アクセス制御機能付き検索可能暗号の ID ベース暗号からの構成

冨田幸嗣[†1]　宮嵜仁志[†1]　毛利公美[†2]　白石善明[†1]

運用コストが低く，利便性が優れている点からクラウドストレージが活用されている．機密性の高いデータを第三者に預ける場合，意図しない人にデータを見られないようにデータを暗号化する手段が用いられる．そこで暗号文を復号することなく検索ができる技術として検索可能暗号が注目されている．用途に応じた検索可能暗号方式が提案されており，暗号文の検索者を限定することのできるアクセス制御機能付き検索可能暗号方式も提案されている．これまでに提案されている公開鍵暗号ベースの検索可能暗号は ID ベース暗号を基に構成されている．また，ID ベース暗号から公開鍵暗号ベースの検索可能暗号(PEKS)を一般的に構成する方法が提案されている．もとにする ID ベース暗号を変更できるようになれば，利用する場面でのセキュリティ基準に応じた検索可能暗号を柔軟に構成することができる．本稿では，アクセス制御機能付き検索可能暗号(SEAC)を定義し，任意の ID ベース暗号から SEAC への変換(ibe-2-seac 変換)する手法を提案する．提案手法により構成されるアクセス制御機能付き検索可能暗号の安全性は ID ベース暗号の安全性に帰着する．

Searchable Encryption with Access Control from Identity-Based Encryption

KOJI TOMIDA[†1]　HITOSHI MIYAZAKI[†1]　MASAMI MOHRI[†2]
YOSHIAKI SHIRAISHI[†1]

1. はじめに

コストが低いことや利便性に優れていることからクラウドストレージが活用されている．クラウドストレージを利用することで，ネットワークに接続すれば任意の場所から容易にファイルの共有ができる．クラウドストレージサービス提供者のような第三者に機密性の高いデータを秘匿することなく預けると，意図した閲覧者以外にデータが見られてしまう懸念がある．

単純に暗号化処理をするだけでは，暗号化されたデータの検索ができなくなりストレージとしての利便性が低下する．一般に暗号化されたデータを検索する場合には，暗号文を一度復号した後で検索処理をするが，この方法ではデータの保管者が平文を知ることができることになる．

暗号化されたデータを安全に検索するために，検索対象を復号せずに検索ができる検索可能暗号が提案されている．Song らは共通鍵暗号ベースの検索可能暗号方式を提案している[1]．この方式は，サーバにキーワードを漏らすことなく暗号化されたキーワードを検索できる．Boneh らは最初の公開鍵暗号方式の検索可能暗号を提案している[2]．その後，複数キーワードを同時に検索する方式[3]や大小比較ができる方式[4]など様々な検索可能暗号の方式が提案されている．暗号文の検索者を限定することのできる，アクセス制御機能を備えた方式[5][6]も提案されている．

暗号方式は種類によって暗号強度，処理速度などに差がある．暗号方式を選択するときの選択基準は利用する場面の安全性の要求によって異なる．これまでに提案されている公開鍵ベースの検索可能暗号は ID ベース暗号を元に構成されている．任意の ID ベース暗号から検索可能暗号への変換ができれば，検索可能暗号を利用する場面のセキュリティ基準に適した暗号方式を柔軟に選択できることになる．

これまでに文献[2]で任意の IBE から公開鍵ベースの検索可能暗号（Public Key Encryption with Keyword Search: PEKS）への一般的な変換方法が示されている．しかしながら，この方式ではアクセス制御機能を備えていない．

本稿では，任意の ID ベース暗号(Identity-Based Encryption: IBE)方式を基にアクセス制御機能付き検索可能暗号(Searchable Encryption with Access Control: SEAC)を構成する手法(ibe-2-seac 変換)を提案する．提案手法によって構成されるアクセス制御機能付き検索可能暗号方式の安全性は，もとにした ID ベース暗号の安全性に帰着される．

以下，第 2 章では ID ベース暗号，第 3 章で Boneh らによる検索可能暗号(PEKS)と PEKS の ID ベース暗号からの構成法 (ibe-2-peks 変換)について述べる．第 4 章でアクセス制御機能付き検索可能暗号(SEAC)を定義し，第 5 章で任意の ID ベース暗号から SEAC を構成する手法(ibe-2-seac 変換)を提案する．提案手法によって構成される SEAC の安全性証明をした後に，第 6 章で本稿をまとめる．

2. ID ベース暗号(IBE)

ID ベース暗号 (Identity-Based Encryption: IBE) は Shamir[7]によって提案された任意の個人を識別する情報 (Identity: ID)を公開鍵とする公開鍵暗号である．例えば，ID には，住所，氏名，メールアドレスなどを利用できる．

