

マルチサービス環境における署名手法のリンク不能性に関する研究

中村, 徹
九州大学大学院システム情報科学府

稲永, 俊介
九州大学大学院システム情報科学研究院

馬場, 謙介
九州大学大学院システム情報科学研究院

池田, 大輔
九州大学大学院システム情報科学研究院

他

<https://hdl.handle.net/2324/13298>

出版情報 : 暗号と情報セキュリティシンポジウム. 2009, 2009-01-20
バージョン :
権利関係 :



マルチサービス環境における署名手法のリンク不能性に関する研究

A Study on Unlinkability for Signature Schemes in Multi-Service Environment

中村 徹* Toru Nakamura
稲永 俊介† Shunsuke Inenaga
馬場 謙介† Kensuke Baba
池田 大輔† Daisuke Ikeda
安浦 寛人† Hiroto Yasuura

あらまし ネットワークを介したサービスの提供が一般的になり、電子商取引など、電子データを用いた契約形態が普及する現在、データ作成者の本人性を保証し、またデータの非改竄性を保証するデジタル署名の重要性は増している。複数のサービスに対して単一の署名鍵を用いる場合、異なるサービスで用いられる署名を容易に関連付けることができ、重大なプライバシー問題を引き起こす危険性がある。我々はこれまでに、相手認証についてのサービス間のリンク不能性を定義し、ICカードの利用を前提とした、安全性とサービス間のリンク不能性、及びメモリ効率性を実現する相手認証を提案した。本稿では、異なるサービスに対する複数の署名が同一の署名者が生成したものであるかどうか判別できない性質をデジタル署名のサービス間のリンク不能性と定義する。さらに、上記の相手認証を変換して得られたデジタル署名手法が、安全性とデジタル署名に対するサービス間のリンク不能性、及びメモリ効率性を実現することを示す。

キーワード デジタル署名, 相手認証, リンク不能性, ICカード

1 はじめに

ネットワークを介したサービスの提供が一般的になり、電子商取引など、電子データを用いた契約形態が普及する現在、データ作成者の本人性を保証し、またデータの非改竄性を保証するデジタル署名の重要性は増している。デジタル署名は、正当な秘密鍵で生成された署名が対応する検証鍵により常に承認され、また秘密鍵を知らない攻撃者が承認される有効な署名を生成することが困難であるという性質を持つ。秘密鍵をICカード内に保持して利用者がICカードを持ち運ぶことで、環境に依存しない利便性の高いデジタル署名が実現できる。そこで本稿では、ICカードの利用を前提としたデジタル署名手法を提案する。

デジタル署名手法の偽造攻撃に対する安全性は重要

な問題であるが、一方で、デジタル署名におけるプライバシー保護も重要な問題となっている。本稿では、一枚のICカードで多数のサービスに対応するデジタル署名を扱うような場合を想定する。複数のサービスに対して単一の秘密鍵を用いる場合、異なるサービスで用いられる署名を容易に関連付けることができ、重大なプライバシー問題を引き起こす危険性がある。ここで、異なるサービスに対する複数の署名から同一の署名者が行った署名であるか判別できない性質をデジタル署名のサービス間のリンク不能性と定義する。サービス間のリンク不能性を持つデジタル署名を実現する単純な方法として、サービスごとに異なる秘密鍵をICカードに保持する方法が考えられる。しかしながら、この実現方法では必要なメモリサイズが利用するサービス数に比例して増加するため、メモリサイズの制約の厳しいICカードには不向きである。

そこで本稿では、サービス間のリンク不能性を満たし、かつ必要なメモリサイズがサービス数に比例しないデジタル署名を提案する。我々はこれまでに、相手認証と疑似ランダム関数を用いて、相手認証におけるサービス間のリンク不能性とメモリ効率性を実現するマルチサー

* 九州大学大学院システム情報科学府 〒 819-0395 福岡市西区元岡 744 番地 Graduate School of Information Science and Electrical Engineering, Kyushu University 744 Motooka Nishi-ku Fukuoka 819-0395

† 九州大学大学院 システム情報科学研究 院 Faculty of Information Science and Electrical Engineering, Kyushu University {toru, inenaga, yasuuru}@c.csce.kyushu-u.ac.jp, {baba, daisuke}@i.kyushu-u.ac.jp

