連接キーワード検索可能な ID ベース暗号文キーワード検索可能暗号方式

片山　貴充 †　　高木　剛 †

† 公立はこだて未来大学大学院システム情報科学研究科
041-8655 北海道函館市亀田中野町 116-2

あらまし 文書を暗号化した状態で，秘密鍵を持つユーザだけが暗号文の中に特定のキーワードが含まれているかどうか検索できる暗号方式として，暗号文キーワード検索可能方式が提案されている．キーワードの検索方法として連接キーワード検索が提案されている．連接キーワード検索により複数のキーワードを含んだ文書を一度に検索することが可能である．Anonymous 階層型 ID ベース暗号を利用することでキーワード検索可能な ID ベース暗号方式が提案されている．本稿では ID ベース暗号文キーワード検索可能方式においてこれまでに提案されていない連接キーワード検索が可能な方式を提案した．本稿ではランダムオラクルモデルにおいて decisional Diffie-Hellman inversion 仮定の下，選択キーワード攻撃に対して識別不可能性の安全性を持つ方式を提案する．

An ID-based Conjunctive Keyword Searchable Encryption

Takamitsu Katayama†　　Tsuyoshi Takagi†

†Graduate School of Systems Information Science, Future University Hakodate
116-2 Kamedanakano-cho Hakodate Hokkaido, 041-8655, Japan

Abstract A keyword searchable encryption scheme was proposed by Song et al., which allows a user to retrieve encrypted data that contains a specific keyword. The concept of a conjunctive keyword searchable encryption scheme was first introduced by Golle et al. The conjunctive keyword search method enables us to retrieve the encrypted data that contains several keywords at one time. Abdalla et al. proposed the notion of ID-based searchable encryption by using anonymous hierarchical ID-based encryption scheme. In this paper, we propose ID-based searchable encryption scheme which can support conjunctive keyword search method. The proposed scheme offers indistinguishability security against chosen keyword attacks under the decisional Diffie-Hellman inversion assumption in the random oracle model.

1　はじめに

2000 年に Song 等によって，暗号化された文書から特定のキーワードが含まれているか検索が可能な暗号文キーワード検索可能方式が初めて提案された [16]．暗号文キーワード検索可能方式により，信頼のおけないサーバにデータの管理をさせた場合でも情報の漏洩を防ぎながらデータの検索を行うことが可能である．また，選択キーワード攻撃に対して semantic secure である安全性の定義が Goh 等によって示されている [10]．Song 等の方式は共通鍵方式である．共通鍵方式はユーザが 1 つの共通鍵を保持して，共通鍵により暗号文を作成する方式である．2004 年に公開鍵方式による暗号文キーワード検索可能方式を初めて実現した方式が Boneh 等によって提案された [6]．公開鍵方式はそれぞれのユーザが公開鍵を公開し，秘密鍵を秘密に保持する．ある受信者の公開鍵を使って送信者がその受信者に対する暗号文を作成する方式である．公開鍵方式により，鍵の配送問題を解決した．この方式は対称ペアリングによって構成され，ランダムオラクルモデルにおいて bilinear Diffie-Hellman（BDH）仮定の下で安全性証明が可能である．前述の方式は一度に 1 つのキーワードのみ検索を行う単一キーワード検索を実現する方式である．2004 年に Golle 等によって，暗号化された文書から 1 回の検索で複数のキーワードを連接した状態で検索できる連接キーワード検索方式が初めて提案された [11]．一度に 1 つのキーワードのみ検索を行う単一キーワード検索方式に比べて詳細な検索を可能とするので，連接キーワード検索方式は実用的な検索方法である．この方式の 1 つが対称ペアリングによって構成され，decisional BDH (DBDH) 仮定の下で安全性証明が可能である．また，2004 年に Park 等によって，連接キーワード検索で初めて公開鍵方式により構成された 2 つの方式が提案されている [13]．この方式は対称ペアリングによって構成され，ランダムオラクルモデルにおいて DBDH 仮定と DBDH inversion (DBDHI) 仮定の下で安全性証明が可能である．その後，連接キーワードの検索に加えて部分集合検索と大小比較可能にした方式が 2007 年に Boneh 等 によって提案された [8]．鍵の方式は公開鍵方式である．連接キーワード検索の検索方法に加えて，検索する数量のキーワードと文書内のキーワードを大小比較できる検索方法と，文書のキーワードが検索したい複数のキーワードの集合の要素であるか検索できる検索方法を持ち，高機能な検索を実現した．この方式は合成数位数ペアリングによって構成され，composite 3-party Diffie-

Hellman 仮定の下で安全性証明が可能である．連接キーワード検索を行うには，各キーワードに対して文中における位置を示すインデックスを指定する必要がある．2008 年に Wang 等によってインデックスを必要せずに連接キーワード検索を実現する方式が提案された [17]．この方式は対称ペアリングによって構成され，DBDHI 仮定の下で安全性証明が可能である．

個人を特定することが可能な情報である ID に基づいて暗号化を実現する方式である ID ベース暗号の概念が Shamir によって提案されている [15]．ID ベース暗号は従来の公開鍵暗号に比べて利便性が高く，暗号利用の普及に貢献すると期待されている [18]．ペアリングを用いることで実用的な ID ベース暗号が Boneh 等によって提案された [7]．Abdalla 等は公開鍵方式の暗号文キーワード検索可能方式が Anonymous ID ベース暗号を用いることで構成できることを示し，Anonymous 階層型 ID ベース暗号によりキーワード検索可能な ID ベース暗号方式の概念が提案されている [1].