ID ベース暗号のモデルを図 1 に示す．

†1 名古屋工業大学
Nagoya Institute of Technology
†2 岐阜大学
Gifu University

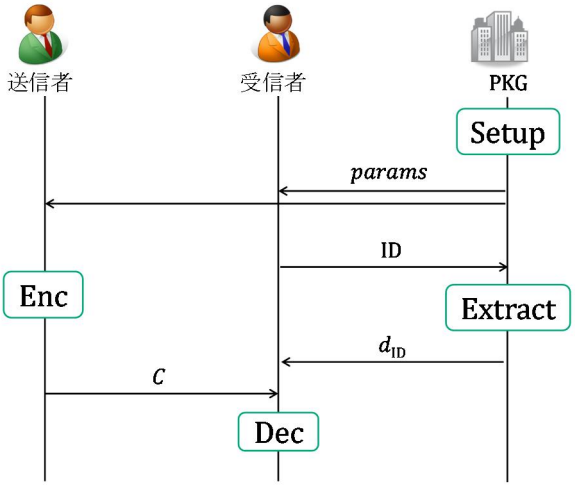

図1　IBEのモデル

2.1 エンティティ

ID ベース暗号は，送信者，受信者，PKG の 3 者のエンティティで構成される．

[送信者]　受信者の ID を公開鍵として暗号文を作成する．暗号文を受信者に送信する．

[受信者]　自身の ID に対応する秘密鍵を PKG に発行してもらう．送信者から受け取った暗号文を自身の秘密鍵で復号する．

[PKG]　受け取った ID に対応する秘密鍵を生成し，受信者に渡す．PKG は信頼のおける第三者であるとする．

2.2 アルゴリズム

Setup(k):　セキュリティパラメータkを入力として，システムの公開パラメータ$params$とマスター秘密鍵mskを出力する．

Extract($params, msk, \mathrm{ID}$):　公開パラメータ$params$, マスター秘密鍵mskと識別子IDを入力として，その ID に対応した秘密鍵d_{ID}を出力する．

Enc($params, \mathrm{ID}, M$):　公開パラメータ$params$と受信者の識別子ID，平文Mを入力として，暗号文Cを出力する．

Dec($params, d_{ID}, C$):　公開パラメータ$params$と暗号文C，秘密鍵d_{ID}を入力し，平文Mを出力する．

2.3 安全性定義

IBE の IND-ID-CPA 安全性は以下のゲームによって定義される．ゲーム図を図 2 に示す．

IND-ID-CPA ゲーム

Step.1　挑戦者 C はSetup(k)アルゴリズムを実行し，公開パラメータ$params$とマスター秘密鍵mskを生成し，公開パラメータ$params$を攻撃者 A に渡す．

Step.2　攻撃者 A は挑戦者 C に対して，適応的に以下の Extractクエリが許される．

[Extractクエリ]

任意の識別子ID ∈ {0,1}*に対する秘密鍵を問い合わせる．挑戦者 C はExtractアルゴリズムを実行して ID に対応した秘密鍵d_{ID}を生成し攻撃者に渡す．

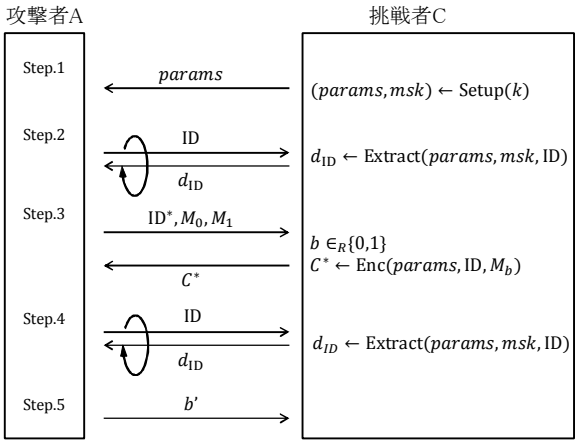

図2　IND-ID-CPAゲーム

Step.3　攻撃者 A は 2 つの異なる平文M_0, M_1とID*を選び挑戦者 C に渡す．唯一の制限はID*に対応する秘密鍵をステップ 2 で入手していないことである．挑戦者 C は$b \in \{0,1\}$をランダムに選び，チャレンジ暗号文$C^* \coloneqq \mathrm{Enc}(params, \mathrm{ID}^*, M_b)$を攻撃者 A に渡す．

Step.4　攻撃者 A は Step.2 と同様に挑戦者 C に問い合わせることができる．ただし，Step.3 で選択したID*に対応する秘密鍵を問い合わせることができない．

