情報処理学会論文誌 Vol.53 No.9 2254–2266 (Sep. 2012)

曖昧性を含んだ多項式による特徴量関数の秘匿評価を利用したテンプレート保護型生体認証

西垣 正勝[1,a)] 渡邊 幸聖[2] 小田 雅洋[2] 米山 裕太[2]
山本 匠[1,3] 高橋 健太[4] 尾形 わかは[5] 菊池 浩明[6]

受付日 2011年12月5日, 採録日 2012年6月1日

概要：証明者と検証者の間で暗号プロトコルを行うことで，ネットワークを介しての生体認証を安全に実現するテンプレート保護型生体認証方式 ZeroBio が提案されている．本論文では，生体情報の特徴量を曖昧な形で多項式の根として符号化し，登録時と認証時の生体情報が近い場合のみ評価関数が多項式となるように特徴量関数を構成することによって，特徴量の変動に対して耐性を有する ZeroBio プロトコルを提案する．従来の ZeroBio プロトコルが登録時と認証時の生体情報の「近さ」を暗号プロトコルによって直接証明していたのに対し，提案方式は，生体情報が近い場合のみ成立する多項式上の Lagrange 補間を利用し，補間値の「一致」を暗号プロトコルによって検査する．提案方式は，サーバへ登録した生体情報のサーバとユーザに対する秘匿性と，類似した生体情報を有するユーザだけが認証できることを保証する．

キーワード：生体認証，テンプレート保護，ZeroBio

Template-protecting Biometric Authentication Using Oblivious Evaluation of Feature Value Function with Fuzzy Polynomial

Masakatsu Nishigaki[1,a)] Yoshimasa Watanabe[2] Masahiro Oda[2] Yuta Yoneyama[2]
Takumi Yamamoto[1,3] Kenta Takahashi[4] Wakaha Ogata[5] Hiroaki Kikuchi[6]

Received: December 5, 2011, Accepted: June 1, 2012

Abstract: "ZeroBio" has been proposed for a secure biometric authentication over the network by conducting cryptographic protocol between prover and verifier. This paper proposes another type of ZeroBio protocol in which the feature value function of biometric information is coded as a "fuzzy" polynomial. The fuzzy polynomial becomes a polynomial only when the enrolled and the presented biometric information are close enough, and thus the evaluation of the authenticity of biometric information can be conducted easily with cryptographic protocol. This paper proves that the proposed ZeroBio protocol is computationally secure.

Keywords: biometric authentication, template protection, ZeroBio

1. はじめに

近年，指紋や静脈，虹彩などの生体的特徴を用いた生体認証が注目されている．ユーザ認証技術にはパスワードなどを用いた記憶による認証や，トークンなどを用いた持ち物による認証がある．しかし，記憶による認証は一般にユーザの記憶負荷が問題であり，持ち物による認証ではトーク

[1] 静岡大学創造科学技術大学院
Graduate School of Science and Technology, Shizuoka University, Hamamatsu, Shizuoka 432–8011, Japan
[2] 静岡大学大学院情報学研究科
Graduate School of Informatics, Shizuoka University, Hamamatsu, Shizuoka 432–8011, Japan
[3] 日本学術振興会特別研究員（PD）
Research Fellow of the Japan Society for the Promotion of Science (PD), Chiyoda, Tokyo 102–8472, Japan
[4] 株式会社日立製作所横浜研究所
Yokohama Lab., Hitachi, Ltd., Yokohama, Kanagawa 244–0817, Japan
[5] 東京工業大学大学院イノベーションマネジメント研究科
Graduate School of Innovation Management, Tokyo Institute of Technology, Meguro, Tokyo 152–8550, Japan
[6] 東海大学電子情報学部情報メディア学科
School of Information Technology and Electronics, Tokai University, Hiratsuka, Kanagawa 259–1292, Japan
[a)] nisigaki@inf.shizuoka.ac.jp

© 2012 Information Processing Society of Japan

ンの所持による利便性の低下や紛失・盗難といった危険性がある．これらに対し，生体認証に用いられる生体情報は紛失・盗難の危険性がなく，記憶する必要もないため高い利便性を有している．

しかし，生体情報は機微な情報であるため，サーバに生体情報を登録することに心理的抵抗を感じるユーザが少なくなく，サーバ側では登録された生体情報の管理が難しいという問題がある．また，生体情報は生涯不変な情報なため，1 度漏洩すると使用することができない．この問題に対して，登録した生体情報を保護する方式としてテンプレート保護型生体認証方式 [1] が研究されている．

その中で，ユーザとサーバの間で暗号プロトコルを行うことで登録用生体情報と認証用生体情報の近さを秘匿計算によって評価する ZeroBio 方式 [5] という概念が，永井らによって提案されている．永井らは，秘匿ニューラルネットワーク評価を用いて，ユーザの生体情報をサーバに秘匿したままで，ユーザが正しい生体情報の持ち主であることをゼロ知識証明（ZKIP）でサーバに示す認証方式を示した．また，尾形らも，登録した生体情報と認証時の生体情報が十分近いことを区間のゼロ知識証明によって示す ZeroBio プロトコルを提案している [14]．ZeroBio 方式は，ユーザの生体情報に関する知識が完全にサーバ側に漏れないという点で，優れたテンプレート保護型生体認証方式であるといえる．

しかし生体認証には，入力のつど，歪や読み取り誤差が生じるという生体情報に特有の問題がある．ゼロ知識証明などの暗号プロトコルは，基本的には，このような曖昧な情報を扱うことができない．すなわち，ZeroBio 方式においては，生体情報の変動に対する対策の併用が不可欠となる．このため，永井らの方式では曖昧な入力に対する認証可否の判定が可能なニューラルネットワークを用いることによって，また，尾形らの方式では生体情報の変動の可能性の数だけ区間のゼロ知識証明を繰り返すことによって，生体情報の変動を吸収している．

本論文では，生体情報の特徴量を曖昧な形で多項式の根として符号化し，登録時と認証時の生体情報が近い場合のみ評価関数 $F(x)$ が多項式となるように特徴量関数を構成することによって，特徴量の変動に対して耐性を有する ZeroBio プロトコルを提案する．従来の ZeroBio プロトコルが登録時と認証時の生体情報の近さを暗号プロトコルによって直接証明していたのに対し，提案方式は，多項式 $F(x)$ の Lagrange 補間を利用し，補間値の一致を暗号プロトコルによって検査する．$F(x)$ が $n-1$ 次多項式であった場合，n 個のサンプルポイントの値から任意の点 β の値 $F(\beta)$ を Lagrange 補間によって求めることができる．よって，n 個のサンプルポイントの集合を 2 組用意し，異なるサンプルポイントから求めた補間値 $F(\beta)$ が一致すれば，$F(x)$ が $n-1$ 次多項式であることが示される．以上より，登録時と認証時の生体情報が近い場合にのみ $n-1$ 次多項式となるように $F(x)$ を構成してやることによって，補間値 $F(\beta)$ の一致/不一致を使って正規ユーザか不正者かの判別が可能となる．

提案方式は，(i) サーバおよび不正ユーザに対する生体情報の秘匿性と，類似した生体情報を有するユーザだけが認証できることを保証する．(ii) 安全性については，計算量的な安全性証明を与える．また，提案方式は (iii) ユーザが記憶・所持すべき情報も不要である．(ii) および (iii) は従来の ZeroBio プロトコルにはない性質であり，提案方式が有する大きな優位点である．詳細は 2.2 節で述べるが，本論文では，「ユーザが記憶・所持すべき情報がない」という利便性が生体認証の大きなメリットであるという観点に立ち，現時点では，十分なエントロピを有する生体情報を用いるという前提をおいている．生体情報が有するエントロピに関する考慮は本研究の重要な今後の検討課題である．

2. 準備

本章では提案方式において取り扱う数学的要素について整理する．

2.1 Lagrange 補間

x の $n-1$ 次多項式 $F(x)$ において，互いに異なる n 個のサンプルポイント $X=\{x_1,\cdots,x_n\}$ における F の値 $F(x_1),\cdots,F(x_n)$ が与えられたとき，任意の点 β における評価値 $F(\beta)$ は

$$F(\beta)=\sum_{i=1}^{n}\Lambda(i,X,\beta)F(x_i) \tag{1}$$

で計算できる．ここで，

$$\Lambda(i,X,\beta)=\prod_{j=1,j\neq i}^{n}\frac{\beta-x_j}{x_i-x_j} \tag{2}$$

である．

2.2 コミットメントと 1 方向性関数

ZeroBio 方式では，暗号プロトコルによって生体情報の近さを評価するために，加法準同型性を満たすコミットメントが用いられる．ここでコミットメントとは，情報を秘匿したまま登録し（コミット），後からその情報を不正のない形で開示する（デコミット）技術である．ただし，生体情報のエントロピは有限であるため，本来であれば，生体情報のコミットメントには乱数のインジェクションが必要である．その具体的な構成として，Fujisaki らのコミットメント [6] がある．

