プライバシ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

中村, 徹
九州大学大学院システム情報科学[府／研究院]

稲永, 俊介
九州大学大学院システム情報科学[府／研究院]

馬場, 謙介
九州大学大学院システム情報科学[府／研究院]

池田, 大輔
九州大学大学院システム情報科学[府／研究院]

他

出版情報：コンピュータセキュリティシンポジウム. 2008, pp.67-72, 2008-10-08
バージョン：
権利関係：

プライバシ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

中村　徹　　稲永　俊介　　馬場　謙介　　池田　大輔　　安浦　寛人

九州大学大学院システム情報科学 [府／研究院]
{toru,inenaga,yasuura}@c.csce.kyushu-u.ac.jp　{baba, daisuke}@i.kyushu-u.ac.jp

あらまし 近年，マルチサービス環境における認証システムが注目されている．本稿では，安全性だけでなくプライバシ保護についても考慮した認証方式を提案する．また形式的なモデルによる安全性定義を拡張し，マルチサービス環境における認証方式の安全性の定義を行う．さらに，同じモデルを用いて，プライバシ保護についての性質であるサービス間のリンク不能性を定義する．提案する認証方式は安全性， サービス間のリンク不能性を持ち，さらにメモリサイズがサービス数に比例しない特長を持つ．そのためメモリサイズに制限のある携帯デバイスを用いた認証システムに適している．

An Authentication System Achieveing Coexisting of Privacy Protection and Memory Efficiency for Multi-Service Environment

Toru Nakamura　Shunsuke Inenaga　Kensuke Baba　Daisuke Ikeda　Hiroto Yasuura

[Graduate School/Faculty] of Information Science and Electrical Engineering, Kyushu University, Japan
{toru,inenaga,yasuura}@c.csce.kyushu-u.ac.jp　　{baba,daisuke}@i.kyushu-u.ac.jp

Abstract In this paper, we propose an authentication scheme for multi-service environment that satisfies not only security but also privacy protection. Moreover, we extend the definition of security on the formal authetication model in order to define the security for multi-service environment. We define also unlinkability, which is a property on privacy protection, on the same model. Our proposing scheme is adaptive for identification scheme with smart cards since the number of secret strings stored in the smart cards depends on the number of service providers.

1　はじめに

1.1　研究背景

現在多くのサービスが電子化されている．サービスの利用には**認証**が必要となる場合が多い．このとき複数のサービスで統一された認証システムを用いることが有益な場合がある．このような認証システムを本稿では**マルチサービス環境**における認証システムと呼ぶ．

本稿では，マルチサービス環境における認証システムについて，特に IC カードのような携帯デバイスを認証に用いるシステムについて議論を行う．本稿で想定する認証システムは，複数のユーザとサービス提供者，及び一つの管理者から構成される．管理者は認証に必要な情報を IC カードに格納し，ユーザに配布する．ユーザはサービス提供者に IC カードを提示することにより認証を行う．

1.2 提案手法の有効性の検証法

本稿で提案する認証システムでは，知識の対話証明を用いた相手認証を利用する．知識の対話証明を用いた相手認証の，チューリング機械を用いた形式的なモデルは，Feige ら [2] により提案され，Goldreich [3] によりまとめられた．本稿では，Goldreich の安全性モデルを拡張し，提案するマルチサービス環境における相手認証の安全性を示す．また同モデルを用いて，**サービス間のリンク不能性**を定義し，提案手法がこれを満たすことを示す．さらに，提案手法の実装例として，知識の対話証明を用いた相手認証の一種である Schnorr 認証を用いた認証システムを構成する．

1.3 問題点

本稿で提案する認証システムは，以下を実現することを目標にしている．

- **安全性:**サービス提供者からいかなる情報が漏えいしても，正規のユーザになり済ますことができない
- **プライバシ保護:**複数のサービス提供者から履歴が漏えいしても，それらを紐づけすることができない
- **メモリ効率性:**情報を格納するメモリサイズがサービスの数に依存しない

関連研究として，マルチサービス環境における IC カードを用いたパスワード認証が盛んに研究されている [5, 4, 6]．これらの手法では，ユーザが繰り返しサービス提供者に登録する必要がなく，また，メモリ効率性を実現する．．しかしながら， [5, 4, 6] はいずれも上記の意味での安全性を満たさない．また， [5, 4] ではプライバシ保護についての議論はなされていない．[6] では，プライバシ保護について，上記の意味よりも強い意味で実現している．

