Computer Security Symposium 2018
22 - 25 October 2018

BundleされたWitness SpacesにΣプロトコルによるWitness-Indistinguishable Argumentsとそのグローバル IDへの適用

穴田 啓晃[1]　有田 正剛[2]

概要：本稿で我々は commit-and-prove タイプの Σ プロトコルの或る一般的構成を与える．提案 Σ プロトコルは共通の commitment を含む statements についての要素 Σ プロトコルの AND 合成である．提案 Σ プロトコルは base witness point と呼ぶ共通の要素を有する witnesses の束（bundle）を証明者が知っていることを証明者が検証者に納得させる．要素 Σ プロトコルが witness-indistinguishable な argument system であるとき，提案 Σ プロトコルは全体として witness-indistinguishable な argument system である．適用例として，分散型多権限機関匿名認証スキームの一般的構成を提案する．提案スキームにおいて，witness は共通のグローバル ID ストリングとその上のデジタル署名から成る各 witness の bundle である．提案スキームの実例を双線形群の設定において与える．

キーワード：対話証明，シグマプロトコル，証拠識別不可能性，分散型，結託耐性

Witness-Indistinguishable Arguments with Sigma-Protocols for Bundled Witness Spaces and its Application to Global Identities

Hiroaki Anada[1]　Seiko Arita[2]

Abstract: We propose a generic construction of a Σ-protocol of commit-and-prove type, which is an AND-composition of Σ-protocols on the statements that include a common commitment. In our protocol a prover convinces a verifier that the prover knows a bundle of witnesses that have a common component which we call a base witness point. When the component Σ-protocols are of witness-indistinguishable argument systems, our Σ-protocol is also a witness-indistinguishable argument system as a whole. As an application, we propose a generic construction of a decentralized multi-authority anonymous authentication scheme. There a witness is a bundle of witnesses each of which consists of a common global identity string and a digital signature on it. We show an instantiation of the generic scheme in the setting of bilinear groups.

Keywords: interactive proof, sigma protocol, witness indistinguishability, decentralized, collusion resistance

1. はじめに

パスポート番号や各国の社会保障番号等のようなグローバル ID は，本人確認のために現在よく用いられている．それらの番号は政府が本人確認するためのみならず，商用利用の目的でも用いられる．すなわち，私たちが商用サービスを利用する際，サービスを管理運営する権限機関に対し属性証明書の発行を参加登録段階において依頼する．その段階においては，権限機関は私たちが本人であることをそれらのグローバル ID によって確認する．属性証明書が

[1] 長崎県立大学 情報セキュリティ学科
Department of Information Security, University of Nagasaki
[2] 情報セキュリティ大学院大学 情報セキュリティ研究科
Graduate School of Information Security, Institute of Information Security

一旦確認されると，サービス利用時の認証段階において受理されるようになる．こうしてグローバル ID ストリングは私たちが属性証明書を発行してもらえるよう機能する．

近年，多要素認証認証スキームが誤認証を防ぐ目的でよく用いられていることに着眼すると，それらのスキームにおいてサービスのユーザは幾つかの分離したエビデンスを提示した後においてのみアクセスを許可される．実際，サービスプロバイダによってインターネットに接続されたノート PC 及び携帯電話業者によって通信可能となったスマートフォンの両方を用いた二要素認証はよく普及しつつある．このように，私たちが認証されサービスの利益を享受するため，独立な複数の権限機関を巻き込む認証の複合モデルが存在する．

プライバシー保護は特に近年，認証において追及されるべき機能である．というのも，インターネット・オブ・シングズの成長及びこれに関連するビッグデータの解析が，巻き込まれるユーザに対しプライバシー保護をより深刻にしているからである．この背景から，ID ストリングとパスワードの認証の枠組みは，認証時に匿名性が保証された枠組みへと進化すべきである．例として，スマート家電が（エコなエアーコンディショニングや練られた調理レシピのような）有益な提案を求めるクエリとして住居の状況についてのレポートをインターネットを介して送信する際，ID 情報があるべき場合と不要な場合がある．別の例として，インターネットに接続されたコネクテッド・カーが局所的な道路交通情報システムや旅行者の web スケジューラ等の複数のサービスの組み合わせを利用する時は，ID 情報は，たとえ参加登録段階においてメンバーシップが必要とされるとしても，漏洩すべきではない．後者の例では，ユーザはサービスプロバイダらによって同時に匿名の内に認証されるべきである．しかしながら，このような匿名認証スキームには結託攻撃という脅威があることが知られている [13]．狡猾なユーザは，異なる属性に対する属性鍵を異なる ID のユーザから収集し，寄せ集めた鍵を用い匿名の内に検証者に受理させようとする．この結託攻撃の観点では正に匿名性こそが深刻な潜在的欠陥となる．

1.1 先行研究との関連と本稿の貢献

分散型多権限機関属性ベース署名スキーム（a decentralized multi-authority attribute-based signature scheme, DMA-ABS）[14] は，属性ベース署名スキームであり分散された鍵発行機関を備えたスキームである．属性ベース署名スキームにおいて署名者は属性鍵を持つ．署名者は，属性を AND/OR/NOT ゲートで結合したブール式，すなわち署名ポリシー，を備えたメッセージに対し署名することができる．そのブール式には複数のアサインメント・パタンがありうる．属性ベース署名スキームの属性プライバシーとは，ある一人のユーザによって生成された署名たちが，そのユーザが用いたアサインメント・パタンについての情報を何ら漏洩しない性質である．この性質はまた（ID 情報についての）匿名性をも要求していることは留意すべきである．属性ベース署名スキームの設計においては，この属性プライバシーと結託耐性の両方を満足することが要所である．他方，分散型多権限機関を許容することは，異なる属性についての属性鍵を発行する独立な鍵発行機関を備えたスキームとすることである．

本稿で適用例として提案する分散型多権限機関匿名認証スキームの一般的構成は，Fiat-Shamir 変換 [10] を適用し，また OR-proof の monotone 論理式への一般化 [6] を適用することで，分散型多権限機関属性ベース署名スキームとなる．その特徴は，双線形写像の設定における実例において，代表的な先行研究である [14] 等と比較しより短い署名長となることが期待される点にある．ただし存在的偽造不可の確率の公平な評価に留意すべきである．（この評価は今後の課題である．）

