様式 C-19

科学研究費補助金研究成果報告書

平成 22 年　5 月　31 日現在

研究種目：基盤研究（B）
研究期間：2006～2009
課題番号：１８３０００２２
研究課題名（和文）　ゼロ知識証明を用いた非対称なリモートバイオメトリクス利用者認証

研究課題名（英文）　Asymmetric Remote Biometric Authentication using Zero-Knowledge Proof

研究代表者
菊池　浩明（Kikuchi Hiroaki）
東海大学・情報通信学部・教授
研究者番号 20266365

研究成果の概要（和文）：
本研究では，ゼロ知識証明を応用する事で，生体情報を検証者に漏らさずに生体情報間の距離が小さいことを証明する認証プロトコルを提案する．生体認証に固有の問題である，特徴量の大きな変動が本研究の大きな課題であった．これに対して，複数の基準データへの照合値を用いて新たな参照ベクトルとすることで，次元の変動がない特徴量を作り出すことが出来る．認証実験に基づいて提案方式の精度を報告し，本方式の課題を検討する．

研究成果の概要（英文）：
In this study, a new method for secure remote biometric authentication preventing the vulnerability of compromised biometrics is presented. The idea is based on a public-key cryptographical protocol, referred as Zero-knowledge Proof, which allows a user to prove that she has surely a valid biometric data without revealing the data. Hence, the scheme is free from the risk of disclosure of biometric data. Even if a malicious administrator has a privilege access to the private database, it is infeasible for him to learn the private template.
The estimation based on the experimental implementation shows that the private Euclidean distance scheme archives better accuracy in terms of false acceptance and rejection than the private cosine coloration scheme, but it requires about 5/2 NL overhead to evaluate N-dimension feature vectors consisting of L-bit integers.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００６年度	3,700,000	1,110,000	4,810,000
２００７年度	1,800,000	540,000	2,340,000
２００８年度	1,900,000	570,000	2,470,000
２００９年度	1,800,000	540,000	2,340,000
総　計	9,200,000	2,760,000	11,960,000

研究分野：総合領域
科研費の分科・細目：情報学・計算機システム・ネットワーク
キーワード：セキュアネットワーク

１．研究開始当初の背景

成りすましや盗聴，辞書攻撃などを受けるパスワードやスマートカードに比べて，手軽で安全性の高いバイオメトリクス認証が注目を集めている．入退出管理，銀行の ATM や電子パスポートなどへの導入が始まり，現在の主流のパスワードや暗証番号に置き換わろうとしている．

しかしながら，インターネットにおいて電子商取引などのリモート認証の目的にバイオメトリクスを利用するためには，大きな課題がある．方式の対称性である．ここで，利用者が持つ生体情報はセンサにより読み取られ，抽出されたマニューシャなどの特徴量としてテンプレートと呼ばれる検証者であるサーバに登録されている．認証の際には，再び抽出した特徴量と照合が行われて認証結果が判定されている．このスキームは，認証者の持つ秘密情報を検証者が共有しなくてはならないという意味で対称性をなしている．それゆえに，サーバ管理者の不正により登録された生体情報が漏洩してしまう危険性が避けられない．しかも，登録情報の漏洩はバイオメトリクス認証にとって致命的である．生体情報はパスワードのように変更できないからである．

２．研究の目的

この問題に対して，本研究ではゼロ知識証明技術を応用して，認証に用いる生体情報を検証者に漏らすことなく，正しく登録されている生体情報であることだけを証明する非対称なバイオメトリクス認証方式を試みる．すなわち， リモート認証に活用できること，登録情報の修正が可能であることの２条件を満たして，リモート認証にも活用可能な認証方式にすることが研究目的である．

３．研究の方法

本研究実施は，次のサブテーマに分割できる．(1) バイオメトリクス認証における生体情報の統計的特性を調べる，(2) ゼロ知識証明によるあいまいな照合を実現する暗号プロトコルを構成する，(3) 提案プロトコルを実装する，(4)提案方式の FFR や FAR などの評価を行い，安全性を検証する，(5) 評価結果に基づき方式の改良を行う．

