Vol.2019-DPS-178 No.33
Vol.2019-CSEC-84 No.33
2019/3/5

リボーク機能を備えた匿名否認可能述語認証スキームの一般的構成の検討

穴田 啓晃[1,a)]　上繁 義史[2,b)]

概要：リボーク機能を備えた匿名否認可能述語認証スキーム rADPA の一般的構成の検討について報告する．アプローチは K.Yamada ら（ESORICS2017）のリボーク可能な属性ベース暗号スキーム RABE を S.Yamada ら（PKC2012）の匿名否認可能述語認証スキーム ADPA に組み込むものである．

キーワード：本人認証，匿名性，否認可能性，リボーク，述語

Towards Generic Construction of Anonymous Deniable Predicate Authentication Schemes with Revocability

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

Abstract: We report our study towards a generic construction of anonymous deniable predicate authentication schemes with revocability. Our approach is to build-in the revocable attribute-based encryption scheme proposed by K.Yamada et al. (ESORICS2017) into the anonymous deniable authentication scheme proposed by S.Yamada et al. (PKC2012).

Keywords: authentication, anonymity, deniability, revocation, predicate

1. はじめに

認証技術はパソコンやスマートデバイスなどへのログオンにおける本人確認に，また，様々な Web サービスにおける権限付与の前段階に適用されている必要不可欠な技術である．後者は認証プロトコルと呼ばれる．2014 年には国内外の多くの企業が参加する FIDO（Fast IDentity Online）アライアンスにて Web 認証プロトコルが標準化され，スマートデバイス上での認証が新段階に入った．2017 年には CEATEC JAPAN2017 においてその実装が展示されるなど，セキュアかつプライバシに配慮した認証プロトコルの要求が高まっている．その背景には，クライアントと認証サーバの間の認証プロトコルが実行されることで，権限付与された Web サービスをクライアントのユーザが利用する状況を認証サーバ側が収集できる問題，そしてこのためにユーザのプライバシ保護が困難になっている懸念がある．

上記の懸念に対し，認証プロトコルに要求される性質の一つに匿名性（anonymity）がある．匿名性は，ユーザのアイデンティティを認証サーバ側が特定できない性質である．匿名性に関わる技術的な解決手法の一つとして匿名認証プロトコルが研究されてきた．

[1] 長崎県立大学情報システム学部情報セキュリティ学科
Department of Information Security, Faculty of Information Systems, 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
[b)] yueshige@nagasaki-u.ac.jp

また，上記の懸念に対し，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，クライアントや認証サーバに残されたデータに関わる性質であり，認証サーバ側が第三者に対し「クライアントは認証を要求した」と主張しても，クライアントのユーザは「認証を私が要求した事実は無い」と否認できる性質である．換言すると，否認可能性はアンチフォレンジックの性質である．

1.1 解決すべき課題

一方，認証プロトコルに要求される必須の機能としてリボーク（revocation）がある．リボークは登録（registration）と対をなす処置であり，アイデンティティ文字列の無効化である．ここで無効化とは，Web サービスを利用する権限を付与しないことを，その前段階である認証において拒否することで実現することを指す．例として，退職した社員のアイデンティティ文字列をリボークすることで，機密データへのアクセス権限を付与せず機密性を守ることができるし，これは重要な処置である．

リボークを実現する方法としてはリボケーションリストを用いる方法が一般的である．これは，リボケーションリストにアイデンティティ文字列が載っているか否かでリボークの状況を判定するものである．ところが，上述のプライバシ保護の観点から匿名性を実現しようとすると，リボーク機能との両立が難しくなる．この背景から，匿名性や否認可能性といったプライバシ保護に望ましい性質を実現しつつリボーク機能をも備えた認証プロトコルを設計することは，研究上も実用上も課題と考えられる．

1.2 貢献と関連研究

本研究報告では，暗号学のアプローチによる上述の課題への取り組みについて報告する．Sahai-Waters[9] により創始された属性ベース暗号スキーム（attribute-based encryption scheme，ABE）や引き続く研究の述語暗号スキーム（predicate encryption scheme，PE，[13] etc.）は，その要件として属性プライバシという性質を備える．これは匿名性を包含するより強い性質である．このため，属性ベース暗号でチャレンジ&レスポンス認証を設計することで匿名性を備えた認証プロトコルを実現できる．