本稿では，提案プロトコルの一般的構成及び提案スキームの一般的構成についての詳細を省略する．省略した事項については International Association for Cryptologic Research Cryptology ePrint Archive 2018/742 [2]（以下 ePrint[2] と略）を参照されたい．従って，本稿の貢献は概要の直観的説明を試みる点にある．なお，本稿は国内の研究会・シンポジウムの技報・予稿論文 [20][19][1][18][15][17][16] に関連し，それらの研究の延長線上にある．

2. 準備

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 x に対しそのビット長を $|x|$ で記す．集合 S からの元 a の一様ランダムサンプリングを $a \in_R S$ と記す．アルゴリズム A が a を入力とし z を出力することを $z \leftarrow A(a)$ もしくは $A(a) \to z$ 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．アルゴリズム A が a を，アルゴリズム B が b を入力とし対話し（すなわち A，B は対話型チューリング機械），B が z を出力することを $z \leftarrow \langle A(a), B(b)\rangle$ 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．アルゴリズム A が n 個のオラクル $\mathcal{O}_1, \ldots, \mathcal{O}_n$ に同時発生的にアクセスすることを $\mathbf{A}^{\mathcal{O}_i|_{i=1}^n}$ と記す．表現 $a =_? b$ は，$a = b$ のときブール値 1(TRUE) を，そうでないとき 0(FALSE) を返すものとする．

事象 E が生起する確率を Pr[E] と記す．確率変数 X の確率分布を $dist\big(X\big)$ と記す．確率変数 X であってその確率が確率変数 $X, Y_1, \ldots, Y_n$ の結合確率で与えられるものの確率分布を $dist\big(X|X, Y_1, \ldots, Y_n\big)$ と記す．

関数 $f(\lambda)$ が λ について negligible であるとは，λ の任意の正値多項式 poly(λ) に対しある定数 λ_0 が存在し，$\lambda > \lambda_0$

ならば $|f(\lambda)|$ が $\mathrm{poly}(\lambda)$ の逆数で上から押さえられるときにいう（i.e. $|f(\lambda)| < 1/\mathrm{poly}(\lambda)$）．

2.1 対話型 Argument システム，Σ プロトコル，Witness-Indistinguishability

対話型証明システム [3][12] を $\Pi = (\Pi.\mathtt{Setup}, \mathtt{P}, \mathtt{V})$ と記す．$\Pi.\mathtt{Setup}$ は public parameter values の組 $\mathtt{PP}$ を生成するアルゴリズムである．$\mathtt{P}$ 及び $\mathtt{V}$ は対話型アルゴリズム（対話型チューリング機械）であり，それぞれ証明者及び検証者と呼ばれる．証明すべき statement x 及びその witness w は述語 Φ により $R \stackrel{\mathrm{def}}{=} \{(x,w) \in (\{0,1\}^*)^2 | \Phi(x,w) = \mathrm{TRUE}\}$. と定められるものとする．関係 R は NP 関係とする．本稿では，$\mathtt{V}$ のみならず $\mathtt{P}$ もまた確率的多項式時間（probabilistic polynomial-time, PPT）である，すなわち対話型 argument システムを考えるものとする．

2.1.1 Σ プロトコル

Σ プロトコルに現れる六つの PPT アルゴリズムを，本稿では $\Sigma = (\Sigma_{\mathrm{com}}, \Sigma_{\mathrm{cha}}, \Sigma_{\mathrm{res}}, \Sigma_{\mathrm{vrf}}, \Sigma_{\mathrm{ext}}, \Sigma_{\mathrm{sim}})$ と記す．それぞれ commitment, challenge, response 生成アルゴリズム，verification アルゴリズム，knowledge extraction アルゴリズム及び simulator アルゴリズムである．Σ プロトコルは三つの性質：compleneness, special soundness, honest-verifier zero-knowledge を満たさなければならない．定義は文献 [5], [7] 及び ePrint[2] を参照されたい．

2.1.2 Witness-Indistinguishability

本稿では perfect witness indistinguishability のみを扱う．すなわち：

Perfect Witness Indistinguishability For any PPT algorithm $\mathtt{V}^*$, any sequences of witnesses $\mathbf{w} = (w_x)_{x \in L}$ and $\mathbf{w}' = (w'_x)_{x \in L}$ s.t. $w_x, w'_x \in W(x)$, any string $x \in L$ and any string $z \in \{0,1\}^*$, the two distributions $dist\big(x, z, transc\langle \mathtt{P}(x, w_x), \mathtt{V}^*(x,z)\rangle\big)$ and $dist\big(x, z, transc\langle \mathtt{P}(x, w'_x), \mathtt{V}^*(x,z)\rangle\big)$ are identical. 詳細は文献 [9], [11] を及び ePrint[2] 参照されたい．

2.2 Commit-and-Prove スキーム

Commit-and-prove スキーム $\mathtt{CmtPrv}$ は五つの PPT アルゴリズム $\mathtt{CmtPrv} = (\mathtt{CmtPrv.Setup}, \mathtt{Cmt} = (\mathtt{Cmt.Com}, \mathtt{Cmt.Vrf}), \Pi = (\mathtt{P}, \mathtt{V}))$. から成るものとする．それぞれ次の入出力とする．

- $\mathtt{CmtPrv.Setup}(1^\lambda) \to \mathtt{PP}$.
- $\mathtt{Cmt.Com}(\mathtt{PP}, m) \to (c, \kappa)$．$m$ はメッセージ，c は commitment，κ は opening key.
- $\mathtt{Cmt.Vrf}(\mathtt{PP}, c, m, \kappa) \to d$．$d$ は boolean decision.

本稿では次の述語 $\Phi_{\mathtt{PP}}$ を考える．

$$\Phi_{\mathtt{PP}}(c, (m, \kappa)) \stackrel{\mathrm{def}}{=} (\mathtt{Cmt.Vrf}(\mathtt{PP}, c, m, \kappa)). \qquad (1)$$

本稿では次の関係 R に対する対話型 argument システム $\Pi = (\mathtt{P}, \mathtt{V})$ を考える．

$$R := \{(c, (m, \kappa)) \in \{0,1\}^* \times (\{0,1\}^*)^2 \mid \Phi_{\mathtt{PP}}(c, (m, \kappa)) = \mathrm{TRUE}\}. \qquad (2)$$

本稿では Commitment スキーム $\mathtt{Cmt}$ について次の二つの性質を扱う．すなわち：

Perfectly Hiding For any security parameter 1^λ, any set of public parameter values $\mathtt{PP}$ and any two messages $m, m' \in \mathcal{M}sg(1^\lambda)$, the two distributions $dist\big(c \mid (c, \kappa) \leftarrow \mathtt{Cmt.Com}(\mathtt{PP}, m)\big)$ and $dist\big(c \mid (c, \kappa) \leftarrow \mathtt{Cmt.Com}(\mathtt{PP}, m')\big)$ are identical.