４．研究成果

次に挙げるゼロ知識証明プロトコルを提案した．

- ニューラルネットワークに基づくプロトコル
- 区間のゼロ知識証明を適用するプロトコル
- 多項式の根を応用するプロトコル
- グラフ彩３色問題を応用したプロトコル
- 参照ベクトルを応用したプロトコル

詳細は，参考文献（主な発表論文）を参照されたし．本研究課題の目的であったゼロ知識を用いたリモートな生体認証を安全にかつ非対称性を満たして実現できることを，具体的ないくつかの方式を提案して示した．今後の課題は，暗号化処理にかかるコストの削減やゼロ知識証明を実現するための補助情報を削除することである．

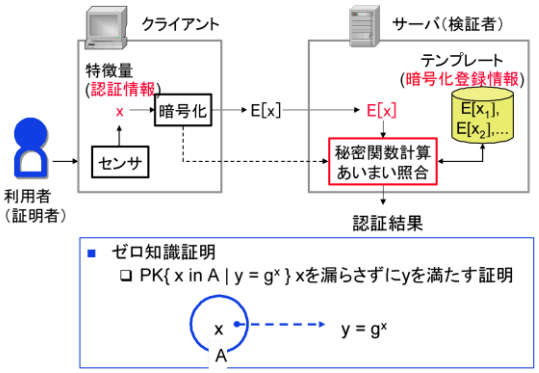

図 1　研究目的：ゼロ知識証明による生体認証

図 1 に本研究の全体構成を示す．利用者から入手した生体情報を漏らすことなく，ゼロ知識証明を用いて安全にサーバに対して証明することを目的としている．

(1) ニューラルネットワークに基づくプロトコル

階層型ニューラルネットワークは，入力層，中間層，出力層の 3 層から成る．入力層は，n個のユニット x_1，x_2，…，x_n と，バイアス項と呼ばれる常に 1 を取るユニットから成る．同様に，中間層は y_1，…，y_n とバイアス項，出力層は z の単一ユニットとする．入力層から中間層へは完全結合で重み w_{ij} によって結び付けられており，中間層から出力層への重みは u_i とする．各ユニットの出力は，シグモイド関数 $s(x) = 1/(1+e^{-x})$ により定める．

入力ユニットに対する正しい出力ユニットの組が教示信号として与えられた時，教師信号とネットワークの出力の誤差の二乗を最小化するように各重みを更新するアルゴリズムとして，バックプロパゲーション(BP)法がよく知られている．BP 法は効率のよい学習規則であり，十分な時間と重みを与えれば任意の連続関数が近似できる．暗号プロトコルの要素技術として，加法準同型性を満たす拡張エルガマル暗号を用いる．

証明者 P と検証者 V，それに，公開鍵暗号の秘密鍵を管理する鍵管理者が存在する．本方式は，登録と証明の二つのフェーズから

なる．登録では，生体情報（特徴点）を複数回取得し，教示データを作って BP 法で学習を行う．学習した重みベクトルを公開鍵暗号で暗号化して，信頼できる第三者(たとえば認証局)に登録して，生体情報証明書を発行してもらう．証明フェーズでは，認証された暗号化重みに対して，その場で取得した生体情報 X が正しく $X \in Ai$ であることをゼロ知識証明する．すなわち，$X = (x_1, \ldots, x_n)$ に対するニューラルネットワークの出力値 $z(x) = 1$ であることを証明してみせる．

(2)　区間のゼロ知識証明を適用するプロトコル

登録時に採取した生体情報 x と認証時に再取得した情報 x' は異なるが,その差 $\delta x = x - x'$ はある閾値 θ 以内に収まっていると仮定する．すると，準同型性を満たすコミットメントを用いて生体情報を $E = Com(x, r)$ とコミットすることで生体情報を秘匿したままで E との間でゼロ知識証明を行って正規利用者であることを証明することが出来る．例えば，2θ の区間の幅に入る全ての x の候補について，選言(または)のゼロ知識証明を行えばよい．しかし，そのままでは通信処理も計算処理も 2θ 倍に増加する．そこで,区間のゼロ知識証明を用いてその効率化を試みる方式である．