1.4 提案手法のアイデア

提案する認証システムにおいて，各ユーザはそれぞれ固有の文字列であるユーザ ID を秘密に所持し (IC カード内に格納しておく)，各サービス提供者はそれぞれ固有のサービス ID を持つとする．提案システムは，2 種類の一方向ハッシュ関数と知識の対話証明を利用した相手認証 [2, 7] から構成される．知識の対話証明を利用した相手認証は，任意の文字列を秘密鍵として扱うことが可能であり，また秘密鍵から検証鍵を推測することが困難である認証方式である．提案する認証手法の概要は，まず 2 種類の一方向ハッシュ関数にユーザ ID とサービス ID を入力し，一方の出力をそのサービスに対して一意な識別情報 (**仮名**と呼ぶ) として，サービス提供者に送る．もう一方の出力をその仮名に対応する秘密鍵とする．サービス提供者は事前に管理者から仮名と対応する検証鍵の組をデータベースとして入手している．サービス提供者は仮名をもとにその仮名に対応する検証鍵を決定する．最後に利用者とサービス提供者はそれぞれ秘密鍵と検証鍵を用いて知識の対話証明により認証を行う．

2 相手認証

本章では知識の対話証明を用いた認証のモデルと，その拡張について述べる．以後本稿では，知識の対話証明を用いた認証を相手認証と呼ぶ．

2.1 対話チューリング機械による相手認証の定義

本稿では，Goldreich [3] によるチューリング機械を用いた相手認証の定義を用いる．

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．ITM が，通信テープのうち読み込みのみ可能なテープの内容を読み取るとき，この内容を**受け取る**といい，同様に書き込みのみ可能なテープに書き込むことを**送る**という．

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，ITM A をアルゴリズム A，また，対話処理 $\langle A, B\rangle$ をプロトコル $\langle A, B\rangle$ と呼ぶ場合がある．A が確率的アルゴリズムのとき，$A_r(x)$ は，入力 x と乱数 r についての A の出力を表す．$\mathbf{N}$ を自然数全体からなる集合とし，$n \in \mathbf{N}$ の任意の多項式を $\mathrm{poly}(n)$ と表す．

定義 1 (相手認証) 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．
(1) 任意の $n \in \mathbf{N}$，任意の $\alpha \in \{0,1\}^n$，および任意の $s \in \{0,1\}^{\mathrm{poly}(n)}$ について以下が成り立つ．

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

(2) 任意の確率的多項式時間 *ITM* A と B，任意の十分に大きな $n \in \mathbf{N}$，および任意の $\alpha \in \{0,1\}^n$ について以下が成り立つ．

$$\Pr[\langle B(T_n), V\rangle(\alpha, I_{S_n}(\alpha)) = 1] < \frac{1}{\mathrm{poly}(n)}$$

ただし，S_n は $\{0,1\}^{\mathrm{poly}(n)}$ に一様分布する確率変数であり，$T_n = \langle P(S_n), A\rangle(\alpha, I_{S_n}(\alpha))$ である．

ここで，I を**情報生成アルゴリズム**，$\langle P, V\rangle$ を**相手認証プロトコル**と呼ぶ．また，P と V をそれぞれ**証明者**と**検証者**と呼ぶ．

2.2 相手認証プロトコルの拡張

ある対話処理についての共通入力とは，2 つの ITM が共有しているテープからの入力であるから，それぞれの ITM について，共通入力と同じ内容を補助入力として読み込み，同じ出力を返す ITM が実現できる．つまり，任意の対話処理 $\langle A, B\rangle$ について，

$$\langle A, B\rangle(x) = 1 \Leftrightarrow \langle A'(x), B'(x)\rangle = 1$$

である $\langle A', B'\rangle$ が存在する．また，片方の ITM が補助入力を読み込む前に，同じ内容をもう一方の ITM が通信テープに書き込むならば，その内容を補助入力として読み込まずに同じ出力を返す ITM が実現できる．つまり，任意の対話処理 $\langle A, B\rangle$ について，

$$\langle A(x), B(x)\rangle = 1 \Leftrightarrow \langle A'(x), B'\rangle = 1$$

である $\langle A', B'\rangle$ が存在する．今，任意のチューリング機械が，α を入力として $I_s(\alpha)$ を出力するオラクルを利用できると仮定すると，以下が成り立つ．