Computationally Binding The attack of breaking binding property of $\mathtt{Cmt}$ by an algorithm $\mathbf{A}$ is defined by the following experiment.

$\mathbf{Exp}^{\mathrm{bind}}_{\mathtt{Cmt},\mathbf{A}}(1^\lambda)$:

$\mathtt{PP} \leftarrow \mathtt{CmtPrv.Setup}(1^\lambda)$

$(c, m, \kappa, m', \kappa') \leftarrow \mathbf{A}(\mathtt{PP})$

If $\mathtt{Cmt.Vrf}(\mathtt{PP}, c, m, \kappa) = \mathtt{Cmt.Vrf}(\mathtt{PP}, c, m', \kappa') = 1$

$\wedge\, m \neq m'$, then Return Win else Return Lose

The advantage of $\mathbf{A}$ over $\mathtt{Cmt}$ is defined as $\mathbf{Adv}^{\mathrm{bind}}_{\mathtt{Cmt},\mathbf{A}}(\lambda) := \Pr[\mathbf{Exp}^{\mathrm{bind}}_{\mathtt{Cmt},\mathbf{A}}(1^\lambda)$ returns Win$]$. The commitment scheme $\mathtt{Cmt}$ is said to be *computationally binding* if for any set of public parameter values $\mathtt{PP}$ and any PPT algorithm $\mathbf{A}$, the advantage $\mathbf{Adv}^{\mathrm{bind}}_{\mathtt{Cmt},\mathbf{A}}(\lambda)$ is negligible in λ.

本稿では，ランダムネス $r \in \{0,1\}^\lambda$ が commitment c を生成するのに用いられるものとする．従って，opening key κ は $\kappa := r$．すなわち，$\mathtt{Cmt.Com}(\mathtt{PP}, m; r) \to (c, r)$.

詳細は文献 [4], [8] 等及び ePrint[2] 参照されたい．

2.3 デジタル署名スキーム

デジタル署名スキーム $\mathtt{Sig}$ は四つの PPT アルゴリズム $\mathtt{Sig} = (\mathtt{Sig.Setup}, \mathtt{Sig.KG}, \mathtt{Sig.Sign}, \mathtt{Sig.Vrf})$ から成るものとする．それぞれ次の入出力とする．

- $\mathtt{Sig.Setup}(1^\lambda) \to \mathtt{PP}$.
- $\mathtt{Sig.KG}(\mathtt{PP}) \to (\mathrm{PK}, \mathrm{SK})$．PK は公開鍵，SK は秘密鍵.
- $\mathtt{Sig.Sign}(\mathtt{PP}, \mathrm{PK}, \mathrm{SK}, m) \to \sigma$．$m$ はメッセージ，σ はデジタル署名.
- $\mathtt{Sig.Vrf}(\mathtt{PP}, \mathrm{PK}, m, \sigma) \to d$．$d$ は boolean decision.

存在的偽造不可（EUF-CMA）の定義は次の experiment による：

$\mathbf{Exp}^{\text{euf-cma}}_{\mathtt{Sig},\mathbf{F}}(1^\lambda)$:

$\mathtt{PP} \leftarrow \mathtt{Sig.Setup}(1^\lambda), (\mathrm{PK}, \mathrm{SK}) \leftarrow \mathtt{Sig.KG}(\mathtt{PP})$,

$(m^*, \sigma^*) \leftarrow \mathbf{F}^{\mathbf{SignO}(\mathtt{PP}, \mathrm{PK}, \mathrm{SK}, \cdot)}(\mathtt{PP}, \mathrm{PK})$

If $m^* \notin \{m_j\}_{1 \le j \le q_{\mathrm{s}}}$ and $\mathtt{Sig.Vrf}(\mathrm{PK}, m^*, \sigma^*) = 1$,

then Return Win else Return Lose

The advantage of $\mathbf{F}$ over $\mathtt{Sig}$ is defined as $\mathbf{Adv}^{\text{euf-cma}}_{\mathtt{Sig},\mathbf{F}}(\lambda) := \Pr[\mathbf{Exp}^{\text{euf-cma}}_{\mathtt{Sig},\mathbf{F}}(1^\lambda) \text{ returns } \textsc{Win}]$. The digital signature scheme $\mathtt{Sig}$ is said to be *existentially unforgeable against adaptive chosen-message attacks* if for any given PPT algorithm $\mathbf{F}$, the advantage $\mathbf{Adv}^{\text{euf-cma}}_{\mathtt{Sig},\mathbf{F}}(\lambda)$ is negligible in λ.

詳細は文献 [10] 等及び ePrint[2] 参照されたい.

3. Bundle された Witness Spaces に対する Σ プロトコルによる Witness-Indistinguishable Argument システム

本節では，要素技術と提案プロトコルの概要を示す．詳細は ePrint[2] を参照されたい.

3.1 要素技術

提案プロトコルは二つの要素技術から成る.

3.1.1 Σ プロトコルを伴う対話型 Argument システム

For a polynomially bounded integer n, let A be the set of indices: $A := \{1, \ldots, n\}$. We start with an efficiently computable predicate $\Phi^a_{\mathtt{PP}}$ for each index $a \in A$, which determines an NP witness relation R^a:

$$R^a = \{(x^a, w^a) \in \{0,1\}^* \times \{0,1\}^* \mid \Phi^a_{\mathtt{PP}}(x^a, w^a) = \text{TRUE}\}. \tag{3}$$

We suppose for each $a \in A$ that there is an interactive argument system $\Pi^a = (\Pi.\mathtt{Setup}, \mathtt{P}^a, \mathtt{V}^a)$ which is executed in accordance with a Σ-protocol for the relation R^a:

$$\Sigma^a = (\Sigma^a_{\text{com}}, \Sigma^a_{\text{cha}}, \Sigma^a_{\text{res}}, \Sigma^a_{\text{vrf}}, \Sigma^a_{\text{ext}}, \Sigma^a_{\text{sim}}). \tag{4}$$

