Computer Security Symposium 2020
26 - 29 October 2020

失効可能な匿名否認可能述語認証スキームの具体化

穴田 啓晃[1,a)]　上繁 義史[2]

概要：本稿では，失効機能を備えた匿名否認可能述語認証スキーム rADPA の具体例を提示する．設計の方針は PKC 2012 で S.Yamada らにより提案された ADPA の一般的構成に従い，また，ESORICS 2017 で K.Yamada らにより提案された失効可能化の一般的構成を用いる．具体化の選択としては SCN 2014 で Takashima により提案された定数サイズ暗号文長で準適応的 IND-CPA 安全な鍵ポリシ ABE（KP-ABE）に着目し，検証可能性と CCA 安全性及び失効機能を持つよう拡張する．我々の rADPA は準適応的同時発生的健全性（semiadaptive concurrent soundness）及び直接失効（direct revocation）といった先行研究の暗号学的性質を受け継ぐ．

キーワード：否認可能，匿名，述語認証，属性，失効

Instantiation of Revocable Anonymous Deniable Predicate Authentication Scheme

Hiroaki Anada[1,a)]　Yoshifumi Ueshige[2]

Abstract: In this paper, we show an instantiation of the revocable anonymous deniable predicate authentication scheme (rADPA). Our design principle owes the generic construction of ADPA proposed at PKC 2012 by S.Yamada et al., and it uses the generic construction to have revocability proposed at ESORICS 2017 by K.Yamada et al. For our instantiation, we choose the key-policy ABE (KP-ABE) which is of constant-size ciphertext and which has Ind-semiadaptive-CPA security, and we extend it to have verifiability, CCA-security and revocation function. Our rADPA is an instantiation that inherits the cryptographic properties in previous work; that is, semiadaptive concurrent soundness and direct revocation.

Keywords: deniable, anonymous, predicate authentication, attribute, revocation

1. はじめに

認証はユーザが IT 機器もしくはネットワークへログインする際に本人確認として実行される必要不可欠なプロトコルである．認証プロトコルの性質の一つに匿名性（anonymity）がある．匿名性は，ユーザのデジタルアイデンティティを認証サーバが特定できない性質である．また，認証プロトコルに要求される別の性質として否認可能性（deniability）がある．否認可能性は，ユーザが認証を要求したと認証サーバ側が第三者へ主張しても，ユーザ側は認証を要求した事実は無いと否認できるという，アンチフォレンジックの性質である．

また，認証プロトコルのスキームの機能として失効（revocation）がある．失効は登録（registration）と対をなす処置でもあり，デジタルアイデンティティの無効化である．失効機能を実現する方法としては失効リストを用いる方法が一般的である．これは，失効リストにデジタルアイデンティティが載っているか否かで失効されているか否かを判定する方法である．ここで，認証プロトコルに匿名性を持たせようとすると，失効機能の実現が困難となる．

[1] 長崎県立大学大学院地域創成研究科情報工学専攻
Division of Computer Science, Graduate School of Regional Design and Creation, University of Nagasaki
[2] 長崎大学 ICT 基盤センター
Center for Information and Communication Technology, Nagasaki University
[a)] anada@sun.ac.jp

1.1 本稿の貢献

本稿では，上記の困難を暗号学のアプローチで解決し否認可能性をも実現する具体策として，失効機能を備えた匿名否認可能述語認証スキーム rADPA の具体例を提示する．提示する rADPA は，穴田-上繁 [1], [17] により提案された rADPA の一般的構成の具体化である．この一般的構成は二つの構成要素から成る．第一は IND-CPA 安全な属性ベース暗号スキーム（ABE）を検証可能性と CCA 安全性の二性質及び失効機能を持つよう拡張したスキーム ABE，第二は公開鍵暗号（PKE）をコミットメントと見たスキーム CmtSch である．ABE の上述の拡張さえできれば，あとは K.Yamada ら [13], [14] の失効可能属性ベース暗号（rABE）の手法及び S.Yamada ら [16] の匿名述語認証スキーム（ADPA）の手法を組み合わせることで実現できる．rADPA を上述のように構成する理由は，先行研究 [16] の貢献のとおり，次の暗号学的性質による．rADPA の準適応的同時発生的健全性は ABE の準適応的 IND-CCA 安全性及び CmtSch の完全拘束性から得られる．rADPA の匿名性は ABE の検証可能性から得られる．rADPA の否認可能性は ABE の正当性及び CmtSch の計算量的秘匿性から得られる．なお，先行研究 [15], [16] の貢献のとおり，IND-CPA 安全な ABE が検証可能性を持つならば，一般的変換を適用し IND-CCA 安全にすることができる．ただし，本稿では [16] の一般的変換を用いる（[15] でなく）．

また，この一般的構成において rADPA の失効機能は ABE の失効機能から得られる．この失効機能は，先行研究 [13], [14] の貢献のとおり，直接失効（direct revocation）である．すなわち，認証サーバ（検証者）が失効リストを直接指定できる特徴を有する．なおかつ，この指定の際，失効されていないユーザの秘密鍵が更新される必要が無い（[13], [14]）．

具体例の提示において，第一の構成要素として Takashima[10], [11] により提案された定数サイズ暗号文長で準適応的 IND-CPA 安全な鍵ポリシ ABE（KP-ABE）に着目し，上述の二性質（検証可能性と CCA 安全性）及び失効機能を持つよう拡張し用いる．また，第二の構成要素として ElGamal[4] の PKE をコミットメントと見たスキーム CmtSch を用いる．次いで，この ABE 及び CmtSch を用い，鍵ポリシ rADPA を具体的に構成する．また，安全性について述べる．Takashima[10], [11] の KP-ABE スキームを構成要素に用いる理由は，一つには，属性ベース暗号をチャレンジ&レスポンス認証プロトコルに用いる際. チャレンジメッセージが定数サイズであることがネットワークプロトコルとして望ましいからである．一方，属性ベース暗号の準適応的（semiadaptive）な攻撃モデルとは，敵アルゴリズムが公開パラメータ及び公開鍵を得た後，なおかつ，種々のクエリをオラクルへ発行する前に標的属性（target attribute）を宣言する攻撃モデルである．この攻撃モデルは属性ベース暗号がチャレンジ&レスポンス認証プロトコルに用いられるとき自然な攻撃モデルとなる．なぜなら，認証プロトコルに対する攻撃は敵が脆弱な認証サーバを（種々のクエリに相当する学習の前に）特定することが典型と考えるからである．このことが Takashima[10], [11] の KP-ABE スキームを構成要素に用いるもう一つの理由である．なお，準適応的 IND-CPA 安全な ABE スキームから準適応的同時発生的健全性[*1]を持つ認証スキームへの一般的変換が提案されている [18].

