T2R2 東京科学大学 リサーチリポジトリ
Science Tokyo Research Repository

論文 / 著書情報
Article / Book Information

論題(和文)	ZKIP とほぼ同等の安全性を有する効率的なリモート生体認証の提案
Title	A Proposal of efficient remote Biometric Authentication Protocol
著者(和文)	坂下泰紀, 柴田陽一, 高橋健太, 尾形わかは, 菊池浩明, 西垣正勝
Authors	Taiki Sakashita, Yoichi Shibata, Kenta Takahashi, Wakaha Ogata, Hiroaki Kikuchi, Masakatsu Nishigaki
出典 / Citation	SCIS2008, Vol. , No. , pp. 2B3-4
発行日 / Pub. date	2008, 1
URL	http://search.ieice.org/
権利情報 / Copyright	本著作物の著作権は電子情報通信学会に帰属します。 Copyright (c) 2008 Institute of Electronics, Information and Communication Engineers.

Powered by T2R2 (Science Tokyo Research Repository)

All rights are reserved and copyright of this manuscript belongs to the authors. This manuscript has been published without reviewing and editing as received from the authors: posting the manuscript to SCIS 2008 does not prevent future submissions to any journals or conferences with proceedings.

SCIS 2008 The 2008 Symposium on Cryptography and Information Security
Miyazaki, Japan, Jan. 22-25, 2008
The Institute of Electronics, Information and Communication Engineers

ZKIP とほぼ同等の安全性を有する効率的なリモート生体認証の提案

A Proposal of efficient remote Biometric Authentication Protocol

坂下泰紀* Taiki Sakashita　柴田陽一*†† Yoichi Shibata　高橋健太† Kenta Takahashi

尾形わかは‡ Wakaha Ogata　菊池浩明‡‡ Hiroaki Kikuchi　西垣正勝**†† Masakatsu Nishigaki

あらまし 証明者と検証者の間で秘密計算を行うことで，ネットワークを介しての生体認証を安全に実現する方式（ZeroBIO 方式）が提案されている．今までに，区間の零知識証明を利用した方式や，秘匿ニューラルネットワーク評価を用いた方式が挙げられている．いずれの方式も高い安全性を有しているが，同時に大きな計算量と通信量を必要とする．本稿では，わずかな安全性の低減を許容することで，より小さな計算量と通信量で実現可能なリモート生体認証方式を提案する．

キーワード 生体認証,キャンセラブルバイオメトリクス

1 はじめに

近年，セキュリティを必要とする分野を中心に日常生活の中でも生体認証技術が活用され始めた．携帯電話での指紋認証[1]，掌や指の静脈を用いた ATM[2]，さらに医療分野では指紋認証を組み込んだ電子カルテ[3]などが導入されており，今後もその適用範囲，量ともに増加すると推測される．

従来のパスワードや IC カードを用いた認証方式と異なり，生体情報は紛失・忘却の恐れがないという利点がある．その一方で，生体認証を行う場合には，検証者がユーザの生体情報を確認するために，証明者の生体情報（もしくはそれに相当するもの）をテンプレートとして検証者に預ける必要がある．ところが，生体情報は各個人の身体的な情報であり，生体情報から本人の特定，または本人に関する副次的な情報を得ることができる可能性があるため，重要なプライバシ情報となる．さらにネットワークを介した生体認証を考えた場合，検証者が常に信頼できるとは限らず，テンプレートを暗号化などの処理をしないままで検証者に保持させる方式は安全とは言えない．また，生体情報は基本的に終生不変であり，生体情報の盗難・悪用に対して，生体情報を登録し直すなどといった方策を採ることが困難である．これらのことから，ネットワークを介して生体認証を安全に行うことができる方式が要求されている．

これに対してRathaらはキャンセラブルバイオメトリクス[4]という概念を導入し，画像ブロック変換，マニューシャ非線形変換などの方式を提案した．また，太田らは虹彩情報に対して回転や歪曲などの変換を施す方式を[5]，比良田らは2次元画像からなる生体情報に対する方式を提案している[6]．キャンセラブルバイオメトリクス方式では，変換に使用した乱数を変更する事で登録した生体情報を更新することが可能である．しかし，キャンセラブルバイオメトリクスは，認証の際に提示された生体情報とテンプレートの類似度を検証者が算出する方式であるため，内部犯（検証者）の攻撃に対してロバストではない．