Step.5　攻撃者 A はチャレンジ暗号文$C^* \coloneqq \mathrm{Enc}(params, \mathrm{ID}^*, M_b)$が平文$M_0$，$M_1$のどちらを暗号化したものか推測し，$b$の推測値$b' \in \{0,1\}$を出力する．$b = b'$であるときに攻撃者 A の勝利であるとする．

ここで攻撃者 A の識別利得を以下のように定義する．

$$\mathrm{Adv}_{\mathrm{A}}(k) \coloneqq |\Pr[b = b'] - \frac{1}{2}|$$

上記のゲームにおいて，攻撃者 A の識別利得$\mathrm{Adv}_{\mathrm{A}}(k)$が無視できるほど小さいとき，その ID ベース暗号方式は IND-ID-CPA 安全であるという．

3. 検索可能公開鍵暗号(PEKS)

文献[2]で Boneh らは，ID ベース暗号方式[8]から最初の公開鍵暗号ベースの検索可能暗号(Public Key Encryption with Keyword Search: PEKS)を構成した．Boneh らは文献[2]で検索可能公開鍵暗号を次のように定義している．

3.1 エンティティ

検索可能公開鍵暗号は，提供者，検索者，サーバの 3 者のエンティティで構成される．PEKS のモデルを図 3 に示す．

[提供者]　受信者の公開鍵でキーワードを暗号化する．暗号文をサーバに送り保管してもらう．

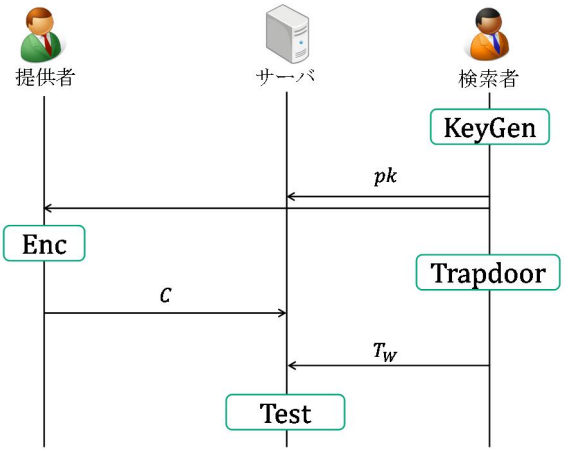

図3　PEKSのモデル

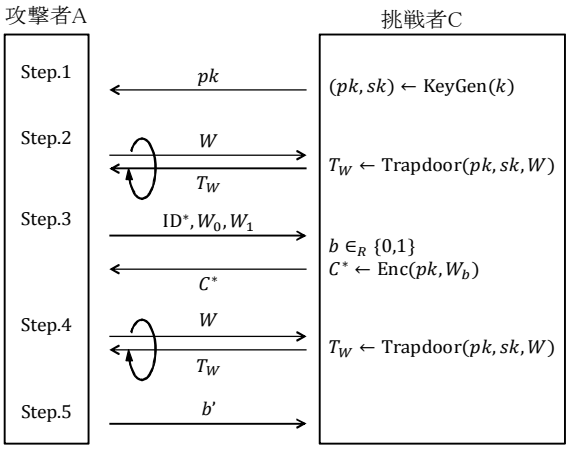

図4　IND-CKAゲーム

[検索者]　自身の秘密鍵と検索するキーワードからトラップドアを作成する．トラップドアを検索クエリとしてサーバに送信する．

[サーバ]　提供者からキーワードの暗号文を受信して保管する．検索者からトラップドアによるキーワードの検索クエリがあれば，検索をして返答する．

3.2 アルゴリズム

PEKS は以下の 4 つのアルゴリズムからなる．

KeyGen(k):　セキュリティパラメータkを入力として，公開鍵pkと秘密鍵skの組を出力する．

Enc(pk, W):　公開鍵pkとキーワードWを入力として，検索可能なキーワードWの暗号文Cを出力する．

Trapdoor(pk, sk, W):　秘密鍵skとキーワードWを入力として，トラップドアTwを出力する．

Test(pk, C, Tw):　公開鍵pk，検索可能な暗号文$C \coloneqq \mathrm{Enc}(pk, W')$，トラップドア$T_w \coloneqq \mathrm{Trapdoor}(sk, W)$を入力として，$W = W'$のときに 1 をそれ以外のときに 0 を出力する．

3.3 安全性定義

PEKS の安全性要件は文献[2]でトラップドアが入手できない限り，暗号文から検索キーワードの情報が 1 ビットも漏れないことと定義されている．この安全性は IND-CKA（Chosen Keyword Attack）安全と呼ばれ，以下のゲームで定義される．PEKS に対する IND-CKA ゲームを図 4 に示す．