2. 準備

本節では，記法及び先行研究の諸概念を述べる．

自然数の集合を $\mathbb{N}$ と記す．セキュリティパラメータを λ と記す（$\lambda \in \mathbb{N}$）．ビット b の反転ビットを $\bar{b}$ と記す（$\bar{b} := 1 - b$）．集合 S からの元 s の一様ランダムサンプリングを $s \in_R S$ と記す．表現 $a =_? b$ は $a = b$ のとき 1 を，そうでないとき 0 を返すものとする．表現 $a \in_? S$ は $a \in S$ のとき 1 を，そうでないとき 0 を返すものとする．アルゴリズム A がストリング a を入力としストリング z を出力することを $z \leftarrow A(a)$ または $A(a) \to z$ と記す．確率的アルゴリズム A が a を入力とし r をランダムネスとし z を出力することを $z \leftarrow A(a; r)$ と記す．対話型確率的アルゴリズム (A, B) について，A, B が x を共通入力，また A が w を個別入力とし，B が z を出力することを $z \leftarrow \langle A(w), B\rangle(x)$ と記す．アルゴリズム A がオラクル $\mathcal{O}$ にアクセスすることを $A^{\mathcal{O}}$ と記す．「確率的多項式時間」を PPT と略す．関数 $f : \mathbb{N} \to \mathbb{R}$ が無視可能であるとは，任意の $c > 0$ に対し定数 $K \in \mathbb{N}$ が存在し，$k > K$ ならば $|f(k)| \leq k^{-c}$ となるときにいう．二つの関数 $f, g : \mathbb{N} \to \mathbb{R}$ が計算量的に識別不可能であるとは，関数 $|f(k) - g(k)|$ が無視可能であるときにいい，$f(k) \approx_{\mathrm{c}} g(k)$ と書く．

2.1 双線形群 [5]

p をビット長 λ の素数とする．p を法とする剰余類環を $\mathbb{Z}_p$ と記す．$\mathcal{BG}$ を対称双線形群を生成する PPT アルゴリズムとする [5]: $\mathcal{BG}(1^\lambda) \to (p, \mathbb{G}, \mathbb{G}_T, e, G, G_T)$. ただし，$\mathbb{G}$ 及び $\mathbb{G}_T$ は位数 p の巡回群で，G 及び G_T はそれぞれの生成元の一つである．G の演算は加法で，G_T の演算は乗法で表す．e は双線形写像 $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ で，アルゴリズムとして λ の多項式時間であるものとする．e は次の二つの性質を満たすものとする:

- 非退化性 : $e(G, G) \neq 1_{\mathbb{G}_T}$,
- 双線形性 : $\forall a \in \mathbb{Z}_p, \forall b \in \mathbb{Z}_p, e(aG, bG) = e(G, G)^{ab}$.

[*1] 文献 [18] では「準適応的中間者攻撃安全性」と呼ばれている．設計方針は本稿と同じである．

2.2 失効可能な匿名否認可能述語認証スキーム

2.2.1 記法

• $\mathcal{ID} = \{0,1\}^k$：アイデンティティ文字列 id の属する集合であり，長さ k ビットのストリングの全体である．

• $m = |\mathcal{ID}|$：$\mathcal{ID}$ の位数である（$m = 2^k$）．

• $\mathcal{RL}$：失効された id の属する集合である：$\mathcal{RL} \in 2^{\mathcal{ID}}$．失効リストと呼ばれる．

• $B \in \mathbb{N}$：$\mathcal{RL}$ の位数の上限である：$|\mathcal{RL}| \leq B$．

• κ：属性集合及び述語関数を指定するインデックスであり，固定された定数 $c \in \mathbb{N}$ が存在し $\kappa = (n_1, \ldots, n_c) \in \mathbb{N}^c$ である．

• $\mathbb{X}^\kappa, \mathbb{Y}^\kappa$：鍵属性集合，及び，暗号文属性集合である．

• $\mathsf{R}^\kappa : \mathbb{X}^\kappa \times \mathbb{Y}^\kappa \to \{0,1\}$：鍵属性 X 及び暗号文属性 Y についての述語関数である．

• $\mathcal{R} = \{\mathsf{R}^\kappa\}^{\kappa \in \mathbb{N}^c}$：述語関数族である．

アイデンティティ文字列 id が失効されているか否かは次のブール値で決まる．

$$\mathsf{id} \in_? \mathcal{RL}.$$

K.Yamada ら [13], [14] に従い，鍵属性 X 及び暗号文属性 Y についての述語関数 R^κ を $\mathsf{id} \in \mathcal{RL}$ の成否に取り込んだ次の述語関数 $\bar{\mathsf{R}}^\kappa_m$ を考える．

$$\bar{\mathsf{R}}^\kappa_m((X,\mathsf{id}),(Y,\mathcal{RL})) \stackrel{\text{def}}{=} \begin{cases} 1 \text{ if } \bar{\mathsf{R}}^\kappa_m(X,Y) = 1 \wedge \mathsf{id} \notin \mathcal{RL}, \\ 0 \text{ otherwise.} \end{cases}$$

つまり，述語関数 $\bar{\mathsf{R}}^\kappa_m$ は述語関数 $\bar{\mathsf{R}}^\kappa_m$ を次のように拡張した概念と捉えられる．

$$X \leftarrow (X,\mathsf{id}),\ Y \leftarrow (Y,\mathcal{RL}).$$

2.2.2 シンタックス

失効機能を備えた匿名否認可能述語認証スキーム rADPA は，述語関数族 $\bar{\mathcal{R}} = \{\bar{\mathsf{R}}^\kappa_m\}^\kappa_m$ に対し定まるものであり，四つの多項式時間アルゴリズムから成る：$\mathsf{rADPA} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{P}, \mathsf{V})$.