一方，永井らは，検証者と証明者間で管理する情報が異なる非対称生体認証（ZeroBIO）方式[7]という概念を提

* 静岡大学情報学部，〒432-8011　静岡県浜松市城北 3-5-1, Faculty of Informatics, Shizuoka University, 3-5-1 Johoku, Hamamatsu-shi, Shizuoka-ken, 432-8011, Japan
† 株式会社日立製作所 システム開発研究所，〒215-0013 神奈川県川崎市麻生区王禅寺 1099 番地，Hitachi, Ltd., System Development, Lab., 1099 Ohzenji, Asao-ku, Kawasaki-shi, Kanagawa 215-0013, Japan
‡ 東京工業大学イノベーションマネジメント研究科，〒152-8552 目黒区大岡山 2－12-1，Tokyo Institute of Technology, 2-12-1 O-okayama, Meguro-ku, Tokyo, Japan
‡‡東海大学電子情報学部情報メディア学科，〒259-1292　神奈川県平塚市北金目　1117　東海大学，Department of Information Media Technology,School of Information Technology and Electronics,Tokai University,1117 Kitakaname,Hiratsuka,Kanagawa,259-1292 Japan
** 静岡大学創造科学技術大学院，〒432-8011 静岡県浜松市城北 3-5-1，Graduate School of Science and Technology, Shizuoka University, Shizuoka University, 3-5-1 Johoku, Hamamatsu-shi, Shizuoka-ken, 432-8011, Japan
††独立行政法人科学技術振興機構，CREST，Japan Science Technology and Agency, CREST

案し，ニューラルネットワークを用いて，証明者の生体情報を検証者に秘匿したままで，証明者が正しい生体情報の持ち主であることをゼロ知識証明にて示す認証方式を示した．また，尾形らも，登録時のテンプレートと認証時の生体情報が「十分に近いこと」を証明するゼロ知識証明に基づいた非対称生体認証方式を提案している[8]．いずれの方式も高い安全性を有しているが，計算量，通信量が大きいことが問題であった．

そこで本稿では，わずかな安全性の低減を許容することで，より小さな計算量と通信量で実現可能なリモート生体認証方式を提案する．具体的には準同型写像の性質を有する暗号化関数を用いて証明者に秘密計算を行わせることで，検証者の不正に対する安全性を保ちつつ，非対称生体認証における計算量および通信量の低減を実現する．

本稿の構成を以下に述べる．2 章で生体認証の要件の提示を行い，3 章で既存研究を説明する．4 章で準同型性写像の性質を有する暗号化関数を用いて秘密計算を行う非対称生体認証プロトコルを提案する．5 章で提案方式が 2 章で挙げた要件を満たしていることを確認し，既存研究よりも計算量・通信量の面で優れていることを示す．最後に 6 章でまとめる．

2　生体認証方式

2.1　生体認証モデル

生体認証のモデルは，テンプレートの保管箇所によって，サーバ認証モデルとクライアント認証モデルに分類できる．サーバ認証モデルにおいては，テンプレートはサーバで集中管理され，認証時にもサーバで照合が行われる．一方，クライアント認証モデルではテンプレートは IC カードなどに格納され，端末側で IC カードの利用者認証が行われる．クライアント認証モデルでは，テンプレートを各個人が管理できるため，利用者に受け入れられやすいという利点があるが，テンプレートの安全性が IC カードの耐タンパ性のみに依存してしまい，コストもかかるという欠点がある．対してサーバ認証モデルではテンプレートをサーバが管理するために利用者の心理的抵抗が大きいという欠点がある．

ところが，サイドチャネル攻撃により IC カードに保存されている情報をかなりの精度で解読可能であるという報告もされており[9]，IC カードにテンプレートを保存するクライアント認証モデルでは，IC カードの盗難などにより攻撃者にユーザの生体情報に関する情報を得られてしまう可能性が否定できない．そこで，本稿ではサーバ認証モデルを対象に議論を行う．ただし，サーバ認証モデルでは，サーバ側で認証を行うため，平文のままで生体情報（テンプレート）をサーバに提示・保存することは安全性，およびプライバシの観点で問題となる．そこで本稿では，ユーザが保持する IC カードに暗号化鍵などの補助情報を格納しておき，その補助情報を用いることでサーバに生体情報そのものは知らせることなく，生体認証を行う方式に焦点を当てる．このとき，IC カードに保存されている補助情報からは生体情報に関する情報を得ることはできず，IC カードが攻撃者に盗難されただけではなりすましなどをされる恐れはない．したがって，本方式の仮定においては，IC カードは耐タンパ性を有する必要はない．