Fujisaki らのコミットメントは以下の性質を満たす．

(1) コミットメント $E(m,r)$ からメッセージ m に関する情報が統計的に漏れない．

(2) 任意の m,m'（$\neq m$）に対して，$E(m,r)=E(m',r')$ を満たす m'，r' を求めることは困難である．

© 2012 Information Processing Society of Japan

(3) 加法準同型性

$$E(m,r) \times E(m',r') = E(m+m', r+r') \quad (3)$$

$$E(m,r)^x = E(mx, rx) \quad (4)$$

を有する．

ここで，m はメッセージ（生体認証では生体情報），r は乱数である．

ただし，Fujisaki らのコミットメントは，デコミットの際にコミットの時点で用いた乱数 r が再び必要となる．したがって，ユーザはこの乱数をスマートカードなどのセキュアデバイスに格納して自身で所持することが求められる．本論文では，「ユーザが記憶・所持すべき情報がない」という利便性が生体認証の大きなメリットであるという観点に立ち，現時点では，十分なエントロピを有する生体情報を用いるという前提を（提案方式を利用するにあたっての要件として）おくことにする．

生体情報が十分なエントロピを有する場合は，(Fujisaki らの) コミットメントを用いなくても，加法準同型性を満たす 1 方向性関数によって，生体情報を秘匿したまま生体情報の一致/不一致を検査することが可能となる．今回は，離散対数の困難性（g^m）によって生体情報（m）を秘匿することとし，便宜上，加法準同型性を満たす 1 方向性関数 $E(m) = g^m$ を m のコミットメントと呼ぶことにする．

2.3 離散対数のゼロ知識証明

サーバに $E(y_B) = C^{y_B}$ が登録されているとき，ユーザはサーバに対して自分が y_B を知っていることのゼロ知識証明

$$PK\{y_B \mid E(y_B) = C^{y_B}\} \quad (5)$$

を次の手順によって実行できる [7], [8]．なお，y_B のエントロピは十分大きいものとする．

Step 1. ユーザは α をランダムに選び，$t = C^\alpha$ を計算し，サーバに送信する．

Step 2. サーバは $r \in Z_N$ をランダムに選び，ユーザに送信する．

Step 3. ユーザは $e = \alpha + y_B r$ を計算し，e をサーバに送信する．

Step 4. サーバは検証式 $C^e = tE^r \bmod N$ が正しければ Valid とする．

2.4 安全素数

p' を素数とし，$p = 2p' + 1$ もまた素数となるとき，p を安全素数と呼び，素数 p' をソフィー・ジェルマン素数 [9] という．安全素数を用い，Z_p の要素の中から $g^2 \neq 1 \bmod p$, $g^{p'} = 1 \bmod p$ を満たす g を選択することで，g で生成される巡回群 $\langle g \rangle$ を体 $Z_{p'}$ と同型にできる．すなわち $\langle g \rangle$ は，零元以外のすべての元が逆元を持つ．

2.5 零因子

零元 $\{0\}$ ではない環 Z_N の元 a，b が，$a * b = b * a = \{0\}$ となるとき，a，b を環 Z_N の零因子 [9] という．

3. 関連研究

近年のテンプレート保護型生体認証技術は，キャンセラブル方式，局所距離保存ハッシュ方式，バイオメトリック暗号方式，ZeroBio 方式の 4 つに大別されると考えられる．本章では，それらの方式のそれぞれを俯瞰する．

3.1 キャンセラブル方式

テンプレートの登録の際に生体情報を攪乱することによって，生体情報を保護する方式である [2], [10], [11]．攪乱関数は攪乱の前後で生体情報間の距離を保つように設計されており，認証時と登録時で同じ攪乱関数を作用させることで，サーバに（攪乱前の）生体情報を知らせることなく，テンプレートと認証用生体情報の「近さ」を判定することができる．また，攪乱関数やパラメータを変えることで，テンプレートの更新も可能となる．

テンプレートと認証用生体情報の近さがサーバ側で計算される方式であるため，サーバが不正者であった場合には，「テンプレートと認証用生体情報の近さ」がサーバ（不正者）に漏洩する．生体情報は攪乱されているため，「テンプレートと認証用生体情報の近さ」が漏洩してもヒルクライミング攻撃 [21] は困難であると考えられる．ただし，「テンプレートと認証用生体情報の近さ」を活用した効率的な攻撃が他に存在しないということが証明されているわけではない．

攪乱の前後で生体情報間の距離が保たれるということは，一般的に，攪乱関数は 1 方向性を持たない．このため，生体情報の攪乱の方法が漏洩してしまうと，テンプレート（攪乱後の生体情報）から（攪乱前の）生体情報が逆計算されてしまう．また，生体情報そのものはエントロピが低いため，総当たり攻撃によるテンプレートの解読に対抗するには，十分大きなエントロピを持つ攪乱方法を使用する必要がある．すなわち，攪乱関数やパラメータは人間の記憶容量をはるかに超えるものとなる（暗記できない）．したがって，攪乱関数およびパラメータは，スマートカードなどのセキュアデバイスに格納してユーザ自身が所持する必要がある．攪乱関数およびパラメータを Trusted Third Party に預ける形態の 3 者モデル型の運用方式 [20] も提案されている．

3.2 局所距離保存ハッシュ方式

キャンセラブル方式と同様，テンプレートの登録の際に生体情報を攪乱することによって，生体情報を保護する．生体情報の攪乱に局所距離保存ハッシュ（local sensitive hash）関数を利用しているため，サーバに（攪乱前の）生

© 2012 Information Processing Society of Japan

体情報を知らせることなく，テンプレートと認証用生体情報の「近さ」を判定することができる [4]．ただし，キャンセラブル方式が攪乱後の空間全体の距離を保存するのに対し，局所距離保存ハッシュ方式は近傍の局所距離しか保存しない．生体情報に乱数を加えてハッシュ化してやれば，乱数を変えることで，テンプレートの更新も可能となる．なお，この乱数は公開可能な情報である．

テンプレートと認証用生体情報の近さがサーバ側で計算される方式であるため，サーバが不正者であった場合には，「テンプレートと認証用生体情報の近さ」がサーバ（不正者）に漏洩する．生体情報は局所距離保存ハッシュによって攪乱されているため，不正者は「テンプレートと認証用生体情報の近さ」を利用したヒルクライミング攻撃 [21] によって生体情報空間内の一部分（ハッシュ値の距離が保存される局所空間）を探索することが可能である．逆にいえば，不正者がヒルクライミング攻撃によって探索できるのは生体情報空間内の一部分のみであるため，不正者が登録用生体情報にある程度類似している生体情報を入手できていない限り，ヒルクライミング攻撃は困難であると考えられる．ただし，キャンセラブル方式の場合と同様，「テンプレートと認証用生体情報の近さ」を活用した効率的な攻撃が他に存在しないということが証明されているわけではない．

局所距離保存ハッシュ関数は 1 方向性関数であるため，局所距離保存ハッシュ関数を公開しても，テンプレートからハッシュ化前の登録用生体情報を逆算することは困難である．このため，局所距離保存ハッシュ方式においては，キャンセラブル方式と異なり，攪乱関数（局所距離保存ハッシュ関数）をスマートカードに入れて守る必要はない．すなわち，持ち物なしの生体認証が実現できる．ただし，生体情報のエントロピが十分に大きくないと，テンプレートが漏洩した場合に（または，サーバが不正者であった場合に），総当たりによって登録された生体情報が探り当てられる危険がある．

また，典型的な局所距離保存ハッシュ関数は，多対 1 関数となっている．すなわち，実際の生体情報空間がハッシュ化によって低次元の空間に圧縮される形となる．このため，攪乱前の空間と攪乱後の空間の距離が保たれるキャンセラブル方式と異なり，本来の生体情報空間においては大きく離れる 2 つの生体情報が，ハッシュ化後の空間においては近いと判定されてしまうことが生じうる．すなわち，キャンセラブル方式と比べ，他人受入率が増大してしまう傾向にあると危惧される．

3.3 バイオメトリック暗号方式

生体情報とバインディングした乱数情報を用いて本人認証を行うことによって生体情報を保護する方式である [3], [12], [16], [17]．生体情報と乱数情報がバインディングされた情報をヘルパ情報と呼ぶ．登録時の生体情報に十分近い生体情報を有しているユーザのみが，ヘルパ情報から乱数情報を再抽出することが可能である．本人認証そのものは，乱数情報を利用して行われる．たとえば，乱数情報のハッシュ値をテンプレートとしてサーバに登録しておき，チャレンジレスポンスなどの認証プロトコルによって，その乱数情報を所持しているユーザであるか否かが検証される．サーバに登録されるテンプレートは生体情報とは無関係な乱数情報であるため，生体情報の保護が可能となる．

ヘルパ情報からの秘密情報の抽出には，誤り訂正技術を用いて認証用生体情報から登録用生体情報を復元する過程を含む．しかし，ある程度の情報量（情報ビット数）を有し，かつ，誤り訂正能力が高く，効率的に復号（誤り訂正）可能な誤り訂正符号の一般的構成法は知られていないため，誤り率が大きい生体情報に対しては，これを効率良く実装することが難しい可能性が懸念される．また，生体情報を誤り訂正符号としてコーディングするにあたっての情報がヘルパ情報に含まれることになるため，不正者がヘルパ情報を入手できた場合には，ヘルパ情報を用いて生体情報の候補を絞り込むことができる可能性がある．