• $\mathsf{Setup}(1^\lambda, \kappa) \to (\mathrm{PK}, \mathrm{MSK})$．このアルゴリズムは PPT であり，セキュリティパラメータ 1^λ 及び述語を叙述するインデックス κ を入力に取り，公開鍵 PK 及びマスター秘密鍵 MSK を出力する．

• $\mathsf{KeyGen}((X,\mathsf{id}),\mathrm{PK},\mathrm{MSK}) \to \mathrm{SK}_{X,\mathsf{id}}$．このアルゴリズムは PPT であり，鍵属性 X，アイデンティティ文字列 id，公開鍵 PK 及びマスター秘密鍵 MSK を引数に取り，プライベート秘密鍵 $\mathrm{SK}_{X,\mathsf{id}}$ を出力する．

• $\langle \mathsf{P}(\mathrm{SK}_{X,\mathsf{id}}), \mathsf{V}\rangle((Y,\mathcal{RL}),\mathrm{PK}) \to 1/0$．これらの対話アルゴリズムは PPT であり，共通入力として暗号文属性 Y，失効リスト $\mathcal{RL}$ 及び公開鍵 PK を，また P の入力としてプライベート秘密鍵 $\mathrm{SK}_{X,\mathsf{id}}$ を入力に取り，ビット 1 もしくは 0 を出力する．

rADPA の満たすべき正当性（correctness）については本稿では省略する．

2.2.3 安全性定義

rADPA の安全性として健全性，匿名性及び否認可能性を定義する．

健全性の定義． なりすまし攻撃に対する耐性は，秘密鍵を持たない証明者が無視可能な確率でしか受理されない性質である．この性質は暗号学では健全性（soundness）として捉えられる．本稿では，S.Yamada ら [16] の定義にならい述語認証スキームの形式で，ただしメッセージ認証でなく本人認証として，同時発生的な（concurrent）攻撃に対する健全性を次の実験アルゴリズム $\mathsf{Expr}^{\text{c-sound}}_{\mathsf{rADPA},\mathbf{A}}$ で定義する．ここで，準適応的（semiadaptive）な攻撃を定義していることに注意されたい．すなわち，敵アルゴリズム $\mathbf{A}$ は公開パラメータ及び公開鍵を得た後，かつ，オラクルへクエリを発行する前に，標的属性を指定している．

$\mathsf{Expr}^{\text{semiad-c-sound}}_{\mathsf{rADPA},\mathbf{A}}(1^\lambda, \kappa)$

$(\mathrm{PK}, \mathrm{MSK}) \leftarrow \mathsf{Setup}(1^\lambda, \kappa)$

$((Y^*, \mathcal{RL}^*), St) \leftarrow \mathbf{A}(\mathrm{PK}, \kappa)$

$b \leftarrow \langle \mathbf{A}^{\mathcal{P}_i(\mathrm{SK}_{X_i,\mathsf{id}_i})|^{q_\mathrm{p}}_{i=1}, \mathcal{KG}}(St), \mathsf{V}\rangle((Y^*, \mathcal{RL}^*), \mathrm{PK})$

If $b = 1$ then return Win else return Lose

上記において，各 $\mathcal{P}_i (i \in \{1,\ldots,q_\mathrm{p}\})$ は証明者オラクルである．$\mathcal{P}_i$ は $\mathbf{A}$ が発行するクエリとして $((X_i,\mathsf{id}_i),(Y_i,\mathcal{RL}_i))$ を受け取ると，これを入力に取り，$\mathsf{KeyGen}((X_i,\mathsf{id}_i),\mathrm{PK},\mathrm{MSK})$ を走らせ秘密鍵 $\mathrm{SK}_{X_i,\mathsf{id}_i}$ を得，証明者 $\mathsf{P}(\mathrm{SK}_{X_i,\mathsf{id}_i},(Y_i,\mathcal{RL}_i),\mathrm{PK})$ として $\mathbf{A}$ と対話する．ただし，$\mathcal{P}_i$ はオラクルゆえ各入出力間の処理は 1 ステップでなされる．$\mathbf{A}^{(\mathcal{P}_i)|^{q_\mathrm{p}}_{i=1}}$ はオラクル $\mathcal{P}_i, i \in \{1,\ldots,q_\mathrm{p}\}$ への $\mathbf{A}$ の同時発生的アクセスである．すなわち，メッセージの順序は $\mathbf{A}$ の指定する任意の順序である．$\mathbf{A}$ に課される制約として，$\mathcal{P}_i$ と $\mathbf{A}$ の対話のトランスクリプトは $\mathbf{A}$ と V の対話のトランスクリプトを含まないものとする．

また上記において，$\mathcal{KG}$ は鍵生成オラクルである．$\mathcal{KG}$ は $\mathbf{A}$ が発行するクエリとして (X_i,id_i) を受け取ると，これを入力に取り，$\mathsf{KeyGen}((X_i,\mathsf{id}_i),\mathrm{PK},\mathrm{MSK})$ を走らせ秘密鍵 $\mathrm{SK}_{X_i,\mathsf{id}_i}$ を得，$\mathrm{SK}_{X_i,\mathsf{id}_i}$ を $\mathbf{A}$ へ返す．ただし，$\mathcal{KG}$ はオラクルゆえ入出力間の処理は 1 ステップでなされる．$\mathbf{A}$ に課される制約として，クエリは $\bar{\mathsf{R}}^\kappa_m((X_i,\mathsf{id}_i),(Y^*,\mathcal{RL}^*)) = 0$ を満たすものとする．

$\mathbf{A}$ の認証スキーム rADPA に対する優位度を次の確率 $\mathbf{Adv}^{\text{semiad-c-sound}}_{\mathsf{rADPA},\mathbf{A}}(\lambda,\kappa)$（$\lambda, \kappa$ の関数）として定義する．

$$\mathbf{Adv}^{\text{semiad-c-sound}}_{\mathsf{rADPA},\mathbf{A}}(\lambda,\kappa) \stackrel{\text{def}}{=} \Pr[\mathsf{Expr}^{\text{semiad-c-sound}}_{\mathsf{rADPA},\mathbf{A}}(1^\lambda,\kappa) \text{ returns Win}].$$

定義 1 (準適応的同時発生的健全性) 与えられた任意の $\kappa \in \mathbb{N}^c$，与えられた任意の多項式時間アルゴリズム $\mathbf{A}$ に

対し，$\mathbf{Adv}^{\text{semiad-c-sound}}_{\mathsf{rADPA},\mathbf{A}}(\lambda,\kappa)$ が λ の関数として無視可能であるとき，認証スキーム rADPA は準適応的同時発生的健全性を有するという：

$$\mathbf{Adv}^{\text{semiad-c-sound}}_{\mathsf{rADPA},\mathbf{A}}(\lambda,\kappa)\approx 0 \text{ as a function in } \lambda. \quad (1)$$

匿名性の定義. 匿名性（anonymity）を暗号学のアプローチで捉える仕方の一つは，述語を満足する二つの秘密鍵についての識別不可能性によるものである．本稿では S.Yamada ら [16] の定義にならい，ただしメッセージ認証でなく本人認証として，匿名性を次の実験アルゴリズム $\mathsf{Expr}^{\text{anonym}}_{\mathsf{rADPA},\mathbf{A}}$ で定義する．ここで $\mathbf{A}$ はアルゴリズムである．