2.2　攻撃モデル

攻撃モデルは攻撃者の目的とアタックモデルに分類できる．

攻撃者の目的　通常のユーザ認証システムにおける攻撃者の目的である「なりすまし」と，生体認証特有の攻撃目的である「生体情報そのものを得ること」の2つとする．

アタックモデル「サーバによる不正」,「IC カードの盗難」,「通信路の盗聴」のいずれかが行われるとする(同時に2つのアタックは行われないこととする).認証プロトコル中に通信路を流れる情報はすべてサーバが送受信するデータであるので,サーバによる不正を防ぐことができれば盗聴者による不正も防ぐことができる．

2.3　生体認証システムの要件

攻撃モデルから生体認証システムは以下の要件を満たす必要がある．

要件 1：サーバに保存されている情報から生体情報に関する情報を得ることはできない．

要件 2：IC カードに保存されている情報から，生体情報に関する情報を得ることはできない．

今回，IC カードの耐タンパ性は仮定しないため，IC カードを入手した攻撃者は IC カード内の全データにアクセスすることができることに注意されたい．

要件 3：IC カードを手に入れても，登録した生体情報に十分近い生体情報を知らない限り，ユーザになりすますことはできない．

要件 4：登録した生体情報に十分近い生体情報を知らない限り，通信路の盗聴で得た情報を用いても，ユーザになりすますことはできない．

3　既存研究

3.1　キャンセラブルバイオメトリクス

キャンセラブルバイオメトリクスでは，何らかの乱数を用いて生体情報をマスクし，マスクされた情報をテンプレートとしてサーバに登録する．安全性のため，生体情報をマスクする乱数はある程度以上の情報量を持つ必要があり，ICカード内で保管される．認証する際には乱数によってマスクされた生体情報を用いて入力された生体情報とテンプレートとの比較を行うため，使用する生体情報の比較手法にあわせ，マスク方法を考える必要がある．

太田らによる方式[5]では，ハミング距離によって比較を行うことができる虹彩情報を対象としたキャンセラブル認証方式を構築している．具体的には，以下のとおりである．虹彩情報は，mビット列とみることができる．登録時の虹彩情報 $X \in \{0,1\}^m$ に対して，認証時の虹彩情報 $X' \in \{0,1\}^m$ が $W_H(X \oplus X') \le m\theta$ を満たすとき，本人

であると判定する．ただし，$W_H(\cdot)$はビット列のハミング重み，$\theta \in [0,1]$は閾値である．文献[5]の方式では，ランダムなビット列$R \in \{0,1\}^m$をICカード内に保管した上で，テンプレートとして$Y = X \oplus R$をサーバに登録する．認証時には，ユーザは虹彩情報X'とRから$Y' = X' \oplus R$を計算し，これをサーバに送信する．サーバはテンプレートYと受信したY'から$Y \oplus Y' = X \oplus X'$を計算し，ハミング重みがしきい値以下であれば本人であると判定する．

比良田らは，2次元画像からなる生体情報を取り扱うことのできるキャンセラブル認証方式を提案している[6]．この方式では，登録時の生体情報（2次元画像のフーリエ変換画像）$G(u,v)$と乱数$R(u,v)$の積$R(u,v)\,G(u,v)$がテンプレートとしてサーバに保管され，認証時には生体情報（2次元画像のフーリエ変換画像）の複素共役$G^*(u,v)$に対して$R^{-1}(u,v)\,G^*(u,v)$がサーバに送信される．サーバで$R^{-1}(u,v)G^*(u,v)R(u,v)G(u,v) = G^*(u,v)G(u,v)$によって乱数要素が相殺され，2つの画像の相互相関関数を計算することが可能である．乱数$R(u,v)$はICカード内に保管する．

これらの方式では，テンプレートは乱数によってマスクされているため，テンプレートからは生体情報について何の情報も漏れない．また，ICカードには乱数しか得ることができず，ICカードからも生体情報は漏洩しない．しかし，通信路を盗聴して得た情報を再送（再送攻撃）することによって，なりすましが可能であるため，要件3を満たさない．また，認証の際に提示された生体情報とテンプレートの類似度をサーバが計算する方式となっているため，サーバは両者の生体情報の差異を知ることができ，要件1を完全に満たしているとは言えない．

