テンプレート保護型生体認証技術の動向と日立の取り組み

日立製作所　システム開発研究所
高橋健太

目次

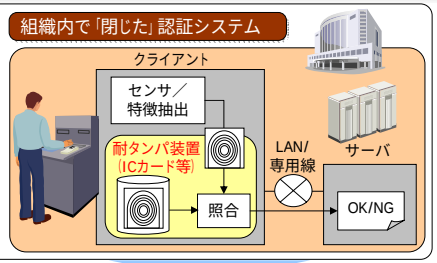
背景
生体認証の問題点

- 未対応者の存在
  - 生体認証システムを利用できない人が存在する
- 生体の偽造によるなりすまし
  - ユーザの生体から直接，あるいは遺留生体情報から偽造生体を作成
  - 登録生体情報（テンプレート）から偽造生体を作成
- 生涯不変（変更不能）
  - 一旦テンプレートが漏洩すると，一生安全性を回復できない
    - テンプレート漏洩 → 電子的偽造，物理的偽造の脅威が発生
- プライバシ問題
  - 生体情報は個人を識別可能な情報：個人情報
  - 人種･民族･健康状態などを特定できる可能性：センシティブ情報

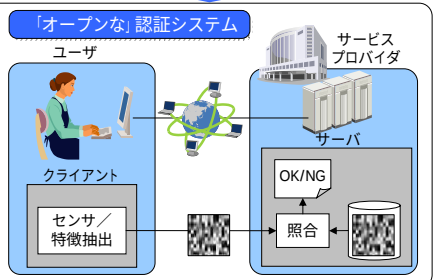
テンプレートの保護が課題

背景
生体認証システムのモデルとテンプレート保護技術

■ローカル生体認証
- 概要：テンプレートをクライアント（認証端末）内で管理･照合し，結果(OK/NG)をサーバへ通知.
- 課題：クライアント内のテンプレート漏洩防止
- 対策：ICカードなどの耐タンパ装置内でテンプレートを管理･照合
- 適用先：銀行ATM，入退管理



■リモート生体認証
- テンプレートをサーバ側で管理･照合.
  クライアントは生体情報をサーバへ送信.
- 課題：内部犯対策，プライバシ保護
- 対策：生体情報を秘匿したまま認証
  テンプレート保護型生体認証
- 適用先：Web認証，インターネット決済など



テンプレート保護型生体認証技術の概要

HITACHI Inspire the Next

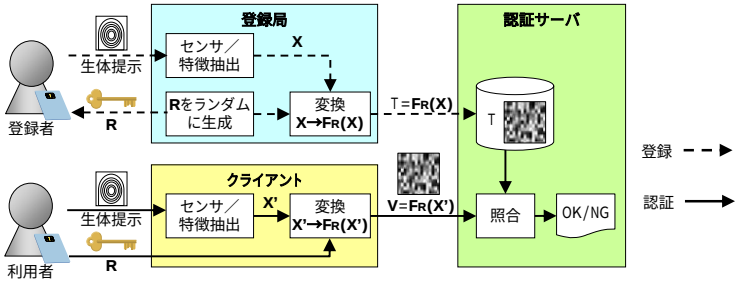
- テンプレート保護型生体認証技術
  - テンプレート（登録生体情報）を保護したまま認証
    - サーバ／クライアント／ICカード等からのテンプレート漏洩を防止
  - 照合生体情報をサーバに対して秘匿したまま認証
    - サーバ管理者の過失・内部不正による生体情報漏洩を防止
    - 利用者のプライバシを保護
  - 生体情報の安全性を耐タンパ装置に依存せず，アルゴリズムレベルで確保
- 研究開発動向
  - 現状は研究段階にあり，実用化（製品化）された例はない
  - 既存研究は大きく3つのアプローチに分類可能

1. キャンセラブルバイオメトリクス
   - 生体情報を変換（スクランブル化）したまま登録・照合
2. バイオメトリック暗号
   - 生体情報を用いて秘密鍵を生成し，暗号技術を利用して認証
3. 非対称生体認証
   - 生体情報の「近さ」をゼロ知識証明

キャンセラブルバイオメトリクス

HITACHI Inspire the Next

- 生体情報を変換（暗号化）したまま登録・照合
  - 登録時：
    - 変換パラメータR（暗号鍵に相当）をランダムに生成して登録者に発行．
    - 登録生体情報を X → T=FR(X) と変換（暗号化に相当）してサーバに登録．
  - 認証時：
    - 照合生体情報を X' →V= FR(X') と変換し，変換したまま照合（元に戻さない）
- 特長
  - 認証サーバに対して生体情報を秘匿したまま認証（プライバシ，セキュリティ向上）
  - 変換パラメータRを変更して，テンプレートT を破棄・更新可能（漏洩してもセキュリティを維持）
  - 従来の照合アルゴリズムの認証精度を大きく劣化させずに実現可能

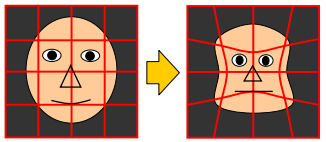


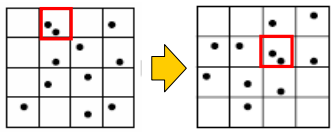
キャンセラブルバイオメトリクスの既存研究

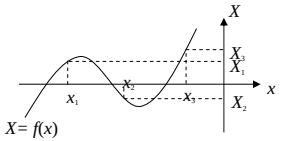
Cancelable Biometrics (IBM 2001)