IND-CKA ゲーム

Step.1　挑戦者 C はKeyGen(k)アルゴリズムを実行し，公開鍵pkと秘密鍵skの組を生成し，公開鍵pkを攻撃者に渡す．

Step.2　攻撃者 A は挑戦者 C に対して任意のキーワード$W \in \{0,1\}^*$に対応するトラップドアを問い合わせ，適応的に入手することができる．

Step.3　攻撃者 A は 2 つの異なるキーワードW_0, W_1を選び挑戦者 C に渡す．W_0, W_1はステップ 2 で入手したトラップドアに対応するものは選べない．挑戦者 C は$b \in \{0,1\}$をランダムに選び，チャレンジ暗号文$C^* \coloneqq \mathrm{PEKS}(pk, W_b)$を攻撃者 A に渡す．

Step.4　攻撃者 A は Step.2 と同様に任意のキーワードに対するトラップドアを挑戦者 C に問い合わせることができる．ただし，Step.3 で選択したチャレンジキーワードW_0, W_1に対応するトラップドアは問い合わせることができない．

Step.5　攻撃者 A はチャレンジ暗号文$C^* \coloneqq \mathrm{PEKS}(pk, W_b)$がキーワード$W_0, W_1$のどちらを暗号化したものか推測し，$b$の推測値$b' \in \{0,1\}$を出力する．$b = b'$であるときに攻撃者 A の勝利であるとする．

ここで攻撃者 A の識別利得を以下のように定義する．

$$\mathrm{Adv}_{\mathrm{A}}(k) \coloneqq \left| \Pr[b = b'] - \frac{1}{2} \right|$$

上記のゲームにおいて，攻撃者 A の識別利得$\mathrm{Adv}_{\mathrm{A}}(k)$が無視できるほど小さいとき，PEKS は IND-CKA 安全であるという．

3.4 IBE から PEKS への変換(ibe-2-peks 変換)

文献 [2] で任意の ID ベース暗号方式 $\mathcal{IBE} = (\mathrm{Setup}, \mathrm{Extract}, \mathrm{Enc}, \mathrm{Dec})$を検索可能公開鍵暗号方式 $\mathcal{PEKS} = (\mathrm{KeyGen}, \mathrm{Trapdoor}, \mathrm{Enc}, \mathrm{Test})$に変換する手法が提案された．この手法は[9]で ibe-2-peks 変換と呼ばれている．ibe-2-peks 変換は IBE の構成アルゴリズムの入力を変えて，PEKS の構成アルゴリズムとするものである．以下に ibe-2-peks 変換前の IBE と変換後の PEKS の構成アルゴリズムの対応を示す．

PEKS：$(pk, sk) \leftarrow \mathrm{KeyGen}(k)$

IBE：$(pk, sk) \leftarrow \mathrm{Setup}(k)$

PEKS の検索者の公開鍵pkと秘密鍵skはそれぞれ IBE の公開パラメータとマスター秘密鍵に対応する．

PEKS：$C \leftarrow \mathrm{Enc}(pk, W)$

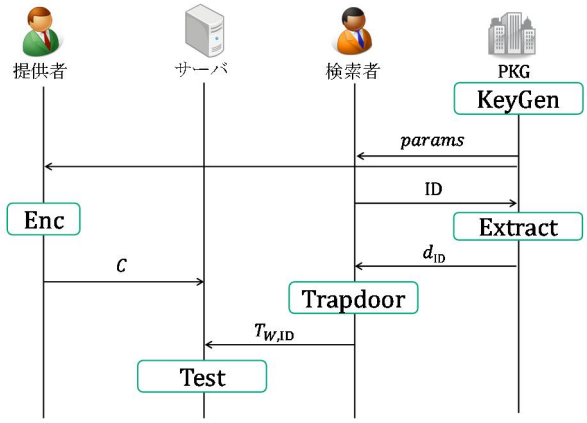

図5　SEACのモデル

IBE：$C \leftarrow \mathrm{Enc}(pk, W, 0^k)$

PEKS におけるキーワードWの暗号文は，IBE の平文Mを0^kで，識別子 ID をキーワードWに置き換えて生成される暗号文Cに対応する．

PEKS：$T_W \leftarrow \mathrm{Trapdoor}(pk, sk, W)$

IBE：$T_W \leftarrow \mathrm{Extract}(pk, sk, W)$

PEKS においてキーワードWに関連づいているトラップドアT_Wは IBE の識別子Wに対応する秘密鍵に対応する．

PEKS：$b \leftarrow \mathrm{Test}(pk, C, T_W)$

IBE：$\mathrm{Dec}(pk, T_W, C) = 0^k$ ならば 1 を出力し，そうでなければ 0 を出力する．

PEKS において暗号文とトラップドアに関連付けられたキーワードの一致を確認する暗号化キーワードの検索は，IBE で暗号文 C を復号したときに0^kが出力されるか確認することに対応する．Decアルゴリズムで出力される値が0^kのときに PEKS でキーワードの一致を表す1，そうでないときにキーワードの不一致を表す0が出力される．

