)を定義した．暗号文分割を行うことにより，NA-HIBE を A-HIBE として扱えるようになるが，本稿では BB1-HIBE をベースとした構成例を示し, その安全性（IND，ANO）を証明した．次に，これを用いる暗号文分割型の IBEKS（CD-IBEKS）を構成した.

更に，匿名 HIBE である BW06-HIBE,RS13-HIBE を基にした IBEKS と非匿名 HIBE である BB1-HIBE から提案手法で構成した CD-IBEKS で, 提供者と検索者の実行する処理の計算コストの比較を行った．CD-IBEKS 方式は IBEKS(BW06-HIBE)と比べて提供者側でおよそ 1/2, 検索者側でおよそ 1/20 の計算コストとなった．また，IBEKS(RS13-HIBE)と比べて提供者側では計算コストが高くなるが，検索者側でおよそ 1/6 の計算コストになった. 提供者の暗号化にかかる計算コストを削減することは今後の課題である.

なお，CD- IBEKS については，変換元の CD-HIBE が ANO 安全性を満たせば，IND 安全性を達成できることをインフォーマルに述べた．CD-IBEKS の一般的な安全性の定義と安全性証明を与えることは, 今後の課題である.

# 謝辞

本研究の一部は JSPS 科研費 25330151, 25330161 の助成を受けたものである.

# 参考文献

[1] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, “Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions”, CRYPTO 2005，LNCS, vol. 3621, pp.205-222，(2005).

[2] D. Boneh, X. Boyen, “Efficient Selective Identity-Based Encryption Without Random Oracles” , EUROCRYPT 2004, LNCS, vol. 3027, pp. 223-238 (2004).

[3] X. Boyen, B. Waters, “Anonymous hierarchical identity-based encryption (without random oracles)”, CRYPTO 2006, LNCS, vol. 4117, pp. 290-307 (2006).

[4] D. Boneh, G. Di Crescenzo, R. Ostrovsky, G. Persiano, ”Public Key Encryption with Keyword Search”, EUROCRYPT 2004, LNCS, vol. 3027, pp. 506-522 (2004).

[5] D. Boneh and M. Franklin, “Identity-Based Encryption from the Weil Pairing", CRYPTO 2001, LNCS, vol. 2139, pp. 213-229 (2001).

[6] C. Gentry, A. Silverberg, “Hierarchical ID-Based Cryptography, “ASIACRYPT 2002, LNCS, vol. 2501, pp. 548-566 (2002).

[7] 佐藤誠, 毛利公美, 土井洋, 白石善明, “クラウド型ファイル送信サービスのための ID ベース暗号方式とその評価”, LOIS2013-77, 信学技報 vol. 113, no. 479, pp. 137-141 (2014).

[8] Somindu C. Ramanna and Palash Sarkar, “Efficient (Anonymous) Compact HIBE From Standard Assumptions”, Cryptology ePrint Archive: Report 2013/806, Available from: https://eprint.iacr.org/2013/806.pdf.