HITACHI Inspire the Next

- N.K.Ratha,et,al.
  “Enhancing security and privacy in biometric-based authentication systems”, 2001
  - Cancelable Biometrics の概念を提唱
- 実現方法例：
  - 顔
    - 画像湾曲（モーフィング）
  - 指紋：
    - マニューシャ（特徴点）座標のブロック置換
  - マニューシャ座標の非線形変換：
    $(x,y) \rightarrow (f(x), f(y))$





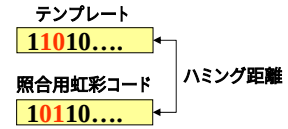


キャンセラブルバイオメトリクスの既存研究

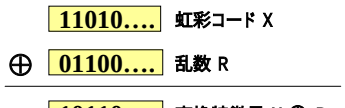
キャンセラブル虹彩認証 (Iridian ’02, KDDI ’04)

HITACHI Inspire the Next

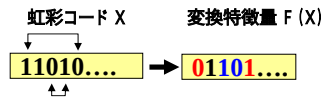
- 虹彩照合
  - 特徴量：虹彩コード（2048bit）
  - 距離：虹彩コードのハミング距離 Hd



- M.Braithwaite, et. al. (Iridian)
  “Application specific biometric templates”, 2002
  - 変換関数： マスキング
    - 虹彩コードXと乱数RとのXOR（虹彩）
    - F（X）＝X⊕R (S: 2048bit)
  - ハミング距離不変 → 精度劣化なし
    - Hd（F（X），F（X’））＝Hd（X，X’）



- 太田 他 (KDDI)
  “虹彩コードを秘匿する虹彩認証方式の提案”, 2004
  - 変換関数： マスキング＋ビット置換
  - ハミング距離不変 → 精度劣化なし

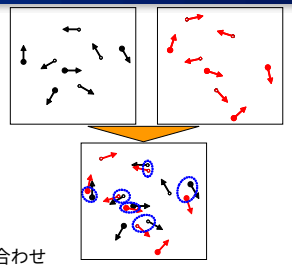


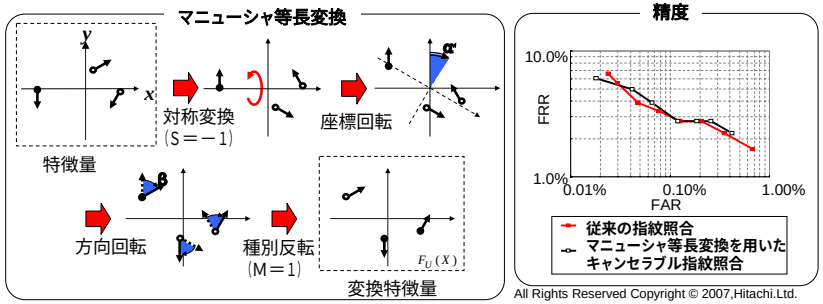
キャンセラブルバイオメトリクスの既存研究

マニューシャ等長変換 (日立 2005)

HITACHI Inspire the Next

- 指紋に適用可能なキャンセラブル変換関数
  - 指紋照合方式：マニューシャマッチング
    - マニューシャ：平面上の方向付き点
    - 平行移動，回転ずれを考慮して重ね合せ
    - 対応点対を探索
- 高橋 他
  “キャンセラブル指紋照合方式の提案”，2005
  - 変換関数：マニューシャ等長変換
    - 種別反転，座標回転，方向回転，対称変換　の組み合わせ
    - 特長：マニューシャ間距離不変 → 精度劣化なし (FRR: 5%, FAR: 0.04%)



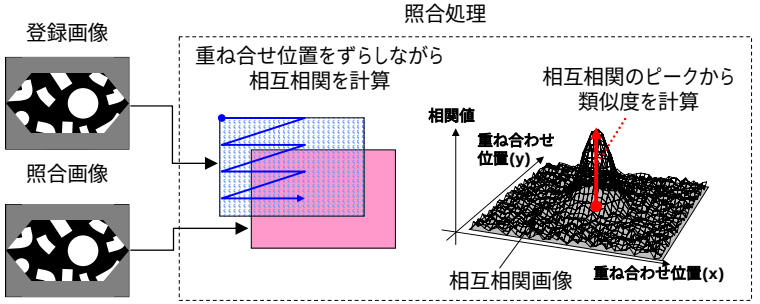


キャンセラブルバイオメトリクスの既存研究

相関不変ランダムフィルタリング (日立 2006)