3.2 ZeroBIO方式1：永井らの方式

永井らは秘匿ニューラルネットワーク評価を用いることで，入力された生体情報が正しい出力を導くことを，生体情報を秘匿した状態で証明するプロトコルを提案した．

具体的には，登録時に本人と他人の複数の指紋データを読み取り，特徴量ベクトル$x = (x_1, x_2, ..., x_n)$の学習セットを作る．すべての特徴量ベクトルをニューラルネットワークの入力として与え，本人の特徴量ベクトルに対してはニューラルネットワークの出力が1，他人の特徴量ベクトルに対しては出力が0となるようにニューラルネットワークの重みを学習させる．そして，学習後のニューラルネットワークの中間層の重みw_{ij}のコミットメントと出力層の重み$\overline{w}_j$をサーバに登録しておく．コミットメントは，以下に示す藤崎，岡本らのコミットメント方式[10]を用いる．Nを誰もその素因数を知らない大きな合成数とし，g, hをZ_Nの要素とする．誰もhの離散対数を知らないとする．このとき，

$$Com(m,r) = g^m h^r \qquad (\mathrm{mod\ N})$$

をmのコミットメントとする．ただしrは十分大きい乱数とする．このコミットメントは準同型性

$$Com(x_1,r_1)\cdot Com(x_2,r_2) = Com(x_1+x_2, r_1+r_2)$$

を満たす．なお，Z_Nの位数は誰にも分らないので，$x_1 + x_2$などはmod演算ではない．

ユーザはその後w_{ij}およびコミットメントに用いた乱数r_{ij}をICカードに保持する．

認証時にユーザはICカードからw_{ij}, r_{ij}を取り出し，新たに取得した生体情報x'用いて，中間層ユニット値

$$y'_j = \sum_{i=1}^{n} w_{ij} x'_i$$

と，y'_jのコミットメント$\left(E\left(y'_j,\ R_j\right)\right)$に等価な

$$Y_j = \prod_{i=1}^{n} W_{ij}^{x'_i} \qquad (1)$$

を求めて，サーバに送る．ここでR_jは

$$R_j = \sum_{i=1}^{n} r_{ij} x'_i$$

と定める．

ユーザは式(1)を満たす生体情報x'を保持していることと，Y_jがy'_jの正しいコミットメントであることをゼロ知識証明する．その後サーバは登録された出力層の重み$\overline{w}_j$と中間層ユニットの値y'_jを用いたニューラルネットの出力値が閾値以上ならば認証を受理する．

3.3 ZeroBIO 方式 2：尾形らの方式

キャンセラブルバイオメトリクスでは生体情報を乱数によってマスクしてテンプレートとするが，尾形らの方式ではマスクキングに前述した藤崎，岡本らのコミットメント方式を使用する．以下に，方式の主な流れを示す．

生体情報の登録時には，ユーザは生体情報xのコミットメント$E = Com(x,r)$を計算し，これをテンプレートとしてサーバに登録する．ここで用いた乱数rはICカード内に保管する．このとき，コミットメントの性質より，テンプレートからは生体情報が漏れることはない．

リモート認証の際には，ユーザは取得した生体情報x'のコミットメント$E' = Com(x',r')$を計算し，これをサーバに送る．ユーザが本人である場合，2つのコミットメントにコミットされている2つの値は「近い」．そこでユーザは，「コミットされている2つの値が十分に近いこと」を証明するゼロ知識証明プロトコルを実行する．

具体的には，登録されている生体情報xの予測値$\tilde{x} \in \{x', x' \pm 1, x' \pm 2, ... x' \pm \theta\}$の全てに対して$\tilde{E} = Com(\tilde{x}, r)$を計算し，$\tilde{E}$にコミットされている$\tilde{x}$と$E'$にコミットされている$x'$が十分近い(差が$\theta$以内である）ことを，区間のゼロ知識証明を用いて証明する．サーバは，2θ+1個の証明のうち，少なくとも1つが正しければ認証を受理する．

4 提案方式

4.1 要素技術

提案プロトコルでは，生体情報の暗号化として準同型写像の性質を有するエルガマル暗号を用いる．

Pを大きな素数，Z_pの原始元をgとして，秘密鍵

$s \in Z_p$ を選択し，公開鍵を $y = g^s \pmod{P}$ ，およびp, gとする．

生体情報xの暗号文$Enc(x)$は乱数r, $k \in Z_p$ として

$$Enc(x) = (g^r, g^{kx} \cdot y^r) = (G, M) \pmod{P}$$

となる．また，復号は

$$g^{kx} = M / G^s \pmod{P}$$

である．このとき，$Enc(x_1) \cdot Enc(x_2) = Enc(x_1 + x_2)$ が成立する．

本稿では，上記の性質を用いて，暗号化された生体情報とテンプレートを復号することなく，生体情報とテンプレートの差分の暗号文をサーバに計算させる．サーバは暗号文を復号できないため，生体情報とテンプレートの差分を知ることができない．