一方，K.Yamada ら [11], [12] が研究発表したリボーク可能な属性ベース暗号スキーム（revocable attribute-based encryption scheme, RABE）は，属性プライバシとリボーク機能を，従って匿名性とリボーク機能を両立する ABE である．この研究 [11], [12] によりリボーク機能と匿名性を備えた認証プロトコルを実現できたことになる．

本研究報告では更に，否認可能性を追究する．S.Yamada ら [13] は匿名否認可能述語認証スキーム（anonymous deniable predicate authentication scheme, ADPA）を研究発表した．この研究に着眼し，本研究報告では RABE を ADPA に組み込むアプローチで，リボーク機能を備えた匿名否認可能述語認証スキーム rADPA を一般的に構成することを検討する．

否認可能性の研究は [2], [3] に遡る．否認可能なリング認証スキーム（deniable ring authentication scheme）[5] や否認可能な認証スキームのマルチトラップドアコミットメントによる構成 [7], [8]，共通参照文字列モデル及びランダムオラクルモデルにおける（不）可能性の研究 [6] などがある．また，アンチフォレンジクスの文脈での研究 [10] もある．

2. 準備

本節では本研究報告で用いる先行研究における諸概念をまとめる．

自然数の集合を $\mathbb{N}$ と記す．$\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ とする．セキュリティパラメータを λ と記す．集合 S に対しその位数を $|S|$ で表す．ストリング s に対しそのビット長を $|s|$ で記す．ビット b の反転ビットを $\bar{b}$ で記す．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．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．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．$|f(k) - g(k)|$ が無視可能であるとき，$f(k) \approx_{\mathrm{c}} g(k)$ と書き，$f(k)$ と $g(k)$ は k について計算量的に識別不可能であるという．

2.1 記法

- $m \in \mathbb{N}$: id が属する集合の位数であり，2 のべき乗である．
- $\mathcal{ID}$: id の属する集合であり，$\mathcal{ID} = \{0,1\}^{\log(m)}$.
- $\mathcal{RL}$: リボークされた id の属する集合である : $\mathcal{RL} \in 2^{\mathcal{ID}}$, $\mathsf{id} \in \mathcal{RL}$ or $\mathsf{id} \notin \mathcal{RL}$．リボケーションリストと呼ばれる．
- $B \in \mathbb{N}$: $\mathcal{RL}$ の位数の上限である : $|\mathcal{RL}| \leq B$.
- κ : 述語を叙述するインデックスであり，或る定数 c が存在し $\kappa = (n_1, \ldots, n_c) \in \mathbb{N}^c$．$\kappa$ は属性集合及び述語関数を指定する．
- $\mathbb{X}^\kappa, \mathbb{Y}^\kappa$: 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．

2.2 リボーク可能な属性ベース暗号スキーム [11], [12]

リボーク可能な属性ベース暗号スキーム RABE 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：RABE = (Setup, Enc, KeyGen, Dec).

• $\mathsf{Setup}(1^\lambda, \kappa) \to (\mathrm{PK}, \mathrm{MSK})$．このアルゴリズムは確率的であり，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確率的であり，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．

• $\mathsf{Enc}((Y, \mathcal{RL}), \mathrm{PK}, M) \to CT$．このアルゴリズムは確率的であり，暗号文属性 Y，リボケーションリスト $\mathcal{RL}$，公開鍵 PK 及び平文 M を入力に取り，暗号文 CT を出力する．

• $\mathsf{Dec}(\mathrm{SK}^X_{\mathsf{id}}, (Y, \mathcal{RL}), \mathrm{PK}, CT) \to \tilde{M}$．このアルゴリズムは確定的であり，プライベート秘密鍵 $\mathrm{SK}^X_{\mathsf{id}}$，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．