ヘルパ情報の具体的な生成方法としては，生体情報と誤り訂正符号の合成 [12] や，生体情報へのチャフ情報（ディストラクタ）の混入 [3] などが存在する．ヘルパ情報から生体情報や乱数情報を逆計算することができないように設計されているため，原理的には，ヘルパ情報は公開してもかまわない．しかし，実際には，生体情報空間のエントロピの低さ，および，誤り訂正符号語空間の性質や生体情報とチャフ情報の特徴の差などから，上述のように，ヘルパ情報から生体情報の絞り込みができる可能性が考えられる．このリスクを回避したい場合には，ヘルパ情報をスマートカードなどのセキュアデバイスに格納してユーザ自身が所持するような運用を選ぶ必要がある．

3.4 ZeroBio 方式

登録時の生体情報と認証時の生体情報の近さを秘匿計算によって評価することで生体情報を保護する方式である [14]．登録時の生体情報は暗号化された形でテンプレートとしてサーバ側に登録される．認証時の生体情報も暗号化されたうえでサーバに届けられ，サーバ上でテンプレートと認証用生体情報の「近さ」が暗号化されたままの状態で評価される．暗号化関数やパラメータを変えることで，テンプレートの更新が可能である．

準同型暗号を利用した秘匿計算によって，暗号化されたままの状態でテンプレートと認証用生体情報の近さが評価される．たとえばエルガマル暗号 [13] ベースの準同型暗号を利用した場合は，登録用生体情報の暗号文がテンプレートとしてサーバにコミットされており，認証用生体情報の暗号文との除算によって，登録用生体情報と認証用生体情報の差が暗号文のまま計算できる．その後，「登録用生体

© 2012 Information Processing Society of Japan

情報と認証用生体情報の差」の暗号文をコミットメントとして，登録用生体情報と認証用生体情報の差が認証閾値以下であることを区間のゼロ知識証明によって確認する [14]．原理的には，認証プロトコルを通じて認証可否の結果以外の情報はいっさい漏洩しない．その代わりに，秘匿計算にかかる計算量が多大となることが欠点である．

生体情報のエントロピが小さい場合は，総当たり攻撃によるテンプレート（暗号化された登録用生体情報）の解読に脆弱となる．これに対抗するには，暗号化の際に十分大きなエントロピを持つ乱数をインジェクションする必要がある．しかし，この場合，準同型演算を行うためには，登録用生体情報のコミットの際に用いた乱数を認証用生体情報の暗号化の際にも使用しなければならない．このため，この乱数はセキュアデバイスに格納したうえで，ユーザ自身が所持する必要がある．エントロピが十分に大きい生体情報を利用することができる場合は，持ち物なしの形態での生体認証の実装も可能であると考えられる．

ZeroBio 方式においては，現時点までにいくつかのバリエーションが提案されている．ニューラルネット型 ZeroBio 方式 [5] は，秘匿計算を利用してニューラルネットワークの演算を暗号ドメインでエミュレートする．生体情報の曖昧性をニューラルネットワークの汎化能力によって吸収することがニューラルネット型 ZeroBio 方式の目的である．ライトウェート型 ZeroBio 方式 [15] は，サーバが「登録用生体情報と認証用生体情報の差」の暗号文を秘匿計算によって計算した後，ユーザにその暗号文をデコミットさせる．ユーザに復号鍵の所持を要求する代わりに，区間のゼロ知識証明を用いなくても本人認証が可能な方式となっている．

4. 提案方式：曖昧多項式型 ZeroBio プロトコル

4.1 概要

提案方式は登録フェーズと認証フェーズに分かれる．登録時の生体情報の特徴量を $A = \{a_1, \cdots, a_n\}$，認証時の特徴量を $B = \{b_1, \cdots, b_n\}$ とする．認証時に生じる特徴量の変動（曖昧性）を $\Delta = \{\pm 1, \pm 2, \cdots, \pm\theta\}$ とする．A のすべての要素を根として持つ n 次多項式を $f_A(x)$ とし，また，B に対して生体情報の曖昧性を含めたすべての要素 $B_\Delta = \{b_1, b_1 \pm 1, b_1 \pm 2, \cdots, b_1 \pm \theta, \cdots, b_n, b_n \pm 1, b_n \pm 2, \cdots, b_n \pm \theta\}$ を根として持つ $(2\theta+1)n$ 次多項式を $f_B(x)$ とする．すなわち，

$$f_A(x) = (x - a_1) \cdots (x - a_n), \tag{6}$$

$$\begin{aligned} f_B(x) = {} & \{x - (b_1 - \theta)\} \cdots \{x - (b_1 - 1)\}(x - b_1) \\ & \{x - (b_1 + 1)\} \cdots \{x - (b_1 + \theta)\} \cdots \\ & \vdots \\ & \{x - (b_n - \theta)\} \cdots \{x - (b_n - 1)\}(x - b_n) \\ & \{x - (b_n + 1)\} \cdots \{x - (b_n + \theta)\} \end{aligned} \tag{7}$$

である．$f_B(x)$ の $f_A(x)$ による除算を

$$F(x) = f_A^{-1}(x) f_B(x) \tag{8}$$

とする．

被認証者が正規ユーザである場合は，認証時の生体情報の特徴量 B の変動範囲内 B_Δ に登録時の特徴量 A がすべて含まれることが期待されるため，$F(x)$ は $2\theta n$ 次多項式となる（$f_A(x)$ は n 次多項式，$f_B(x)$ は $(2\theta+1)n$ 次多項式であることに留意されたい）．被認証者が正規ユーザでない場合は，A の要素の中の少なくとも 1 つが B_Δ から外れるため，$F(x)$ は多項式の形を維持できない．よって，$F(x)$ が $2\theta n$ 次多項式となれば正規ユーザとして認証される．

$F(x)$ が $2\theta n$ 次多項式であれば，$F(x)$ 上の $2\theta n + 1$ 個のサンプルポイントからの Lagrange 補間によって，任意の点 β における $F(\beta)$ が計算できる．したがって，「$2\theta n + 1$ 個のサンプルポイントの集合」を 2 組 $(\Omega_1, \Omega_2 \mid \Omega_1 \neq \Omega_2)$ 用意し，Ω_1 から補間した $F(\beta)$ と Ω_2 から補間した $F(\beta)$ が一致することを示すことにより，$F(x)$ が $2\theta n$ 次多項式であることを証明することができる．この Lagrange 補間による $F(\beta)$ の一致の検査を暗号プロトコルにより実現するものが，本論文で提案する曖昧多項式型 ZeroBio プロトコルである．

4.2 登録フェーズ

A1. ユーザは，自身の生体情報の特徴量 $A = \{a_1, \cdots, a_n\}$ を読み取り，そのすべての要素を根とする n 次多項式

$$f_A(x) = (x - a_1) \cdots (x - a_n) \tag{6}$$

を作成する．

A2. ユーザは，十分に大きな安全素数 p（$= 2p' + 1$）を選ぶ．また，$f_A(x)$ に任意の値 $\{x_i \mid x_i \notin A,\ i = 1, \cdots, 2\theta n + 2\}$ を代入し $f_A(x_i)$ を求める．そして，p' を法とする $f_A(x_i)$ の逆元 $f_A^{-1}(x_i)$ を求める．2.4 節で述べたように，任意の x_i に対する逆元 $f_A^{-1}(x_i)$ が零因子となることなく，正しく求まる．これら $2\theta n + 2$ 個の x_i が，認証時の Lagrange 補間に必要なサンプルポイントとなる．

A3. ユーザは，Z_p の要素から以下の 2 式を満たす g を 1 つ選ぶ．これにより g の指数部を剰余体 $Z_{p'}$ にすることができる．なお，g は公開されるパラメータである．

$$g^2 \neq 1 \bmod p, \quad g^{p'} = 1 \bmod p \tag{9}$$

A4. ユーザは，手順 A2 のすべての逆元 $f_A^{-1}(x_i)$ のコミットメント

$$C_i = E(f_A^{-1}(x_i)) = g^{f_A^{-1}(x_i)} \bmod p \tag{10}$$

を計算する．そして，すべてのサンプルポイントにおけるコミットメントを $\{(C_1, x_1), \cdots, (C_{2\theta n+2}, x_{2\theta n+2})\}$

© 2012 Information Processing Society of Japan

の形でサーバに登録する．サーバがコミットメントから生体情報 A を求めることは，計算量的に困難である．また，ユーザが IC カードなどに保持すべき秘密情報は存在しない．

4.3 認証フェーズ

B1. ユーザは，自身の生体情報の特徴量 $B = \{b_1, \cdots, b_n\}$ を読み取り，これに対して生体情報の曖昧性 $\Delta = \{\pm 1, \pm 2, \cdots, \pm\theta\}$ を含めたすべての要素 $B_\Delta = \{b_1, b_1 \pm 1, b_1 \pm 2, \cdots, b_1 \pm \theta, \cdots, b_n, b_n \pm 1, b_n \pm 2, \cdots, b_n \pm \theta\}$ を根とする $(2\theta+1)n$ 次多項式 $f_B(x)$

$$\begin{aligned} f_B(x) = {} & \{x-(b_1-\theta)\}\cdots\{x-(b_1-1)\}(x-b_1) \\ & \{x-(b_1+1)\}\cdots\{x-(b_1+\theta)\}\cdots \\ & \qquad\vdots \\ & \{x-(b_n-\theta)\}\cdots\{x-(b_n-1)\}(x-b_n) \\ & \{x-(b_n+1)\}\cdots\{x-(b_n+\theta)\} \end{aligned} \tag{7}$$