本稿では，ID ベース暗号文キーワード検索可能方式において，これまで提案されていない連接キーワード検索を実現する方式 (IBE-CKS) の提案を行う．単一キーワード検索を実現する Anonymous 階層型 ID ベース暗号の構造を直接的に連接キーワード検索可能な方式に適応する方法は知られていない．そこで，ID ベース暗号文キーワード検索可能方式の概念に従来の連接キーワード検索可能な暗号文キーワード検索可能方式を組み合わせることで提案方式を構成する．提案方式の秘密鍵生成アルゴリズムと暗号化アルゴリズムには境等が提案した ID ベース暗号 [14] を基にしており，検証アルゴリズムには従来の連接キーワード検索可能な暗号文キーワード検索可能方式の仕組みと ID ベース暗号の復号化の仕組みを組み合わせることで構成した．Abdalla 等は IND-CPA 安全性を持つ Anonymous 階層型 ID ベース暗号により IND − CPA 安全性を持つ ID ベース暗号文キーワード検索可能方式を提案している．提案方式は選択キーワード攻撃に対して識別不可能性 (IND-CKA) を有する安全性の証明を与えている．ID ベース暗号の安全性レベルには adaptive-ID 安全性と selective-ID 安全性があるが，提案方式は selective-ID 安全性を持つ．本稿では，提案方式が DBDHI 仮定の下，選択キーワード攻撃に対して識別不可能性 (IND-sID-CKA) の安全性を持つ方式である安全性証明をランダムオラクルモデルにおいて与えた．

2 数論的仮定

本章では，双線形写像と数論的仮定を述べる．

$\mathbb{G}, \mathbb{G}_T$ を同じ素数 p を位数に持つ巡回群とする．写像 $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ が次の性質を持つとき写像 e は双線形写像であるという．この双線形写像が対称ペアリングと呼ばれている．

- 双線形性

  $a, b \in \mathbb{Z}_p, g_1, g_2 \in \mathbb{G}$ に対して、$e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$ が成立する。

- 非退化性

  g を $\mathbb{G}$ の生成元とするときに、$e(g, g)$ が $\mathbb{G}_T$ の生成元である。

群生成アルゴリズム $\mathcal{G}(k)$ は，セキュリティパラメーター k を入力として k ビットサイズの素数 p をランダムに生成し，位数が p である巡回部分群 $\mathbb{G}, \mathbb{G}_T$ を決定し，双線形写像 $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ を出力するアルゴリズムとする．

$(p, \mathbb{G}, \mathbb{G}_T, e) \leftarrow \mathcal{G}(k)$ とする．$(g, g^x, g^{x^2}, ..., g^{x^q}) \in \mathbb{G}^{q+1}$ と $Z \in \mathbb{G}_T$ が与えられたとき，$Z = e(g, g)^{\frac{1}{x}}$ かどうか判別する問題を q-decisional bilinear Diffie-Hellman inversion(q-DBDHI) 問題という．

q-DBDHI 問題を解く確率 $Adv(k)$ が non-negligile な確率 $Adv(k) > \epsilon(k)$ で、多項式時間で動作するアルゴリズムは存在しないという仮定を q-DBDHI 仮定という [4].

3 IBE-CKS

3.1 モデルの定義

IBE-CKS を構成する上で以下のように定義する．

(1) キーワード

ユーザが検索する語句をキーワードとし，1 つのキーワードを $w \in \{0,1\}^*$ と表記する．複数のキーワードを羅列することで文書が構成される．

(2) 文書

ユーザが所持し暗号化を行う対象を文書とし，D と表記し，i 番目の文書を D_i と表記する．文書は複数のキーワードの羅列とその他の語句によって構成されるので，それぞれの文書は m 個のキーワードによって構成され，文書を特定できると決める．

文書中にキーワードが書き込まれる場所をキーワードフィールドとする．1 つの文書は m 個のキーワードによって構成されるためキーワードフィールドは m 個存在する．さらに文書においてキーワードフィールドを特定するために名前を付け，これをフィールド名と呼ぶ．i 番目の文書に対するキーワード列は $W_i = \{w_{i,1}, ..., w_{i,m}\}$ と表記して，$w_{i,j}$ を i 番目の文書の j 番目のキーワードであるとする．ただし，$(1 \leq j \leq m)$ である．

簡略化するために文書に対して以下の仮定をしても一般性を失わない [11].