$\mathsf{Expr}^{\text{anonym}}_{\mathsf{rADPA},\mathbf{A}}(1^\lambda,\kappa)$
$(\mathrm{PK},\mathrm{MSK})\leftarrow \mathsf{Setup}(1^\lambda,\kappa)$
$((X_0^*,\mathtt{id}_0^*),(X_1^*,\mathtt{id}_1^*),St)\leftarrow \mathbf{A}(\mathrm{PK},\mathrm{MSK})$
$\mathrm{SK}_{X_0^*,\mathtt{id}_0^*}\leftarrow \mathsf{KeyGen}((X_0^*,\mathtt{id}_0^*),\mathrm{PK},\mathrm{MSK})$
$\mathrm{SK}_{X_1^*,\mathtt{id}_1^*}\leftarrow \mathsf{KeyGen}((X_1^*,\mathtt{id}_1^*),\mathrm{PK},\mathrm{MSK})$
$((Y^*,\mathcal{RL}^*),St)\leftarrow \mathbf{A}(St)$ such that
$\bar{\mathsf{R}}^\kappa_m((X_0^*,\mathtt{id}_0^*),(Y^*,\mathcal{RL}^*))=\bar{\mathsf{R}}^\kappa_m((X_1^*,\mathtt{id}_1^*),(Y^*,\mathcal{RL}^*))$
$b\in_R\{0,1\},\hat{b}\leftarrow \mathbf{A}^{\mathcal{P}(\mathrm{SK}_{X_b^*,\mathtt{id}_b^*})}(St,\mathrm{SK}_{X_0^*,\mathtt{id}_0^*},\mathrm{SK}_{X_1^*,\mathtt{id}_1^*})$
If $b=0$ then return Win else return Lose

上記において，各 $\mathcal{P}$ は証明者オラクルである．$\mathcal{P}$ は証明者 $\mathsf{P}(\mathrm{SK}_{X_b^*,\mathtt{id}_b^*},(Y^*,\mathcal{RL}^*),\mathrm{PK})$ として $\mathbf{A}$ と対話する．ただし，$\mathcal{P}_i$ はオラクルゆえ各入出力間の処理は 1 ステップでなされる．

アルゴリズム $\mathbf{A}$ の認証スキーム rADPA に対する優位度を次の確率 $\mathbf{Adv}^{\text{anonym}}_{\mathsf{rADPA},\mathbf{A}}(\lambda,\kappa)$（$\lambda,\kappa$ の関数）として定義する．

$$\mathbf{Adv}^{\text{anonym}}_{\mathsf{rADPA},\mathbf{A}}(\lambda,\kappa)\stackrel{\text{def}}{=}\left|\Pr[\mathsf{Expr}^{\text{anonym}}_{\mathsf{rADPA},\mathbf{A}}(1^\lambda,\kappa)\text{ returns Win}]-\frac{1}{2}\right|.$$

定義 2 (匿名性) 与えられた任意の $\kappa\in\mathbb{N}^c$，与えられた任意の多項式時間アルゴリズム $\mathbf{A}$ に対し，$\mathbf{Adv}^{\text{anonym}}_{\mathsf{rADPA},\mathbf{A}}(\lambda,\kappa)$ が λ の関数として無視可能であるとき，認証スキーム rADPA は匿名性を有するという：

$$\mathbf{Adv}^{\text{anonym}}_{\mathsf{rADPA},\mathbf{A}}(\lambda,\kappa)\approx 0 \text{ as a function in } \lambda. \quad (2)$$

否認可能性の定義. 否認可能性（deniability）を暗号学のアプローチで捉える仕方の一つは，証明者と検証者の対話のトランスクリプト及び検証者のランダムネスを秘密鍵無しでシミュレーションするものである．本稿では S.Yamada ら [16] の定義にならい，否認可能性を次のトランスクリプト Real 及び Sim の識別不可能性として定義する．ここで $\mathbf{A}$ はアルゴリズムである．

$\mathsf{Real}(\lambda,\kappa,m,(X,\mathtt{id}),(Y,\mathcal{RL}))$
$\stackrel{\text{def}}{=}\mathsf{View}\big(\langle\mathsf{P}(\mathrm{SK}_{X,\mathtt{id}}),\mathbf{A}\rangle((Y,\mathcal{RL}),\mathrm{PK})\ \big|$
$\mathsf{Setup}(1^\lambda,\kappa)\to(\mathrm{PK},\mathrm{MSK});$
$\mathsf{KeyGen}((X,\mathtt{id}),\mathrm{MSK})\to\mathrm{SK}_{X,\mathtt{id}}\big),$
$\mathsf{Sim}(\lambda,\kappa,m,(X,\mathtt{id}),(Y,\mathcal{RL}))$
$\stackrel{\text{def}}{=}\mathsf{View}\big(\langle\mathsf{S},\mathbf{A}\rangle((Y,\mathcal{RL}),\mathrm{PK})\ \big|$
$\mathsf{Setup}(1^\lambda,\kappa)\to(\mathrm{PK},\mathrm{MSK});$
$\mathsf{KeyGen}((X,\mathtt{id}),\mathrm{MSK})\to\mathrm{SK}_{X,\mathtt{id}}\big).$

定義 3 (否認可能性) 与えられた任意の多項式時間アルゴリズム $\mathbf{D}$，与えられた任意の $\kappa\in\mathbb{N}^c$，与えられた任意の $(X,\mathtt{id})\in\mathbb{X}\times\mathcal{ID},(Y,\mathcal{RL})\in\mathbb{Y}\times 2^{\mathcal{ID}}$ such that $\bar{\mathsf{R}}^\kappa_m((X,\mathtt{id}),(Y,\mathcal{RL}))=1$，与えられた任意の多項式時間アルゴリズム $\mathbf{A}$ に対し，ある多項式時間アルゴリズム S が存在し，$\Pr[\mathbf{D}(\mathsf{Real}(\lambda,\kappa,m,(X,\mathtt{id}),(Y,\mathcal{RL})))=1]$ と $\Pr[\mathbf{D}(\mathsf{Sim}(\lambda,\kappa,m,(X,\mathtt{id}),(Y,\mathcal{RL})))=1]$ が λ の関数として計算量的に識別不可能であるとき，認証スキーム rADPA は否認可能性を有するという：

$$\begin{aligned}&\Pr[\mathbf{D}(\mathsf{Real}(\lambda,\kappa,m,(X,\mathtt{id}),(Y,\mathcal{RL})))=1]\\ \approx&\Pr[\mathbf{D}(\mathsf{Sim}(\lambda,\kappa,m,(X,\mathtt{id}),(Y,\mathcal{RL})))=1]. \quad (3)\end{aligned}$$