4.　アクセス制御機能付き検索可能暗号(SEAC)

Boneh らが提案した PEKS では暗号文とトラップドアの両方にキーワードの情報が含まれている．双方に含まれるキーワードの一致を確認することでキーワード検索を実現している．検索者を識別子 ID で表現し，暗号文とトラップドアに検索者の ID も含ませることで，キーワードの一致と ID の一致の 2 つを確認でき，検索者を限定できる．PEKS を基にして以下の様なアクセス制御機能付き検索可能暗号(Searchable Encryption with Access Control: SEAC)を定義する．

SEAC のモデルを図 5 に示す．

4.1　エンティティ

SEAC は提供者，検索者，サーバ，PKG の 4 者のエンティティから構成される．

[提供者]　キーワードWと検索者の ID を指定し，Wの暗号文 C を作成する．暗号文を保管者に送る．

[検索者]　保管者が持つ暗号文をキーワードで検索する．それぞれの検索者は固有の ID を持つ．保管者に検索キーワードから生成したトラップドアを送り，保管者から暗号文が検索キーワードを暗号化したものであるか否か返答を受ける．

[サーバ]　提供者からキーワードの暗号文を受け取り保管する．検索者からトラップドアによる問い合わせを受け，返答する．

[PKG]　公開パラメータとマスター鍵を作成し，公開パラメータを公開する．マスター鍵と検索者から受け取った ID から秘密鍵を作成し，秘密鍵を検索者に秘密裏に渡す．PKG は信頼のおける第三者であるとする．

4.2　アルゴリズム

SEAC は以下の 5 つのアルゴリズムから構成される．

KeyGen(k)：　セキュリティパラメータkを入力として，公開パラメータ$params$とマスター鍵msk，ハッシュ関数hを出力する．

Extract ($params, msk$, ID)：　公開パラメータ$params$とマスター鍵msk，検索者の ID を入力として秘密鍵d_{ID}を出力する．

Enc($params$, ID, $h(W)$)：　公開パラメータ$params$，検索者の ID，キーワードWのハッシュ値$h(W)$を入力として検索者を限定して検索できる暗号文 C を出力する．

Trapdoor($params, d_{\mathrm{ID}}, h(W)$)：　公開パラメータ$params$と秘密鍵$d_{\mathrm{ID}}$，キーワード$W$のハッシュ値$h(W)$を入力としてトラップドア$T_{W,\mathrm{ID}}$を出力する．

Test($params, C, T_{W,\mathrm{ID}}$)：　公開パラメータ$params$と暗号文C ≔ Enc ($params$, ID′, W')，キーワードWと検索者の識別子 ID から作られたトラップドア$T_{W,\mathrm{ID}}$を入力として，$W = W'$かつID = ID'のとき 1 を，それ以外のときに 0 を出力する．

検索者に対するアクセス制御は Test アルゴリズムで行われる．Test アルゴリズムの入力の暗号文Cとトラップドア$T_{W,\mathrm{ID}}$の生成には双方とも入力としてキーワードに対応する情報だけでなく ID に対応する情報が含まれている．Test アルゴリズムで双方に含まれるキーワードだけでなく ID の情報も一致を確認することでアクセス制御機能を実現している．

4.3　安全性定義

SEAC の IND-ID-CKA 安全性は以下のゲームによって定義される．ゲームを図 6 に示す．

IND-ID-CKA ゲーム

Step.1　挑戦者 C はKeyGen(k)アルゴリズムを実行し，公開パラメータ$params$とマスター秘密鍵mskを生成し，公開パラメータ$params$を攻撃者 A に渡す．

Step.2　攻撃者 A は挑戦者 C に対して適応的に以下の Trapdoor クエリが許される．

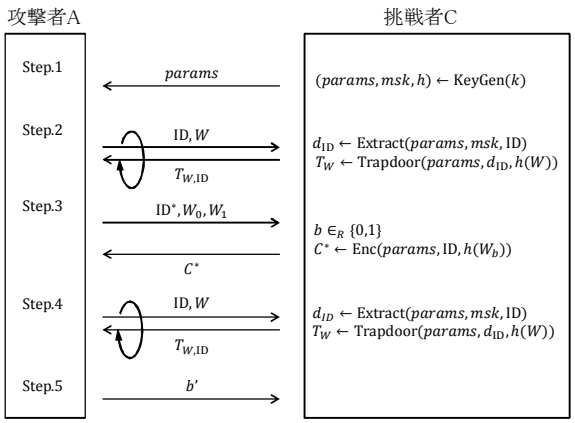

図6　IND-ID-CKAゲーム

[Trapdoor クエリ]