- 1 つの文書には同じキーワードが存在しないこととする．フィールド名と格納されるキーワードを合わせることで 1 つの文書内に同一のキーワードが存在しない.

- すべての文書は m 個のキーワードによって構成される．キーワードフィールドにキーワードが含まれない場合は NULL 文字を書き込むことで全ての文書が m 個のキーワードで構成される.

(3) インデックス

文書はキーワードの羅列によって構成されるため，文書内におけるキーワードフィールドの位置によって

キーワードを順序付し，これをインデックスと呼ぶ．キーワードフィールドは m 個あるので，インデックスを $j_l \in \{1, ..., m\}$ ただし $(1 \leq l \leq m)$ とする．文書 D_i から l 個のキーワードを選び出すとき，書き込まれているキーワードフィールドを指定することで選択する．これをインデックスの集合 $J = (j_1, ..., j_l)$ ただし $(1 \leq l \leq m)$，を指定することに対応させる．

(4) ID

ユーザは個人を特定することが可能な情報である $id \in \{0,1\}^*$ を持つとする．

3.2 IBE-CKS のモデル

IBE-CKS は次の 5 つのアルゴリズムによって構成される．

(1) 設定アルゴリズム

入力としてセキュリティパラメータ $k \in \mathbb{N}$ を入力として，システムパラメータ $params$ を生成して，マスター秘密鍵である MSK と公開鍵である PK を出力する．$(MSK, PK, params) \leftarrow Setup(k)$ を実行し，$params, PK$ を公開して MSK を秘密に保持する．

Setup	
INPUT	$k \in \mathbb{N}$
OUTPUT	$MSK, PK, params$

(2) 鍵生成アルゴリズム

入力としてマスター秘密鍵 MSK と受信者の id を入力として，受信者の秘密鍵 SK_{id} を出力する．Private Key Generator（PKG）が $SK_{id} \leftarrow KeyGen(id, MSK)$ を実行し，SK_{id} を受信者に秘密裏に送信する．

KeyGen	
INPUT	$id \in \{0,1\}^*, MSK$
OUTPUT	SK_{id}

(3) 暗号化アルゴリズム

暗号化する文書 $D_i = \{w_{i,1}, ..., w_{i,m}\}$ を入力として，文書 D_i の暗号文 C_i を出力する．送信者が暗号化アルゴリズム，$C_i \leftarrow Encrypt(D_i, id, PK)$ を実行し，暗号文 C_i をサーバにアップロードする．

Encrypt	
INPUT	$D_i = \{w_{i,1}, ..., w_{i,m}\}, id, PK$
OUTPUT	C_i

(4) 落とし戸アルゴリズム

秘密鍵 SK_{id} と検索するキーワードのインデックスの集合 $J = (j_1, ..., j_l)$ ただし $(1 \leq l \leq m)$，と検索するキーワード列 $W' = (w'_{j_1}, ..., w'_{j_l})$ を入力として，キーワード列に対応した落とし戸 $T_{W'}$ を作成する．受信者が落とし戸アルゴリズム $T_{W'} \leftarrow Trapdoor(J, W', SK_{id})$ を実行し，サーバに問い合わせを行う．

Trapdoor	
INPUT	$J = (j_1, ..., j_l), W' = (w'_{j_1}, ..., w'_{j_l}), SK_{id}$
OUTPUT	$T_{W'}$

(5) 検証アルゴリズム

暗号文 C_i と落とし戸 $T_{W'}$ を入力とする．暗号文 C_i を作成するときに入力した文書 $D_i = \{w_{i,1}, ..., w_{i,m}\}$ のうちインデックスに対応するキーワード $(w_{i,j_1}, ..., w_{i,j_l})$ と落とし戸を作成するときに入力したキーワード $W' = (w'_{j_1}, ..., w'_{j_l})$ が，$(w_{i,j_1} = w'_{j_1} \wedge ... \wedge w_{i,j_l} = w'_{j_l})$ を満たすときに “$true$”を出力し，それ以外は “$false$”を出力する．サーバ が検証アルゴリズム $true\ or\ false \leftarrow Test(C_i, T_{W'})$ を実行して，結果を受信者に返答する．

Test	
INPUT	$C_i, T_{W'}$
OUTPUT	if $(w_{i,j_1} = w'_1 \wedge ... \wedge w_{i,j_l} = w'_l)$ then true, oherwize false

3.3 セキュリティの定義

IBE-CKS のセキュリティの定義を示す．攻撃者 $\mathcal{A}$ とチャレンジャーによる以下のゲームを定義することで，選択キーワード攻撃に対して識別不可能性の安全性を持つことを定義する．