区間のゼロ知識証明は，区間の幅に対してログオーダーで実行が出来るため効率よく認証できる見込みがある．

特徴量の多くはスカラーではなくて，多次元のベクトルである．そこで，単純に区間のゼロ知識証明を繰り返すのではなく，代表的な類似度評価尺度を用いて，コミットされたベクトルから類似度のスカラー値に変換できれば効率が良い．認証の精度と計算時間は,この類似度方式に依存する．コミットしたベクトルと乱数要素を持ち，ベクトルを持っていることをゼロ知識証明するプロトコルを構築した．

(3)　多項式の根を応用するプロトコル

生体情報の特徴量は，値の変動だけではなく，次元をまたがって変動する．そこで，このような特徴量の要素の入れ替えや次元の変動に対して頑強な認証技術が必要である．マニューシャマッチングはそのような照合方式の例であるが，暗号ドメインでそれを実現するのは簡単ではない．ここでは，次に示す方式で，要素の変動への対応を試みる．

Alice は秘密リスト $A = \{a1, \ldots, an\}$ を持っている．Bob も秘密リスト $B = \{b1, \ldots, bn\}$ を持っており，B が A に近い，すなわち，

$|A \cap B| > \theta$

であることを知っているが，どの要素が A に属しているかは分からない．この時，Bob が B を漏らすことなく，A を知らないままで，上式を満足する B を持っていることを A に納得させたい．

リストマッチング問題についてはいくつかの先行研究があり，例えば，Kissner と Song らはマルチ集合に対する積集合の秘匿関数計算プロトコルを提案している．加法準同型性を持つ公開鍵暗号と多項式による符号化を用いて，マルチパーティで秘匿計算を実現している．しかし，本論文で扱う問題は「部分」リストマッチングであり，彼らのプロトコルをそのまま適用すると $A \cap B$ の要素が漏れる．そこで，秘密リストを多項式の根で符号化し，その多項式の補間ができることを示すことで，根の一部を持っている知識を証明するプロトコルを考える．

V は加法準同型性を満たす公開鍵暗号 $E()$ の秘密鍵 SKと公開鍵 PK の組を生成し,PK を P に公開する．$E()$ の例には，変形 ElGamal 暗号や Paillier 暗号が存在する．

検証者 V は,A の要素を根として持つ多項式 f を用いて A を符号化する．すなわち，f は $f(x) = (x - a1)(x - a2) \cdots (x - an)$ と定義される n 次の多項式である．もしも，証明者 P がこの中の k 個以上の根の集合 $C \subset B$ を持っているとすると，

$f(c1) = f(c2) = \cdots = f(ck) = 0$ である．

そこで，検証者が $D \cap A = \varnothing$ となるランダムな $D = \{d_1, \ldots, d_{n-k+1}\}$ の $n - k + 1$ 個の f の射像 $f(D)$ を与えれば，Bob は Lagrange の補間公式を用いて，任意の点 α の多項式評価 $f(\alpha)$ が出来る．しかし，そのまま補間を実行してしまっては,$f(D)$ から f の情報が漏れてしまうので，加法準同型性を満たす公開鍵暗号で暗号化したまま評価を行えばよい.ただし,P は C を知らないので,B の中からサイズ k の全ての部分集合について，多項式評価を行う必要がある．V はその nk 個の暗号文を復号して，一つでも f を満たすものがあれば P の知識を知る．

(4)　グラフ 3 彩色問題を応用したプロトコル

任意の NP 完全問題は，ゼロ知識証明できることが知られている．ここでは，グラフ 3 彩色問題，すなわち，グラフの全ての頂点を隣り合う頂点が異なる色になるように3 色に塗り分けることが出来ることを，その塗りわけ方を秘密にしたままで証明するプロトコルを応用して，正規の生体情報を持っていることをプロトコルによって証明する．