ビス向け相手認証を提案した [9, 7]。相手認証とは、任意の文字列を秘密鍵として用いることが可能な、安全な認証手法である [4, 3, 8]。提案するデジタル署名手法は、マルチサービス向け相手認証に対して、相手認証からデジタル署名への変換 [1] を用いて実現する。提案手法では、利用者の IC カード内に文字列から文字列への 2 つの関数を保持することを想定する。署名時には、まず、署名を提示するサービスに一意に対応するサービス ID をそれらの関数に入力し、出力をそれぞれ秘密鍵とサービス内で利用者の識別子 (仮名) とみなす。そして、相手認証からの変換によって得られた署名手法を用いて署名を生成する。

本稿では、デジタル署名におけるサービス間のリンク不能性を定義する。さらに、上記のマルチサービス向けデジタル署名がその性質を持つことを示す。

2 相手認証からデジタル署名への変換

本章では、文献 [1] で示された、カノニカル相手認証によるデジタル署名の構成法について説明する。

2.1 表記

対話チューリング機械 (Interactive Turing Machine, ITM) は、入力テープ、出力テープ、作業テープの他に、通信テープと呼ばれる片方が読み込みのみ可能で、もう一方は書き込みのみ可能である一対のテープを持つチューリング機械である。

2 つの ITM による対話処理とは、以下の状況の下での、各 ITM の計算状況 (つまり、状態、テープ上の内容、ヘッドの位置) の対の列のことである。

- 2 つの ITM は共通の入力テープを持っている (このテープからの入力を共通入力、それ以外の入力テープからの入力を各 ITM の補助入力と呼ぶ)。
- 片方の ITM の読み取りのみ可能な通信テープは、もう一方の ITM の書き込みのみ可能な通信テープであり、逆も同様である。
- 片方の ITM の計算状況が変化する時は、もう一方の ITM の計算状況は変化しない (この状況は、各 ITM に 1 ビットの情報を付加することで実現できる)。

また、対話処理の出力は片方の ITM の出力である。

チューリング機械 A に x を入力した場合の出力を $A(x)$ と表す。ITM A と B による対話処理を $\langle A, B \rangle$ と表す。また、共通入力を x 、 A と B の補助入力をそれぞれ y と z としたときの対話処理の出力を $\langle A(y), B(z) \rangle(x)$ と表す。ただし、明示的に言及しない内容は省略し、明示的に言及する内容の無い入力は括弧とともに省略する場

合がある。以降、チューリング機械をアルゴリズム、また、対話処理をプロトコルと呼ぶ場合がある。 $\text{poly}(n)$ は $n \in \mathbb{N}$ についてのある多項式を表し、 $p(n)$ は $n \in \mathbb{N}$ についての任意の多項式を表すものとする。

2.2 相手認証

本節では、文献 [5] に従い、相手認証の定義を示す。

定義 1 相手認証とは、確率的多項式時間アルゴリズム I と、確率的多項式時間 ITM P と V による対話処理 $\langle P, V \rangle$ の対のうち、以下をみたすものである。

- 実現可能性：任意の $n \in \mathbb{N}$ 、任意の $\alpha \in \{0, 1\}^n$ 、および任意の $s \in \{0, 1\}^{\text{poly}(n)}$ について以下が成り立つ。

$$\Pr[\langle P(s), V \rangle(\alpha, I(s, \alpha)) = 1] = 1$$

- 安全性：任意の確率的多項式時間 ITM B' と B'' 、任意の十分に大きな $n \in \mathbb{N}$ 、任意の $\alpha \in \{0, 1\}^n$ 及び任意の z について以下が成り立つ。

$$\Pr[\langle B''(z, T_n), V \rangle(\alpha, I(U_n, \alpha)) = 1] < \frac{1}{p(n)}$$

ただし、 U_n は $\{0, 1\}^{\text{poly}(n)}$ 上に一様に分布する確率変数であり、 T_n は共通入力 $(\alpha, I(U_n, \alpha))$ のとき、 $P(U_n)$ と多項式回対話を行った後の $B'(z)$ の出力を表す確率変数である。