HITACHI Inspire the Next

- 画像マッチング
  - 2枚の画像をずらしながら重ね合わせ，相互相関のピークから類似度を計算
  - 顔，指紋，静脈認証などに適用可能

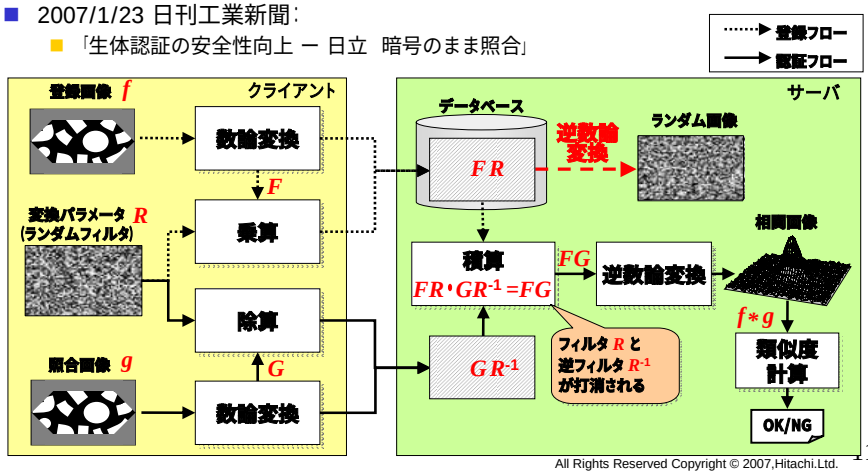


キャンセラブルバイオメトリクスの既存研究

相関不変ランダムフィルタリング (日立 2006)

HITACHI Inspire the Next

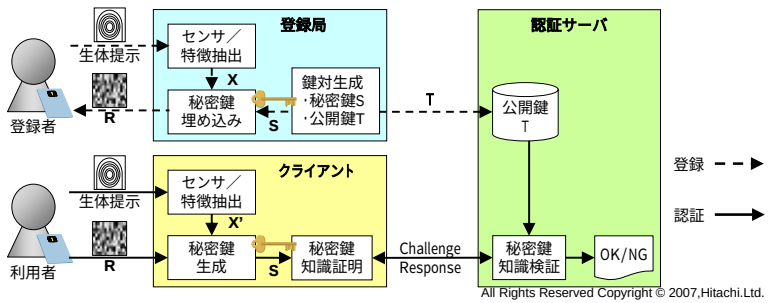
- 比良田 他
  “画像マッチングに基づく生体認証に適用可能なキャンセラブルバイオメトリクスの提案”，2006
  - 変換関数：相関不変ランダムフィルタリング
  - 数論変換 (有限体上のフーリエ変換) を利用
- 2007/1/23 日刊工業新聞：
  - 「生体認証の安全性向上 ー 日立　暗号のまま照合」



バイオメトリック暗号

HITACHI Inspire the Next

- 概要
  - 生体情報を用いて秘密鍵を生成し，暗号技術を利用して認証
  - 登録時：
    - 秘密鍵S，公開鍵Tのペアを生成し，Sを生体情報Xに埋め込んで補助情報Rを作成
    - Tを認証サーバに登録し，Rを登録者に発行．(RからS,Xは復元できない)
  - 認証時：
    - 利用者の生体情報 X’ を用いて R から S を取り出す (X’がXに十分近いときのみSを取り出せる)
    - S が T に対応する正しい秘密鍵であることをサーバに証明
- 特長
  - 認証サーバに対して生体情報を秘匿したまま認証 (プライバシ，セキュリティ向上)
  - 鍵ペア S,Tを変更して 補助情報 R を破棄・更新可能 (漏洩してもセキュリティを維持)
  - ＰＫＩやパスワード認証と生体認証をアルゴリズムレベルで連携可能



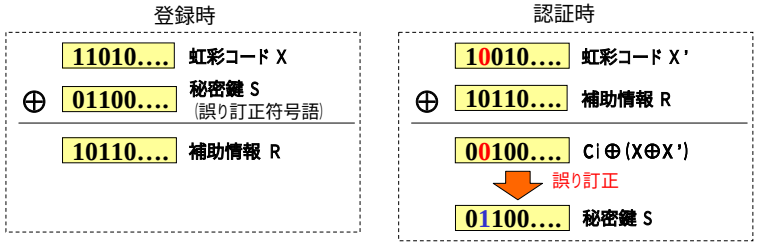
バイオメトリック暗号の既存研究

Fuzzy Commitment (RSA 1999)

HITACHI Inspire the Next

- A.Juel, et. al. (RSA), “A fuzzy commitment scheme”, 1999
  - 特徴量X，X’の距離がハミング距離で与えられる場合に，誤り訂正符号を用いて秘密鍵を生成するアルゴリズム．
  - 登録時：
    - Xと同じビット長の誤り訂正符号C＝{C|} から符号語をランダムに選択し秘密鍵Sとする
    - 補助情報： R＝X⊕S
  - 認証時 (鍵復元時)：
    - X’⊕R＝S⊕(X⊕X’) を誤り訂正してSを生成