We suppose further that the witness space W^a decomposes into two components $W^a = W^a_0 \times W^a_1$ for each $a \in A$. *In this paper, our interest is in the case that all the 0th components $W^a_0, a \in A$, are equal, which we denote by W_0.* We call the equal set W_0 the *base witness space* of the witness spaces $W^a, a \in A$, and an element $w_0 \in W_0$ a *base witness point*. Then a witness $w^a \in W^a$ consists of w_0 and w^a_1. That is,

$$\begin{array}{ccc} W^a & = & W_0 \times W^a_1, \\ \cup & & \cup \\ w^a & = & (w_0, w^a_1). \end{array}$$

3.1.2 Σ プロトコルを伴う Commit-and-Prove スキーム

To construct an interactive argument system for the relations $(R^a)^{a\in A}$ with the base witness space W_0, we employ a commit-and-prove scheme with a Σ-protocol: $\mathtt{CmtPrv} = (\mathtt{CmtPrv}.\mathtt{Setup}, \mathtt{Cmt} = (\mathtt{Cmt.Com}, \mathtt{Cmt.Vrf}), \Pi_0 = (\mathtt{P}_0, \mathtt{V}_0))$, where the predicate $\Phi_{0,\mathtt{PP}}$ and the relation R_0 is defined as follows, and Π_0 is executed in accordance with a Σ-protocol Σ_0:

$$\Phi_{0,\mathtt{PP}}(c_0, (w_0, r_0)) \stackrel{\text{def}}{=} (\mathtt{Cmt.Com}(\mathtt{PP}_0, w_0; r_0) =_? (c_0, r_0)),$$

$$R_0 \stackrel{\text{def}}{=} \{(c_0, (w_0, r_0)) \in \{0,1\}^* \times (\{0,1\}^*)^2 \mid \Phi_{0,\mathtt{PP}}(c_0, (w_0, r_0)) = \text{TRUE}\}, \tag{5}$$

$$\Sigma_0 = (\Sigma_{0,\text{com}}, \Sigma_{0,\text{cha}}, \Sigma_{0,\text{res}}, \Sigma_{0,\text{vrf}}, \Sigma_{0,\text{ext}}, \Sigma_{0,\text{sim}}). \tag{6}$$

Note that a message m to be committed is a base witness point w_0.

3.2 二つの述語を同時に満足する関係に対する Σ プロトコルの構成について

上記の二つの要素技術を基に，各 index $a \in A$ について次の関係 R^a_0 を考える：

$$R^a_0 := \Big\{(x^a_0 = (x^a, c_0), w^a_0 = (w_0, w^a_1, r_0)) \Big| \begin{cases} \Phi^a_{\mathtt{PP}}(x^a, (w_0, w^a_1)) = \text{TRUE} \\ \Phi_{0,\mathtt{PP}}(c_0, (w_0, r_0)) = \text{TRUE} \end{cases}\Big\}. \tag{7}$$

ここで，二つの Σ プロトコル Σ^a 及び Σ_0 が一つの Σ プロトコル Σ^a_0 にまとめられることを要求する．Σ^a_0 は上記の関係 R^a_0 に対する対話型 argument システム $\Pi^a_0 = (\Pi.\mathtt{Setup}, \mathtt{CmtPrv.Setup}, \mathtt{P}^a_0, \mathtt{V}^a_0)$ についてのものであるべきである:

$$\Sigma^a_0 = (\Sigma^a_{0,\text{com}}, \Sigma^a_{0,\text{cha}}, \Sigma^a_{0,\text{res}}, \Sigma^a_{0,\text{vrf}}, \Sigma^a_{0,\text{ext}}, \Sigma^a_{0,\text{sim}}). \tag{8}$$

要所は $\Sigma^a_{0,\text{com}}$ 及び $\Sigma^a_{0,\text{res}}$ を構成することであり，構成できるかどうかは自明でない．本稿のアプローチは，実例（instantiation）を作る際，その実例に即し具体的に $\Sigma^a_{0,\text{com}}$ 及び $\Sigma^a_{0,\text{res}}$ を構成するものである．詳細は ePrint[2] 参照されたい.

3.3 Bundle された Witness Spaces

Bundle された関係を次のように考える.[*1]

$$R^{a\in A}_{\text{bnd}} \stackrel{\text{def}}{=} \{\big((x^a)^{a\in A}, w_0, (w^a_1)^{a\in A}\big) \mid (x^a, (w_0, w^a_1)) \in R^a, a \in A\} \tag{9}$$

$$\simeq \bigcup_{w_0 \in W_0} \Big(\prod_{a\in A} R^a_{w_0}\Big). \tag{10}$$

ただし，$a \in A$ について $R^a_{w_0}$ は base witness point w_0 で parametrize された関係である：

$$R^a_{w_0} := \{(x^a, w^a) \in R^a \mid \exists w^a_1, w^a = (w_0, w^a_1)\}. \tag{11}$$

[*1] なお，「bundle された」と呼んでいる理由は，a witness が共通のストリングと残りのストリングから成る各 witness の束（bundle）だからである．また，集合としての同型 (10) から，base witness space W_0 の上にそれ以外の空間が parametrize されてあるからでもある.

本稿では次の関係や witness spaces についての対話型 argument システムを構成する．

Definition1 (Bundle された関係) For a polynomially bounded integer n, an NP witness relation for the bundled witness spaces is defined as $R_{\mathrm{bnd}}^{a\in A}$.

Definition2 (Bundle された Witness Spaces) For a polynomially bounded integer n, let A be the set of indices $\{1,\ldots,n\}$. Let $R^a, a \in A$ be NP witness relations where each witness space decomposes $W^a = W_0 \times W_1^a, a \in A$. Then the bundled witness space is defined as follows.

$$W_{\mathrm{bnd}}^{a\in A} \stackrel{\mathrm{def}}{=} W_0 \times (W_1^a)^{a\in A}. \tag{12}$$