RABE の満たすべき正当性（correctness）は ABE の満たすべき正当性として捉えられる．[11], [12] を参照されたい．

アイデンティティ文字列 id がリボークされているか否かは次の述語関数の値で決まる．

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

K.Yamada ら [11], [12] 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．

$$\bar{\mathsf{R}}^\kappa_m((X, \mathsf{id}), (Y, \mathcal{RL})) \stackrel{\mathrm{def}}{=} \begin{cases} 1 \text{ if } \bar{\mathsf{R}}^\kappa_m(X, Y) = 1 \wedge \mathsf{id} \notin \mathcal{RL}, \\ F0 \text{ otherwise.} \end{cases}$$

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．

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

結果，プライベート秘密鍵は SK^X でなく $\mathrm{SK}^X_{\mathsf{id}}$ となる．

2.3 匿名否認可能述語認証スキーム [13]

匿名否認可能述語認証スキーム ADPA は四つの多項式時間アルゴリズムから成る：ADPA = (Setup, KeyGen, P, V).

• $\mathsf{Setup}(1^\lambda, \kappa) \to (\mathrm{PK}, \mathrm{MSK})$．このアルゴリズムは確率的であり，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確率的であり，鍵属性 X，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．

• $\langle \mathsf{P}(\mathrm{SK}^X), \mathsf{V}\rangle(Y, \mathrm{PK}) \to 1/0$．これらの対話アルゴリズムは確率的であり，共通入力として暗号文属性 Y 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 SK^X を入力に取り，ビット 1 もしくは 0 を出力する．

ADPA の満たすべき正当性（correctness），選択暗号文攻撃に対する識別不可能性（IND-CCA）及び暗号文の公開検証可能性（public verifiability）については [13] を参照されたい．

2.4 コミットメントスキーム [1], [4]

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：CmtSch = (Setup, Com, Open).

• $\mathsf{Setup}(1^\lambda) \to \mathrm{CK}$．このアルゴリズムは確率的であり，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確率的であり，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），拘束性（binding property）及び秘匿性（hiding property）については [4] 等の文献を参照されたい．

3. スキームのシンタックス

本節では，本研究報告で提案するリボーク機能を備えた匿名否認可能述語認証スキーム rADPA のシンタックスを定義する．

提案する 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：rADPA = (Setup, KeyGen, P, V).

• $\mathsf{Setup}(1^\lambda, \kappa) \to (\mathrm{PK}, \mathrm{MSK})$．このアルゴリズムは確率的であり，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確率的であり，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確率的であり，共通入力として暗号文属性 Y，リボケーションリスト $\mathcal{RL}$ 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）については本研究報告では省略する．また，先述のとおり，アイデンティティ文字列 id がリボークされているか否かは述語関数 $\mathsf{id} \in_? \mathcal{RL}$ の値で決まる．

4. スキームの安全性定義

本節では，本研究報告で提案するリボーク機能を備えた匿名否認可能述語認証スキーム 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．

4.1 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として捉えられる．本研究報告では，S.Yamada ら [13] 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）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 $\mathbf{A}$ はアルゴリズムである．

$\mathsf{Expr}^{\text{c-sound}}_{\mathsf{rADPA},\mathbf{A}}(1^\lambda, \kappa)$
$(\mathrm{PK}, \mathrm{MSK}) \leftarrow \mathsf{Setup}(1^\lambda, \kappa)$
$((Y^*, \mathcal{RL}^*), St) \leftarrow \mathbf{A}(\mathrm{PK})$
$b \leftarrow \langle \mathbf{A}^{\mathcal{P}_i(\mathrm{SK}^{X_i}_{\mathsf{id}_i})|^{q_\mathrm{p}}_{i=1}, \mathcal{KG}}(St), \mathsf{V}\rangle((Y^*, \mathcal{RL}^*), \mathrm{PK})$
If $b = 0$ 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．

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 $\mathbf{Adv}^{\text{c-sound}}_{\mathsf{rADPA},\mathbf{A}}(\lambda, \kappa)$（$\lambda, \kappa$ の関数）として定義する．

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

定義 1 (同時発生的健全性，Concurrent Soundness) 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，$\mathbf{Adv}^{\text{c-sound}}_{\mathsf{rADPA},\mathbf{A}}(\lambda, \kappa)$ が λ の関数として無視可能であるとき，認証スキーム rADPA は同時発生的健全性を有するという：