ハミング重み小 (X,X’が近い) なら正しく誤り訂正可能

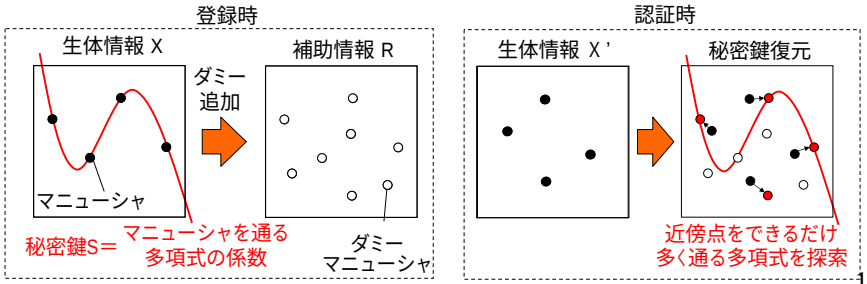


バイオメトリック暗号の既存研究

Fuzzy Vault (RSA 2001)

HITACHI Inspire the Next

- A.Juels, et.al. (RSA), “A fuzzy vault scheme”, 2002
  - 生体情報X，X’が集合として表現され，その距離がset difference (共通要素の数) で与えられる場合に，
  - 誤り訂正理論を応用して一意のデータ (秘密鍵) を埋込み／復元するアルゴリズム
- T. Clancy, et.al. (Univ. of Meryland) “Secure smartcard-based fingerprint authentication”, 2003
  - Fuzzy Vault を指紋に適用
  - 生体情報X：マニューシャ (特徴点) の集合
- その後，多くの研究グループにより改良研究が進められている

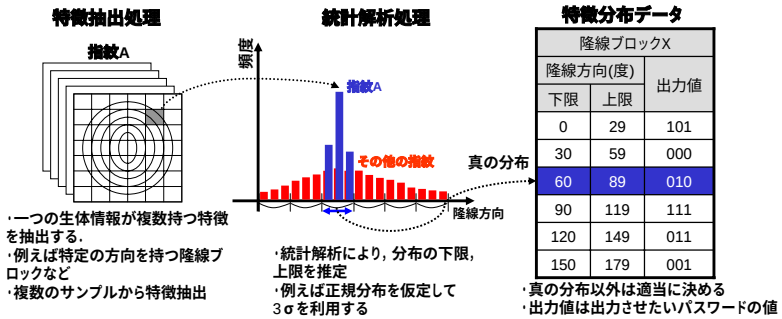


バイオメトリクス暗号の既存研究

統計的AD変換 (静岡大学他 2004)

HITACHI Inspire the Next

- 柴田 他，“メカニズムベースPKI ― 指紋からの秘密鍵動的生成”, 2004
  - 「統計的ＡＤ変換」による秘密鍵生成
    - 生体情報Xは独立なn個の値xiからなるベクトルX=(X1,...,Xn)とする
  - 各Xiの量子化幅を複数の登録生体情報から統計的に学習



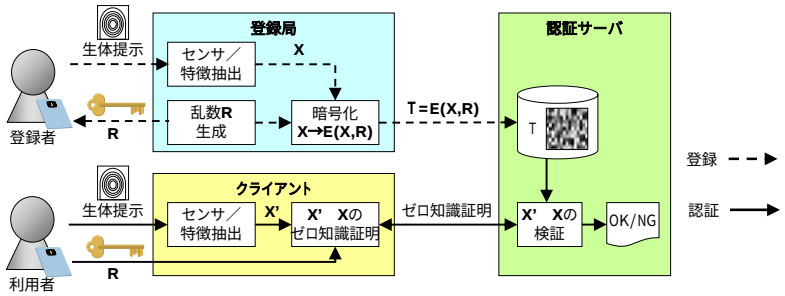
隆線ブロックX		
隆線方向(度)		出力値
下限	上限	
0	29	101
30	59	000
60	89	010
90	119	111
120	149	011
150	179	001

・真の分布以外は適当に決める
・出力値は出力させたいパスワードの値

非対称生体認証

HITACHI Inspire the Next

- 概要
  - クライアントが認証サーバに対し，Xに十分近いX’の知識をゼロ知識証明
  - 登録時：
    - 生体情報 X の暗号文 (又はコミットメント) T=E(X,R) をサーバに登録
    - 乱数 R を登録者に発行
  - 認証時：
    - 利用者の生体情報 X’ が X に十分「近い」ことをゼロ知識証明
- 特長
  - 認証サーバに対して生体情報を秘匿したまま認証 (プライバシ，セキュリティ向上)
  - 乱数 R を変更して，テンプレート T を破棄・更新可能 (漏洩してもセキュリティを維持)
  - 生体情報の秘匿性 (安全性) を証明可能

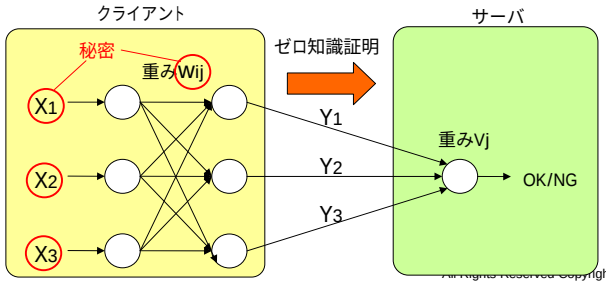


非対称生体認証の既存研究

東海大学 2005（秘匿ニューラルネット）

HITACHI Inspire the Next

- 菊池，“非対称生体認証”，2005
  - ニューラルネットワーク(NN)を用いて照合可能な生体認証方式を対象
  - 登録時：
    - 登録生体情報を受理するNNを学習
      - 中間層ノードの重み Wij をクライアントが保持
      - 出力層ノードの重み Vj と，Wij の暗号文 E(Wij, R) をサーバが保持
    - 乱数 R を登録者に発行
  - 認証時：
    - クライアントがNNの中間層までを計算し，その出力 Yj をサーバへ送信
    - NNの秘密計算により入力ベクトル（生体情報）Xiを秘匿したまま，Yiの正しさをゼロ知識証明
    - 中間層ノード数に比例した回数のゼロ知識証明が必要
- 指紋への適用報告あり（永井 他，2006）
  - FAR 8.3%，　FRR 9.8%