3.4 Bundle された Witness Spaces に対する Σ プロトコルの一般的構成

上記の Σ プロトコル $(\Sigma_0^a)^{a\in A}$ 及び commitment 生成アルゴリズム Cmt.Com から，bundle された関係 $R_{\mathrm{bnd}}^{a\in A}$ に対する対話型 argument システム $\Pi_{\mathrm{bnd}}^{a\in A} = (\mathtt{P}, \mathtt{V})$ を構成する．$\Pi_{\mathrm{bnd}}^{a\in A}$ についての提案プロトコル $\Sigma_{\mathrm{bnd}}^{a\in A}$ の構成を Fig.1 に示す．$\Sigma_{\mathrm{bnd}}^{a\in A}$ は六つのアルゴリズムから成る：

$$\Sigma_{\mathrm{bnd}}^{a\in A} = (\Sigma_{\mathrm{bnd,com}}^{a\in A}, \Sigma_{\mathrm{bnd,cha}}^{a\in A}, \Sigma_{\mathrm{bnd,res}}^{a\in A}, \Sigma_{\mathrm{bnd,vrf}}^{a\in A}, \Sigma_{\mathrm{bnd,ext}}^{a\in A}, \Sigma_{\mathrm{bnd,sim}}^{a\in A}). \tag{13}$$

実際，$\Sigma_{\mathrm{bnd}}^{a\in A}$ は 3-move public coin プロトコルであり，Σ プロトコルである．これを示すための要所は knowledge extraction アルゴリズムの構成と証明にある．詳細は ePrint[2] を参照されたい．結果のみをまとめると，次の定理となる．

Theorem1 If Cmt is correct, computationally binding and perfectly hiding, and if Σ_0^a is a Σ-protocol for $a \in A$, then our protocol $\Sigma_{\mathrm{bnd}}^{a\in A}$ is a Σ-protocol.

Theorem2 If the component interactive proof system Π_0^a with Σ_0^a is perfectly witness-indistinguishable for each $a \in A$, and if Cmt is perfectly hiding, then our interactive argument system $\Pi_{\mathrm{bnd}}^{a\in A}$ with $\Sigma_{\mathrm{bnd}}^{a\in A}$ is perfectly witness-indistinguishable.

4. 分散型多権限機関匿名認証スキーム

本節では，提案スキームの概要を示す．詳細は ePrint[2] を参照されたい．

4.1 分散型多権限機関匿名認証スキームのシンタックスと安全性定義

分散型多権限機関匿名認証スキーム（decentralized multi-authority anonymous authentication scheme, DMA-AAUTH）a-auth は五つの PPT アルゴリズムから成る：(Setup, AuthKG, PrivKG, P, V)．

- $\mathtt{Setup}(1^\lambda) \to \mathtt{PP}$.
- $\mathtt{AuthKG}(\mathtt{PP}, a) \to (\mathrm{PK}^a, \mathrm{MSK}^a)$．$a \in A$ は権限機関を指定する index，PK^a は公開鍵，MSK^a はマスター秘密鍵．
- $\mathtt{PrivKG}(\mathtt{PP}, \mathrm{PK}^a, \mathrm{MSK}^a, \mathtt{gid}) \to \mathrm{sk}_{\mathtt{gid}}^a$．$\mathrm{sk}_{\mathtt{gid}}^a$ はグローバル ID ストリング gid の属性鍵．
- $\langle \mathtt{P}(\mathtt{PP}, (\mathrm{PK}^a, \mathrm{sk}_{\mathtt{gid}}^a)^{a\in A'}), \mathtt{V}(\mathtt{PP}, (\mathrm{PK}^a)^{a\in A'})\rangle \to d$.

安全性定義は誤認証（misauthentication）及び匿名性（anonimity）から成る．定義を experiments により示す．

Security against Concurrent and Collusion Attack of Misauthentication

$\mathbf{Expr}_{\mathtt{a\text{-}auth},\mathbf{A}}^{\text{conc-coll}}(1^\lambda)$:

$q_A \leftarrow \mathbf{A}(1^\lambda), A := \{1,\ldots,q_A\}$

$\mathtt{PP} \leftarrow \mathtt{Setup}(1^\lambda)$

For $a \in A$: $(\mathrm{PK}^a, \mathrm{MSK}^a) \leftarrow \mathtt{AuthKG}(\mathtt{PP}, a)$

$q_I \leftarrow \mathbf{A}(\mathtt{PP}, (\mathrm{PK}^a)^{a\in A}), I := \{1,\ldots,q_I\}$

For $i \in I$: $\mathtt{gid}_i \in_R \{0,1\}^\lambda$

For $a \in A$: For $i \in I$:

$\mathrm{sk}_{\mathtt{gid}_i}^a \leftarrow \mathtt{PrivKG}(\mathtt{PP}, \mathrm{PK}^a, \mathrm{MSK}^a, \mathtt{gid}_i)$

$(A^*, St^*) \leftarrow$

$\mathbf{A}^{\mathtt{P}(\mathtt{PP},(\mathrm{PK}^a,\mathrm{sk}_{\mathtt{gid}_i}^a)^{a\in A})|_{i\in I}, \mathbf{PrivKO}(\mathtt{PP},\mathrm{PK}^\cdot,\mathrm{MSK}^\cdot,\cdot)}(\mathtt{PP}, (\mathrm{PK}^a)^{a\in A})$

$\langle \mathbf{A}(St^*), \mathtt{V}(\mathtt{PP}, (\mathrm{PK}^a)^{a\in A^*})\rangle \to d$

If $d = 1$ then Return Win else Return Lose

The advantage of an adversary $\mathbf{A}$ over our authentication scheme a-auth in the experiment is defined as: $\mathbf{Adv}_{\mathtt{a\text{-}auth},\mathbf{A}}^{\text{conc-coll}}(\lambda) \stackrel{\mathrm{def}}{=} \Pr[\mathbf{Expr}_{\mathtt{a\text{-}auth},\mathbf{A}}^{\text{conc-coll}}(1^\lambda) = \text{Win}]$. An authentication scheme a-auth is called secure against concurrent and collusion attacks of misauthentication if, for any given PPT algorithm $\mathbf{A}$, the advantage $\mathbf{Adv}_{\mathtt{a\text{-}auth},\mathbf{A}}^{\text{conc-coll}}(\lambda)$ is negligible in λ.