以後 s を秘密鍵、 α を仮名、 I の出力を検証鍵と呼び、 $\langle P, V \rangle$ を認証プロトコルと呼ぶ。

次に、カノニカル相手認証 [1] と呼ばれる 3 交信プロトコルに基づく相手認証について述べる。カノニカル相手認証は、鍵生成アルゴリズム K 、コミットメント生成アルゴリズム Cmt 、チャレンジ生成アルゴリズム Ch 、レスポンス生成アルゴリズム R 、検証アルゴリズム Vf から構成される。文献 [1] では、鍵生成アルゴリズム K は、セキュリティパラメータ $k \in \mathbb{N}$ を入力とし、検証鍵と秘密鍵のペア (v, s) を出力するアルゴリズムと定義されている。本稿では、任意の文字列を秘密鍵として扱うことができることを強調するため、秘密鍵 s と仮名 α を入力とし、検証鍵 v を出力する決定性アルゴリズムとする。コミットメント生成アルゴリズム Cmt は、秘密鍵 s を入力としてコミットメント t を出力する確率的アルゴリズムである。チャレンジ生成アルゴリズム Ch は、入力を与えられることなくチャレンジ u を出力する確率的アルゴリズムである。レスポンス生成アルゴリズム R は、秘密鍵 s とコミットメント t 及びチャレンジ u を入力として、レスポンス w を出力する決定性アルゴリズムである。検証アルゴリズム Vf は、検証鍵 v 、チャレン

ジ u 及びレスポンス w を入力として、コミットメント t' を出力する。 V は $t = t'$ であれば 1 を出力し、そうでなければ 0 を出力する。

カノニカル相手認証の認証プロトコル $\langle P, V \rangle$ を以下に示す。

1. ITM P は $Cmt(s)$ を実行し、得られた t を対となる ITM V に送る。
2. V は $Ch()$ を実行し、得られた u を P に送る。
3. P は $R(s, t, u)$ を実行し、得られた w を V に送る。
4. V は $Vf(v, u, w)$ を実行し、得られた t' と t を比較して、 $t = t'$ であれば 1 を、そうでなければ 0 を出力する。

図 1 にカノニカル相手認証の概要を示す。

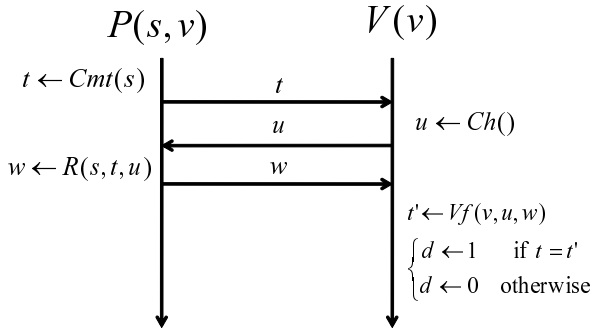


図 1: カノニカル相手認証

2.3 デジタル署名

本節では、文献 [5] に従い、デジタル署名の定義を示す。

定義 2 デジタル署名とは、以下の条件を満たす確率的多項式時間アルゴリズムの 3 つ組 (K, S, V) である。

1. 鍵生成アルゴリズム K は、入力 1^n に対して対となる 2 つのビット列を出力する。
2. $K(1^n)$ の任意の出力対 (s, v) 、任意の $m \in \{0, 1\}^*$ に対して、署名アルゴリズム S と検証アルゴリズム V は、

$$\Pr[V(v, m, S(s, m)) = 1] = 1$$

を満たす。

ここで、デジタル署名の選択文書攻撃 [6] に対する安全性の一般的な定義について述べる。選択文書攻撃とは、任意の文書に対する署名を得ることができる攻撃者が行う偽造攻撃である。

定義 3 オラクル O にアクセス可能な確率的オラクル機械 M に入力 x が与えられた場合に、 O に対するオラクル問い合わせの集合を $Q_M^O(x)$ と表す。 $M^O(x)$ は、オラクル O にアクセス可能な M の入力 x が与えられた場合の出力を表す。

デジタル署名は以下の条件を満たすとき、選択文書攻撃に対して安全である。任意の確率的多項式時間オラクル機械 M 、任意の十分に大きい $n \in \mathbb{N}$ について、

$$\Pr[V(v, m, \beta)] = 1 < \frac{1}{p(n)}$$

である。ただし、 (s, v) は $K(1^n)$ の出力であり、 (m, β) は $M^{S(s)}(v)$ の出力である (ただし、 $m \notin Q_M^{S(s)}(v)$ である)。