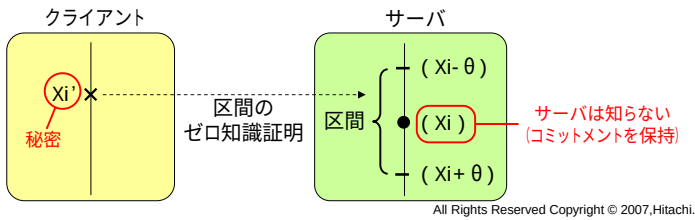


非対称生体認証の既存研究

東工大他 2006（「近さ」のゼロ知識証明）

HITACHI Inspire the Next

- 尾形，菊池，西垣
  “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”，2006
  - 対象とする生体認証方式
    - 生体情報：　ベクトル X= (X1,X2,・・・,Xn)
    - 生体情報X,Yが「近い」 ≡ max(|Xi – Yi|) ≦ m
  - 登録時：
    - 登録生体情報 X=(X1,・・・,Xn) のコミットメント {E(Xi,Ri)} をサーバに登録
    - 乱数 {Ri} を利用者に発行
  - 認証時：
    - 照合生体情報 X’ = (X1’,・・・,Xn’) の各 Xi’ が区間 [Xi- θ ,Xi+ θ]に含まれることをゼロ知識証明（「区間のゼロ知識証明」を利用）
    - クライアントは Xi を知らないため，Xi ∈{X’- θ ,・・・,X’+ θ } を総当りで試す
    - n θ 回の区間のゼロ知識証明が必要



目次

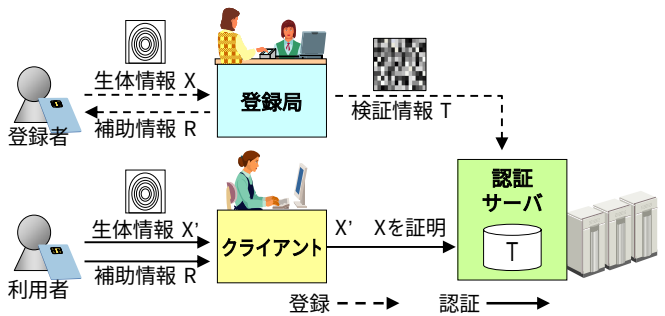
HITACHI Inspire the Next

要件抽出

リモート生体認証システムのモデル化

HITACHI Inspire the Next

- 登録局：
  - 登録者の生体情報Xを取得
  - 検証情報Tを作成
    → 認証サーバに発行
  - 補助情報Rを作成
    → 登録者に発行
- クライアント：
  - 利用者の生体情報X’を取得
  - Rを用いて認証サーバに対し X　X’を証明
- 認証サーバ：
  - Tを用いてX　X’を検証



要件抽出
リモート生体認証の前提条件

HITACHI Inspire the Next

- 登録局：
  - 不正を行わない（信頼できる）
  - 登録処理終了後にXを消去．漏洩はないとする
- クライアント：
  - 耐タンパー性を持たない： 補助情報Rが漏洩する危険性あり
  - タンパー証拠性を持つ： 不正改造された端末を利用者が知らずに使ってX'が漏洩するといった脅威は想定しない
- 認証サーバ：
  - 管理者のミスや内部不正により検証情報Tが漏洩する危険性あり
- クライアント・認証サーバ：
  - RとTの両方が漏洩することはないとする
  - 暗号化により通信路の盗聴はないものとする

要件抽出
脅威識別と要件抽出

HITACHI Inspire the Next

脅威の識別

攻撃者の条件 ＼ 攻撃の目的	生体情報入手	なりすまし
認証サーバ管理者	脅威1	ー
Tを入手した攻撃者	[脅威1に含まれる]	脅威2
Rを入手した攻撃者	脅威3	脅威4

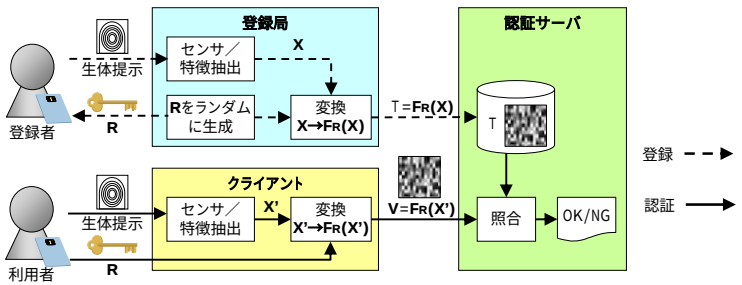
要件の抽出

- セキュリティ要件
  - 要件1：認証サーバが生体情報 X,X' を知ることができないこと(⇔脅威1)
  - 要件2：Tだけを知っていても認証成功できないこと（⇔脅威2）
  - 要件3：Rだけを知っていても X を知ることができず，また認証成功できないこと（⇔脅威3,4）
- 生体認証としての要件
  - 要件4：X'(X)をクライアントが知っていることを，認証サーバが確認できること
  - 要件5：従来の生体認証技術に対し，認証精度を大きく劣化させずに実現できること