4.2 概要

2章で述べた要件をすべて満たし，永井ら，尾形らの方式より小さな計算量と通信量で実行可能な非対称生体認証方式を提案する．

本方式は登録フェーズと認証フェーズの2つのフェーズからなる．登録フェーズで本人の生体情報を暗号化し，サーバに登録する．認証フェーズでは，ユーザは自らの生体情報を暗号化し，サーバに送る．サーバは登録されている生体情報と認証時の生体情報の差分の暗号文を暗号化関数の準同型性を利用して計算し，ブラインド定数を掛けてユーザに返送する．ユーザは，その差分が閾値以下であることをサーバに証明する．なお，本稿では説明を簡単にするため，生体情報間の距離が差の絶対値で定式化できると仮定する．

4.3 認証方式

・事前処理

共通パラメータ：素数p，剰余類Z_p の原始元g（以下では$\bmod p$を省略する），ハッシュ関数$Hash(\cdot)$，閾値θ，$\Delta = \{0, \pm 1, \pm 2, \ldots \pm \theta\}$とする．つまり生体情報間の差異が$\Delta$に含まれるなら，2つの生体情報は「十分近い」と判断する．

・登録フェーズ

Step 1-1: ユーザは$k, r \in Z_p \quad (k \neq 0)$をランダムに選ぶ．

Step 1-2: ユーザはエルガマル暗号の秘密鍵sとそれに対応する公開鍵$y = g^s$を生成し，生体情報x(登録情報)の暗号文$(t_1, t_2) = (g^r, g^{kx} \cdot y^r)$を計算する．

Step 1-3: ユーザはyと(t_1, t_2)をサーバに送信する．

Step 1-4: サーバはユーザのIDと共にy，(t_1, t_2)を保管し，ユーザはICカードにs, y, kを保存する．

・認証フェーズ

Step 2-1: ユーザはICカードから乱数kを取り出し，乱数r'を生成した上で，新たに生体情報x'を取得し，暗号文$(t_1', t_2') = (g^r, g^{kx'} \cdot y^{r'})$を計算してサーバに送信する．

Step 2-2: サーバは乱数$z, R \in Z_p$を生成し，$(w_1, w_2) = (g^z t_1 / t_1', R y^z t_2 / t_2')$をユーザに送信する．

Step 2-3: ユーザは秘密鍵を用いて(w_1, w_2)を復号し，平文$m = R \cdot g^{k(x-x')}$を得る．その後，乱数$S \in Z_p$を生成して，$\Delta' = \{Hash(S \| m \cdot g^{kd} \mid d \in \Delta)\}$を計算し，サーバに$\Delta'$と$S$を送信する．ここで‘ || ’は連結を意味する．

Step 2-4: サーバは$Hash(S \| R)$を計算し，$Hash(S \| R) \in \Delta'$を満たすならば，ユーザが本人であると認める．

上記で，$x - x' \in \Delta$であれば$m \cdot g^{kd} = R$となる$d \in \Delta$が必ず存在するはずである．よってxに十分近いx'を保持しているユーザであれば，認証に成功する．

上記のプロトコルの流れを図1に示す．

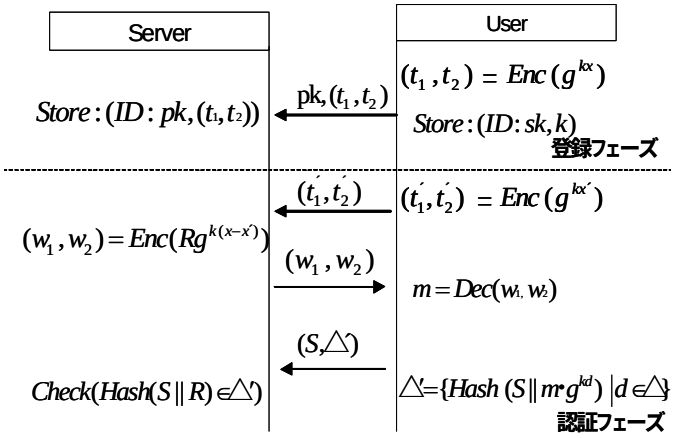

図1：提案プロトコル

5 考察

5.1 安全性

上記のプロトコルが2章で挙げた要件を満たすことを示す．

要件1：サーバは登録時に$(t_1, t_2) = (g^r, g^{kx} \cdot y^r)$と，認証時に$(t_1', t_2') = (g^r, g^{kx'} \cdot y^{r'})$を得るが，秘密鍵$s$を持たないため，生体情報に関する情報を得ることはできない．