を作成する．

B2. サーバは，乱数 s を選び，登録情報のすべての $C_1, \cdots, C_{2\theta n+2}$ を s 乗し，

$$C_i^s = E(sf_A^{-1}(x_i)) \tag{11}$$

を求める．そして，ユーザに $\{(C_1^s, x_1), \cdots, (C_{2\theta n+2}^s, x_{2\theta n+2})\}$ を送信する．

B3. ユーザは，$x_1, \cdots, x_{2\theta n+2}$ のそれぞれの値を $f_B(x)$ に代入し，$f_B(x_i)$ を求める．そして，

$$\begin{aligned} D_i &= (C_i^s)^{f_B(x_i)} = C_i^{sf_B(x_i)} \\ &= E(sf_A^{-1}(x_i)f_B(x_i)) = g^{sf_A^{-1}(x_i)f_B(x_i)} \bmod p \end{aligned} \tag{12}$$

を計算する．ここで，

$$F(x) = f_A^{-1}(x)f_B(x) \tag{8}$$

とおく．被認証者が正規ユーザである場合，認証時における生体情報 B の変動範囲内 B_Δ に登録時の特徴量 A がすべて含まれることが期待され，$F(x)$ 中の分母 $f_A(x)$ のすべての因子が分子の因子と約分されることになる．すなわち $F(x)$ は $2\theta n$ 次多項式となる（$f_A(x)$ は n 次多項式，$f_B(x)$ は $(2\theta+1)n$ 次多項式であることに留意されたい）．被認証者が正規ユーザでない場合は，A の要素の中の少なくとも 1 つが B_Δ から外れると考えられ，$F(x)$ は多項式の形を維持できない．

B4. ユーザは，サーバに $\{(D_1, 1), \cdots, (D_{2\theta n+2}, 2\theta n+2)\}$ を送信する．

B5. 2.3 節の離散対数のゼロ知識証明プロトコルを用いて，ユーザはサーバに対し，以下のゼロ知識証明を行う．ユーザは，$y_B = f_B(x_i)$ とおいて，ユーザが y_B の知識を有していることをサーバに対して証明する．

$$PK\{y_B \mid D_i = (C_i^s)^{y_B}\} \tag{13}$$

サーバは，その証明の正しさ（y_B を所持しないユーザが，不正に入手・加工した D_i をサーバに送ったものではないこと）を確認する．

B6. サーバは，$2\theta n+2$ 個のサンプルポイント $\{x_1, x_2, \cdots, x_{2\theta n+1}, x_{2\theta n+2}\}$ から $2\theta n+1$ 個の要素を任意に選び，集合 Ω_1 とする．同様に，集合 Ω_2 を作る．Ω_1 と Ω_2 は $2\theta n$ 個の要素が重なっており，残る 1 要素だけが異なっている．以下では簡単のために，Ω_1 と Ω_2 が

$$\Omega_1 = \{x_1, \cdots, x_{2\theta n+1}\},\ \Omega_2 = \{x_2, \cdots, x_{2\theta n+2}\},$$

であったとする．

B7. サーバは，任意の値 β を選び，Ω_1 と Ω_2 のそれぞれのサンプルポイントから Lagrange 補間によって $F(\beta)$ を求める．ここで，Lagrange 補間は下記の暗号プロトコルによって実施される．サーバは E_v（$v = 1, 2$）を計算する．

$$\begin{aligned} E_v &= \prod_{i=v}^{2\theta n+v} D_i^{\Lambda(i,\Omega_v,\beta)} = g^{s\sum_{i=v}^{2\theta n+v}\Lambda(i,\Omega_v,\beta)F(x_i)} \\ &= g^{sF(\beta)} \qquad v = 1, 2 \end{aligned} \tag{14}$$

$E_1 = E_2$ であれば，サーバは $F(x)$ が $2\theta n$ 次多項式であることを確信する．つまり，ユーザを正規利用者として認証する．

4.4 計算量および通信量

提案方式では，特徴量の変動を許容する閾値である θ の値のとり方が計算量と通信量に影響する．以下では，θ に対する計算量と通信量を評価する．

4.4.1 計算量

計算コストが最も大きいべき乗計算の回数に注目して，登録時と認証時におけるユーザとサーバそれぞれの計算コストを評価する．

登録時：ステップ A4 において，ユーザ側でサンプルポイントの数（$2\theta n+2$）だけべき乗計算が行われる．登録時にサーバのべき乗計算はない．

認証時：ステップ B2 では，サーバ側でサンプルポイントの数（$2\theta n+2$）だけべき乗計算が行われる．ステップ B3 では，ユーザ側でサンプルポイントの数（$2\theta n+2$）だけべき乗計算が行われる．ステップ B5 では，ゼロ知識証明をサンプルポイントの数（$2\theta n+2$）だけ行っている．ゼロ知識証明 1 回あたりのべき乗計算は，ユーザ側で 1 回，サーバ側で 2 回である．ステップ B7 では，サーバ側でサンプルポイントの数（$2\theta n+1$）のべき乗計算が 2 回行われる．認証時のべき乗計算回数

© 2012 Information Processing Society of Japan

を合計すると，ユーザ側で $2(2\theta n+2)$ 回，サーバ側で $3(2\theta n+2)+2(2\theta n+1)$ 回となる．

4.4.2 通信量

提案方式にて発生する通信は，ユーザ・サーバ間のコミットメントの送受信である．コミットメント 1 つあたりのデータサイズは，およそ $\log_2 p$ ビットとなる．ここでは，コミットメントの送信個数によって通信コストを評価する．

登録時：ステップ A4 において，ユーザがサーバへサンプルポイントの数（$2\theta n+2$）だけコミットメントを送信する．サーバからユーザへの送信はない．

認証時：ユーザからサーバへは，ステップ B4 でサンプルポイントの数（$2\theta n+2$）のコミットメントと，ステップ B5 でサンプルポイントの数（$2\theta n+2$）のコミットメントが送られる．サーバからユーザへは，ステップ B2 でサンプルポイントの数（$2\theta n+2$）のコミットメントと，ステップ B5 でサンプルポイントの数 $2(2\theta n+2)$ 個のコミットメントが送られる．認証時に送受信されるコミットメントの個数を合計すると，ユーザからサーバに $2(2\theta n+2)$ 個，サーバからユーザに $3(2\theta n+2)$ 個となる．

5. 安全性についての検討

本章では，提案方式の安全性について検討を行う．

5.1 安全性の定義

提案方式は，暗号プロトコルによる秘匿計算によってテンプレート保護型生体認証を実現しているため，正常な認証プロセスを経た場合に，認証の際に提示された生体情報と登録時の生体情報の類似度がサーバに漏洩しないことは明らかである．また，同様の理由から，生体情報に関して何の知識も有さない不正者がリプレイ攻撃などによってなりすましを成功させることは不可能であることも自明である．

このため本論文では，不正なユーザやサーバに対して生体情報がいっさい漏れなければ安全であると定義し，その検証を行う．具体的には，登録フェーズおよび認証フェーズにおいて正規のサーバが知りうるすべての情報から生体情報を類推することが困難であることを証明する．ここで，不正なユーザやサーバが入手できる情報は，たかだか，登録フェーズおよび認証フェーズにおいて正規のサーバが知りうる情報の部分集合にすぎないことに注意されたい．

なお，提案方式はユーザにスマートカードなどのトークンの所持を要求しない方式となっている．このため，生体情報の識別不可能性は保証されない．したがって，提案方式の安全性は，認証プロトコル自体が完全であっても，生体情報が有するエントロピの大きさに抑えられる．

5.2 対象とする攻撃

攻撃者として不正なユーザとサーバを想定する．ただし，ユーザ側の端末に備えられている認証モジュールは耐タンパデバイス内に実装された形で市場に提供されており，スキャンした生体情報をそのままタッピングするなどのリバースエンジニアリングは不可能であるという前提をおく．

本論文では，以下の 3 つの攻撃を対象とする．

5.2.1 登録情報解読攻撃

登録フェーズでユーザ・サーバ間でやりとりされた情報と公開パラメータから，登録生体情報を解読する攻撃である．提案方式においては，$\{g,(C_i,x_i)\mid i=1,2,\cdots,2\theta n+2\}$ より登録時の生体情報 $\{a_1,a_2,\cdots,a_n\}$ を推測する攻撃となる．下式に C_i を再掲しておく．

$$C_i = g^{\frac{1}{(x_i-a_1)(x_i-a_2)\cdots(x_i-a_n)}} \quad i=1,2,\cdots,2\theta n+2 \tag{15}$$