補題 1 任意の相手認証プロトコル $\langle P, V\rangle$，任意の $n \in \mathbf{N}$，任意の $\alpha \in \{0,1\}^n$，および任意の $s \in \{0,1\}^{\mathrm{poly}(n)}$ について，

$$\langle P(s), V\rangle(\alpha, I_s(\alpha)) = 1 \Leftrightarrow \langle P'(s, \alpha), V'\rangle = 1$$

である $\langle P', V'\rangle$ が存在する．

ある $\langle P, V\rangle$ に対して，上の補題の性質を持つ具体的な $\langle P', V'\rangle$ を考える．

- V^1 は，V において，共通入力の $I_s(\alpha)$ を読み込む動作を，オラクルに α を入力し $I_s(\alpha)$ を得る動作に置き換えて得られる ITM である．
- P^1 は，まず，補助入力の α を読み込み，それを通信テープに書き込んだ後，P と同様の動作を行う ITM である．
- V^2 は，V^1 において，共通入力の α を読み込む動作を，通信テープから α を受け取る動作に置き換えて得られる ITM である．

上の P^1 と V^2 による対話処理を，$\langle P, V\rangle$ に対する**拡張プロトコル**と呼び，$\langle P^+, V^+\rangle$ と表す．

補題 2 任意の十分に大きな $n \in \mathbf{N}$，任意の確率的多項式時間 *ITM* A と B，および任意の $\alpha \in \{0,1\}^n$ について，S_n を $\{0,1\}^{\mathrm{poly}(n)}$ に一様分布する確率変数，$T_n = \langle P(S_n), A\rangle(\alpha, I_{S_n}(\alpha))$ として，

$$\Pr[\langle B(T_n), V\rangle(\alpha, I_{S_n}(\alpha)) = 1] < \frac{1}{\mathrm{poly}(n)}$$

が成り立つとき，かつ，そのときに限って，任意の確率的多項式時間 *ITM* C と D，および任意の $\beta \in \{0,1\}^n$ について，X_n を $\{0,1\}^{\mathrm{poly}(n)}$ に一様分布する確率変数，$Y_n = \langle P^+(X_n, \beta), C\rangle$ として，

$$\Pr[\langle D(Y_n, \beta), V^+\rangle = 1] < \frac{1}{\mathrm{poly}(n)}$$

が成り立つ．

定理 1 $\langle P, V\rangle$ が相手認証であることは，拡張プロトコル $\langle P^+, V^+\rangle$ が以下をみたすことと同値である．
(1) 任意の $n \in \mathbf{N}$，任意の $\alpha \in \{0,1\}^n$，および任意の $s \in \{0,1\}^{\mathrm{poly}(n)}$ について以下が成り立つ．

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

(2) 任意の確率的多項式時間 *ITM* A と B，任意の十分に大きな $n \in \mathbf{N}$，および任意の $\alpha \in \{0,1\}^n$ について以下が成り立つ．

$$\Pr[\langle B(T_n, \alpha), V^+\rangle = 1] < \frac{1}{\mathrm{poly}(n)}$$

ただし，S_n は $\{0,1\}^{\mathrm{poly}(n)}$ に一様分布する確率変数であり，$T_n = \langle P^+(S_n, \alpha), A\rangle$ である．

3 マルチサービス環境における相手認証

本章では，相手認証の定義を拡張しマルチサービスにおける認証プロトコルを定義する．またそのプロトコルを用いた認証について，サービス間のリンク不能性を定義する．

3.1 マルチサービス環境における認証プロトコル

相手認証のモデルにおいて，P, V はそれぞれユーザとサービス提供者が認証を行う際のふるまいを表している．ここで，ユーザとサービス提供者を一意に表す文字列 (それぞれユーザ ID，サービス ID と呼ぶ) を a, b とする．ある 2 つの関数 f, g について，$s = f(a, b)$, $\alpha = g(a, b)$ と表すことにする．s, α をそれぞれ $f(a, b), g(a, b)$ と置き換える．オラクル I を $g(a, b)$ を入力として $I_{f(a,b)}(g(a, b))$ を出力するオラクルとする．