2.3 ABE の検証可能性 [16]

ABE（第 A.1 節）の検証可能性（verifiability）は次の性質として定義される [16]：任意の $\lambda\in\mathbb{N}$, 任意の $\kappa\in\mathbb{N}^c$, 任意の $(\mathrm{PK},\mathrm{MSK})\leftarrow\mathsf{Setup}(1^\lambda,\kappa)$, 任意の $X,X'\in\mathbb{X}^\kappa$, 任意の $Y\in\mathbb{Y}^\kappa$, 任意の $\mathrm{SK}_X\leftarrow\mathsf{KeyGen}(X,\mathrm{PK},\mathrm{MSK})$ 及び任意の $\mathrm{SK}_{X'}\leftarrow\mathsf{KeyGen}(X',\mathrm{PK},\mathrm{MSK})$ に対し，もし $\bar{\mathsf{R}}^\kappa(X,Y)=\bar{\mathsf{R}}^\kappa(X',Y)$ ならば，任意の $CT\in\{0,1\}^*$ について次の式が成立する：

$$\mathsf{Dec}(\mathrm{SK}_X,Y,\mathrm{PK},CT)=\mathsf{Dec}(\mathrm{SK}_{X'},Y,\mathrm{PK},CT). \quad (4)$$

式 (4) は必ずしも legitimately に生成された CT でない場合にも復号アルゴリズムの出力が同じになることを主張している．すなわち，上記の検証可能性は復号アルゴリズムの性質である（[16]）.

3. 定数サイズ暗号文長で準適応的 IND-CPA 安全な KP-ABE の拡張

本節では，Takashima[10], [11] により提案された定数サイズ暗号文長で準適応的 IND-CPA 安全な KP-ABE スキームを，検証可能性と CCA 安全性の二性質及び失効機能を持つよう拡張する方針を示す．次いで，拡張後の KP-ABE スキーム ABE を提示する．この ABE は次節で鍵ポリシ rADPA を具体的に構成する際の構成要素として用いられる．

3.1 拡張の方針

述語暗号スキームとしての属性ベース暗号スキーム ABE は，述語関数族 $\mathcal{R} = \{\mathsf{R}^\kappa\}^{\kappa\in\mathbb{N}^c}$ に対し定まるものであり，四つの多項式時間アルゴリズムから成る：ABE = (Setup, KeyGen, Enc, Dec)．シンタックスと準適応的 IND-CPA 安全性定義については第 A.1 節を参照されたい．

検証可能への拡張． Takashima[10], [11] の KP-ABE は dual system encryption [12] の手法を安全性証明において適用するスキームである．このため，公開検証可能性を持たない（[16]）．検証可能性を持たせるための手法として S.Yamada ら [16] の方針がある．すなわち，オリジナル [11] のプライベート秘密鍵を 2 個，ただしランダムネスが異なるもの，を改めてプライベート秘密鍵とする．復号時にはこれら 2 個のプライベート秘密鍵を用い復号アルゴリズムを 2 回走らせ，復号結果が同じならその結果を，復号結果が異なれば $\perp$ を出力するようにする（[16] 参照）．本稿でもこの方針に従う．

CCA 安全への拡張． 一般的に，ABE が準適応的 IND-CPA 安全性及び検証可能性を持つならば，準適応的 IND-CCA 安全性を持つよう拡張することができる．その仕方は S.Yamada ら [16] による：インデックス κ を κ' へ拡張する（[16] 参照）．ワンタイム署名 [7] を走らせ検証鍵と署名の組 (vk, σ) を得，暗号文 CT を $(\mathrm{vk}, CT, \sigma)$ へ拡張する（[16] 参照）．また，鍵属性 X 及び暗号文属性 Y をそれぞれ X' 及び Y' へ拡張する（[16] 参照）．

失効可能への拡張． 一般的に，ABE が monotone span program のアクセス構造を持つならば，失効機能を持つよう拡張することができる．その仕方は K.Yamada ら [13], [14] による．本稿では [14] の提案手法の中でも Section 3.2 “C_2: RABE from ABE for Boolean Formula” を適用する：鍵属性 X 及び暗号文属性 Y を，アイデンティティ文字列 id 及び失効リスト $\mathcal{RL}$ を用い，それぞれ X'' 及び Y'' へ拡張する（[14] 参照）．

3.2 拡張後のスキーム

以下，拡張後のスキームを示す．記法についてはオリジナル論文 Takashima[10], [11] を参照されたい．

- $\mathsf{Setup}'(1^\lambda, \kappa) \to (\mathrm{PK}, \mathrm{MSK})$．このアルゴリズムはオリジナル [11] の Setup に $(1^\lambda, \kappa')$ を入力し，次の公開鍵 PK 及びマスター秘密鍵 MSK を出力する：$\mathrm{PK} := (1^\lambda, \mathtt{param}, \{\hat{\mathbb{B}}_t\}_{t=0,1})$，$\mathrm{MSK} := \{\hat{\mathbb{B}}^*_t\}_{t=0,1}$．
- $\mathsf{KeyGen}'((X, \mathsf{id}), \mathrm{PK}, \mathrm{MSK}) \to \mathrm{SK}_{X,\mathsf{id}}$．このアルゴリズムはオリジナル [11] の KeyGen に $(X'', \mathrm{PK}, \mathrm{MSK})$ を入力し，次のプライベート秘密鍵 $\mathrm{SK}_{X,\mathsf{id}}$ を出力する．このとき，オリジナル [11] のプライベート秘密鍵を 2 個，ただしランダムネスが異なるもの，を改めてプライベート秘密鍵とする（^{0} 及び ^{1} の系列）：$\mathrm{SK}^{X,\mathsf{id}} := ((X'', \mathsf{id}), (\boldsymbol{(k}^*_0)^0, (\boldsymbol{k}_1*)^0, \ldots, (\boldsymbol{k}^*_\ell)^0), ((\boldsymbol{k}^*_0)^1, (\boldsymbol{k}_1*)^1, \ldots, (\boldsymbol{k}^*_\ell)^1))$．
- $\mathsf{Enc}'((Y, \mathcal{RL}), \mathrm{PK}, M) \to CT$．このアルゴリズムはオリジナル [11] の Enc に (Y'', PK, M) を入力し，次の暗号文 CT を得る：$CT := (\boldsymbol{c}_0, \{C_{1,j}, C_{2,j}\}_{j=1,\ldots,6}, c_T)$．また，ワンタイム署名を走らせ (vk, σ) を得，$CT := (\mathrm{vk}, CT, \sigma)$ を出力する．
- $\mathsf{Dec}'(\mathrm{SK}_{X,\mathsf{id}}, (Y, \mathcal{RL}), \mathrm{PK}, CT) \to \tilde{M}$．このアルゴリズムはオリジナル [11] の Dec に $(\mathrm{SK}_{X,\mathsf{id}}, Y'', \mathrm{PK}, CT)$ を入力し，復号結果 $\tilde{M}$ を出力する．このとき，^{0} 及び ^{1} の系列のプライベート秘密鍵 2 個を用いオリジナル [11] の復号アルゴリズムを 2 回走らせ，復号結果が同じならその結果を，復号結果が異なれば $\tilde{M} := \perp$ を出力する．