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

4.2 匿名性の定義

匿名性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．本研究報告では S.Yamada ら [13] 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．

$\mathsf{Expr}^{\text{anonym}}_{\mathsf{rADPA},\mathbf{A}}(1^\lambda, \kappa)$
$(\mathrm{PK}, \mathrm{MSK}) \leftarrow \mathsf{Setup}(1^\lambda, \kappa)$
$((X^*_0, \mathsf{id}^*_0), (X^*_1, \mathsf{id}^*_1), St) \leftarrow \mathbf{A}(\mathrm{PK}, \mathrm{MSK})$
$\mathrm{SK}^{X^*_0}_{\mathsf{id}^*_0} \leftarrow \mathsf{KeyGen}((X^*_0, \mathsf{id}^*_0), \mathrm{PK}, \mathrm{MSK})$
$\mathrm{SK}^{X^*_1}_{\mathsf{id}^*_1} \leftarrow \mathsf{KeyGen}((X^*_1, \mathsf{id}^*_1), \mathrm{PK}, \mathrm{MSK})$
$((Y^*, \mathcal{RL}^*), St) \leftarrow \mathbf{A}(St)$ such that
$\bar{\mathsf{R}}^\kappa_m((X^*_0, \mathsf{id}^*_0), (Y^*, \mathcal{RL}^*)) = \bar{\mathsf{R}}^\kappa_m((X^*_1, \mathsf{id}^*_1), (Y^*, \mathcal{RL}^*))$
$b \in_R \{0, 1\}, \hat{b} \leftarrow \mathbf{A}^{\mathcal{P}(\mathrm{SK}^{X^*_b}_{\mathsf{id}^*_b})}(St, \mathrm{SK}^{X^*_0}_{\mathsf{id}^*_0}, \mathrm{SK}^{X^*_1}_{\mathsf{id}^*_1})$
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 $\mathsf{P}(\mathrm{SK}^{X^*_b}_{\mathsf{id}^*_b}, (Y^*, \mathcal{RL}^*), \mathrm{PK})$ 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，Anonymity) 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：

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

4.3 否認可能性の定義

否認可能性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．本研究報告では S.Yamada ら [13] 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．

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

定義 3 (否認可能性，Deniability) 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 $(X,\mathsf{id})\in\mathbb{X}\times\mathcal{ID}, (Y,\mathcal{RL})\in\mathbb{Y}\times 2^{\mathcal{ID}}$ such that $\bar{\mathsf{R}}^\kappa_m((X,\mathsf{id}),(Y,\mathcal{RL}))=1$，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，$\Pr[\mathbf{D}(\mathrm{Real}(\lambda,\kappa,m,(X,\mathsf{id}),(Y,\mathcal{RL})))=1]$ と $\Pr[\mathbf{D}(\mathrm{Sim}(\lambda,\kappa,m,(X,\mathsf{id}),(Y,\mathcal{RL})))=1]$ 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：

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

5. スキームの一般的構成及び安全性

本節では，K.Yamada ら [11], [12] の RABE を S.Yamada ら [13] の ADPA に組み込むことによりリボーク機能を備えた匿名否認可能述語認証スキーム rADPA を一般的に構成する．次いで，rADPA の安全性として健全性，匿名性，否認可能性について述べる．

5.1 スキームの一般的構成

リボーク機能を備えた匿名否認可能述語認証スキーム rADPA $=$ (Setup, KeyGen, P, V) の一般的構成を示す（図 1 参照）．

- $\mathsf{Setup}(1^\lambda,\kappa)\to(\mathrm{PK},\mathrm{MSK})$．このアルゴリズムは確率的であり，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，$\mathsf{RABE.Setup}(1^\lambda,\kappa)$ 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．
- $\mathsf{KeyGen}(X,\mathrm{MSK})\to \mathrm{SK}^X$．このアルゴリズムは確率的であり，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，$\mathsf{RABE.KeyGen}((X,\mathsf{id}),\mathrm{MSK})$ 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．
- $\langle \mathsf{P}(\mathrm{SK}^X_{\mathsf{id}}),\mathsf{V}\rangle((Y,\mathcal{RL}),\mathrm{PK})\to 1/0$.
- $\langle \mathsf{P}(\mathrm{SK}^X_{\mathsf{id}}),\mathsf{V}\rangle((Y,\mathcal{RL}),\mathrm{PK})\to 1/0$．これらの対話アルゴリズムは確率的であり，共通入力として暗号文属性 Y，リボケーションリスト $\mathcal{RL}$ 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 [5], [13] を参照されたい．