今，任意のチューリング機械が，ある関数 f, g を計算できると仮定し，かつ g は一方向性関数であると仮定する．一方向性関数の定義を以下に示す．

定義 2 (一方向性関数) 任意の確率的多項式時間アルゴリズム A, 任意の十分に大きい $n \in \mathbf{N}$, $x \in \{0,1\}^{\mathrm{poly}(n)}$ について，

$$\Pr[A(f(x)) = f^{-1}(f(x))]$$

を満たすとき，f を一方向性関数と呼ぶ．

補題 3 任意の $n \in \mathbf{N}$ に関して，$f : \{0,1\}^{\mathrm{poly}(n)} \times \{0,1\}^{\mathrm{poly}(n)} \to \{0,1\}^n$，$g : \{0,1\}^{\mathrm{poly}(n)} \times \{0,1\}^{\mathrm{poly}(n)} \to \{0,1\}^{\mathrm{poly}(n)}$ となるある関数の対 (f, g)，任意の拡張プロトコル $\langle P^+, V^+\rangle$，および任意の $a, b \in \{0,1\}^n$ について，

$$\begin{aligned} & \langle P^+(f(a,b), g(a,b)), V^+\rangle(b) = 1 \\ \Leftrightarrow\ & \langle P^{++}(a), V^+\rangle(b) = 1 \end{aligned}$$

である $\langle P^{++}, V^+\rangle$ が存在する．

ある $\langle P^+, V^+\rangle$ に対して，上の補題の性質を持つ具体的な $\langle P^{++}, V^+\rangle$ を考える．

- P^{++} は P^+ において，補助入力の $f(a,b)$, $g(a,b)$ を読み込む動作を，補助入力の a と共通入力の b から計算し，$f(a,b)$, $g(a,b)$ を得る動作に置き換えた ITM である．

上の P^{++} と V^+ による対話処理を，$\langle P, V\rangle$ に対する**マルチサービスプロトコル**と呼ぶ．

定理 2 $\langle P, V\rangle$ が相手認証であることは，マルチサービスプロトコル $\langle P^{++}, V^+\rangle$ が以下をみたすことと同値である．
(1) 任意の $n \in \mathbf{N}$ および任意の $a, b \in \{0,1\}^n$ について以下が成り立つ．

$$\Pr[\langle P^{++}(a), V^+\rangle(b) = 1] = 1$$

(2) 任意の確率的多項式時間 *ITM* A と B，任意の十分に大きな $n \in \mathbf{N}$，および任意の $b \in \{0,1\}^n$ について以下が成り立つ．

$$\Pr[\langle B(T_n), V^+\rangle(b) = 1] < \frac{1}{\mathrm{poly}(n)}$$

ただし，a^* は $\{0,1\}^{\mathrm{poly}(n)}$ に一様分布する確率変数であり，$T_n = \langle P^{++}(a^*), A\rangle(b)$ である．

3.2 サービス間のリンク不能性

定義 3 (サービス間のリンク不能性) 情報生成アルゴリズム I とマルチサービスプロトコル (P^{++}, V^+) から構成される相手認証は以下を満足すれば**サービス間のリンク不能性**を持つ．

任意の確率的多項式時間チューリング機械 A, 任意の十分に大きい $n \in \mathbf{N}$, 任意の $a, a', b, b' \in \{0,1\}^n$(ただし $a \neq a', b \neq b'$) について，

$$|\Pr[A(z, z_r) = r] - \frac{1}{2}| < \frac{1}{\mathrm{poly}(n)}$$

ただし，r は *1* ビットの乱数であり，z, z_0, z_1 はそれぞれ $\langle P(a), A\rangle(b)$, $\langle P(a), A\rangle(b')$, $\langle P(a'), A\rangle(b')$ を多項式回繰り返した時に通信テープに書き込まれた文字列である．

定理 3 g が一方向性関数であれば情報生成アルゴリズム I とマルチサービスプロトコル (P^{++}, V^+) から構成される相手認証はサービス間のリンク不能性を持つ．

4 提案システムの構成例

本章では，一方向ハッシュ関数と Schnorr 認証 [7] を用いた提案システムの構成例を示す．

4.1 Schnorr 認証

Schnorr 認証は，離散対数問題の困難性仮定に基づいた 3 交信プロトコルを用いた認証である [7]．Bellare らは，離散対数問題の one-more-inversion 問題の困難性仮定の上で，Schnorr 認証が安全であることを証明した [1]．

Schnorr 認証のアルゴリズムを示す．Schnorr 認証における情報生成アルゴリズム I は α を入力として，セキュリティパラメータ k について，2^k 以下の十分大きな素数 $2^{k-1} \leq p < 2^k$，及び位数が q となる $\mathbf{Z}_p$ の原始元 g，$x \in \mathbf{Z}_q$ における $(p, q, g, X = g^x \bmod p)$ の組を出力する．共通入力が $(\alpha, I_x(\alpha))$，P の補助入力が x の場合について，Schnorr 認証における認証プロトコル $\langle P, V\rangle$ を以下に示す．