既存技術の評価
キャンセラブルバイオメトリクス

HITACHI Inspire the Next

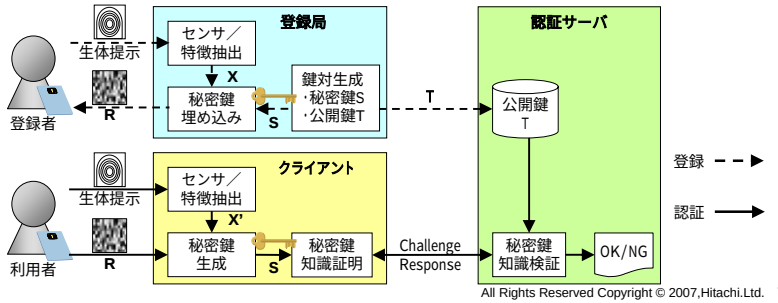
- 問題点
  - Tを入手した攻撃者がなりすまし可能（要件2を満たさない）
    - V として T を送信すればよい
  - 「クライアントがXに十分近いX'を知っている」ことを，認証サーバが確認できない（要件4を満たさない）
    - X' を知らずに V を送信している可能性がある



既存技術の評価
バイオメトリック暗号

HITACHI Inspire the Next

- 問題点
  - クライアントがXに十分近いX'を知っていることを，認証サーバが直接確認できない（要件4を満たさない）
    - Sの知識証明だけでは，X'の知識を証明したことにはならない．
  - 従来の生体認証技術と比較して現状，認証精度が低い（要件5を満たさない）
    - 例：Fuzzy Finverprint Vault：FRR 21%，FAR 0%

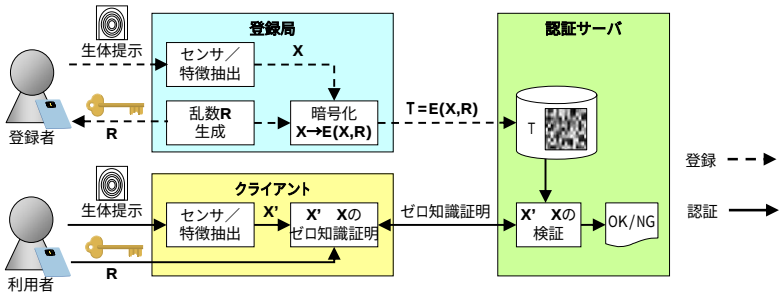


既存技術の評価

非対称生体認証

HITACHI Inspire the Next

- 問題点
  - 従来の生体認証技術と比較して現状，認証精度が低い（要件5を満たさない）
    - 例：NNの秘密計算に基づく非対称指紋認証：FRR=9.8%, FAR=8.3%
    - NNは任意の距離関数を近似できる可能性を持つため精度向上は可能だが，中間ノード数が増加する
  - 生体情報の次元数やNNノード数に比例した回数のゼロ知識証明プロトコルが必要
    - 計算量・通信量が膨大



既存技術の評価

テンプレート保護型生体認証技術の比較

HITACHI Inspire the Next

- キャンセラブルバイオメトリクス： 精度，計算量に優れる→実用化研究先行
- バイオメトリック暗号，非対称生体認証： 安全性に優れる→理論的研究先行
- 全ての要件を満たす方式の開発が課題

プロトコル	要件1 生体情報秘匿	要件2 検証情報漏洩時の安全性	要件3 補助情報漏洩時の安全性	要件4 生体情報の知識検証	要件5 精度保存	計算量
キャンセラブル バイオメトリクス	○	×	○	×	○	小
バイオメトリック 暗号	○	○	○	×	△	小〜中 誤り訂正＋ 公開鍵暗号計算O(1)
非対称生体認証	○	○	○	○	×	大 秘密計算 O(n) ゼロ知識証明 O(n)

（＊）従来プロトコル：
生体情報をそのまま，又は一般的な暗号化を施して登録，送信するプロトコル
暗号化した場合，照合時に生体情報を復号化して照合する

目次

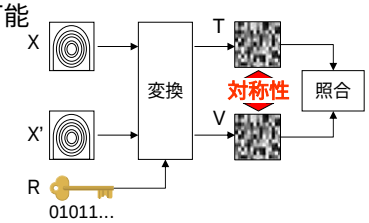
HITACHI Inspire the Next

提案プロトコル： 準備

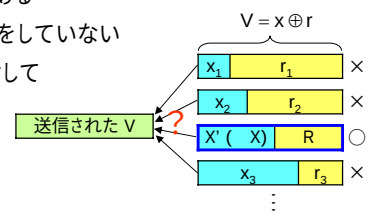
キャンセラブルバイオメトリクスの問題点分析

HITACHI Inspire the Next

- 問題点1：
  T=FR(X)を入手した攻撃者がなりすまし可能
  - 認証時に送る変換生体情報 V として，
    FR(X')の代わりに T を送信すればよい
  - 原因： 認証情報の対称性