4. 具体例〜鍵ポリシ rADPA〜

本節では，失効機能を備えた匿名否認可能述語認証スキーム rADPA の具体例として，鍵ポリシ rADPA を具体的に構成する．この構成は二つの構成要素から成る．第一は，前節で拡張し得られた KP-ABE スキーム ABE，第二は，ElGamal[4] の PKE をコミットメントスキーム CmtSch と見たものである（CmtSch については第 A.2 節参照）．次いで，提案スキーム rADPA の安全性を述べる．

4.1 スキーム

スキーム rADPA = (Setup, KeyGen, P, V) の具体例を以下のように定める（図 1 参照）．

- $\mathsf{Setup}(1^\lambda, \kappa) \to (\mathrm{PK}, \mathrm{MSK})$．このアルゴリズムは PPT であり，セキュリティパラメータ 1^λ 及び述語を叙述するインデックス κ を入力に取り，$\mathsf{ABE.Setup}(1^\lambda, \kappa)$ を動かし，公開鍵 PK 及びマスター秘密鍵 MSK を得，$(\mathrm{PK}, \mathrm{MSK})$ を出力する．
- $\mathsf{KeyGen}(X, \mathrm{MSK}) \to \mathrm{SK}_{X,\mathsf{id}}$．このアルゴリズムは PPT であり，鍵属性 X，アイデンティティ文字列 id，公開鍵 PK 及びマスター秘密鍵 MSK を引数に取り，$\mathsf{ABE.KeyGen}((X, \mathsf{id}), \mathrm{MSK})$ を動かし，プライベート秘密鍵 $\mathrm{SK}_{X,\mathsf{id}}$ を得，$\mathrm{SK}_{X,\mathsf{id}}$ を出力する．
- $\langle \mathsf{P}(\mathrm{SK}_{X,\mathsf{id}}), \mathsf{V}\rangle((Y, \mathcal{RL}), \mathrm{PK}) \to 1/0$．これらの対話アルゴリズムは PPT であり，共通入力として暗号文属性 Y，失効リスト $\mathcal{RL}$ 及び公開鍵 PK を，また P の入力としてプライベート秘密鍵 $\mathrm{SK}_{X,\mathsf{id}}$ を入力に取り，ビット 1 もしくは 0 を出力する．証明者 P と検証者 V の対話については図 1 及び文献 [9], [16] を参照されたい．

4.2 安全性

定理 1 (準適応的同時発生的健全性) ABE が準適応的 IND-CCA 安全性を有し，かつ，CmtSch が完全拘束性を有するならば，我々の rADPA は準適応的同時発生的健全性を有する．より詳しくは，任意に与えられた PPT アル

$\mathsf{Setup}(1^\lambda, \kappa)$		$\mathsf{KeyGen}((X, \mathtt{id}), \mathrm{PK}, \mathrm{MSK})$
$\mathsf{ABE.Setup}(1^\lambda, \kappa)$		$\mathsf{ABE.KeyGen}((X, \mathtt{id}), \mathrm{PK}, \mathrm{MSK})$
$\to (\mathrm{PK}, \mathrm{MSK})$		$\to \mathrm{SK}_{X,\mathtt{id}}$
return $(\mathrm{PK}, \mathrm{MSK})$		return $\mathrm{SK}_{X,\mathtt{id}}$
$\mathsf{P}(\mathrm{SK}_{X,\mathtt{id}}, (Y, \mathcal{RL}), \mathrm{PK})$		$\mathsf{V}((Y, \mathcal{RL}), \mathrm{PK})$
		$r \in_R \mathbb{G}_T$
		$\mathsf{ABE.Enc}((Y, \mathcal{RL}), \mathrm{PK}, r; \rho)$
		$\to CT$
	CT	
$\mathsf{ABE.Dec}(\mathrm{SK}_{X,\mathtt{id}}, (Y, \mathcal{RL}), \mathrm{PK}, CT)$	$\leftarrow$	
$\to \tilde{r}$		
If $\tilde{r} = \perp$ then		
For $i = 1$ to λ:		
$(r_{i0}, r_{i1}) \in_R \mathbb{G}_T \times \mathbb{G}_T$		
else		
For $i = 1$ to λ:		
$r_{i0} \in_R \mathbb{G}_T, r_{i1} := \tilde{r} \cdot r_{i0}^{-1}$		
For $i = 1$ to λ:		
For $j = 0, 1$:		
$\gamma_{ij} \in_R \mathbb{G}_T, \mathsf{Com}(r_{ij}; \gamma_{ij}) \to C_{ij}$		
	$(C_{ij})_{j=0,1}^{1 \le i \le \lambda}$	
	$\to$	For $i = 1$ to λ:
		$b_i \in_R \{0, 1\}$
	$(b_i)^{1 \le i \le \lambda}$	
For $i = 1$ to λ:	$\leftarrow$	
$\mathsf{Open}(C_{ib_i}, \gamma_{ib_i}) \to \hat{r}_{ib_i}$		
	$(\hat{r}_{ib_i}, \gamma_{ib_i})^{1 \le i \le \lambda}$	
	$\to$	
	(r, ρ)	
For $i = 1$ to λ:	$\leftarrow$	
$\mathsf{Open}(C_{i\bar{b}_i}, \gamma_{i\bar{b}_i}) \to \hat{r}_{i\bar{b}_i}$		
	$(\hat{r}_{i\bar{b}_i}, \gamma_{i\bar{b}_i})^{1 \le i \le \lambda}$	
	$\to$	For $i = 1$ to λ:
		$r =_? r_{i0} \cdot r_{i1}$
		If all eqs. hold then return 1
		else return 0

図 1 具体例：失効機能を備えた匿名否認可能述語認証スキーム rADPA.

