様式 C-7-2

自己評価報告書

平成　21 年　4 月　3 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．研究計画の概要

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実現する。(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。

２．研究の進捗状況

課題(1)から(3)に関して，ニューラルネットワークに基づく方式と参照ベクトルを応用した方式を発表し，論文にまとめた。

３．現在までの達成度

②おおむね順調に進展している。

生体情報の認証方式について調査を行い，指紋照合を対象とすることを決めた。ゼロ知識証明技術の調査を行い，適用可能なものがあることを明らかにした。これまでの成果を評価するために，外部有識者を招いて，2007 年と 2009 年に 2 回ワークショップを開催した。

４．今後の研究の推進方策

課題(4)の提案方式の安全性と課題(3)の実装の改良について進める予定である。

５．　代表的な研究成果
（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　3 件）

① H. Kikuchi, K. Nagai, W. Ogata and M. Nishigaki, “Privacy-Preserving Similarity Evaluation and Application to Remote Biometrics Authentication”, Modeling Decisions for Artificial Intelligence, LNCS 5285, pp. 3-14, Springer, 2008.
② 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.

他国際会議 1 件。

〔学会発表〕（計　8 件）

① 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.
② 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.
③ 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.

他国内シンポジウム 5 件。

〔図書〕（計　0 件）

〔産業財産権〕
○出願状況（計　0 件）

○取得状況（計　0 件）

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