5.2.2 認証情報解読攻撃

認証フェーズでユーザ・サーバ間でやりとりされた情報と公開パラメータから，認証時に入力された生体情報を解読する攻撃である．提案方式においては，$\{g,s,(D_i,C_i,x_i)\mid i=1,2,\cdots,2\theta n+2\}$ より認証時の生体情報 $\{b_1,b_2,\cdots,b_n\}$ を推測する攻撃となる．下式に D_i を再掲しておく．

$$D_i = C_i^{\frac{s(x_i-b_1+\theta)\cdots(x_i-b_1)\cdots(x_i-b_1-\theta)\cdots}{(x_i-b_n+\theta)\cdots(x_i-b_n)\cdots(x_i-b_n-\theta)}} \quad i=1,2,\cdots,2\theta n+2 \tag{16}$$

5.2.3 複数認証情報解読攻撃

複数回の認証でやりとりされた情報と公開パラメータから，認証時に入力された生体情報を解読する攻撃である．提案方式においては，$\{g,s_\tau,(D_{i,\tau},C_i,x_i)\mid i=1,2,\cdots,2\theta n+2,\tau=1,2,\cdots\}$ より認証時の生体情報 $\{b_{1,\tau},b_{2,\tau},\cdots,b_{n,\tau}\}$ を推測する攻撃となる．ここで，τ は認証の回数を表す．式 (16) の認証情報解読攻撃に対して，$D_{i,\tau}$ は以下のように記述される．

$$D_{i,\tau} = C_i^{\frac{s_\tau(x_i-b_{1,\tau}+\theta)\cdots(x_i-b_{1,\tau})\cdots(x_i-b_{1,\tau}-\theta)\cdots}{(x_i-b_{n,\tau}+\theta)\cdots(x_i-b_{n,\tau})\cdots(x_i-b_{n,\tau}-\theta)}} \quad i=1,2,\cdots,2\theta n+2,\ \tau=1,2,\cdots \tag{17}$$

5.3 安全性証明

5.3.1 準備

前述した各攻撃に対する安全性の証明に用いる困難性の仮定について説明する．

● q-DHI 仮定 [18], [19]

巡回群 G における q-Diffie-Hellman inversion（q-DHI）問題は以下のように定義される．

「$g,g^x,\cdots,g^{x^q}\in G$ が与えられた際に，$g^{\frac{1}{x}}\in G$ を求めよ．ただし，g は G の生成元とする．」

攻撃者 $\mathcal{A}$ の G における q-DHI 問題に対するアドバンテージ $Adv_{G,\mathcal{A}}^{q\text{-}DHI}$ を，$\mathcal{A}$ が q-DHI 問題を解ける確率と定義

© 2012 Information Processing Society of Japan

する．動作時間 t 以下のすべてのアルゴリズム $\mathcal{A}$ に対し，$Adv_{G,\mathcal{A}}^{q\text{-}DHI} \leq \varepsilon$ が満たされる場合，G において (t,ε)-q-DHI 仮定が成り立つという．また，ε が無視できる値のとき，単に G において q-DHI 仮定が成り立つという [18]．

q-DHI 問題の困難性は広く知られており，q-DHI 仮定は擬似乱数生成機などの安全証明においても使われている困難性の仮定である．

● q-CA 仮定 [19]

巡回群 G における collusion attack with q traitors（q-CA）問題は以下のように定義される．

「$u_0, u_1, \cdots, u_q \in Z_p$ および $g^{1/y+u_1}, g^{1/y+u_2}, \cdots, g^{1/y+u_q} \in G$ が与えられた際に，$g^{1/y+u_0} \in G$ を求めよ．ただし，g は G の生成元とする．」

攻撃者 $\mathcal{A}$ の G における q-CA 問題に対するアドバンテージ $Adv_{G,\mathcal{A}}^{q\text{-}CA}$ を，$\mathcal{A}$ が q-CA 問題を解ける確率と定義する．動作時間 t 以下のすべてのアルゴリズム $\mathcal{A}$ に対し，$Adv_{G,\mathcal{A}}^{q\text{-}CA} \leq \varepsilon$ が満たされる場合，G において (t,ε)-q-CA 仮定が成り立つという．また，ε が無視できる値のとき，単に G において q-CA 仮定が成り立つという．

q-CA 問題そのものの困難性に関する議論は少ない．しかし，q-DHI 問題を効率的に計算するアルゴリズムを q-DHI$\mathcal{A}$，q-CA 問題を効率的に計算するアルゴリズムを q-CA$\mathcal{A}$ としたとき，次の定理が成り立つ．

定理 1 q-CA$\mathcal{A}$ が存在することと $(q-1)$-DHI$\mathcal{A}$ が存在することは同値である．

定理の証明は文献 [19] を参照されたい．この定理は q-DHI 仮定が成り立つならば q-CA 仮定も成り立つことを意味する．よって，q-CA 仮定の困難性を q-DHI 仮定の困難性に帰着させることが可能である．

5.3.2 各種攻撃に対する計算量的安全性の証明

5.2 節で説明した攻撃に対する安全性の証明を行う．解読攻撃は攻撃者の立場からは解読問題となる．それぞれの問題を前節で述べた困難性仮定に帰着させることによって計算量的安全性を証明する．ここで本論文では，この証明にあたって生体情報に関する次の 2 つの前提条件をおく．1 つは，2.2 節で述べたように，「生体情報のエントロピは十分大きい」とする．もう 1 つは，生体情報の特徴量 $\{a_1, a_2, \cdots, a_n\}$ の各要素 a_i について，「各ユーザの特徴量 a_i は全ユーザの特徴量 a_i をすべて集めた空間上で一様に分布している（すなわち，各ユーザの特徴量 a_i は，$Z_{p'}$ 上で一様分布している）」とする．

● 登録情報解読攻撃に対する安全性

5.2.1 項に示した登録情報解読問題を無視できない確率で効率的に解くアルゴリズム $\mathcal{A}_{\mathrm{TOA}}$ が存在すると仮定して，これを利用して q-CA 問題を解かせる（**図 1**）．

1. q-CA 問題の入力として
$$u_0, u_1, \cdots, u_q \in Z_p \text{ および } g^{1/y+u_1}, g^{1/y+u_2}, \cdots, g^{1/y+u_q} \in G \quad (18)$$
が与えられる．ただし，$q = 2\theta n + 2$ であるとする．
2. $z_1, z_2, \cdots, z_{n-1}$ をランダムに選択し，与えられた $u_0, u_1, \cdots, u_q$ を用いて
$(u_1 - z_1)(u_1 - z_2)\cdots(u_1 - z_{n-1})$,
$(u_2 - z_1)(u_2 - z_2)\cdots(u_2 - z_{n-1}), \cdots,$
$(u_q - z_1)(u_q - z_2)\cdots(u_q - z_{n-1})$
を計算する．そして，各要素の逆元
$1/(u_1 - z_1)(u_1 - z_2)\cdots(u_1 - z_{n-1})$,
$1/(u_2 - z_1)(u_2 - z_2)\cdots(u_2 - z_{n-1}), \cdots,$
$1/(u_q - z_1)(u_q - z_2)\cdots(u_q - z_{n-1})$
を求める．
3. 与えられた $g^{1/y+u_1}$, $g^{1/y+u_2}$, $\cdots$, $g^{1/y+u_q}$ に対して，手順 2 で求めた逆元をそれぞれべき乗し，
$$g^{1/(y+u_1)(u_1-z_1)(u_1-z_2)\cdots(u_1-z_{n-1})},$$
$$g^{1/(y+u_2)(u_2-z_1)(u_2-z_2)\cdots(u_2-z_{n-1})}, \cdots,$$
$$g^{1/(y+u_q)(u_q-z_1)(u_q-z_2)\cdots(u_q-z_{n-1})} \quad (19)$$

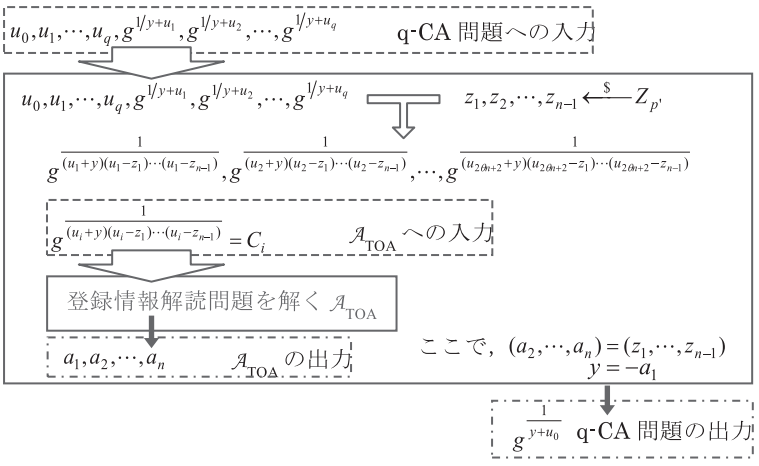

図 1 登録情報解読問題
Fig. 1 Enrollment data decoding problem.