- **Init:** アルゴリズム $\mathcal{A}$ は攻撃対象である $S^* = (id^*_1, ..., id^*_s)$ を出力する．
- **Setup:** チャレンジャーは PK, MSK を得るため $PK, MSK \leftarrow Setup(k)$ を実行する．攻撃者 $\mathcal{A}$ に PK を与える．
- **Query Phase 1:** 攻撃者 $\mathcal{A}$ はチャレンジャーに以下の問い合わせを行う．
  - Key generation query (id): $id \notin S^*$ に対する秘密鍵 SK_{id} を得るためチャレンジャーは $SK_{id} \leftarrow KeyGen(id, MSK)$ を実行して, 秘密鍵 SK_{id} を返答する．
  - Trapdoor query $(J, W', id \in S^*)$: $T_{W'}$ を得るためにチャレンジャーは $T_{W'} \leftarrow Trapdoor(J, W', SK_{id})$ を実行し，$T_{W'}$ を返答する．
- **Challenge:** 攻撃者 $\mathcal{A}$ は 2 つの文書 D_0, D_1 と $id^* \in S^*$ をチャレンジャーに送る．ただし Query Phase 1 で D_0, D_1 に対する Trapdoor query を行うことができない．チャレンジャーは $b \overset{R}{\leftarrow} \{0,1\}$ としてランダムに選択し $C_b \leftarrow Encrypt(D_b, id^*, PK)$ を実行する．チャレンジャーは攻撃者 $\mathcal{A}$ に C_b を与える．
- **Query Phase 2:** 攻撃者 $\mathcal{A}$ は Query Phase 1 と同様に問い合わせを行う．
  - Key generation qury (id): ただし $id \neq id^*$ とする．
  - Trapdoor query (J, W', id): ただし D_0 と D_1 を判別できないとする．
- **Guess:** 攻撃者 $\mathcal{A}$ は $b' \leftarrow \{0,1\}$ を出力する．$b' = b$ ならば攻撃者 $\mathcal{A}$ の攻撃成功とする．

攻撃者 $\mathcal{A}$ がゲームに勝つ場合の攻撃成功確率，$Adv_{\mathcal{A}}^{ind-sID}$ は以下である．

$$Adv_{\mathcal{A}}^{ind-sID} = |Pr[b' = 1|b = 1] - Pr[b' = 1|b = 0]|$$

任意の多項式時間アルゴリズム $\mathcal{A}$ に対して攻撃成功確率 $Adv_{\mathcal{A}}^{ind-sID} = \epsilon(k)$ が negligible になる場合，IND-sID-CKA 安全性を持つ．

4 提案方式

本章では提案する IBE-CKS の構成方法を示す．2 つのハッシュ関数 $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_p^*, H_2 : \{0,1\}^* \rightarrow \mathbb{G}$, を用意する．

(1) 設定アルゴリズム

Setup	
INPUT	$k \in \mathbb{N}$
OUTPUT	$MSK, PK, params$
1.	$(p, \mathbb{G}, \mathbb{G}_T, e) \leftarrow \mathcal{G}(k)$
2.	$params \leftarrow (p, \mathbb{G}, \mathbb{G}_T, e, H_1, H_2)$
3.	g_1, g_2 are generator of $\mathbb{G}$
4.	$s \overset{R}{\leftarrow} \mathbb{Z}_p^*$
5.	$g' \leftarrow g_1^s$
6.	$h \leftarrow e(g_1, g_2)$
7.	$MSK \leftarrow (s, g_2)$
8.	$PK \leftarrow (g_1, g', h)$
9.	*return* $MSK, PK, params$

(2) 鍵生成アルゴリズム

KeyGen	
INPUT	$id \in \{0,1\}^*, MSK, PK,$ $params$
OUTPUT	SK_{id}
1.	$d_1 \leftarrow g_1^{\left(\frac{1}{s+H_1(id)} \bmod p\right)}$
2.	$d_2 \leftarrow g_2^{\left(\frac{1}{s+H_1(id)} \bmod p\right)}$
3.	$SK_{id} \leftarrow (d_1, d_2)$
4.	*return* SK_{id}

(3) 暗号化アルゴリズム

Encrypt	
INPUT	$D_i = \{w_{i,1}, ..., w_{i,m}\}, id,$ $PK, params$
OUTPUT	C_i
1.	$r, r_1, ..., r_m \overset{R}{\leftarrow} \mathbb{Z}_p^*$
2.	$c_{0,1} \leftarrow \{H_2(w_{i,1}) \cdot g_1^{r_1}\}^r, ...,$ $c_{0,m} \leftarrow \{H_2(w_{i,m}) \cdot g_1^{r_m}\}^r$
3.	$c_{1,1} \leftarrow (g' \cdot g_1^{H_1(id)})^{rr_1}, ...,$ $c_{1,m} \leftarrow (g' \cdot g_1^{H_1(id)})^{rr_m}$
4.	$c_{2,1} \leftarrow h^{rr_1}, ..., c_{2,m} \leftarrow h^{rr_m}$
5.	$c_3 \leftarrow g_1^r$
6.	$C_i \leftarrow (c_{0,1}, ..., c_{0,m}, c_{1,1}, ..., c_{1,m}, c_{2,1},$ $..., c_{2,m}, c_3)$
7.	*return* C_i