(5) 参照ベクトルを応用したプロトコル

生体情報から特徴量を抽出するにはいくつかの方法がある．指紋画像の特徴量として代表的な次の二つを考える．

① 隆線ベクトル方式.
指紋の隆線の中心を基準とした平方領域における隆線の傾きから成る n 次元のベクトルによる特徴量．登録指紋（テンプレート）と入力指紋のベクトル間類似度について本人か他人かを判断する．平行移動や画像の回転に弱く，正確な位置あわせを必要とする．

② マニューシャマッチング方式.
隆線の分岐点や端点であるマニューシャを抽出し，それらを節点とするグラフを特徴量とする方式．登録指紋と入力指紋の間の共通の部分グラフの大きさによって本人の指紋であるかどうかを判定するため，一部の節点の損失や画像の回転などの変動に対して頑強である．

指紋による生体認証では，精度が高く読み取り時の外乱に強いマニューシャマッチングが主流である．

坂田恒次らによって提案された参照ベクトル法に着目する．本方式では，基準データを複数用意して，それらに対する照合値で参照ベクトルを作る．任意の特徴量抽出アルゴリズムやマッチングアルゴリズムを基本として拡張することが可能である．参照ベクトルの次元は固定であり，マニューシャマッチングのような次元を超えた変動も起きない．基準データには人工的な指紋データを用いてもよく，秘密を漏らさずに証明を行うゼロ知識証明の対象として適している．

本論文では，参照ベクトル方式の精度を実験的に検証することを目的とする．生体情報スキャナの品質に頼らずに精度を上げる試みとして，直交基底を導入する改良方式を提案する．登録する生体情報は単一でなく，統計的な特徴が表れるのに十分な量を用意して，その中から適切な生体情報を n 個選びそれを基準データとする．認証には，入力生体情報と n 個の基準ベクトルとの間で基本特徴量比較を行い，その照合値で参照ベクトルを作る．参照ベクトルそのものを公開鍵コミットメントアルゴリズムでコミットして登録し，認証時には入力ベクトルとの間の距離が近いことを区間のゼロ知識証明プロトコルで証明する．コミットメントに用いた乱数を知らない限り，第三者がなりすましをすることが出来ないので，FAR を任意の精度で小さくすることが出来る．しかし，耐性のあるデバイスにその乱数を格納しておく必要がある．

A の中から n 個の基準データを考える．ここで，類似度関数 $f: A \rightarrow X$ を用いて，入力データ A と各基準データ i との間の類似度を $xi = f(A, i)$ を定める．f はマニューシャマッチングアルゴリズムの場合には，A と i との間で一致の条件を満たしたマニューシャの数であり，値域 X は整数の集合となる．隆線ベクトルの場合には，任意のベクトル間の類似尺度を用いることが出来，例えば，ユークリッド距離やコサイン相関などがある．

n 個の基準データ_1,...，n のそれぞれについての類似度からなる n 次元ベクトル X = ($x1$，．．．，xn)_ を入力の参照ベクトルと呼ぶ．生体情報から抽出した基本特徴量から n 個の基準データを選び，固定 n 次元の特徴量ベクトルとする．乱数を用いて公開鍵アルゴリズムでコミットして G とする．

安全なデバイスに格納しておく．入力生体情報と十分近いことを，秘匿類似度評価プロトコルにより証明する．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 5 件）