2.4 カノニカル相手認証からデジタル署名への変換

カノニカル相手認証 $(I, \langle P, V \rangle)$ を用いてデジタル署名 (I, S, V') を構成する場合を考える。デジタル署名の鍵生成アルゴリズムは基となるカノニカル相手認証と同じである。カノニカル相手認証を構成するアルゴリズムを用いた、署名アルゴリズム S と検証アルゴリズム V' の構成法を以下に示す。まず署名アルゴリズムを示す。ただし、 m を任意のビット長のメッセージとする。

Algorithm $S^H(s, m)$

$t \leftarrow Cmt(s)$

$u \leftarrow Ch()$

$z \leftarrow h(t \parallel u \parallel m)$

$w \leftarrow R(s, t, z)$

Return $\sigma \leftarrow (t \parallel u \parallel w)$

次に検証アルゴリズムを示す。

Algorithm $V'^H(v, m, \sigma)$

σ を $t \parallel u \parallel w$ として解釈する

$z' \leftarrow h(u \parallel t \parallel m)$

$t' \leftarrow Vf(v, z', w)$

if $t = t'$ then $d \leftarrow 1$, otherwise, $d \leftarrow 0$

Return d

定理 1 上記のように構成されたアルゴリズムの 3 つ組 (I, S, V') は、以下の条件を満たす。

- 署名: 任意の $n \in \mathbb{N}$ 、任意の $m \in \{0, 1\}^*$ 、任意の $\alpha \in \{0, 1\}^n$ および任意の $s \in \{0, 1\}^{\text{poly}(n)}$ について、

$$\Pr[V'(\alpha, I(s, \alpha), m, S(s, m)) = 1] = 1$$

である。

- 安全性: 任意の確率的多項式時間オラクル機械 M 、任意の十分に大きい $n \in \mathbb{N}$ 、任意の $\alpha \in \{0, 1\}^n$

について,

$$\Pr[V'(\alpha, I(U_n, \alpha), m, \beta)] = 1 < \frac{1}{p(n)}$$

である。ただし, U_n は $\{0, 1\}^n$ 上に一様に分布する確率変数であり, (m, β) は $M^{S(U_n)}(I(U_n, \alpha))$ の出力である (ただし, $m \notin Q_M^{S(U_n)}(I(U_n, \alpha))$ である)。

上記の構成法で構成されたデジタル署名を, 相手認証に基づくデジタル署名と呼ぶことにする。相手認証に基づくデジタル署名は, 文献 [1] において, ランダムオラクル仮定 [2] の上で選択文書攻撃に対して安全であることが示されている。図 2 に相手認証に基づくデジタル署名の署名アルゴリズムと検証アルゴリズムの概要を示す。

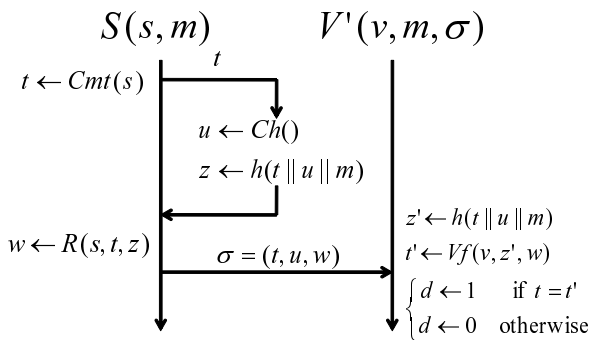


図 2: 相手認証に基づくデジタル署名

3 マルチサービス環境向けデジタル署名

本章では, 以下のような性質を持つデジタル署名の構成法について述べる。

- 安全性: 選択平文攻撃に対して安全である。
- リンク不能性: 異なるサービスに対する署名から同一の署名者が行った署名であるかどうか判別できない。
- メモリ効率性: 署名に必要なメモリサイズがサービスの数に依存しない。

このような性質を持つデジタル署名をマルチサービス環境向けデジタル署名と呼ぶ。我々は文献 [9, 7] において, 安全性とサービス間のリンク不能性, 及びメモリ効率性を実現する相手認証を定義し, 疑似ランダム関数を用いた構成法を示した。このような相手認証をマルチサービス環境向け相手認証と呼ぶ。本章では, 相手認証からデジタル署名への変換法をマルチサービス環境向け相手認証に適用することで, マルチサービス環境向けデジタル署名を構成することができることを示す。