また，Step 2-3においてユーザは復号結果にハッシュを掛けた値をサーバに返す．そのため，サーバが(w_1, w_2)として任意の暗号文をユーザに送信して，復号させるような攻撃を行っても，復号結果にハッシュを掛けた値がサーバに返されるため，サーバはユーザを復号マシンとして用いることはできない．

さらに，生体情報の取り得る範囲が限定されていることを利用して，テンプレートや提示された生体情報およびStep 2-3のΔ'に対する総当りでxや$x - x'$を突き止める攻撃も考えられるが，生体情報に乱数kを乗じることでkxの取り得る範囲をZ_p全体に広げているため，kを知らない攻撃者にとってのそのような総当りを実時間内に終えることは不可能である．したがって，サーバの不正により生体情報に関する情報が漏れることはない．

要件2：ICカードに格納されている情報は秘密鍵s，乱数kのみである．よってICカードに保存されている情報からは生体情報に関する情報を得ることはできない．

要件3：上記で示したように，本方式では，ICカードに保存されている情報から生体情報に関する情報を得ることはできないため，ユーザが正しく計算を行うことが仮定で

きるのであれば，要件3についても満たしていると言える．

ただし，実際には攻撃者が必ず正しい計算を行うことを期待することはできない．Step 2-3において，サーバは「ユーザが確かに$d \in \Delta$を用いてΔ'を計算しているか」どうかを判別することはできないため，登録されている生体情報と自身の生体情報の差分を知っている攻撃者ならば，dの代わりにその差分値を用いてΔ'を計算することで，本人認証を不正に成功させることが可能である．しかし，登録されている生体情報と自身の生体情報の差分を知っている攻撃者は，登録されている生体情報を知っていることと等価であると言えるため，そのような攻撃者を想定する必要性はそれほど大きくないと言える．

なお，5.3節では，この問題に対して提案方式を改良し，より安全性を向上させた認証方式について検討する．

要件4：攻撃者はStep 2-1において，通信路の盗聴によって得た正規ユーザの(t_1', t_2')を再送することができる．しかし，Step 2-2でサーバは毎回異なる乱数z, Rを用いて(w_1, w_2)を計算するため，秘密鍵sを知らない攻撃者はこれを復号することができず，なりすましは成功しない．

5.2　既存の非対称生体認証方式との比較

永井らの方式，尾形らの方式はいずれも高い安全性を有していたが，計算量，通信量が大きくなるという欠点も有していた．本節ではそれらの方式と提案方式について，通信量と計算量の点でどれほどの差異があるかを考察する．計算量は1回の認証フェーズ中に必要となる累乗計算の数で比較を行ない，通信量は1回の認証フェーズ中に送信する$\log p$[bit]のデータの転送個数で比較を行う．なお，尾形らの方式は，ICカード内に格納する補助情報を追加することにより，安全性を低減させることなく，計算量・通信量を削減するという改良方式が文献[11]で報告されている．しかし，同様の効率化は本提案方式にも適用可能であるため，今回は尾形らの方式も本提案方式も効率化を行わない状態で比較を行うことにする．

提案方式と永井らの方式，尾形らの方式の計算量および通信量の見積もりを行った結果は表1の通りである．なお表中のlはニューラルネットワークにおける中間層ユニットの数である．

まず，永井らの方式と比較を行う．永井らの方式では，生体情報をn次元ベクトルとしてニューラルネットの入力層に代入するが，今回は我々の方式との比較のために，ニューラルネットへの入力ベクトルの要素数は1とした．表1から，永井らの方式は計算量，通信量共にニューラルネットの中間層の数lに比例することがわかる．lは認証精度に直結するものであり，提案方式においてはθに相当する．lとθは尺度が異なるため，両方式と直接比較することはできないが，少なくとも永井らの方式では，登録時にニューラルネットワークの重みを学習させる必要があり，そのコストは決して小さくない．

次に尾形らの方式と比較すると，提案方式はユーザの計算量・通信量：およそ1/20，サーバの計算量：1/(18θ+9)，通信量：1/(2θ+1)の効率化を達成している．