(4) 落とし戸アルゴリズム

Trapdoor	
INPUT	$J = (j_1, ..., j_l), W' = (w'_{j_1}, ...,$ $w'_{j_l}), SK_{id}, PK, params$
OUTPUT	$T_{W'}$
1.	$t \overset{R}{\leftarrow} \mathbb{Z}_p^*$
2.	$t_0 \leftarrow g_1^t$
3.	$t_1 \leftarrow \{H_2(w'_{j_1}) \cdot ... \cdot H_2(w'_{j_l})\}^t$
4.	$t_2 \leftarrow (d_1)^t \cdot d_2$
5.	$T_{W'} \leftarrow (t_0, t_1, t_2, J = (j_1, ..., j_l))$
6.	*return* $T_{W'}$

(5) 検証アルゴリズム

Test	
INPUT	$C_i, T_{W'}, params$
OUTPUT	$(w_{i,j_1} = w'_{j_1} \wedge ... \wedge w_{i,j_l} = w'_{j_l})$ then true, otherwize false
1.	$X \leftarrow e(\prod_{i=1}^{l} c_{0,j_i}, t_0) \cdot \prod_{i=1}^{l} c_{2,j_i}$
2.	$Y \leftarrow e(c_3, t_1) \cdot e(\prod_{i=1}^{l} c_{1,j_i}, t_2)$
3.	*if* $X = Y$ *then return true, otherwise return false*

5 安全性証明

本章では，ランダムオラクルモデルを用いて提案方式の安全性の証明を行う．

定理 提案方式はランダムオラクルモデルにおいて選択キーワード攻撃に対して q-DBDHI 仮定の下で IND-sID-CKA 安全性を持つ．

[証明] 選択キーワード攻撃により確率 ϵ で提案方式の識別不可能性を破るアルゴリズム $\mathcal{A}$ が存在すると仮定する．アルゴリズム $\mathcal{A}$ は鍵生成クエリを q_k $(q_k < q)$ 回行うとする．

アルゴリズム $\mathcal{A}$ を用いて．q-DBDHI 問題を確率 ϵ' で解くアルゴリズム $\mathcal{R}$ を構成する．

アルゴリズム $\mathcal{R}$ は入力として $(g, g^x, ..., g^{x^q}, Z)$ が与えられ，$Z = e(g,g)^{\frac{1}{x}}$ であるか判別することがアルゴリズム $\mathcal{R}$ の目的である．

Init:

アルゴリズム $\mathcal{A}$ は攻撃対象である $S^* = (id_1^*, ..., id_s^*)$ を出力する．

Setup:

アルゴリズム $\mathcal{R}$ は次の条件を満たす q 次の多項式，$F(x)$ を選択する．アルゴリズム $\mathcal{R}$ は $\sigma_1, ..., \sigma_{q_k} \overset{R}{\leftarrow} \mathbb{Z}_p^*$ としてランダムに値を選択する．多項式 $f(x) = \sum_{i=0}^{q_k} a_i \cdot x^i$ は $f(x) = \prod_{i=1}^{q_k}(x + \sigma_i)$ を満たすとする．このとき，多項式 $F(x)$ は $F(x) = f(x) \cdot f'(x) = \sum_{i=0}^{q} a'_i \cdot x^i$ で表わせるとする．

アルゴリズム $\mathcal{R}$ は公開鍵 PK を以下のように計算する．

$$g_1 = g^{f(x)} = \prod_{i=0}^{q_k}(g^{x^i})^{a_i}$$

$$g_2 = g^{F(x)} = \prod_{i=0}^{q}(g^{x^i})^{a'_i}$$

$$h = e(g_1, g_2)$$

ここで，s の値を未知の値 x であると仮定して以下のように計算する．

$$g' = \prod_{i=0}^{q_k} (g^{x^{i+1}})^{a'_i} = g^{x \cdot f(x)} = (g^{f(x)})^x$$

アルゴリズム $\mathcal{R}$ は公開鍵を $PK = (g_1, g', h)$ として，アルゴリズム $\mathcal{A}$ に与える．

Hash 1 Queries:

Hash 1 query (id_i) に返答するため，アルゴリズム $\mathcal{R}$ は組 (id_i, u_i) から成る表 L_{H_1} を管理する．初期状態は空であるとする．アルゴリズム $\mathcal{R}$ は以下のように返答する．