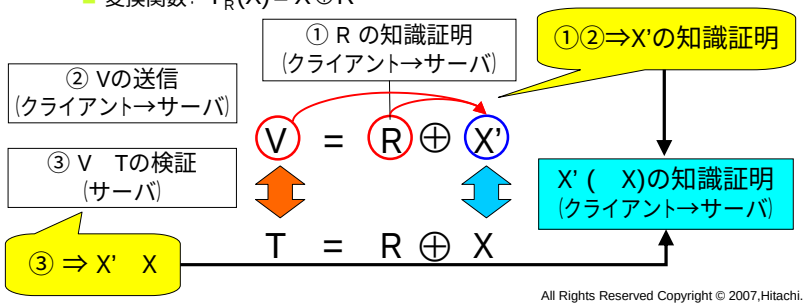
- 問題点2：
  「クライアントがXに十分近いX'を知っている」ことを認証サーバが確認できない
  - X' を知らずに V を送信している可能性がある
  - 原因：クライアントが X' (X)の知識証明をしていない
  - 例：$F_R(X) = X \oplus R$ のとき，送信されたVに対して
    - $V = x \oplus r$ なる (x,r) は 2^n 通り
    - V (T) を送信しても
      X' (X) の知識証明にはならない



提案プロトコル： アプローチ

キャンセラブルバイオメトリクスの非対称化

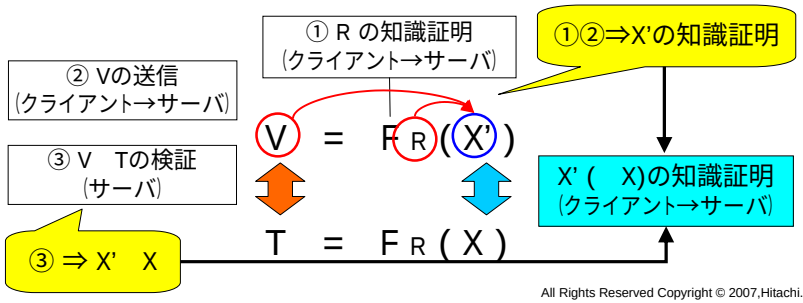
- 方針
  - クライアントが V(　T) を送信するとともに，R の知識をゼロ知識証明
- 問題1の解決
  - 攻撃者が T を入手しても，R が分からないため認証に失敗
- 問題2の解決
  - 「クライアントがV(　T) とRを知っている」⇒「クライアントは X’(　X)を知っている」
  - 例： キャンセラブル虹彩認証 [Braithwaite02]
    - 距離関数： ハミング距離
    - 変換関数： $F_R(X) = X \oplus R$



提案プロトコル： アプローチ

キャンセラブルバイオメトリクスの非対称化

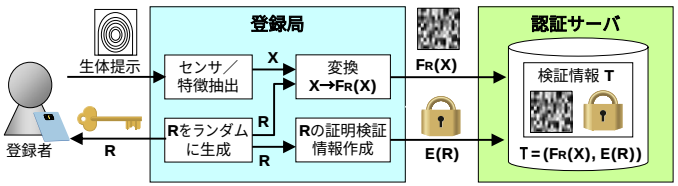
- 問題2の解決
  - 「クライアントがV(　T) とRを知っている」⇒「クライアントは X’(　X)を知っている」
  - 一般化：
    - 条件： 任意の r に対して変換関数 v=Fr(x) が逆関数 $x=Fr^{-1}(v)$ を持つ
      (V,R　を決めると　$V=F_R(X')$ なる X’ が一意に決まる)
  - ゼロ知識証明の必要性
    - R を直接サーバに開示してはならない
    - $X=F_R^{-1}(V)$ より，サーバに X が知られてしまうため (要件1に反する)



提案プロトコル

非対称キャンセラブルバイオメトリクス： 登録

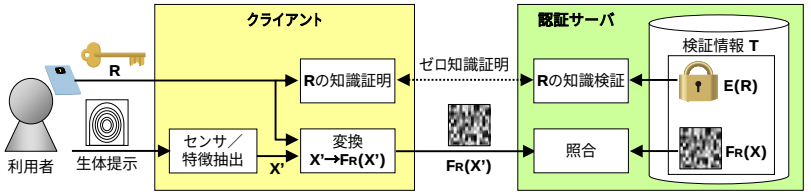
- 準備
  - キャンセラブル変換関数 F_R ： 任意の R に対して逆関数 F_R^{-1} が存在する
    - Application Specific Biometric Template [Braithwaite02]
    - 相関不変ランダムフィルタリング[Hirata06]
    - マニューシャ等長変換[Takahashi05]
  - R の知識のゼロ知識証明プロトコル：
    - Schnorr認証, Fujisaki-Okamoto commitment など
- 登録プロトコル
  - Step1: 登録局はパラメータ R をランダムに選択して F_R を決定
  - Step2: Rの知識のゼロ知識証明を検証するために必要な情報 E(R) を作成
  - Step3: 登録者の生体情報 X を取得し，$F_R(X)$ に変換
  - Step4: T=(F_R(X), E(R)) を検証情報として認証サーバに発行
    - T は X の (あいまいさを考慮した) コミットメントの一種
  - Step5: R を登録者に発行