Anonymity

$\mathbf{Expr}_{\mathtt{a\text{-}auth},\mathbf{A}}^{\text{ano}}(1^\lambda)$:

$q_A \leftarrow \mathbf{A}(1^\lambda), A := \{1,\ldots,q_A\}$

$\mathtt{PP} \leftarrow \mathtt{Setup}(1^\lambda)$

For $a \in A$: $(\mathrm{PK}^a, \mathrm{MSK}^a) \leftarrow \mathtt{AuthKG}(\mathtt{PP}, a)$

$\mathtt{gid}_0, \mathtt{gid}_1 \leftarrow \mathbf{A}(\mathtt{PP}, (\mathrm{PK}^a)^{a\in A})$

For $a \in A$: For $i \in 0, 1$:

$\mathrm{sk}_{\mathtt{gid}_i}^a \leftarrow \mathtt{PrivKG}(\mathtt{PP}, \mathrm{PK}^a, \mathrm{MSK}^a, \mathtt{gid}_i)$

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

$b^* \leftarrow \mathbf{A}^{\mathtt{P}(\mathtt{PP},(\mathrm{PK}^a,\mathrm{sk}_{\mathtt{gid}_b}^a)^{a\in A})}(\mathtt{PP}, (\mathrm{PK}^a, \mathrm{sk}_{\mathtt{gid}_0}^a, \mathrm{sk}_{\mathtt{gid}_1}^a)^{a\in A})$

If $b = b^*$, then Return Win, else Return Lose

The advantage of an adversary $\mathbf{A}$ over our authentication scheme a-auth in the experiment is defined

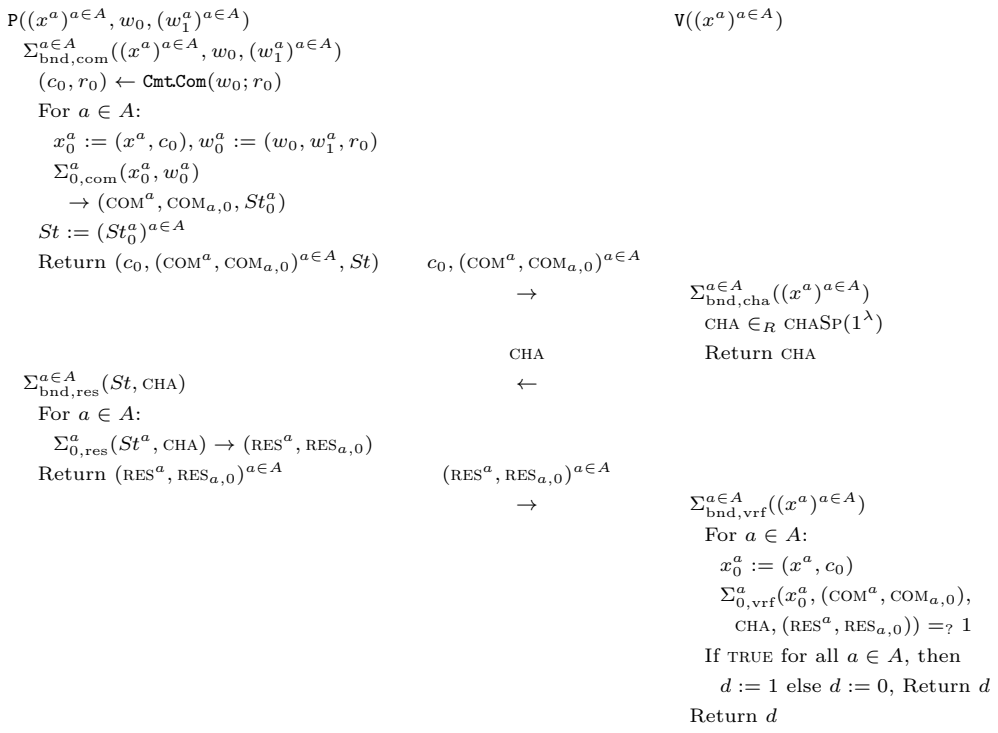

図 1 The protocol $\Sigma^{a\in A}_{\mathrm{bnd}}$ of our proof system $\Pi^{a\in A}_{\mathrm{bnd}}$ for the NP witness relation $R^{a\in A}_{\mathrm{bnd}}$.

as: $\mathbf{Adv}^{\mathrm{ano}}_{\mathtt{a\text{-}auth},\mathbf{A}}(\lambda) \stackrel{\mathrm{def}}{=} \left|\Pr[\mathbf{Expr}^{\mathrm{ano}}_{\mathtt{a\text{-}auth},\mathbf{A}}(1^\lambda) = \mathrm{WIN}] - (1/2)\right|$. An authentication scheme a-auth is called to have anonymity if, for any PPT algorithm $\mathbf{A}$, the advantage $\mathbf{Adv}^{\mathrm{ano}}_{\mathtt{a\text{-}auth},\mathbf{A}}(\lambda)$ is negligible in λ.

4.2 提案スキーム

提案スキーム a-auth の一般的構成を Fig. 2 に示す．提案スキームにおいて，witness は共通のグローバル ID ストリングとその上のデジタル署名から成る各 witness の bundle である．

4.3 安全性

提案スキーム a-auth の安全性を次の定理にまとめる．

Theorem3 If the component proof system Π^a_0 is perfectly witness-indistinguishable for each $a \in A$, if the commitment scheme Cmt is perfectly hiding and computationally binding, and if the digital signature scheme Sig is existentially unforgeable against adaptive chosen-message attacks, then our a-auth is secure against concurrent and collusion attacks. More precisely, let q_A denote the maximum number of authorities. For any given PPT algorithm $\mathbf{A}$ that executes a concurrent and collusion attack on our a-auth in accordance with the experiment $\mathbf{Expr}^{\mathrm{conc\text{-}coll}}_{\mathtt{a\text{-}auth},\mathbf{A}}(1^\lambda)$, there exists a PPT algorithm $\mathbf{F}$ that generates an existential forgery on Sig in accordance with the experiment $\mathbf{Exp}^{\mathrm{euf\text{-}cma}}_{\mathtt{Sig},\mathbf{F}}(1^\lambda)$ and there exists a PPT algorithm $\mathbf{B}$ that breaks the bandaging property of Cmt in accordance with the experiment $\mathbf{Exp}^{\mathrm{bind}}_{\mathtt{Cmt},\mathbf{B}}(1^\lambda)$ satisfying the following inequality.

$$\mathbf{Adv}^{\mathrm{conc\text{-}coll}}_{\mathtt{a\text{-}auth},\mathbf{A}}(\lambda) \leq \frac{1}{\mathrm{CHASP}(1^\lambda)} + \sqrt{\frac{2^\lambda}{2^\lambda - 1} \cdot q_A \cdot \mathbf{Adv}^{\mathrm{euf\text{-}cma}}_{\mathtt{Sig},\mathbf{F}}(\lambda) + \mathbf{Adv}^{\mathrm{bind}}_{\mathtt{Cmt},\mathbf{B}}(\lambda)}.$$