3.1 マルチサービス環境向け相手認証

マルチサービス環境における相手認証とは, 相手認証を構成する $I, \langle P, V \rangle$ に加えて, 文字列から文字列への関数を値とする 2 つの確率変数から構成され, この確率変数を用いて複数サービスに対する秘密鍵と仮名を表現するよう変形したものである。マルチサービス環境向け相手認証の認証プロトコルの概要を述べる。まず, 秘密鍵とその秘密鍵に対応する検証鍵を検索するために用いる仮名を生成するための 2 つの異なる関数を値とする確率変数を用意する。各証明者は固有の, それぞれの確率変数の値となる関数を 2 つ持つ。認証の際には, まず証明者は認証要求を検証者に送り, 検証者から検証者を一意に示す識別子 (サービス ID) を得る。次に, サービス ID を所持する 2 つの関数に入力し, 出力をそれぞれ秘密鍵と仮名とみなす。そして仮名を検証者に送り, 検証者は仮名から対応する検証鍵を検索する。最後に秘密鍵と検証鍵を用いて認証プロトコル $\langle P, V \rangle$ を実行する。このような認証プロトコルを $\langle P, V \rangle$ に対する拡張プロトコルと呼ぶ。

サービス間のリンク不能性とは, 認証履歴を集めることができる攻撃者に対して, 異なる検証者に対して得られた 2 つの認証履歴が同一の証明者であるかどうか判別できない性質である。文献 [9, 7] においては, 仮名と検証鍵のみ利用可能な攻撃者に対して議論を行ったが, 本稿では, 通信テープの内容の複製を利用可能な攻撃者に対するサービス間のリンク不能性について議論し, これを満たすものをマルチサービス環境向け相手認証とする。

以下にカノニカル相手認証を用いたマルチサービス環境向け相手認証の定義を示す。ここで, $x, y, z \in \{0, 1\}^n$ について,

- $v(x, y) \stackrel{def}{=} I(f_x(y), g_x(y))$
- $t(x, y) \stackrel{def}{=} Cmt(f_x(y))$
- $w(x, y, z) \stackrel{def}{=} (R(f_x(z), Cmt(f_x(z)), y))$

とする。

定義 4 カノニカル相手認証 $(I, \langle P, V \rangle)$ について, I と, $\langle P, V \rangle$ に対する拡張プロトコル $\langle P', V' \rangle$ 及び関数を値とする確率変数 F_n, G_n が以下の性質を満たすとき, $(I, \langle P, V \rangle, F_n, G_n)$ をマルチサービス環境向け相手認証と呼ぶ。

- 実現可能性: 任意の $n \in \mathbb{N}$, 任意の $a \in \{0, 1\}^n$ 及び任意の $b \in \{0, 1\}^n$ について,

$$\Pr[\langle P'(\langle f_a \rangle, \langle g_a \rangle), V'(b, v(a, b)) = 1] = 1$$

である。ただし, $\langle f_a \rangle, \langle g_a \rangle$ はそれぞれ関数 f_a, g_a の記述を表す。

- 安全性：任意の確率的多項式時間 $ITM B'$ と B'' , 任意の十分に大きな $n \in \mathbb{N}$, 任意の $b \in \{0, 1\}^n$ 及び任意の z について ,

$$\Pr[\langle B''(z, T'_n), V' \rangle(b, v(U_n, b)) = 1] < \frac{1}{p(n)}$$

である . ただし U_n は $\{0, 1\}^n$ 上に一様に分布する確率変数であり , T'_n は共通入力 $(b, v(U_n, b))$ のとき , $P'(\langle f_a \rangle, \langle g_a \rangle)$ と多項式回対話を行った後の $B'(z)$ の出力を表す確率変数である .

- リンク不能性：任意の確率的多項式時間アルゴリズム A , 十分に大きい $n \in \mathbb{N}$, 任意の $b \neq b'$ について ,

$$\begin{aligned} & \Pr[A(g_{U_n}(b), g_{U_n}(b')) = 1] \\ & - \Pr[A(g_{U_n}(b), g_{W_n}(b')) = 1] < \frac{1}{p(n)} \end{aligned}$$

かつ ,

$$\begin{aligned} & |\Pr[A(v(U_n, b), v(U_n, b')) = 1] \\ & - \Pr[A(v(U_n, b), v(W_n, b')) = 1]| < \frac{1}{p(n)} \end{aligned}$$