© 2012 Information Processing Society of Japan

を計算する．

4. g と手順 3 で得られた各要素 $\{g^{1/(u_i+y)(u_i-z_1)\cdots(u_i-z_{n-1})} \mid i = 1,2,\cdots,q\}$ を，すべてアルゴリズム $\mathcal{A}_{\mathrm{TOA}}$ へ入力する．式 (19) は 5.2.1 項の式 (15) と同じ形になっているので，アルゴリズム $\mathcal{A}_{\mathrm{TOA}}$ は無視できない確率で $\{a_1, a_2, \cdots, a_n\}$ を出力する．式 (19) と式 (15) の関係を見ると，$(a_1, a_2, \cdots, a_n)$ が $(-y, z_1, \cdots, z_{n-1})$ に相当していることが分かる．よって，$\{a_1, a_2, \cdots, a_n\}$ が分かれば，$y = -a_1$ より $g^{1/y+u_0}$ を計算できる．

以上より，登録情報解読問題を無視できない確率で効率的に解くアルゴリズム $\mathcal{A}_{\mathrm{TOA}}$ が存在したとすると，q-CA 問題が無視できない確率で解けることになる．さらに定理 1 より，登録情報解読問題を無視できない確率で効率的に解くアルゴリズム $\mathcal{A}_{\mathrm{TOA}}$ が存在したとすると，q-DHI 問題が無視できない確率で解けることになる．この対偶から，q-DHI 問題が効率的に解くことが難しいならば登録情報解読問題を効率的に解くことも難しいといえる．

● 認証情報解読攻撃に対する安全性

5.2.2 項に示した認証情報解読問題を無視できない確率で効率的に解くアルゴリズム $\mathcal{A}_{\mathrm{AOA}}$ が存在すると仮定して，これを利用して q-DHI 問題を解かせる（**図 2**）．ここでは説明を簡略化するために生体情報の数 n を 2 として考える．$n \geq 3$ のときは $n = 2$ から自明である．

まず，サンプルポイント $x_1, \cdots, x_r$ に対して，多項式 $h(\cdot), h_1(\cdot), \cdots, h_r(\cdot)$ を

$$h(a_1) = (x_1 - a_1)\cdots(x_r - a_1) = \sum_{l=0}^{r} K_l a_1^l \tag{20}$$

$$h_i(a_1) = \frac{(x_1 - a_1)\cdots(x_r - a_1)}{x_i - a_1} = \sum_{l=0}^{r-1} K_{l,i} a_1^l \quad i = 1,2,\cdots,r \tag{21}$$

と定義する．このとき，

$$g = \prod_{l=0}^{r} (\hat{g}^{\alpha^l})^{K_l} \quad (= \hat{g}^{h(\alpha)}) \tag{22}$$

とおくと，

$$g^{\alpha^i} = \prod_{l=0}^{r} (\hat{g}^{\alpha^{l+i}})^{K_l}, \tag{23}$$

$$g^{\frac{1}{x_i-\alpha}} = \hat{g}^{h_i(\alpha)} = \prod_{l=0}^{r-1} (\hat{g}^{\alpha^l})^{K_{l,i}} \quad i = 1,2,\cdots,r \tag{24}$$

と書ける．

また，$\delta_1, \delta_2 \in \{-\theta, \cdots, +\theta\}$，$a_2$ に対して，多項式 $h'_i(\cdot)$ を

$$\begin{aligned} h'_i(a_1) &= \frac{(x_i - (a_1 + \delta_1 - \theta))\cdots(x_i - (a_1 + \delta_1 + \theta))}{x_i - a_1} \\ &\quad \times \frac{(x_i - (a_2 + \delta_2 - \theta))\cdots(x_i - (a_2 + \delta_2 + \theta))}{x_i - a_2} \\ &= \sum_{l=0}^{2\theta} K'_{l,i} a_1^l \quad i = 1,2,\cdots,r \end{aligned} \tag{25}$$

と定義する．5.2.2 項の式 (16) に示されている D_i は $n = 2$ の場合は次式となる．

$$D_i = C_i^{s(x_i-(b_1-\theta))\cdots(x_i-(b_1+\theta))\times(x_i-(b_2-\theta))\cdots(x_i-(b_2+\theta))} \quad i = 1,2,\cdots,4\theta+2 \tag{26}$$

よって，$C_i = g^{\frac{1}{(x_i-a_1)(x_i-a_2)}}$，$b_1 = a_1 + \delta_1$，$b_2 = a_2 + \delta_2$ とおくと，

$$D_i = g^{s h'_i(a_1)} = \prod_{l=0}^{2\theta} (g^{a_1^l})^{s K'_{l,i}} \tag{27}$$

と書ける．ここで，サンプルポイント数は $r = 4\theta + 2$ である．

次に，上述の分析結果を利用して，$n = 2$ のときの認証

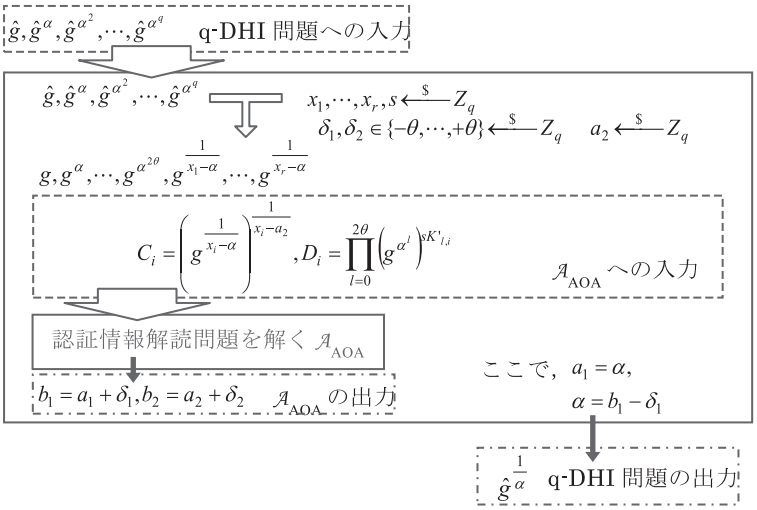

図 2 認証情報解読問題

Fig. 2 Authentication data decoding problem.

© 2012 Information Processing Society of Japan

情報解読アルゴリズム $\mathcal{A}_{\mathrm{AOA}}$ によって q-DHI 問題を解かせる具体的な手順を説明する．

1. q-DHI 問題の入力として，$\hat{g}, \hat{g}^{\alpha}, \cdots, \hat{g}^{\alpha^q} \in G$ が与えられる．ただし，$q = 6\theta + 2$ であるとする．
2. サンプルポイント $x_1, \cdots, x_r$ と乱数 s をランダムに選択する．また，$\delta_1, \delta_2 \in \{-\theta, \cdots, +\theta\}$，$a_2$ もランダムに選択する．
3. 式 (22), (23), (24) を用いて，与えられた $\hat{g}, \hat{g}^{\alpha}, \cdots, \hat{g}^{\alpha^q}$ から $g, g^{\alpha}, \cdots, g^{\alpha^{2\theta}}$ と $g^{\frac{1}{x_1-\alpha}}, \cdots, g^{\frac{1}{x_r-\alpha}}$ を計算する．
4. すべての $i \in \{1, 2, \cdots, r\}$ に対して

$$C_i = \left(g^{\frac{1}{x_i-\alpha}}\right)^{\frac{1}{x_i-a_2}} \tag{28}$$

$$D_i = \prod_{l=0}^{2\theta} \left(g^{\alpha^l}\right)^{sK'_{l,i}} \tag{29}$$

を計算する．

5. (g, s) と手順 4 で得られた各要素 $\{x_i, C_i, D_i \mid i = 1, 2, \cdots, r\}$ を，すべてアルゴリズム $\mathcal{A}_{\mathrm{AOA}}$ へ入力する．式 (29) は，$b_1 = a_1 + \delta_1$，$b_2 = a_2 + \delta_2$ であるときの式 (27) と同じ形になっているので，アルゴリズム $\mathcal{A}_{\mathrm{AOA}}$ は無視できない確率で $\{b_1, b_2\}$ を出力する．式 (29) と (27) の関係を見ると，a_1 が α に相当していることが分かる．よって，$\{b_1, b_2\}$ が分かれば，$a_1 = b_1 - \delta_1$ より $\hat{g}^{1/\alpha}$ を計算できる．

以上より，認証情報解読問題を無視できない確率で効率的に解くアルゴリズム $\mathcal{A}_{\mathrm{AOA}}$ が存在したとすると，q-DHI 問題が無視できない確率で解けることになる．この対偶から，q-DHI 問題が効率的に解くことが難しいならば認証情報解読問題を効率的に解くことも難しいといえる．

● 複数認証情報解読攻撃に対する安全性

複数認証情報解読問題を無視できない確率で効率的に解くアルゴリズム $\mathcal{A}_{\mathrm{MAA}}$ が存在すると仮定して，これを利用して q-DHI 問題を解かせる（**図 3**）．ここでも説明を簡略化するために生体情報の数 n を 2，認証セッションの傍受回数 τ を 2 として考える．$n \geq 3$，$\tau \geq 3$ のときは $n = 2$，$\tau = 2$ から自明である．