表1:提案方式と既存方式との計算量と通信量の比較

		永井らの方式	尾形らの方式	提案方式
通信量	ユーザ	$6l$	$40\theta+21$	$2\theta+4$
	サーバ	$2l$	$4\theta+2$	2
計算量	ユーザ	$5l+1$	$40\theta+22$	$2\theta+4$
	サーバ	$5l$	$36\theta+18$	2

5.3　提案方式の改良

ここでは，5.1節の要件3にて述べた問題に対して提案方式を改良し，ユーザは必ず正しいdの値$(d \in \Delta)$を用いてΔ'を計算しなければならないプロトコルを実現する．

具体的には，登録フェーズで，ユーザはすべてのdの暗号文をサーバに送信しておく．認証フェーズでは，サーバがランダムビットbを生成し，$b=0$の時には，Rdの暗号文をユーザに送信し，ユーザの返答が$Hash(S \| R) \in \Delta'$を満たすことを検証することにより，ユーザが正しいdの値を用いて計算していることを確認する．次にプロトコルの詳細を述べる．

・事前処理

4.3節の事前処理と同様である．

・登録フェーズ

Step 1-1:　ユーザは$k, r \in Z_p$　$(k \neq 0)$，および，各dに対して$r[d] \in Z_P (d \in \Delta)$をランダムに選ぶ．ここで，$r[d]$はそれぞれの$d$を暗号化するために用いる乱数である．

Step 1-2:　ユーザはエルガマル暗号の秘密鍵sとそれに対応する公開鍵$y = g^s$を生成し，生体情報x(登録情報)の暗号文$(t_1, t_2) = (g^r, g^{kx} \cdot y^r)$と，$d \in \Delta$の暗号文の集合$E(\Delta) = \{(g^{r[d]}, g^{kd} \cdot y^{r[d]}) \mid d \in \Delta\}$を生成する．

Step 1-3:　ユーザはyと(t_1, t_2)と$E(\Delta)$をサーバに送信する．この時，$E(\Delta)$の順序は暗号文と平文の対応関係がわからないように任意に並び替えてサーバに送信する．

Step 1-4:　サーバはユーザのIDと共にy，(t_1, t_2)，$E(\Delta)$を保管し，ユーザはICカードにs, y, kを保存しておく．

・認証フェーズ

Step 2-1:　ユーザはICカードから乱数kを取り出し，乱数r'を生成した上で，新たに生体情報x'を取得し，これの暗号文$(t_1', t_2') = (g^r, g^{kx'} \cdot y^{r'})$を計算してサーバに送信する．

Step 2-2からStep 2-4はL回独立に平行して行う．

Step 2-2:　サーバはランダムビット$b \in \{0,1\}$を生成し，$b=0$のとき，$z, R \in Z_p$，$(e_1, e_2) = e \in E(\Delta)$をそれぞれランダムに選択し，$(w_1, w_2) = (e_1 g^z, e_2 R y^z)$をユーザに送信する．

$b=1$のとき，$z, R \in Z_p$をランダムに選択し，$(w_1, w_2) = (g^z t_1/t_1', R y^z t_2/t_2')$をユーザに送信する．

Step 2-3:　ユーザは秘密鍵を用いて(w_1, w_2)を復号し，平文mを得る．その後，乱数$S \in Z_p$を生成した上で，$\Delta' = \{Hash(S \| m \cdot g^{kd} \mid d \in \Delta)\}$を計算し，サーバに$\Delta'$