- すでに表 L_{H_1} に組 (id_i, u_i) が存在するならば，アルゴリズム $\mathcal{R}$ は $H_1(id_i) = u_i$ を返答する．
- それでなければ，アルゴリズム $\mathcal{R}$ は次のように返答する．
  - もし $id_i \in S^* = \{id_1^*, ..., id_s^*\}$ ならば，アルゴリズム $\mathcal{R}$ は $u_i \overset{R}{\leftarrow} \mathbb{Z}_p^*$ としてランダムに値を選択する．
  - それでなければ，アルゴリズム $\mathcal{R}$ は $u_i \leftarrow \sigma_j (1 \le j \le q_k)$ として値を決定する．

  アルゴリズム $\mathcal{R}$ は表 L_{H_1} に組 (id_i, u_i) を追加し，アルゴリズム $\mathcal{R}$ は $H_1(id_i) = u_i$ を返答する．

Hash 2 Queries:

Hash 2 query (w_i) に返答するため，アルゴリズム $\mathcal{R}$ は組 (w_i, v_i) から成る表 L_{H_2} を管理する．初期状態は空であるとする．アルゴリズム $\mathcal{R}$ は以下のように返答する．

- すでに表 L_{H_2} に組 (w_i, v_i) が存在するならば，アルゴリズム $\mathcal{R}$ は $H_2(w_i) = g^{v_i}$ を返答する．
- それでなければ，アルゴリズム $\mathcal{R}$ は $v_i \overset{R}{\leftarrow} \mathbb{Z}_p^*$ として値を決定する．アルゴリズム $\mathcal{R}$ は表 L_{H_2} に組 (w_i, v_i) を追加し，アルゴリズム $\mathcal{R}$ は $H_2(w_i) = g^{v_i}$ を返答する．

Query phase 1:

(1) Key generation query

Key geneation query (id_i) に対して，アルゴリズム $\mathcal{R}$ は以下のように返答する．

アルゴリズム $\mathcal{R}$ は表 L_{H_1} から $H_1(id_i) = u_i$ を得て，組 (id_i, u_i) を取得する．アルゴリズム $\mathcal{R}$ は以下の計算を行う．

$$d_1 = g^{\frac{f(x)}{x+u_i}} = (g^{f(x)})^{\frac{1}{x+u_i}}$$

$$d_2 = g^{\frac{F(x)}{x+u_i}} = (g^{F(x)})^{\frac{1}{x+u_i}}$$

アルゴリズム $\mathcal{R}$ は $SK_{id_i} = (d_1, d_2)$ を返答する．

(2) Trapdoor query

Trapdoor query $(J = (j_1, ..., j_l), W' = (w'_{j_1}, ..., w'_{j_l}), id_i)$ に対して，アルゴリズム $\mathcal{R}$ は以下のように返答する．

アルゴリズム $\mathcal{R}$ は表 L_{H_1} から $H_1(id_i) = u_i$ を得て，組 (id_i, u_i) を取得する．アルゴリズム $\mathcal{R}$ は表 L_{H_2} から $H_2(w'_{j_i}) = g^{v_i} (1 \le i \le l)$ を得て，組 (w'_{j_i}, v_i) を取得する．アルゴリズム $\mathcal{R}$ は以下の計算を行う．

$$\begin{aligned} t_2 &= g^{f(x) \cdot \frac{f'(x) - f'(-u_i)}{x - (-u_i)}} \\ &= (g^{f(x)})^{\frac{-f'(-u_i)}{x+u_i}} \cdot (g^{F(x)})^{\frac{1}{x+u_i}} \\ t_0 &= g^{-f'(-u_i) \cdot f(x)} = (g^{f(x)})^{-f'(-u_i)} \\ t_1 &= g^{-f'(-u_i) \cdot (v_{j_1} + ... + v_{j_l})} \\ &= \{H_2(w'_{j_1}) \cdot ... \cdot H_2(w'_{j_l})\}^{-f'(-u_i)} \end{aligned}$$

アルゴリズム $\mathcal{R}$ は $T_{W'} = (t_0, t_1, t_2)$ を返答する．

Challenge Query:

Query Phase 1 が終了後に，アルゴリズム $\mathcal{A}$ は Challenge query$(D_0 = \{w_{0,1}, ..., w_{0,m}\}, D_1 = \{w_{1,1}, ..., w_{1,m}\}, id^*)$ を行う．Challenge query(D_0, D_1, id^*) に対して，アルゴリズム $\mathcal{R}$ は以下のように返答する．

アルゴリズム $\mathcal{R}$ は $b \overset{R}{\leftarrow} \{0, 1\}$ としてランダムに値を選択する．アルゴリズム $\mathcal{R}$ は表 L_{H_1} から $H_1(id^*) = u_i$ を得て，組 (id^*, u_i, c_i) を取得する．アルゴリズム $\mathcal{R}$ は表 L_{H_2} から $H_2(w_{b,i}) = g^{v_{b,i}} (1 \le i \le m)$ を得て，組 $(w_{b,i}, v_{b,i})$ を取得する．