まず，「認証情報解読攻撃に対する安全性」の証明の際に定義した多項式 $h(\cdot)$，$h_i(\cdot)$，$h'_i(\cdot)$（式 (20)，式 (21)，式 (25)）を用いる．また，$\delta_3, \delta_4 \in \{-\theta, \cdots, +\theta\}$ に対して，多項式 $h''_i(\cdot)$ を

$$\begin{aligned} h''_i(a_1) &= \frac{(x_i - (a_1 + \delta_3 - \theta)) \cdots (x_i - (a_1 + \delta_3 + \theta))}{x_i - a_1} \\ &\quad \times \frac{(x_i - (a_2 + \delta_4 - \theta)) \cdots (x_i - (a_2 + \delta_4 + \theta))}{x_i - a_2} \\ &= \sum_{l=0}^{2\theta} K''_{l,i} a_1^l \quad i = 1, 2, \cdots, r \end{aligned} \tag{30}$$

と定義する．

5.2.3 項の式 (17) に示されている $D_{i,\tau}$ は，$n = 2$ の場合，$\tau = 1$ および $\tau = 2$ において下式となる．

$$D_{i,1} = C_i^{\frac{s_1(x_i - b_{1,1} + \theta) \cdots (x_i - b_{1,1}) \cdots (x_i - b_{1,1} - \theta)}{(x_i - b_{2,1} + \theta) \cdots (x_i - b_{2,1}) \cdots (x_i - b_{2,1} - \theta)}} \tag{31}$$

$$D_{i,2} = C_i^{\frac{s_2(x_i - b_{1,2} + \theta) \cdots (x_i - b_{1,2}) \cdots (x_i - b_{1,2} - \theta)}{(x_i - b_{2,2} + \theta) \cdots (x_i - b_{2,2}) \cdots (x_i - b_{2,2} - \theta)}} \tag{32}$$

$$i = 1, 2, \cdots, 4\theta + 2$$

よって，$C_i = g^{\frac{1}{(x_i - a_1)(x_i - a_2)}}$，$b_{1,1} = a_1 + \delta_1$，$b_{2,1} = a_2 + \delta_2$，$b_{1,2} = a_1 + \delta_3$，$b_{2,2} = a_2 + \delta_4$ とおくと，

$$D_{i,1} = g^{sh'_i(a_1)} = \prod_{l=0}^{2\theta} (g^{a_1^l})^{s_1 K'_{l,i}} \tag{33}$$

$$D_{i,2} = g^{sh''_i(a_1)} = \prod_{l=0}^{2\theta} (g^{a_1^l})^{s_2 K''_{l,i}} \tag{34}$$

と書ける．ここで，サンプルポイント数は $r = 4\theta + 2$ である．

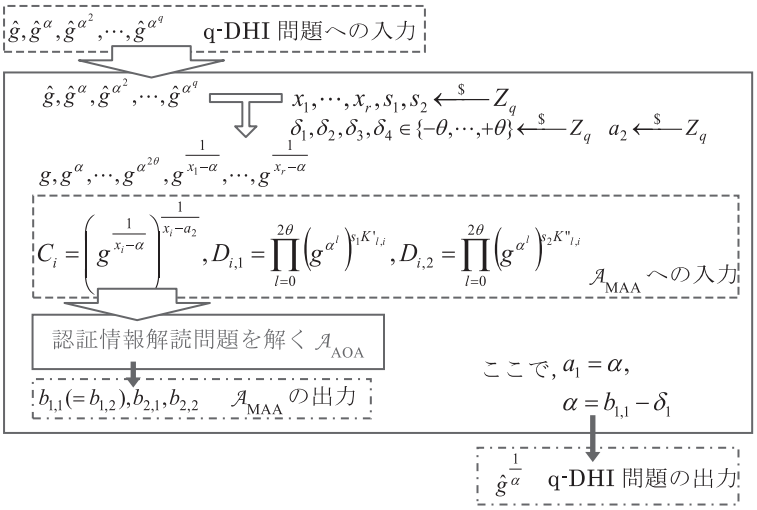

図 3 複数認証情報解読問題

Fig. 3 Multiple authentication data decoding problem.

© 2012 Information Processing Society of Japan

通常，第1認証セッションでの生体情報 $\{b_{1,1}, b_{2,1}\}$ と第2認証セッションでの生体情報 $\{b_{1,2}, b_{2,2}\}$ は異なりうる．しかし，ここでの目的は攻撃耐性を証明することにあるため，攻撃者にとって有利な状況（攻撃者にとっての未知変数の数が少ない）を想定し，生体情報の第1要素については第1セッションと第2セッションの値がちょうど一致しており（$b_{1,1} = b_{1,2}$，$\delta_1 = \delta_3$），生体情報の第2要素だけが第1セッションと第2セッションで値が違っていた（$b_{2,1} \neq b_{2,2}$，$\delta_2 \neq \delta_4$）とする．なお，同一ユーザの生体情報であるので，$b_{2,1}$ と $b_{2,2}$ は完全には一致していないが十分に近い（$\delta_4 = \delta_2 + \theta' \neq \delta_2$，ここで $\theta' \in Z_\theta$）．

次に，上述の分析結果を利用して，$n = 2$，$\tau = 2$ のときの複数認証情報解読アルゴリズム $\mathcal{A}_{\mathrm{MAA}}$ によって q-DHI 問題を解かせる具体的な手順を説明する．

1. q-DHI 問題の入力として，$\hat{g}, \hat{g}^{\alpha}, \cdots, \hat{g}^{\alpha^q} \in G$ が与えられる．ただし，$q = 6\theta + 2$ であるとする．
2. サンプルポイント $x_1, \cdots, x_r$ と乱数 s_1，s_2 をランダムに選択する．また，$\delta_1, \delta_2, \delta_3, \delta_4 \in \{-\theta, \cdots, +\theta\}$，$a_2$ もランダムに選択する．
3. 式 (22), (23), (24) を用いて，与えられた $\hat{g}, \hat{g}^{\alpha}, \cdots, \hat{g}^{\alpha^q}$ から $g, g^{\alpha}, \cdots, g^{\alpha^{2\theta}}$ と $g^{\frac{1}{x_1-\alpha}}, \cdots, g^{\frac{1}{x_r-\alpha}}$ を計算する．
4. すべての $i = 1, 2, \cdots, 4\theta + 2$，$\tau = 1, 2$ に対して，

$$C_i = \left(g^{\frac{1}{x_i-\alpha}}\right)^{\frac{1}{x_i-a_2}} \tag{35}$$

$$D_{i,1} = \prod_{l=0}^{2\theta} \left(g^{\alpha^l}\right)^{s_1 K'_{l,i}} \tag{36}$$

$$D_{i,2} = \prod_{l=0}^{2\theta} \left(g^{\alpha^l}\right)^{s_2 K''_{l,i}} \tag{37}$$

を計算する．

5. (g, s) と手順3で得られた要素 $\{x_i, C_i, D_{i,\tau} \mid i = 1, 2, \cdots, 4\theta+2, \tau = 1, 2\}$ をすべてアルゴリズム $\mathcal{A}_{\mathrm{MAA}}$ へ入力する．式 (36) は，$b_{1,1} = a_1 + \delta_1$，$b_{2,1} = a_2 + \delta_2$ であるとき（$\tau = 1$ のとき）の式 (33) と同じ形になっており，式 (37) は $b_{1,2} = a_1 + \delta_3$，$b_{2,2} = a_2 + \delta_4$ であるとき（$\tau = 2$ のとき）の式 (34) と同じ形になっているので，アルゴリズム $\mathcal{A}_{\mathrm{MAA}}$ は無視できない確率で $\{b_{1,1}(= b_{1,2}), b_{2,1}, b_{2,2}\}$ を出力する．式 (36) と式 (33) の関係を見ると，a_1 が α に相当していることが分かる．よって，$b_{1,1}$ が分かれば，$a_1 = b_{1,1} - \delta_1$ より $\hat{g}^{1/\alpha}$ を計算できる．

以上より，複数認証情報解読問題を無視できない確率で効率的に解くアルゴリズム $\mathcal{A}_{\mathrm{MAA}}$ が存在したとすると，q-DHI 問題が無視できない確率で解けることになる．この対偶から，q-DHI 問題が効率的に解くことが難しいならば複数認証情報解読問題を効率的に解くことも難しいといえる．なお，ここでは $(b_{1,1} = b_{1,2}$，$b_{2,1} \neq b_{2,2})$ の場合を示したが，$(b_{1,1} \neq b_{1,2}$，$b_{2,1} \neq b_{2,2})$ の場合も同様に証明できる．また，$(b_{1,1} = b_{1,2}$，$b_{2,1} = b_{2,2})$ の場合は 5.2.2 項の認証情報解読問題に帰着する．

以上より，提案方式は q-DHI 仮定のもとで 5.2 節に示した3つの攻撃に対する計算量的安全性を示すことができた．

5.4 情報理論的安全性に関する補足

正規ユーザになりすまして正規サーバとの認証プロトコルの実行を試みる不正ユーザに対しては，提案方式の軽微な変更により情報理論的安全性を示すことができる．提案方式の認証フェーズでは，4.3 節のステップ B2 で，すべての i に対して同一の乱数 s を用いているが，これを，それぞれの i に対して異なる乱数 s_i を選ぶように変更する．この結果，乱数 s_i を知らない不正ユーザにとっては，サーバから送られてくる情報は乱数にしか見えなくなる．サーバ側では，認証セッションの間，s_i を一時的に保存するようにし，ステップ B5 の直前に各 D_i に対してそれぞれの s_i の逆元をべき乗することによって s_i による撹乱を元に戻すことができる．