- P はランダムに $y \in \mathbf{Z}_q$ を選択し，V に $Y \leftarrow g^y \bmod q$ を送る．
- V はランダムに $r \in \mathbf{Z}_q$ を選択し，P に r を送る．
- P は V に $z \leftarrow y + cx \bmod q$ を送る．
- V は，もし $g^z = YX^c$ であれば 1 を出力し，そうでないならば 0 を出力する．

4.2 提案システムの構成

利用者の集合を $\{U_1, \ldots, U_n\}$，サービス提供者の集合を $\{S_1, \ldots, S_\ell\}$，管理者を M と表す．ユーザはそれぞれ管理者に割り当てられた固有のユーザ ID を秘密に持つ，すなわち U_i は a_i を持ち，$i \neq j$ ならば $a_i \neq a_j$ である．同様にサービス提供者 S_j はそれぞれ固有のサービス IDb_j を持ち，$i \neq j$ ならば $b_i \neq b_j$ である．サービス ID はユーザ ID と異なり，公開されている．f, g を一方向ハッシュ関数とする．S_j に対する U_i の仮名，秘密鍵，検証鍵をそれぞれ $n_{i,j}$, $c_{i,j}$, $d_{i,j}$ とする．

管理者が行う準備を以下に挙げる．

- **セキュリティパラメータの設定：**適当なセキュリティパラメータ k を選択し，(p, q, g) を決定する．
- **ユーザの登録：**U_i にランダムに選択したビット列 a_i，および (p, q, g) を秘密に渡す．
- **サービス提供者の登録：**S_i にランダムに選択したビット列 b_i，および (p, q, g) を渡す．
- **サービスの開始：**以下の手順からなる．

  STEP1:U_i が S_j に登録要求を送る．

  STEP2:S_j は U_i に b_j を送る．

  STEP3:U_i は S_j に $n_{i,j} = g(a_i, b_j)$ を送る．

  STEP4:S_j は M に $b_j, n_{i,j}$ を送る．

  STEP5:M は $b_j, n_{i,j}$ から a_i を特定し，$d_{i,j} = g^{f(a_i,b_j)} \bmod p)$ を S_j に送る．

  STEP6:S_j は $(n_{i,j}, d_{i,j})$ の対をデータベースに保持する．

次に提案するマルチサービス環境における認証プロトコルについて述べる．

STEP1:U は S に認証要求を出す．

STEP2:S は U に b を送る．

STEP3:U は $n = g(a, b)$, $c = f(a, b)$ を計算し，n を S に送る．

STEP4:S は n を用いてデータベースを検索し，d を得る．

STEP5:U, S はそれぞれ c, d を用いて Schnorr 認証のプロトコルに従う．

5 終わりに

本稿では，Goldreich の安全性モデルを拡張し，提案するマルチサービス環境における相手認証の安全性を示した．また同様のモデルを用いて，プライバシ保護に関する性質であるサービス間のリンク不能性を定義し，提案手法がこれを満たすことを示した．さらに，提案手法の実装例として，知識の対話証明を用いた相手認証の一種である Schnorr 認証を用いた認証システムを構成した．

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] M. Bellare and A. Palacio. GQ and schnorr identification schemes: Proofs of security against impersonation under active and concurrent attacks. In *Advances in Cryptology - CRYPTO 2002*, LNCS. Springer-Verlog, 2002.

[2] U. Feige, A. Fiat, and A. Shamir. Zero-knowledge proofs of identity. *Journal of Cryptology*, 1(2):77–94, 1988.

[3] O. Goldreich. *Foundations of Cryptography*. Cambridge University, 2001.

[4] R.-J. Hwang and S.-H. Shiau. Provably efficient authenticated key agreement protocol for multi-servers. *The Computer Journal*, 50:602–615, 2007.

[5] W.-S. Juang. Efficient multi-server password authenticated key agreement using smart cards. *IEEE Transactions on Consumer Electronics*, 50:251–255, 2004.

[6] Y.-P. Liao and S.-S. Wang. A secure dynamic id based remote user authentication scheme for multi-server environment. *Computer standards and interfaces*, 2007.

[7] C. P. Schnorr. Efficient signature generation by smart cards. In *Journal of Cryptology*, volume 4, pages 161–174. Springer New York, 1991.