5.2 スキームの安全性

リボーク機能を備えた匿名否認可能述語認証スキーム rADPA の安全性を以下にまとめる．

定理 1 RABE が選択暗号文安全性及び公開検証可能性を有し，かつ，Com が完全拘束性を有するならば，我々の rADPA は健全性を有する．
（証明は省略する．）

定理 2 RABE が選択暗号文安全性及び公開検証可能性を有するならば，我々の rADPA は匿名性を有する．
（証明は省略する．）

定理 3 RABE が正当性を有し，かつ，Com が計算量的秘匿性を有するならば，我々の rADPA は計算量的否認可能性を有する．
（証明は省略する．）

6. まとめと今後の課題

本研究報告では匿名性，否認可能性といったプライバシ保護に望ましい性質を実現しつつリボーク機能をも備えた認証プロトコルを，暗号学のアプローチで設計した．そのアプローチは RABE を ADPA に組み込むものであり，これによりリボーク機能を備えた匿名否認可能述語認証スキーム rADPA を一般的に構成できることを示した．

しかしながら，提案認証スキーム rADPA は証明者 P と検証者 V の対話のラウンド数が 6 と多い．今後の課題の一つはこのラウンド数の削減にある．また，本研究報告では一般的な構成について検討したのみである．楕円曲線上のペアリング（pairing）による双線形群（bilinear map）を用いた計算効率の良い設定，あるいは，格子（lattice）を用いた耐量子計算機性の期待される設定などで，個別に具体的に設計し効率を追究し，また安全性証明の計算量仮定を比較検討することも今後の課題である．

謝辞 本研究は JSPS 科研費 JP18K11297 の助成を受けたものです．

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

図 1 提案方式：リボーク機能を備えた匿名否認可能述語認証スキーム rADPA.

参考文献

[1] G. Brassard, D. Chaum, and C. Crépeau.
Minimum disclosure proofs of knowledge.
J. Comput. Syst. Sci., 37(2):156–189, 1988.

[2] C. Dwork, M. Naor, and A. Sahai.
Concurrent zero-knowledge.
In *Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing, Dallas, Texas, USA, May 23-26, 1998*, pages 409–418, 1998.

[3] C. Dwork, M. Naor, and A. Sahai.
Concurrent zero-knowledge.
J. ACM, 51(6):851–898, 2004.

[4] O. Goldreich.
The Foundations of Cryptography - Volume 1, Basic Techniques.
Cambridge University Press, 2001.

[5] 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.

[6] R. Pass.
On deniability in the common reference string and random oracle model.
In *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, pages 316–337, 2003.

[7] M. D. Raimondo and R. Gennaro.
New approaches for deniable authentication.
In *Proceedings of the 12th ACM Conference on Computer and Communications Security, CCS 2005, Alexandria, VA, USA, November 7-11, 2005*, pages 112–121, 2005.

[8] M. D. Raimondo and R. Gennaro.
New approaches for deniable authentication.
J. Cryptology, 22(4):572–615, 2009.

[9] A. Sahai and B. Waters.
Fuzzy identity-based encryption.
In *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*, pages 457–473, 2005.

[10] Y. Ueshige and K. Sakurai.

Analysis of "receipt-freeness" and "coercion-resistance" in biometric authentication protocols.
In *30th IEEE International Conference on Advanced Information Networking and Applications, AINA 2016, Crans-Montana, Switzerland, 23-25 March, 2016*, pages 769–775, 2016.

[11] 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.

[12] 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.

[13] 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.