提案プロトコル

非対称キャンセラブルバイオメトリクス： 認証

- 認証プロトコル
  - Step1: クライアントは R の知識を認証サーバに対してゼロ知識証明
  - Step2: 認証サーバは証明を検証し，失敗したらプロトコルを終了
  - Step3: クライアントは利用者の生体情報 X’ を取得
  - Step4: クライアントは $F_R(X')$ に変換し，認証サーバに送信
  - Step5: 認証サーバは $F_R(X')$ と $F_R(X)$ を照合し，十分近ければ認証成功とする



評価

HITACHI Inspire the Next

セキュリティ要件の評価

- 要件1：認証サーバが生体情報 X,X' を知ることができないこと
  - 既存のキャンセラブル方式を用いることで達成
    - Application Specific Biometric Template，相関不変ランダムフィルタリング，マニューシャ等長変換 等
  - ただし，X,X' 間の距離を含む部分情報は漏れる → 今後の課題
- 要件2：Tのみを用いてなりすましできないこと
  - R を知っていなくては認証成功することはできない
- 要件3：Rのみを用いて，生体情報入手やなりすましができないこと
  - R はランダムに選択された値なので，生体情報は漏洩しない．
  - V(T) を知っていなくては認証成功できない

生体認証としての要件の評価

- 要件4：X'(X)をクライアントが知っていることを，認証サーバが確認できること
  - 前述
- 要件5：従来の生体認証技術に対し，認証精度を大きく劣化させずに実現できること
  - 既存のキャンセラブル方式を用いることで達成

計算量の評価

- 認証プロトコルの計算量
  - 既存のキャンセラブル方式の計算量 ＋ R のゼロ知識証明（1回）の計算量

提案方式と既存方式の比較

HITACHI Inspire the Next

- 提案方式は全ての要件を満たす

プロトコル	要件1 生体情報秘匿	要件2 検証情報漏洩時の安全性	要件3 補助情報漏洩時の安全性	要件4 生体情報の知識検証	要件5 精度保存	計算量
キャンセラブルバイオメトリクス	○	×	○	×	○	小 生体情報変換（ビット演算，FFT等）
バイオメトリック暗号	○	○	○	×	△	小～中 誤り訂正＋公開鍵暗号計算O(1)
非対称生体認証	○	○	○	○	×	大 秘密計算 O(n) ゼロ知識証明 O(n)
提案プロトコル 非対称キャンセラブル	○	○	○	○	○	小 生体情報変換＋ゼロ知識証明 O(1)

まとめ

HITACHI Inspire the Next

- テンプレート保護型生体認証技術の研究動向
  - キャンセラブルバイオメトリクス → 実用化研究先行
  - バイオメトリック暗号
  - 非対称生体認証 → 理論的研究先行
- 既存技術の評価･比較
  - リモート生体認証プロトコルの要件を明確化
  - 既存技術は一長一短，全要件を満たす方式はない
- 非対称キャンセラブルバイオメトリクスの提案･評価
  - キャンセラブルバイオメトリクスを部分的に非対称化して全要件を満足
  - 課題： 秘匿性を証明可能な方式への拡張

参考文献

HITACHI Inspire the Next

[1] M. Braithwaite, U. Cahn von Seelen, J.Cambier, J.Daugman, R.Glass, R.Moore, and I. Scott, "Application-specific biometric templates," In *AutoID02*, pp. 167–171, 2002.

[2] Clancy, T.C., Kiyavash, N., and Lin, D.J., "Secure smartcard-based fingerprint authentication," ACM Workshop on Biometrics: Methods and Applications, Nov. 2003, pp. 45-52, Berkeley, CA

[3] Ari Juels and Martin Wattenberg, A fuzzy commitment scheme," In *Proc. ACM CCS1999*, pp. 28–36, 1999.

[4] N.K. Ratha, J.H. Connell, and R.M. Bolle, "Enhancing security and privacy in biometric based authentication systems," *IBM System Journal*, Vol.40, No.3, 2001.

[5] U.Uludag, S.Pankanti, , and A.K. Jain, "Fuzzy vault for fingerprints," In *AVBPA*, pp. 310–319, 2005.

[6] 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," In *CSS2006*, pp. 633–638, 2006.

[7] 高橋健太, 三村昌弘, "キャンセラブル指紋照合方式の提案," In *CSS2005*, pp. 379–384, 2005.

[8] 菊池浩明, "非対称生体認証," In *CSS2005*, pp.307–311, 2005.

[9] 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, 2006-CSEC-34, pp. 435–440, 2006.

[10] 柴田陽一, 三村昌弘, 高橋健太, 中村逸一, 曽我正和, 西垣正勝, "メカニズムベースPKI—指紋からの秘密鍵動的生成," 情報処理学会論文誌, Vol.45, No.8, pp. 1833–1844, 2004.

[11] 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.