任意のID ∈ {0,1}*とキーワードW ∈ {0,1}*に対するトラップドアを問い合わせる．挑戦者 C はまず Extract アルゴリズムを実行して ID に対応する秘密鍵d_{ID}を生成する．次に挑戦者 C は Trapdoor アルゴリズムを実行して秘密鍵d_{ID}とキーワードWに対応するトラップドア$T_{W,\mathrm{ID}}$を生成し攻撃者に渡す．

Step.3　攻撃者 A は 2 つの異なるキーワードW_0，W_1とID*を挑戦者 C に渡す．ID*は Step.2 で問い合わせていない ID に限られる．挑戦者 C は$b \in \{0,1\}$をランダムに選び，チャレンジ暗号文$C^* = \mathrm{Enc}(params, \mathrm{ID}^*, W_b)$を攻撃者 A に渡す．

Step.4　攻撃者 A は Step.2 と同様に任意のキーワードWと ID に対応するトラップドア$T_{W,\mathrm{ID}}$を挑戦者 C に適応的に問い合わせることができる．ただし，Step.3 で選択した ID*を選ぶことはできない．

Step.5　攻撃者 A はチャレンジ暗号文$C^* \coloneqq \mathrm{Enc}(params, \mathrm{ID}, W_b)$がキーワード$\mathrm{W}_0, \mathrm{W}_1$のどちらを暗号化したものか推測し，$b$の推測値$\mathrm{b}' \in \{0,1\}$を出力する．$b = b'$であるとき攻撃者 A の勝利であるとする．

ここで攻撃者 A の識別利得を以下のように定義する．

$$\mathrm{Adv}_{\mathrm{A}}(k) \coloneqq |\Pr[b = b'] - \frac{1}{2}|$$

上記のゲームにおいて，攻撃者 A の識別利得$\mathrm{Adv}_{\mathrm{A}}(k)$が無視できるほど小さいとき, SEAC は IND-ID-CKA 安全であるという．

5. 提案手法

5.1 ibe-2-seac 変換の構成

本章では ID ベース暗号方式 IBE= (Setup, Extract, Enc, Dec)をアクセス制御検索可能公開鍵暗号方式 SEAC= (KeyGen, Extract, Trapdoor, Enc, Test) に変換する手法 (ibe-2-seac 変換)を提案する．

文献[9]で提案された ibe-2-peks 変換では，検索者が IBE の暗号化アルゴリズムEnc$(params, \mathrm{ID}, M)$に ID の代わりにキーワードWを，平文Mの代わりに0^kを入力したときの出力を検索可能な暗号文とする．ibe-2-seac 変換では ibe-2-peks 変換における平文0^kの部分をキーワードを表す情報に置き換え，トラップドアにキーワードを表す情報を含める．以下に ibe-2-seac 変換アルゴリズムの変換前の IBE と変換後の SEAC の構成アルゴリズムの対応を示す．

SEAC：$(\boldsymbol{params}, \boldsymbol{msk}) \leftarrow \mathbf{KeyGen}(\boldsymbol{k})$
IBE：$(\boldsymbol{params}, \boldsymbol{msk}) \leftarrow \mathbf{Setup}(\boldsymbol{k})$

SEAC の公開パラメータ$params$とマスター秘密鍵mskはそれぞれ IBE の受信者の公開鍵と秘密鍵に対応する．

SEAC：$\boldsymbol{d}_{\mathrm{ID}} \leftarrow \mathbf{Extract}(\boldsymbol{params}, \boldsymbol{msk}, \mathbf{ID})$
IBE：$\boldsymbol{d}_{\mathrm{ID}} \leftarrow \mathbf{Extract}(\boldsymbol{params}, \boldsymbol{msk}, \mathbf{ID})$

SEAC における ID と対になっている秘密鍵は IBE の ID と対になっている秘密鍵に対応する．

SEAC：$\boldsymbol{T}_{W,\mathrm{ID}} \leftarrow \mathbf{Trapdoor}(\boldsymbol{params}, \boldsymbol{d}_{\mathrm{ID}}, \boldsymbol{W})$
IBE：$\boldsymbol{H}_W \coloneqq \boldsymbol{h}(\boldsymbol{W})$
$\boldsymbol{T}_{W,\mathrm{ID}} \leftarrow [\boldsymbol{d}_{\mathrm{ID}}, \boldsymbol{H}_W]$