とSを送信する．

Step 2-4: サーバは$Hash(S \| R)$を計算し，$Hash(S \| R) \in \Delta'$を満たすか確認する．

Step 2-5: Step 2-4が常に成り立つならば本人であると認める．

上記のプロトコルを図2に示す．

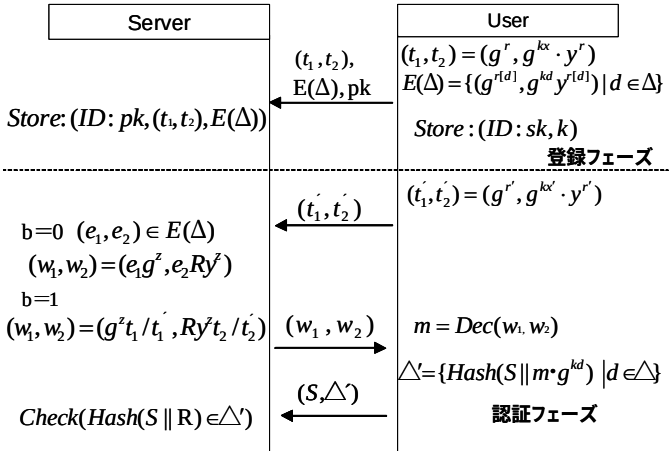

図2：改良プロトコル

・考察

まず，提案方式においては，ユーザが正しい計算を行わなければ認証に成功しないことを示す．$b = 0$の時，サーバが無作為に選んだeの平文であるdを用いた計算がΔ'に含まれていなければStep 2-4でのチェックに成功しない．しかし，攻撃者はサーバがどのeを選んだのかを知ることができないため，すべての$d \in \Delta$を用いて，正しく計算を行わなければならない．一方，$b = 1$の時は，攻撃者が任意のdでΔ'の計算を行うことができる．よって，攻撃者は$b = 0$のときは，正しく計算を行い，$b = 1$の時に不正を行えばよい．ところが，改良方式において，(w_1, w_2)は乱数Rでブラインドされているため，ユーザはbの値を知ることはできない．よって，攻撃者がL回のチェックをすべてクリアできる確率は$(1/2)^L$となり，十分に大きなLをとれば，これは無視できるほど小さくなる．

次に改良による計算量および通信量の増減について考察する．ユーザはStep 2-2からStep 2-4をL回行う必要があるため，改良方式の通信量および計算量は表2のようになる．改良方式では通信量と計算量はθだけでなくセキュリティパラメータLにも依存することにため，安全性と計算量および通信量はトレードオフの関係となる．したがって改良方式においては，要求されるセキュリティレベルに応じたLを設定することが重要である．

表2：改良方式の計算量および通信量

		永井らの方式	尾形らの方式	提案方式	改良方式
通信量	ユーザ	$6l$	$40\theta+21$	$2\theta+4$	$L(2\theta+2)+2$
	サーバ	$2l$	$4\theta+2$	2	$2L$
計算量	ユーザ	$5l+1$	$40\theta+22$	$2\theta+4$	$L(2\theta+2)+2$
	サーバ	$5l$	$36\theta+18$	2	$2L$

6 まとめ

本稿ではユーザが秘密計算を行うことにより，生体情報の漏洩となりすましに耐性のあるリモート生体認証プロトコルを提案した．また既存手法と計算量，通信量の比較を行い，提案方式が比較的小さな計算量，通信量で非対称生体認証を実現できることを示した．

参考文献

[1] 富士通，“ FMWORLD.NET（個人）：携帯電話(FOMA F901iC)：富士通 ” http://www.fmworld.net/product/phone/f901ic/

[2] 三菱東京UFJ銀行，“ スーパーICカード キャッシュカード機能：三菱東京UFJ銀行 ”，http://www.bk.mufg.jp/kouza/card/visa/cash/biometrics.html

[3] 東京武蔵野病院，“ 医療情報システム ”，http://www.tmh.or.jp/system.htm

[4] N. K. Ratha, J. H. Connell and R. M.Bolle, “Enhancing Security and Privacy in Biometrics-based Authentication Systems”, IBM Systems Journal, Vol. 40, No. 3, 2001.

[5] 太田陽基，清本晋作，田中俊昭，虹彩コードを秘匿する虹彩認証方式の提案，情報処理学会論文誌，Vol. 45, No. 8, pp. 1845-1855, 2004.

[6] 比良田真史，高橋健太，三村昌弘，「画像マッチングに基づく生体認証に適用可能なキャンセラブルバイオメトリクスの提案」2006-CSEC-34, pp. 435–440(2006)

[7] 永井慧，菊池浩明,尾形わかは,西垣正勝,「ZeroBio-秘匿ニューラルネットワーク評価を用いた非対称指紋認証システムの開発と評価」情報処理学会論文誌，Vol48,No.7,pp.2307-2318,(2007)

[8] 尾形わかは，菊池浩明，西垣正勝，「リモートバイオメトリクス認証に有効な「近い」ことを示す零知識証明プロトコル」，情報理論とその応用シンポジウム予稿集，SITA2006, pp.319–322 (2006)

[9] Paul Kocher, Joshua Jaffe, Benjamin Jun, "Differential Power Analysis", CRYPTO'99, pp.388-397, 1999.

[10] E. Fujisaki, T. Okamoto, “Statistical Zero KnowledgeProtocols ro Prove Modular Polynomial Relations,”Prpc. of CRYPTO ’99, LNCS vol. 1666,pp. 413–430 (1999)

[11] 尾形わかは，菊池浩明，西垣正勝，「区間のZKIPを用いた生体認証方式の改良」，情報理論とその応用シンポジウム予稿集，SITA2007, pp.689–693