かつ ,

$$\begin{aligned} & |\Pr[A(t(U_n, b), t(U_n, b')) = 1] \\ & - \Pr[A(t(U_n, b), t(W_n, b')) = 1]| < \frac{1}{p(n)} \end{aligned}$$

かつ ,

$$\begin{aligned} & |\Pr[A(w(U_n, X_n, b), w(U_n, Y_n, b')) = 1] \\ & - \Pr[A(w(U_n, X_n, b), w(W_n, Y_n, b')) = 1]| < \frac{1}{p(n)} \end{aligned}$$

である . ただし , U_n, W_n, X_n, Y_n は互いに独立で $\{0, 1\}^n$ 上に一様に分布する確率変数である .

ここでリンク不能性の定義は , 仮名 , 検証鍵 , コミットメント , レスポンス全てについて , 2 つの異なるサービス ID に対しそれぞれ同一の確率変数により選択された関数の出力を得た場合と , 異なる確率変数により選択された関数の出力を得た場合で , 効率よく識別することができるアルゴリズムが存在しないことを表現している .

文献 [7] において , 任意の相手認証と疑似ランダム関数を用いることでマルチサービス環境向け相手認証が実現可能であることが示されている . 疑似ランダム関数とは , 文字列から文字列への関数を値とする確率変数であり , 真のランダム関数と識別することが困難である特徴を持つ .

3.2 マルチサービス向けデジタル署名

相手認証同様に , 関数を値とする確率変数を用いてマルチサービス環境におけるデジタル署名を表現する .

定義 5 (I, S, V', F_n, G_n) が以下の条件を満たすとき , マルチサービス向けデジタル署名と呼ぶ .

- 署名：任意の $n \in \mathbb{N}$, 任意の $m \in \{0, 1\}^*$, 任意の $a \in \{0, 1\}^n$ および任意の $b \in \{0, 1\}^n$ について ,

$$\Pr[V'(g_a(b), v(a, b), m, S(f_a(b), m)) = 1] = 1$$

である .

- 安全性：任意の確率的多項式時間オラクル機械 M , 任意の十分に大きい $n \in \mathbb{N}$, 任意の $b \in \{0, 1\}^n$ について ,

$$\Pr[V'(g_{U_n}(b), v(U_n, b), m, \beta) = 1] < \frac{1}{p(n)}$$

である . ただし , U_n は $\{0, 1\}^n$ 上に一様に分布する確率変数であり , (m, β) は $M^{S(U_n)}(v(U_n, b))$ の出力である (ただし , $m \notin Q_M^{S(U_n)}(v(U_n, b))$ である) .

- リンク不能性：任意の確率的多項式時間アルゴリズム A , 十分に大きい $n \in \mathbb{N}$, 任意の $b \neq b'$, 任意の $m \in \{0, 1\}^*$ について ,

$$\begin{aligned} & \Pr[A(g_{U_n}(b), g_{U_n}(b')) = 1] \\ & - \Pr[A(g_{U_n}(b), g_{U'_n}(b')) = 1] < \frac{1}{p(n)} \end{aligned} \quad (1)$$

かつ ,

$$\begin{aligned} & |\Pr[A(v(U_n, b), v(U_n, b')) = 1] \\ & - \Pr[A(v(U_n, b), v(W_n, b')) = 1]| < \frac{1}{p(n)} \end{aligned} \quad (2)$$

かつ ,

$$\begin{aligned} & |\Pr[A(S(f_{U_n}(b), m), S(f_{U_n}(b'), m)) = 1] \\ & - \Pr[A(S(f_{U_n}(b), m), S(f_{W_n}(b'), m)) = 1]| < \frac{1}{p(n)} \end{aligned} \quad (3)$$

である . ただし , U_n, W_n は互いに独立で $\{0, 1\}^n$ 上に一様に分布する確率変数である .

ここでリンク不能性の定義は , 仮名 , 検証鍵 , 署名全てについて , 2 つの異なるサービス ID に対しそれぞれ同一の確率変数により選択された関数の出力を得た場合と , 異なる確率変数により選択された関数の出力を得た場合で , 効率よく識別することができるアルゴリズムが存在しないことを表現している .