ゴリズム $\mathbf{A}$ に対し PPT アルゴリズム $\mathbf{B}$ が存在し次の不等式が成り立つ．

$$\mathbf{Adv}^{\text{semiad-c-sound}}_{\mathsf{rADPA},\mathbf{A}}(\lambda, \kappa) < \mathbf{Adv}^{\text{ind-semiadp-cca}}_{\mathsf{ABE},\mathbf{B}}(\lambda, \kappa). \quad (5)$$

Proof. 一般的構成 [1], [17] による． □

定理 2 (匿名性) ABE が検証可能性を有するならば，我々の rADPA は匿名性を有する．より詳しくは，任意に与えられたアルゴリズム $\mathbf{A}$ に対し次の不等式が成り立つ．

$$\mathbf{Adv}^{\text{anonym}}_{\mathsf{rADPA},\mathbf{A}}(\lambda, \kappa) = 0. \quad (6)$$

Proof. 一般的構成 [1], [17] による． □

定理 3 (否認可能性) ABE が正当性を有し，かつ，CmtSch が計算量的秘匿性を有するならば，我々の rADPA は否認可能性を有する．より詳しくは，任意に与えられた PPT アルゴリズム $\mathbf{D}$ に対し次の計算量的識別不可能性が成り立つ．

$$\Pr[\mathbf{D}(\mathsf{Real}(\lambda, \kappa, (X, \mathtt{id}), (Y, \mathcal{RL}))) = 1] \quad (7)$$

$$\approx_c \Pr[\mathbf{D}(\mathsf{Sim}(\lambda, \kappa, (X, \mathtt{id}), (Y, \mathcal{RL}))) = 1]. \quad (8)$$

Proof. 一般的構成 [1], [17] による． □

5. まとめと今後の課題

本稿では，Takashima[10], [11] の定数サイズ暗号文長で準適応的 IND-CPA 安全な KP-ABE スキームを，検証可能性と CCA 安全性の二性質及び失効機能を持つよう拡張する方針を示した．拡張後の KP-ABE スキーム ABE，及び，ElGamal[4] の PKE をコミットメントスキームと見たもの CmtSch を構成要素に用いた鍵ポリシ rADPA の具体例を提示した．

なお，この KP-ABE スキームに対し Attrapadung ら [2] の変換を施すことで，定数サイズ暗号文長で準適応的 IND-CPA 安全な CP-ABE スキームを得ることができる．一方，認証スキームではポリシ Y を検証者（認証サーバ）が設定することが自然と考えられる．このため，その CP-ABE スキームを検証可能性と CCA 安全性の二性質及び失効機能を持つよう拡張することは今後の課題である．

謝辞 本研究は JSPS 科研費 JP18K11297 の助成を受けたものです．著者らは ABE スキームの semiadaptive security 及び direct revocation に関しコメント下さった江村恵太氏に深謝致します．著者らは ABE スキームの verifiability に関しコメント下さったアッタラパドゥン ナッタポン氏に深謝致します．

参考文献

[1] H. Anada and Y. Ueshige.
Generic construction of anonymous deniable predicate authentication scheme with revocability.
In *Innovative Security Solutions for Information Technology and Communications - 12th International Conference, SecITC 2019, Bucharest, Romania, November 14-15, 2019, Revised Selected Papers*, pages 142–155, 2019.

[2] N. Attrapadung, G. Hanaoka, and S. Yamada.
Conversions among several classes of predicate encryption and applications to ABE with various compactness tradeoffs.
In *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part I*, pages 575–601, 2015.

[3] J. Chen and H. Wee.
Semi-adaptive attribute-based encryption and improved delegation for boolean formula.
In *Security and Cryptography for Networks - 9th International Conference, SCN 2014, Amalfi, Italy, September 3-5, 2014. Proceedings*, pages 277–297, 2014.

[4] T. El Gamal.
A public key cryptosystem and a signature scheme based on discrete logarithms.
In *Proceedings of CRYPTO 84 on Advances in Cryptology*, pages 10–18, New York, NY, USA, 1985. Springer-Verlag New York, Inc.

[5] S. D. Galbraith, K. G. Paterson, and N. P. Smart.
Pairings for cryptographers.
Discrete Applied Mathematics, 156(16):3113–3121, 2008.

[6] R. Goyal, V. Koppula, and B. Waters.
Semi-adaptive security and bundling functionalities made generic and easy.
In *Theory of Cryptography - 14th International Conference, TCC 2016-B, Beijing, China, October 31 - November 3, 2016, Proceedings, Part II*, pages 361–388, 2016.

[7] J. Katz and Y. Lindell.
Introduction to Modern Cryptography, Second Edition.
CRC Press, 2014.

[8] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters.
Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption.
In H. Gilbert, editor, *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Monaco / French Riviera, May 30 - June 3, 2010. Proceedings*, volume 6110 of *Lecture Notes in Computer Science*, pages 62–91. Springer, 2010.

[9] M. Naor.
Deniable ring authentication.
In *Advances in Cryptology - CRYPTO 2002, 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 2002, Proceedings*, pages 481–498, 2002.

[10] K. Takashima.
Expressive attribute-based encryption with constant-size ciphertexts from the decisional linear assumption.
In *Security and Cryptography for Networks - 9th International Conference, SCN 2014, Amalfi, Italy, September 3-5, 2014. Proceedings*, pages 298–317, 2014.

[11] K. Takashima.
Expressive attribute-based encryption with constant-size ciphertexts from the decisional linear assumption.
IEICE Trans. Fundam. Electron. Commun. Comput. Sci., 103-A(1):74–106, 2020.

[12] B. Waters.
Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions.
In S. Halevi, editor, *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings*, volume 5677 of *Lecture Notes in Computer Science*, pages 619–636. Springer, 2009.

[13] K. Yamada, N. Attrapadung, K. Emura, G. Hanaoka, and K. Tanaka.
Generic constructions for fully secure revocable attribute-based encryption.
In *Computer Security - ESORICS 2017 - 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11-15, 2017, Proceedings, Part II*, pages 532–551, 2017.

[14] K. Yamada, N. Attrapadung, K. Emura, G. Hanaoka, and K. Tanaka.
Generic constructions for fully secure revocable attribute-based encryption.
IEICE Transactions, 101-A(9):1456–1472, 2018.

[15] S. Yamada, N. Attrapadung, G. Hanaoka, and N. Kunihiro.
Generic constructions for chosen-ciphertext secure attribute based encryption.
In D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi,

editors, *Public Key Cryptography - PKC 2011 - 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, March 6-9, 2011. Proceedings*, volume 6571 of *Lecture Notes in Computer Science*, pages 71–89. Springer, 2011.

[16] S. Yamada, N. Attrapadung, B. Santoso, J. C. N. Schuldt, G. Hanaoka, and N. Kunihiro.
Verifiable predicate encryption and applications to CCA security and anonymous predicate authentication.
In *Public Key Cryptography - PKC 2012 - 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, May 21-23, 2012. Proceedings*, pages 243–261, 2012.