アルゴリズム $\mathcal{R}$ は $r'_1, ..., r'_m \overset{R}{\leftarrow} \mathbb{Z}_p^*$ としてランダムに値を選択する．値 r を $r = f'(x) - f'(0)$ とする．また，値 $r_1, ..., r_m$ を未知の値 x を用いて $r_1 = \frac{r'_1}{x}, ..., r_m = \frac{r'_m}{x}$ であると仮定する．アルゴリズム $\mathcal{R}$ は以下の計算を行う．

$$\begin{aligned} c_{0,j} &= g^{v_{b,j} \cdot (f'(x) - f'(0))} \cdot g^{r'_j \cdot f(x) \cdot \frac{f'(x) - f'(0)}{x}} \\ &= \{H_2(w_{b,j}) \cdot (g^{f(x)})^{\frac{r'_j}{x}}\}^{f'(x) - f'(0)} \\ &\qquad (1 \le j \le m) \\ c_{1,j} &= g^{r'_j \cdot f(x) \cdot (f'(x) - f'(0))} \cdot g^{u_i \cdot r'_j \cdot f(x) \cdot \frac{f'(x) - f'(0)}{x}} \\ &= \{(g^{f(x)})^x \cdot (g^{f(x)})^{u_i}\}^{\{f'(x) - f'(0)\} \cdot \frac{r'_j}{x}} \\ &\qquad (1 \le j \le m) \end{aligned}$$

$$c_3 = g^{f(x) \cdot (f'(x) - f'(0))} = (g^{f(x)})^{f'(x) - f'(0)}$$

多項式 $\{f(x)\}^2 \cdot f'(x)$ は $\{f(x)\}^2 \cdot f'(x) = \sum_{i=0}^{q'} b_i \cdot x^i (q' < 2q)$ で表わされるとする．

$$\begin{aligned} c_{2,j} = &\{Z^{F(0)^2} \cdot e(g^{F(0)} \cdot g^{F(x)}, g^{\frac{F(x) - F(0)}{x}}) \\ &\cdot (Z^{b_0} \cdot e(\prod_{i=0}^{q} (g^{x^i})^{b_{i+1}}, g) \\ &\cdot \prod_{i=q+1}^{q'-1} e(g^{x^{i-q}}, g^{x^q})^{b_{i+1}})^{-f'(0)}\}^{r'_j} \\ &\qquad (1 \le j \le m) \end{aligned}$$

ここで，$Z = e(g,g)^{\frac{1}{x}}$ とすると，以下を満たす．

$$\begin{aligned} c_{2,j} =& \{e(g^{F(x)}, g^{F(x)})^{\frac{1}{x}} \cdot e(g^{f(x)}, g^{F(x)})^{\frac{-f'(0)}{x}}\}^{r'_j} \\ =& e(g^{f(x)}, g^{F(x)})^{\{f'(x)-f'(0)\}\cdot\frac{r'_j}{x}} \\ & (1 \leq j \leq m) \end{aligned}$$

アルゴリズム $\mathcal{R}$ は，$C_b = (c_{0,1}, ..., c_{0,m}, c_{1,1}, ..., c_{1,m}, c_{2,1}, ..., c_{2,m}, c_3)$ を返答する．

Query Phase 2:
アルゴリズム $\mathcal{A}$ の Query Phase 1 と同様な質問に対して，アルゴリズム $\mathcal{R}$ は Query Phase 1 と同様に返答する．

Guess:
最後に，アルゴリズム $\mathcal{A}$ は $b' \in \{0,1\}$ を出力し，$b' = b$ ならばアルゴリズム $\mathcal{A}$ の攻撃は成功である．もし $b' = b$ ならばアルゴリズム $\mathcal{R}$ は “1”を出力する．つまり $Z = e(g,g)^{\frac{1}{x}}$ である．それでなければ，“0”を出力する．Z はランダムな値である．ここで，

$$\begin{aligned} Adv_{\mathcal{R}}^{DBDHI} =& Pr[b' = b|real] - Pr[b' = b|rand] \\ =& \frac{1}{2} \times (Pr[b' = 1|b = 1 \wedge real] \\ & - Pr[b' = 1|b = 0 \wedge real]) \\ & - \frac{1}{2} \times (Pr[b' = 1|b = 1 \wedge rand] \\ & - Pr[b' = 1|b = 0 \wedge rand]) \end{aligned}$$

ランダムな値であった場合，以下の確率を得る．

$$Pr[b' = 1|b = 1 \wedge rand] = Pr[b' = 1|b = 0 \wedge rand]$$

それでないならば，アルゴリズム $\mathcal{R}$ の出力はゲームに従うので以下の確率を得る．

$$\begin{aligned} Adv_{\mathcal{A}}^{ind-sID} =& Pr[b' = 1|b = 1 \wedge real] \\ & - Pr[b' = 1|b = 0 \wedge real] \end{aligned}$$