マルチサービス向け相手認証を変換して得られたデジタル署名が署名, 及び安全性を満たすことについては文献 [1], メモリ効率性については文献 [7] と同様の証明により示すことができる. 本稿では証明の詳細は省略する. 以下ではマルチサービス向け相手認証を変換して得られたデジタル署名がサービス間のリンク不能性を持つことを証明する.

定理 2 ($I, \langle P, V \rangle, F_n, G_n$) をカノニカル相手認証に基づいたマルチサービス向け相手認証としたとき, これを変換して得られたマルチサービス環境におけるデジタル署名 (I, S, V', F_n, G_n) は, サービス間のリンク不能性を持つ.

証明 ここでは証明の概要のみ述べる. 式 1, 2 は定義 4 から成り立つ. S の出力 σ はアルゴリズム Cmt, Ch, R の出力から構成される. Cmt については, 定義 4 のリンク不能性から,

$$|\Pr[A(t(U_n, b), t(U_n, b')) = 1] - \Pr[A(t(U_n, b), t(W_n, b')) = 1]| < \frac{1}{p(n)}$$

である. Ch については, 入力を与えられないアルゴリズムであるので無視してよい. R については, 定義 4 のリンク不能性から,

$$|\Pr[A(w(U_n, X_n, b), w(U_n, Y_n, b')) = 1] - \Pr[A(w(U_n, X_n, b), w(W_n, Y_n, b')) = 1]| < \frac{1}{p(n)}$$

である. ただし, U_n, W_n, X_n, Y_n は互いに独立で $\{0, 1\}^n$ 上に一様に分布する確率変数である. 定理 2 のデジタル署名では X_n, Y_n がそれぞれハッシュ値に置き換えられるが, ランダムオラクルモデルであるため, 同様に考えて問題ない. ゆえに式 3 が成り立つ. 以上から, サービス間のリンク不能性を持つことが導かれる. \square

文献 [7] において, 相手認証と疑似ランダム関数を用いることで, マルチサービス環境向け相手認証を実現することを示した. ゆえに, 以下の定理が成り立つ.

定理 3 任意のカノニカル相手認証と疑似ランダム関数を用いて, マルチサービス環境向けデジタル署名が実現可能である.

4 おわりに

本稿では, デジタル署名のサービス間のリンク不能性を定義した. さらに, 我々がこれまでに提案した, 安全性とサービス間のリンク不能性, メモリ効率性を実現する相手認証を変換して得られたデジタル署名が, デジタル署名に対するリンク不能性を持つことを示した.

謝辞

本研究の一部は「次世代研究スーパースター養成プログラム」の支援による.

参考文献

- [1] Michel Abdalla, Jee Hea An, Mihir Bellare, and Chanathip Namprempre. From identification to signatures via the Fiat-Shamir transform: Minimizing assumptions for security and forward-security. In *Advances in Cryptology – EUROCRYPT 2002*, Vol. 2332 of *LNCS*, pp. 418–433. Springer-Verlag, 2002.
- [2] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *In Proc. 1st ACM Conference on Computer and Communications Security*, pp. 62–73. ACM Press, 1993.
- [3] Uriel Feige, Amos Fiat, and Adi Shamir. Zero-knowledge proofs of identity. In *Proc. 19th Annual ACM Symposium on Theory of Computing*, pp. 210–217, 1987.
- [4] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *Advances in Cryptology – CRYPTO’86*, Vol. 263 of *LNCS*, pp. 186–194. Springer-Verlag, 1987.
- [5] Oded Goldreich. *Foundations of Cryptography*. Cambridge University, 2001.
- [6] Shafi Goldwasser, Silvio Micali, and Ronald L. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on Computing*, Vol. 17, No. 2, pp. 281–308, 1988.
- [7] Toru Nakamura, Shunsuke Inenaga, Kensuke Baba, Daisuke Ikeda, and Hiroto Yasuura. A provably secure and unlinkable authentication system with smart cards for massive services. In *DOI Technical Report*, Vol. 234. Department of Informatics, Kyushu University, 2008.
- [8] C. P. Schnorr. Efficient signature generation by smart cards. In *Journal of Cryptology*, Vol. 4, pp. 161–174. Springer New York, 1991.
- [9] 中村徹, 稲永俊介, 馬場謙介, 池田大輔, 安浦寛人. プライバシー保護とメモリ効率性の両立を実現するマルチサービス環境向け認証方式. コンピュータセキュリティシンポジウム 2008(CSS2008) 予稿集, 2008.