① Hiroaki Kikuchi, Kei Nagai, Wakaha Ogata and Masakatsu Nishigaki, ″Privacy-preserving similarity evaluation and application to remote biometrics authentication″, Soft Computing, Special Issue on Soft Computing in Decision Modeling, Vol. 14, No. 5, pp. 529-536, Springer, 2010.
② Taiki Sakashita, Yoichi Shibata, Takumi Yamamoto, Kenta Takahashi, Wakaha Ogata, Hiroaki Kikuchi, Masakatsu Nishigaki, ``A Proposal of Efficient Remote Biometric Authentication Protocol'', Advances in Information and Computer Security (IWSEC 2009), LNCS 5824, Springer, pp. 212-227, 2009.
③ Hiroaki Kikuchi, Kei Nagai, Wakaha Ogata and Masakatsu Nishigaki, “Privacy-Preserving Similarity Evaluation and Application to Remote Biometrics Authentication”, Modeling Decisions for Artificial Intelligence, LNCS 5285, pp. 3-14, Springer, 2008.
④ Kei Nagai, Hiroaki Kikuchi, Wakaha Ogata, and Masakatsu Nishigaki, ``ZeroBio--Evaluation and Development of Asymmetric Fingerprint Authentication System Using Oblivious Neural Network Evaluation Protocol'', In Proc. of the 2nd International Conference on Availability, Reliability and Security (ARES 2007), pp. 1155-1159, 2007.
⑤ 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指紋認証システム”，情報処理学会論文誌，査読あり，Vol.48, No. 7, pp. 2307-2318, 2007.

〔学会発表〕（計 9 件）

① 渡邊幸聖，小田雅洋，山本匠，尾形わかは，菊池浩明，西垣正勝，``曖昧性を含んだ多項式による特徴量関数を利用した非対称生体認証''，暗号と情報セキュリティシンポジウム（SCIS 2010），2F1-3，pp.1 - 6，2010 年 1 月 20 日，かがわ国際会議場（香川県）．

② 菊池浩明，尾形わかは，西垣正勝，``多項式の類似度を利用した非対称生体認証''，コンピュータセキュリティシンポジウム（CSS 2009），D4，No. 2，pp. 1-6，2009 年 10 月 27 日，富山国際会議場（富山県）．

③ 菊池浩明，河野瞬，畔上洋平，西垣正勝，尾形わかは，``直交基底指紋への参照度を特徴量とした安全な生体認証プロトコル''，暗号と情報セキュリティシンポジウム SCIS 2009，2F4-3，pp. 1-6，2009 年 1 月 21 日，大津プリンスホテル（滋賀）

④ 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，“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”，暗号と情報セキュリティシンポジウム(SCIS2008)，2B3-4，電子情報通信学会，2008 年 1 月 23 日，フェニックス・シーガイア・リゾート（宮崎）．

⑤ 小田雅洋，尾形わかは，菊池浩明，西垣 正勝，G3C-ZKIP を用いた非対称生体認証，コンピュータセキュリティシンポジウム（CSS 2008），pp. 695-700，2008 年 10 月 10 日，沖縄コンベンションセンター．

⑥ 永井慧，菊池浩明，尾形わかは，西垣正勝，秘密計算に適する距離の使用によるリモート生体認証，暗号と情報セキュリティシンポジウム SCIS 2008， 2008 年 1 月 23 日，フェニックス・シーガイア・リゾート（宮崎）．

⑦ 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''，第 30 回情報理論とその応用シンポジウム予稿集（SITA 2007），2007，2007 年 11 月 29 日，賢島宝生苑(三重)．

⑧ 菊池浩明，尾形わかは，西垣正勝，``多項式の根のゼロ知識証明とリモートバイオメトリクスへの応用''，2007 年暗号と情報セキュリティシンポジウム概要集，電子情報通信学会，1C2-4，pp. 2007 年 1 月 23 日，ハウステンボス（長崎）．

⑨ 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，第 29 回情報理論とその応用シンポジウム予稿集（SITA 2006），Vol. I，pp. 319- 322，2006 年 11 月 29 日，花びしホテル（北海道）．

〔図書〕（計 0 件）

〔産業財産権〕

○出願状況（計 0 件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計 0 件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕

ホームページ等
プロジェクトホームページ
http://zerobio.cs.dm.u-tokai.ac.jp/

６．研究組織

(1)研究代表者
菊池 浩明（HIROAKI KIKUCHI）
東海大学・情報通信学部・教授
研究者番号：20266365

(2)研究分担者
西垣 正勝（MASAKATSU NISHIGAKI）
静岡大学・情報学部・准教授
研究者番号：20283335

(3)連携研究者
尾形 わかは（WAKAHA OGATA）
東京工業大学・イノベーションマネジメント研究科・准教授
研究者番号：90275313