6. まとめと今後の課題

本論文では，生体情報の特徴量を曖昧な形で多項式の根として符号化し，登録時と認証時の生体情報が近い場合のみ評価関数が多項式となるように特徴量関数を構成することによって，特徴量の変動に対して耐性を有するテンプレート保護型生体認証（ZeroBio）プロトコルを提案した．従来の ZeroBio プロトコルが登録時と認証時の生体情報の「近さ」を暗号プロトコルによって直接証明していたのに対し，提案方式は，生体情報が近い場合のみ成立する多項式上の Lagrange 補間を利用し，補間値の「一致」を暗号プロトコルによって検査する．提案方式は，生体情報のエントロピは十分大きいという前提の下で，ユーザが記憶・所持すべき情報が不要である ZeroBio プロトコルを実現している．また，q-DHI 仮定，q-CA 仮定を用いることで，登録情報解読攻撃，認証情報解読攻撃，複数認証情報解読攻撃に対する提案方式の計算量的安全性を証明した．ただし，今回の安全性証明では，各ユーザの特徴量 a_i が $Z_{p'}$ 上で一様分布であることを前提としている．

今後，提案方式の実装を行い，基礎実験を通じて認証精度（他人受入率と本人拒否率）の評価を行う予定である．また，登録時の通信データと認証時の通信データをともに所有する攻撃者に対する安全性について検討していく必要がある．

参考文献

[1] 清水將吾，瀬戸洋一：国際標準化に向けたテンプレート保護技術の体系化，産業技術大学院大学紀要，No.1, pp.93–104 (2007).
[2] Ratha, N.K., Connell, J.H. and Bolle, R.M.: Enhancing Security and Privacy in Biometrics-based Authentication

© 2012 Information Processing Society of Japan

Systems, *IBM Systems Journal*, Vol.40, No.3 (2001).
[3] Juels, A. and Sudan, M.: A Fuzzy Vault Scheme, *IEEE International Symposium on Information Theory*, p.408 (2002).
[4] Andrew, B.J., Teoh, C.L., Ngo, D. and Goh, A.: Biohashing: Two factor authentication featuring fingerprint data and tokenised random number, *Pattern Recognition*, Vol.37, No.11, pp.2245–2255 (2004).
[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，Vol.48, No.7, pp.2307–2318 (2007).
[6] Fujisaki, E. and Okamoto, T.: Statistical Zero Knowledge Protocols to Prove Modular Polynomial Relations, *Proc. CRYPTO '99*, LNCS, Vol.1666, pp.413–430, Springer (1999).
[7] 永井 慧，菊池浩明：ゼロ知識証明を用いた安全なリモート生体認証プロトコル "ZeroBio"，東海大学大学院 2007 年度修士論文 (2007).
[8] 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 2009 論文集，pp.325–330 (2009).
[9] Buchmann, J.A.: 暗号理論入門—暗号アルゴリズム，署名と認証，その数学的基礎，p.35, Springer Japan (2007).
[10] Cambier, J.L., Ulf, M., von Seelen, C., Glass, R., Moore, R., Scott, I., Braithwaite, M. and Daugman, J.: Application-Specific Biometric Templates, *IEEE Workshop on Automatic Identification Advanced Technologies*, pp.167–171 (2002).
[11] 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，情報処理学会研究報告，Vol.2006, No.81, pp.435–440 (2006).
[12] Juels, A. and Wattenberg, M.: Fuzzy commitment scheme, *ACM Conf. Computer and Communications Security*, pp.28–36 (1999).
[13] Elgamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Trans. Information Theory*, Vol.31, No.4, pp.469–472 (1985).
[14] 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（SITA2006）予稿集，pp.319–322 (2006).
[15] Sakashita, T., Shibata, Y., Yamamoto, T., Takahashi, K., Ogata, W., Kikuchi, H. and Nishigaki, M.: A proposal of efficient remote biometric authentication protocol, *Proc. International Workshop on Security 2009*, LNCS, Vol.5824, pp.212–227, Springer (2009.10).
[16] S. Lee, et al.: Protecting Secret Keys with Fuzzy Fingerprint Vault Based on a 3D Geometric Hash Table, LNCS, Vol.4432, pp.432–439, Springer (2007).
[17] Moon, D., Lee, S. and Chung, Y.: Configurable fuzzy fingerprint vault for Match-on-Card System, *IEICE Electronics Express* (*ELEX*), Vol.6, No.14, pp.993–999 (2009).
[18] Dodis, Y. and Yampolskiy, A.: A verifiable random function with short proofs and keys, LNCS, Vol.3386, pp.416–431, Springer (2005).
[19] Mitsunari, S., Sakai, R. and Kasahara, M.: A new traitor tracing, *IEICE Trans. Fundamentals*, Vol.E85-A, No.2, pp.481–484 (2002).
[20] Takahashi, K. and Hirata, S.: Parameter management schemes for cancelable biometrics, *Proc. IEEE Workshop on Computational Intelligence in Biometrics and Identity Management*, pp.145–151 (2011).
[21] Uludag, U. and Jain, A.K.: Attacks on biometric systems: A case study in fingerprints, *Proc. SPIE-EI 2004, Security, Steganography and Watermarking of Multimedia Contents VI*, pp.622–633 (2004).

西垣 正勝 （正会員）

1990 年静岡大学工学部光電機械工学科卒業．1992 年同大学大学院修士課程修了．1995 年同博士課程修了．日本学術振興会特別研究員（PD）を経て，1996 年静岡大学情報学部助手．同講師，助教授の後，2006 年より同創造科学技術大学院助教授．2007 年同准教授，2010 年同教授．博士（工学）．情報セキュリティ全般，特にヒューマニクスセキュリティ，メディアセキュリティ，ネットワークセキュリティ等に関する研究に従事．

渡邊 幸聖

2009 年静岡大学理学部数学科卒業．2011 年同大学大学院情報学研究科情報学専攻修了．在学中，情報セキュリティに関する研究に従事．

小田 雅洋

2009 年静岡大学情報学部情報科学科卒業．2011 年同大学大学院修士課程修了．現在，株式会社デンソーに勤務．在学中，情報セキュリティに関する研究に従事．

米山 裕太

2012 年静岡大学情報学部卒業．現在，同大学大学院修士課程．情報セキュリティに関する研究に従事．

© 2012 Information Processing Society of Japan

山本 匠

2006 年静岡大学情報学部情報科学科卒業．2007 年 9 月同大学大学院修士課程修了．2010 年 9 月同創造科学技術大学院博士課程修了．日本学術振興会特別研究員（DC1），同研究員（PD）を経て，2011 年 4 月三菱電機株式会社情報技術総合研究所入社．情報セキュリティに関する研究に従事．

高橋 健太 （正会員）

1998 年東京大学理学部情報科学科卒業．2000 年同大学大学院理学系研究科情報科学専攻修士課程修了．同年（株）日立製作所入社．以来，同横浜研究所（旧システム開発研究所）にて生体認証および情報セキュリティの研究開発に従事．平成 13 年情報処理学会高度交通システム研究会優秀論文賞受賞．平成 20 年度情報処理学会論文賞受賞．電子情報通信学会，IEEE 各会員．

尾形 わかは

1989 年東京工業大学理学部卒業，1991 年同大学大学院修士課程修了，1994 年同博士後期課程修了．1995 年兵庫県立姫路工業大学助手．2000 年東京工業大学理財研究センター助教授，2005 年より同大学大学院イノベーションマネジメント研究科助教授，現在は同准教授．博士（工学）．暗号理論，暗号プロトコル，情報セキュリティに関する研究に従事．

菊池 浩明 （フェロー）

東海大学情報通信学部通信ネットワーク工学科教授．1988 年明治大学工学部電子通信工学科卒業．1990 年同大学大学院博士前期課程修了．1994 年同博士（工学）．1990 年富士通研究所勤務．1994 年東海大学工学部電気工学科助手，1995 年同専任講師，1999 年同助教授，2000 年同電子情報学部情報メディア学科助教授，2006 年同情報理工学部情報メディア学科教授，2008 年同情報通信学部通信ネットワーク工学科教授．1997〜1998 年カーネギーメロン大学計算機科学科訪問研究員．2009 年より情報処理学会コンピュータセキュリティ研究会（CSEC）主査．WIDE プロジェクト暗号メールシステム FJPEM の開発，認証実用化実験協議会（ICAT），IPA 独創情報技術育成事業等に従事．暗号プロトコル，ネットワークセキュリティ，ファジィ論理，ソフトコンピューティング等に興味を持つ．1990 年日本ファジィ学会奨励賞，1993 年情報処理学会奨励賞，1996 年 SCIS 論文賞，2010 年情報処理学会 JIP Outstanding Paper Award．電子情報通信学会，日本知能情報ファジィ学会，IEEE，ACM 各会員．

© 2012 Information Processing Society of Japan