ここで SEAC の公開パラメータであるハッシュ関数hを導入する．hの値域は IBE の平文空間$\mathbb{M}$のサイズに依る．平文空間が$\mathbb{M}$=$\{0,1\}^k$であるとするならば，ハッシュ関数hはh: $\{0,1\}^* \rightarrow \{0,1\}^k$ となる．キーワードWのハッシュ値H_W:=$h(W)$と IBE の ID に対応する秘密鍵d_{ID}の組$[d_{\mathrm{ID}}, H_W]$が SEAC のトラップドア$T_{W,\mathrm{ID}}$と対応する．

SEAC：$\boldsymbol{C} \leftarrow \mathbf{Enc}(\boldsymbol{params}, \mathbf{ID}, \boldsymbol{W})$
IBE：$\boldsymbol{H}_{\mathbf{W}} \coloneqq \boldsymbol{h}(\boldsymbol{W})$
$\mathbf{C} \leftarrow \mathbf{Enc}(\boldsymbol{params}, \mathbf{ID}, \boldsymbol{H}_W)$

SEAC におけるキーワードWと ID の暗号文は，IBE の平文Mをキーワードのハッシュ値$h(W)$で置き換えて生成される暗号文に対応する．

SEAC：$\boldsymbol{b} \leftarrow \mathbf{Test}(\boldsymbol{params}, \mathbf{C}, \boldsymbol{T}_{W,\mathrm{ID}})$
IBE：$\mathbf{Dec}(\boldsymbol{params}, \boldsymbol{C}, \boldsymbol{d}_{\mathrm{ID}}) = \boldsymbol{H}_W$ならば 1 を出力し，そうでなければ 0 を出力する．

SEAC における暗号文の検索処理では暗号文とトラップドアに関連付けられているキーワードと ID の双方の一致を確認する．この確認は IBE における暗号文Cを秘密鍵d_{ID}で復号して出力される値が，検索キーワードのハッシュ値H_Wであるか確認することに対応している．

5.2 安全性

以下, IND-ID-CPA 安全な ID ベース暗号の方式を IBE, IBE から ibe-2-seac 変換することで得られるアクセス制御機能付き検索可能暗号を SEAC と記す．

[定理 1]

ID ベース暗号方式 IBE が IND-ID-CPA 安全であれば，

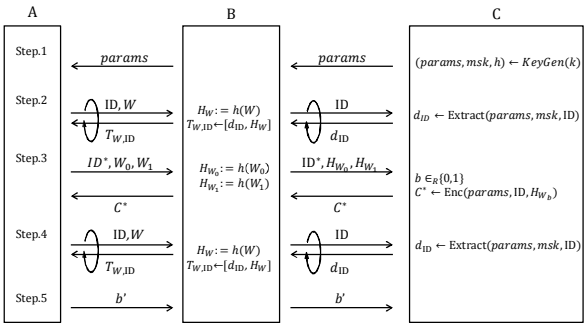

図7 証明のゲームの流れ

IBE から ibe-2-seac 変換によって構成されるアクセス制御機能付き検索可能暗号方式 *SEAC* は IND-ID-CKA 安全である.

[証明の方針]

ibe-2-seac 変換により構成された *SEAC* を識別利得 ε で破る攻撃者 A が存在すると仮定する．このとき IND-ID-CPA 安全な ID ベース暗号方式を少なくとも識別利得 ε で破る攻撃者 B が存在することを示す.

[証明]

以下の 3 つのアルゴリズム A, B, C 間のゲームを考える.

- アルゴリズム A は *SEAC* に対して ε の識別利得を持つ IND-ID-CKA の攻撃者とする
- アルゴリズム B は C に対しては *IBE* を破ろうとする攻撃者であり，A に対しては *SEAC* の挑戦者とする．B は SEAC の公開パラメータであるハッシュ関数 h を持つものとする
- アルゴリズム C は B に対して IND-ID-CPA 安全な *IBE* の挑戦者とする

ゲームの様子を図 7 に示す.

Step.1　挑戦者 C は *IBE* の Setup アルゴリズムを実行して公開パラメータ $params$ とマスター秘密鍵 msk を生成し，$params$ を攻撃者 B に渡す．挑戦者 B は $params$ を *SEAC* の公開パラメータとして攻撃者 A に渡す．msk は挑戦者 C が秘密に保持する.

Step.2　攻撃者 A は挑戦者 B に任意の ID とキーワード W に対応するトラップドア $T_{W,\mathrm{ID}}$ を問い合わせる．攻撃者 B は攻撃者 A から受け取った ID を挑戦者 C に渡し，対応する秘密鍵を問い合わせる．挑戦者 C は Extract アルゴリズムを実行し，生成された秘密鍵 d_{ID} を攻撃者 B に渡す. 挑戦者 B は攻撃者 A から受け取ったキーワード W から $H_W := h(W)$ を計算し，$T_{W,\mathrm{ID}} := [d_{\mathrm{ID}}, H_W]$ を攻撃者 A に渡し問い合わせに対する返答とする．攻撃者 A の問い合わせは適応的に任意の回数繰り返される.