以上より確率は $Adv_{\mathcal{R}}^{DBDHI} = \frac{1}{2} \times Adv_{\mathcal{A}}^{ind-sID}$ である．よって，アルゴリズム $\mathcal{R}$ が q-DBDHI 問題を破る確率は $\epsilon' = \frac{1}{2} \times \epsilon$ である．

6 おわりに

本稿では ID ベース暗号文キーワード検索可能方式において連接キーワード検索を実現する方式 (IBE-CKS) の提案を行った．公開鍵方式の暗号文キーワード検索可能暗号方式は公開鍵の正当性の検証を行う必要性があるが，提案方式では ID ベース暗号の利点である公開鍵の正当性を確認する必要がない．さらに ID ベース暗号文キーワード検索可能方式において連接キーワード検索を実現しており，検索する複数のキーワードを含んだ文書を一度に検索することが可能である．

提案方式はランダムオラクルモデルにおいて q-DBDHI 仮定の下，選択キーワード攻撃に対して識別不可能性 (IND-sID-CKA) の安全性を持つ安全性証明可能な方式である．

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: Consistencyproperties, Relation to Anonymous IBE, and Extensions,” CRYPTO 2005, volume 3621 of LNCS, pp. 205-222, 2005.

[2] L. Ballard S. Kamara F. Monrose,“Achieving Efficient Conjunctive Keyword Searches over Encrypted Data,” ICICS 2005, volume 3783 of LNCS, pp.414-426, 2004.

[3] M. Bellare and P. Rogaway, “Random Oracle are Practical: a Paradigm for Designing Efficient Protocols,” Proceedings of the First ACM Conference on Computer and Communications Security, pp.62-73, 1993.

[4] D. Boneh, X. Boyen, “Efficient Selective-ID Secure Identity Based Encryption without Random Oracle, ” EUROCRYPT 2004, volume 3027 of LNCS, pp.56-73, 2004.

[5] D. Boneh, X. Boyen, “Hierarchical Identity Based Encryption with Constant Size Ciphertext, ” EUROCRYPT 2005, volume 3493 of LNCS, pp.440-456, 2005.

[6] D. Boneh, G. Di Crescenzo, R. Ostrovsky, G. Persiano, “Public Key Encryption with Keyword Search,” EUROCRYPT 2004, volume 3027 of LNCS, pp.506-522, 2004.

[7] D. Boneh, M. Franklin, “Identity-based Encryption from the Weil Pairings,” CRYPT 2001, volume 2139 of LNCS, pp.213-219, 2001.

[8] D. Boneh, B. Waters, “Conjunctive, Subset, and Range Queries on Encrypted Data”, TCC 2007, volume 4392 of LNCS, pp.535-554, Springer, 2007.

[9] C. Delerablee,“Identity-Based Broadcast Encryption with Constant Size Ciphertexts and Private Keys,” ASIACRYPT 2007, volume 4833 of LNCS, pp.200-215, 2007.

[10] E. J. Goh “Secure Indexes,” Cryptgraphy ePrint Archive, Report 2003/216, http://eprint.iacr.org/2003/216, 2003.

[11] P. Golle, J.Staddon, B. Waters,“Secure Conjunctive Keyword Search over Encrypted Data,” ACNS 2004, volume 3089 of LNCS, pp.31-45, 2004.

[12] Y. H. Hwang and P. J. Lee, “Public Key Encryption with Conjunctive Keyword Search and Its Extension to a Multi-user System,” Pairing 2007, volume 4575 of LNCS, pp.2-22, 2007.

[13] D. J. Park, K. Kim, P. J. Lee, “Public Key Encryption with Conjunctive Field Keyword Search,” WISA 2004 volume 3325 of LNCS, pp.73-86, 2004.

[14] R. Sakai, K. Ohgishi, and M. Kasahara, “Cryptosystems Based on Pairing over Elliptic curve,” 暗号と情報セキュリティシンポジウム 2001 予稿集, 2001.

[15] A. Shamir, “Identity-based Cryptosystem and Signature Schemes,” CRYPT 1984, volume 196 of LNCS, pp.47-53, 1984.

[16] D. Song, D. Wagner, A. Perrig, “Practical Techniques for Searching on Encrypted Data,” IEEE Symposium on Research in Security and Privacy 2000, pp.44-55, 2000.

[17] P. Wang, H. Wang, J. Pieprzyk, “Keyword Field-Free Conjunctive Keyword Searches on Encrypted Data and Extension for Dynamic Groups,” CANS 2008, volume 5339 of LNCS, pp.178-195, 2008.

[18] CRYPTREC ID ベース暗号調査 WG, “ID ベース暗号に関する調査報告書,” CRYPTREC 報告書, pp.1-11,http://www.cryptrec.go.jp/report.html, 2009.