Theorem4 If the component proof system Π^a_0 is perfectly witness-indistinguishable for each $a \in A$, and if the commitment scheme Cmt is perfectly hiding, then our a-auth has anonymity. More precisely, for any given PPT algorithm $\mathbf{A}$ that executes the anonymity game on our a-auth in accordance with the experiment $\mathbf{Expr}^{\mathrm{ano}}_{\mathtt{a\text{-}auth},\mathbf{A}}(1^\lambda)$, the following equality holds.

$$\mathbf{Adv}^{\mathrm{ano}}_{\mathtt{a\text{-}auth},\mathbf{A}}(\lambda) = 0.$$

4.4 実例

提案スキームの実例を双線形群の設定において与える．Fig. 3 はこの実例を示す．

5. まとめ

本稿で我々は commit-and-prove タイプの Σ プロトコルの或る一般的構成を与えた．提案 Σ プロトコルは base witness point を共通の要素とする witnesses の bundle を証明者が知っていることを証明者が検証者に納得させるものであった．要素 Σ プロトコルが witness-indistinguishable な argument system であるとき，提案 Σ プロトコルは全

$\mathtt{Setup}(1^\lambda)$	$\mathtt{AuthKG}(\mathtt{PP}, a)$	$\mathtt{PrivKG}(\mathtt{PP}, \mathrm{PK}^a, \mathrm{MSK}^a, \mathtt{gid})$
$\mathtt{PP}_{\mathtt{Sig}} \leftarrow \mathtt{Sig.Setup}(1^\lambda)$	$(\mathrm{SK}, \mathrm{PK}) \leftarrow \mathtt{Sig.KG}(\mathtt{PP}_{\mathtt{Sig}})$	$\sigma^a_{\mathtt{gid}} \leftarrow \mathtt{Sig.Sign}(\mathtt{PP}_{\mathtt{Sig}}, \mathrm{PK}^a,$
$\mathtt{PP}_\Pi \leftarrow \Pi.\mathtt{Setup}(1^\lambda)$	$\mathrm{PK}^a := \mathrm{PK}, \mathrm{MSK}^a := \mathrm{SK}$	$\mathrm{MSK}^a, \mathtt{gid})$
$\mathtt{PP}_{\mathtt{CmtPrv}} \leftarrow \mathtt{CmtPrv.Setup}(1^\lambda)$	Return $(\mathrm{PK}^a, \mathrm{MSK}^a)$	$\mathrm{sk}^a_{\mathtt{gid}} := \sigma^a_{\mathtt{gid}}$
$\mathtt{PP} := (\mathtt{PP}_\Pi, \mathtt{PP}_{\mathtt{CmtPrv}}, \mathtt{PP}_{\mathtt{Sig}})$		Return $\mathrm{sk}^a_{\mathtt{gid}}$
Return $\mathtt{PP}$		

$\mathtt{P}(\mathtt{PP}, (\mathrm{PK}^a)^{a\in A}, (\mathrm{sk}^a_{\mathtt{gid}})^{a\in A})$		$\mathtt{V}(\mathtt{PP}, (\mathrm{PK}^a)^{a\in A})$
For $a \in A$: $x^a := \mathrm{PK}^a, w_1^a := \mathrm{sk}^a_{\mathtt{gid}}$		For $a \in A$: $x^a := \mathrm{PK}^a$
$w_0 := \mathtt{gid}$		
	(Execute $\Sigma^{a\in A}_{\mathrm{bnd}}$)	
		Return $(d \leftarrow \Sigma^{a\in A}_{\mathrm{bnd,vrf}})$

図 2 Generic construction of our decentralized multi-authority anonymous authentication scheme a-auth.

$\mathtt{Setup}(1^\lambda)$	$\mathtt{AuthKG}(\mathtt{PP}, a)$	$\mathtt{PrivKG}(\mathtt{PP}, \mathrm{PK}^a, \mathrm{MSK}^a, \mathtt{gid})$
$\Lambda := (p, e, \mathbb{G}, \tilde{\mathbb{G}}, \mathbb{G}_T, G, \tilde{G}) \leftarrow \mathcal{BG}(1^\lambda)$	$\alpha_a \in_R \mathbb{Z}_p, \tilde{G}_{a,1} := \tilde{G}_0^{\alpha_a}$	$\gamma_a, \delta_a \in_R \mathbb{Z}_p$
$G_0, G_1, G_2, H \in_R \mathbb{G}, \tilde{G}_0 \in_R \tilde{\mathbb{G}}$	$\mathrm{PK}^a := \tilde{G}_{a,1}, \mathrm{MSK}^a := \alpha_a$	$V_a := (G_0 G_1^{\mathtt{gid}} G_2^{\gamma_a})^{1/(\delta_a+\alpha_a)}$
$\mathtt{PP} := (\Lambda, G_0, G_1, G_2, H, \tilde{G}_0)$	Return $(\mathrm{PK}^a, \mathrm{MSK}^a)$	$\mathrm{sk}^a_{\mathtt{gid}} := (V_a, \gamma_a, \delta_a)$
Return $\mathtt{PP}$		Return $\mathrm{sk}^a_{\mathtt{gid}}$