Step.3　攻撃者 A は ID* と 2 つのキーワード W_0, W_1 を挑戦者 B に渡す. B は $H_{W_0} := h(W_0)$，$H_{W_1} := h(W_1)$ を計算し，ID* と合わせて挑戦者 C に渡す．挑戦者 C はランダムに $b \in \{0,1\}$ を選び，チャレンジ暗号文 $C^* := \mathrm{Enc}(params, \mathrm{ID}^*, H_{W_b})$ を攻撃者 B に渡す. B は受け取ったチャレンジ暗号文 C^* をそのまま攻撃者 A にチャレンジ暗号文として渡す．ただし ID* は Step.2 でトラップドアの問い合わせに使った ID を選ぶことはできない.

Step.4　攻撃者 A は Step.2 と同様に任意の ID とキーワード W を選択して，挑戦者 B に問い合わせる．ただし，Step.3 で選択した ID* を選ぶことはできない．B,C も Step.2 と同様に動作する.

Step.5　攻撃者 A は b の推測値 $b' \in \{0,1\}$ を出力し挑戦者 B に渡す. 攻撃者 B は受け取った推測値 b' を挑戦者 C に渡す.

攻撃者 A の推測値 b' が $b = b'$ となり攻撃者 A が挑戦者 B との IND-ID-CKA ゲームに勝利するとき，同じく攻撃者 B も挑戦者 C との IND-ID-CPA ゲームに勝利する．攻撃者 A と攻撃者 B のゲームの勝敗は一致している．攻撃者 A が識別利得 ε を持つので，攻撃者 B も識別利得 ε を持つ．以上のシミュレーションより，ID ベース暗号方式 *IBE* が IND-ID-CPA 安全であれば，*IBE* から ibe-2-seac 変換によって構成されるアクセス制御機能付き検索可能暗号方式 *SEAC* は IND-ID-CKA 安全である.

6. おわりに

暗号文を復号することなく，検索することができる技術に検索可能暗号がある．検索可能暗号に暗号文の検索者を限定するアクセス制御機能を追加した方式が IBE から構成されている．本稿ではアクセス制御機能付き検索可能暗号 SEAC を定義し，任意の ID ベース暗号方式 IBE から SEAC へ変換できる ibe-2-seac 変換を提案した．提案手法を使って IND-ID-CPA 安全性を持つ ID ベース暗号から構成された SEAC は，ID ベース暗号の安全性に帰着させることで IND-ID-CKA 安全な方式であることを示した.

今後の課題として IND-ID-CPA 以外の安全性をもつ ID ベース暗号方式から構成した SEAC の安全性について示すことがあげられる.

参考文献

1) Song, D., Wagner, D. and Perrig, A.: Practical Techniques for Searching on Encrypted Data, IEEE Symposium on Research in Security and Privacy 2000, pp.44-55 (2000).
2) Boneh, D., Crescenzo, D. G., Ostrovsky, R. and Persiano, G.: Public Key Encryption with Keyword Search, EUROCRYPT 2004, vol.3027 of LNCS, pp.506-522 (2004).
3) Golle, P., Staddon, J. and Waters, B.: Secure conjunctive keyword search over encrypted data, ACNS 2004 (2004).
4) Boneh, D. and Waters, B.: Conjunctive, subset, and range queries on encrypted data, TCC 2007, LNCS, vol.4392, pp.535-554 (2007).
5) Attrapadung, N., Furukawa, J. and Imai, H.: Forward-Secure and Searchable Broadcast Encryption with Short Ciphertexts and Private Keys, ASIACRYPT 2006, vol.4284 of LNCS, pp.161-177 (2006).

6) 片山貴充，高木剛：アクセス制限可能なキーワード検索可能暗号方式, 暗号と情報セキュリティシンポジウム SCIS2008, 4E2-2 (2008).
7) Shamir, A.: Identity-based cryptosystems and signature schemes, Crypto'84, vol.196 of LNCS, pp.47-53 (1984).
8) Boneh, D. and Franklin, M.: Identity-based Encryption from the Weil Pairing, SIAM J. of Computing, vol.32, No.3, pp.586-615, 2003, Extended abstract in Crypto 2001 (2003).
9) Abdalla, M., Bellare, M., Catalano, D., Kiltz, E., Kohno, T., Lange, T., Malone-Lee, J., Neven, G., Paillier, P. and Shi, H.: Searchable Encryption Revisited: Consistency, Properties, Relation to Anonymous IBE, and Extensions, CRYPTO2005, vol.3621 of LNCS, pp.205-222 (2005).