[17] 穴田啓晃 and 上繁義史.
リボーク機能を備えた匿名否認可能述語認証スキームについて.
In **暗号と情報セキュリティシンポジウム** *2020*(*SCIS2020*) **予稿集**, pages 3B2–3, 高知, 1 月 2020.

[18] 知念広太郎 and 穴田啓晃.
属性ベース認証方式の準適応的中間者攻撃に対する安全性の提案と garbled circuits を用いた一般的構成.
In **コンピュータセキュリティシンポジウム** *2020* (*CSS2020*) **予稿集**, pages xxx–x, オンライン開催, 10 月 2020.

付　　録

A.1　述語暗号としての属性ベース暗号 [8]

A.1.1　シンタックス

述語暗号スキームとしての属性ベース暗号スキーム ABE は，述語関数族 $\mathcal{R} = \{\mathsf{R}^\kappa\}^{\kappa\in\mathbb{N}^c}$ に対し定まるものであり，四つの多項式時間アルゴリズムから成る：$\mathsf{ABE} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$.

• $\mathsf{Setup}(1^\lambda, \kappa) \to (\mathrm{PK}, \mathrm{MSK})$．このアルゴリズムは PPT であり，セキュリティパラメータ 1^λ 及び述語を叙述するインデックス κ を入力に取り，公開鍵 PK 及びマスター秘密鍵 MSK を出力する．

• $\mathsf{KeyGen}(X, \mathrm{PK}, \mathrm{MSK}) \to \mathrm{SK}_X$．このアルゴリズムは PPT であり，鍵属性 X，アイデンティティ文字列 id，公開鍵 PK 及びマスター秘密鍵 MSK を引数に取り，プライベート秘密鍵 SK^X を出力する．

• $\mathsf{Enc}(Y, \mathrm{PK}, M) \to CT$．このアルゴリズムは PPT であり，暗号文属性 Y，失効リスト $\mathcal{RL}$，公開鍵 PK 及び平文 M を入力に取り，暗号文 CT を出力する．

• $\mathsf{Dec}(\mathrm{SK}_X, Y, \mathrm{PK}, CT) \to \tilde{M}$．このアルゴリズムは確定的であり，プライベート秘密鍵 SK_X，公開鍵 PK 及び暗号文 CT を引数に取り，復号結果 $\tilde{M}$ を出力する．

A.1.2　準適応的 IND-CCA 安全性 [3], [6], [10], [11]

ABE の準適応的 IND-CCA 安全性（IND-semiadp-CCA）は ABE とアルゴリズム $\mathbf{A}$ についての次の実験アルゴリズムで定義される [3]．ここで，準適応的（semiadaptive）な攻撃を定義していることに注意されたい．すなわち，敵アルゴリズム $\mathbf{A}$ は公開パラメータ及び公開鍵を得た後，かつ，オラクルへクエリを発行する前に，標的属性を指定している．

$\mathsf{Expr}^{\text{ind-semiadp-cca}}_{\mathsf{ABE},\mathbf{A}}(1^\lambda, \kappa)$
$(\mathrm{PK}, \mathrm{MSK}) \leftarrow \mathsf{Setup}(1^\lambda, \kappa)$
$(Y^*, St) \leftarrow \mathbf{A}(\mathrm{PK}, \kappa)$
$((M_0, M_1), St) \leftarrow \mathbf{A}^{\mathcal{DEC}, \mathcal{KG}}(\mathrm{PK}, St)$
$b \in_R \{0,1\}, CT^* \leftarrow \mathsf{Enc}(Y^*, \mathrm{PK}, M_b)$
$b^* \leftarrow \mathbf{A}^{\mathcal{DEC}, \mathcal{KG}}(CT^*, St)$
If $b = b^*$ then return Win else return Lose

上記で $|M_0| = |M_1|$ である．$\mathbf{A}$ は復号オラクル $\mathcal{DEC}$ に対し $(X_i, (Y_i, CT_i))$ というクエリを発行し，応答として M_i を得る（復号クエリ）．また，$\mathbf{A}$ は鍵生成オラクル $\mathcal{KG}$ に対し X_j というクエリを発行し，応答として SK_{X_j} を得る（鍵抽出クエリ）．これら二種類のクエリの発行回数は λ の多項式で押さえられている．Y^* は標的属性と呼ばれる．二つの制約がある．第一は，$\mathbf{A}$ は次のような復号クエリ $(X_i, (Y_i, CT_i))$ を発行しないものとする：$\bar{\mathsf{R}}^\kappa(X_i, Y_i) = 1$ and $(Y_i, CT_i) = (Y^*, CT^*)$．第二に，$\mathbf{A}$ は次のような鍵抽出クエリ X_j を発行しないものとする：$\bar{\mathsf{R}}^\kappa(X_j, Y^*) = 1$.

$\mathbf{A}$ の ABE に対する優位度は次の確率で定義される：

$$\mathbf{Adv}^{\text{ind-semiadp-cca}}_{\mathsf{ABE},\mathbf{A}}(\lambda, \kappa) \stackrel{\text{def}}{=} \Pr[\mathsf{Expr}^{\text{ind-semiadp-cca}}_{\mathsf{ABE},\mathbf{A}}(1^\lambda, \kappa) \text{ returns Win}]. \quad \text{(A.1)}$$

ABE は次のとき準適応的 IND-CCA 安全であるといわれる：任意の PPT アルゴリズム $\mathbf{A}$ に対し $\mathbf{Adv}^{\text{ind-semiadp-cca}}_{\mathsf{ABE},\mathbf{A}}(\lambda, \kappa)$ が λ について無視可能である．

A.2　コミットメントスキーム [7]

コミットメントスキーム CmtSch は三つの多項式時間アルゴリズムから成る：$\mathsf{CmtSch} = (\mathsf{Setup}, \mathsf{Com}, \mathsf{Open})$.

• $\mathsf{Setup}(1^\lambda) \to \mathrm{CK}$．このアルゴリズムは PPT であり，セキュリティパラメータ 1^λ を入力に取り，コミットメント鍵 CK を出力する．

• $\mathsf{Com}(\mathrm{CK}, M; \gamma) \to C$．このアルゴリズムは PPT であり，コミットメント鍵 CK 及びメッセージ M を入力に取り，コミットメント C を出力する．ただし，開封の必要に応じ，用いたランダムネス γ を開封鍵として出力する．

• $\mathsf{Open}(C, \gamma) \to \hat{M}$．このアルゴリズムは確定的であり，コミットメント C 及び開封鍵 γ を入力に取り，開封されたメッセージ $\hat{M}$ を出力する．

CmtSch の満たすべき正当性（correctness）については文献 [7] 等を参照されたい．