$\mathtt{P}(\mathtt{PP}, (\mathrm{PK}^a)^{a\in A}, (\mathrm{sk}^a_{\mathtt{gid}})^{a\in A})$		$\mathtt{V}(\mathtt{PP}, (\mathrm{PK}^a)^{a\in A})$
$u \in_R \mathbb{Z}_p, C_0 := G^{\mathtt{gid}} H^u$		
For $a \in A$:		
$v_a \in_R \mathbb{Z}_p, R_a := V_a G_2^{v_a}, z_a := \gamma_a + v_a \delta_a$		
$r_{a,\mathtt{gid}}, r_{a,z}, r_{a,v}, r_{a,\delta} \in_R \mathbb{Z}_p$		
$T_a := e(G_1, \tilde{G}_0)^{r_{a,\mathtt{gid}}} e(G_2, \tilde{G}_0)^{r_{a,z}}$		
$\cdot e(G_2, \tilde{G}_1)^{r_{a,v}} e(R_a, \tilde{G}_0)^{-r_{a,\delta}}$		
$r_{a,u} \in_R \mathbb{Z}_p, A_a := G^{r_{a,\mathtt{gid}}} H^{r_{a,u}}$	$C_0, (R_a, T_a, A_a)^{a\in A}$	
	$\rightarrow$	
For $a \in A$:	c	$c \in_R \mathbb{Z}_p$
$s_{a,\mathtt{gid}} := r_{a,\mathtt{gid}} + c\mathtt{gid}, s_{a,z} := r_{a,z} + cz_a$	$\leftarrow$	
$s_{a,v} := r_{a,v} + cv_a, s_{a,\delta} := r_{a,\delta} + c\delta_a$		
$s_{a,u} := r_{a,u} + cu$	$(s_{a,\mathtt{gid}}, s_{a,z}, s_{a,v}, s_{a,\delta}, s_{a,u})^{a\in A}$	For $a \in A$:
	$\rightarrow$	$e(G_1, \tilde{G}_0)^{s_{a,\mathtt{gid}}} e(G_2, \tilde{G}_0)^{s_{a,z}}$
		$\cdot e(G_2, \tilde{G}_1)^{s_{a,v}} e(R_a, \tilde{G}_0)^{-s_{a,\delta}}$
		$=_?$ $T_a (e(R_a, \tilde{G}_{a,1})/e(G_0, \tilde{G}_0))^c$
		and $G^{s_{a,\mathtt{gid}}} H^{s_{a,u}} =_?$ $A_a C_0^c$
		If all eqs. hold, Return 1
		else Return 0

図 3 Instantiation of our decentralized multi-authority anonymous authentication scheme a-auth in the setting of bilinear groups.

体として witness-indistinguishable な argument system である．適用例として，分散型多権限機関匿名認証スキームの一般的構成を提案した．提案スキームにおいて，witness は共通のグローバル ID ストリングとその上のデジタル署名から成る各 witness の bundle である．提案スキームの実例を双線形群の設定において与えた．

Post-quantum の実例を与えることが今後の課題である．

参考文献

[1] H. Anada and S. Arita. Anonymous authentication scheme with decentralized multi-authorities. In *2017 IEEE International Conference on Smart Computing, SMARTCOMP 2017, Hong Kong, China, May 29-31, 2017*, pages 1–6, 2017.

[2] H. Anada and S. Arita. Witness-indistinguishable arguments with σ-protocols for bundled witness spaces and its application to global identities. *IACR Cryptology ePrint Archive*, 2018:742, 2018.

[3] L. Babai. Trading group theory for randomness. In *Proceedings of the 17th Annual ACM Symposium on Theory of Computing, May 6-8, 1985, Providence, Rhode Island, USA*, pages 421–429, 1985.

[4] R. Canetti, Y. Lindell, R. Ostrovsky, and A. Sahai. Universally composable two-party and multi-party secure computation. In *Proceedings on 34th Annual ACM Symposium on Theory of Computing, May 19-21, 2002, Montréal, Québec, Canada*, pages 494–503, 2002.

[5] R. Cramer. *Modular Designs of Secure, yet Practical*

Cyptographic Protocols. PhD thesis, University of Amsterdam, Amsterdam, the Netherlands, 1996.

[6] R. Cramer, I. Damgård, and B. Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. In *CRYPTO '94*, pages 174–187. Springer-Verlag, 1994.

[7] I. Damgård. On σ-protocols. In Course Notes, http://cs.au.dk/ ivan/CPT.html, 2010.

[8] A. Escala and J. Groth. Fine-tuning groth-sahai proofs. In *Public-Key Cryptography - PKC 2014 - 17th International Conference on Practice and Theory in Public-Key Cryptography, Buenos Aires, Argentina, March 26-28, 2014. Proceedings*, pages 630–649, 2014.

[9] U. Feige and A. Shamir. Witness indistinguishable and witness hiding protocols. In *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing, May 13-17, 1990, Baltimore, Maryland, USA*, pages 416–426, 1990.

[10] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *Advances in Cryptology - CRYPTO '86, Santa Barbara, California, USA, 1986, Proceedings*, pages 186–194, 1986.

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

[12] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof-systems. In *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*, STOC '85, pages 291–304, New York, NY, USA, 1985. ACM.

[13] A. B. Lewko and B. Waters. Decentralizing attribute-based encryption. In *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings*, pages 568–588, 2011.

[14] T. Okamoto and K. Takashima. Decentralized attribute-based signatures. In *PKC 2013*, volume 7778 of *LNCS*, pages 125–142. Springer, 2013.

[15] 穴田啓晃. 結託耐性を備えたアイデンティティ識別不可能な属性認証方式. In **火の国情報シンポジウム** *2017*, pages 4B–2, 鹿児島, 3 月 2017. 2017 年 3 月 1 日 (水)-3 月 2 日 (木) 鹿児島大学 郡元キャンパス.

[16] 穴田啓晃 and 有田正剛. 知識の証明のバンドリングとそのデジタル署名への応用. In **信学技報**, volume 116-207 of *ISEC2016-39*, pages 9–14, 東京, 9 月 2016. 2016 年 9 月 2 日 (金)　機械振興会館 (ISEC).

[17] 穴田啓晃 and 有田正剛. 効率が良く追跡可能な属性ベース署名. In **暗号と情報セキュリティシンポジウム** *2017* (*SCIS2017*) **予稿集**, pages 3F1–3, 沖縄, 1 月 2017.

[18] 穴田啓晃 and 有田正剛. 対角線上証拠識別不可能な証明システム. In **信学技報**, volume 116 of *IT2016-121, ISEC2016-111, WBS2016-97*, pages 145–148, 東京, 3 月 2017. 2017 年 3 月 9 日 (木)-3 月 10 日 (金) 東海大学 高輪キャンパス (ISEC, WBS, IT).

[19] 穴田啓晃 and 有田正剛. 複数の鍵発行権限機関がある設定における匿名属性認証スキーム. In **信学技報**, volume 117 of *ISEC2017-59, SITE2017-41, LOIS2017-36*, pages 63–70, 京都, 11 月 2017. 2017 年 11 月 9 日 (木)-11 月 10 日 (金) 京都産業大学むすびわざ館 (LOIS, ISEC, SITE).

[20] 穴田啓晃 and 有田正剛. バンドルされた証拠空間に対する証明システムとその複数の権限機関を伴う匿名属性認証スキームへの応用. In **暗号と情報セキュリティシンポジウム** *2018* (*SCIS2018*) **予稿集**, pages 3B2–6, 新潟, 1 月 2018.