情報処理学会論文誌 Vol.54 No.11 2383–2391 (Nov. 2013)

推薦論文

Fuzzy Commitment Schemeを用いたバイオメトリック暗号における保護テンプレートの安全性評価

披田野 清良[1,a)] 大木 哲史[2] 高橋 健太[3]

受付日 2012年10月21日, 採録日 2013年9月13日

概要：ここ 10 年あまりにわたり，生体情報を秘匿して認証を行うテンプレート保護型生体認証が注目されている．しかしながら，それらの安全性に関する議論では，生体情報間の相関性により，当該情報量が減少し，保護テンプレートが漏洩した際に，生体情報の推定が容易となる可能性については必ずしも十分に言及されていない．そこで，本論文では，テンプレート保護型生体認証の一方式である Fuzzy Commitment Scheme（FCS）を用いたバイオメトリック暗号に着目し，生体情報間の相関性を考慮して保護テンプレートの安全性を評価する．FCS では，ユーザが提示する生体情報から生成されたビット列と誤り訂正符号の符号語との排他的論理和を計算してコミットメントを作成し，これを保護テンプレートとすることにより安全性を確保している．本論文では，まず，ビット間に相関性の残る可能性が高い指紋情報に着目し，筆者らが提案する 2 次の Renyi エントロピーを用いた生体情報の情報量評価手法に基づき，実際に指紋ビット列のビット間には何らかの相関性があることを明らかにする．次いで，生体ビット列のビット間の相関性を利用したなりすましに関する新たな脅威として Decodable Biometric Dictionary Attack（DBDA）を提案し，DBDA に対する安全性を理論的に考察するとともに，シミュレーション結果を交えて定量的に評価する．

キーワード：テンプレート保護型生体認証，Fuzzy Commitment Scheme，推定攻撃，安全性評価

Evaluation of Security for Protected Template in Biometric Cryptosystem Using Fuzzy Commitment Scheme

Seira Hidano[1,a)] Tetsushi Ohki[2] Kenta Takahashi[3]

Received: October 21, 2012, Accepted: September 13, 2013

Abstract: Biometric authentication based template protection has attracted attention in the past decade. However, in the discussion on the security of these systems, the content of biometric information is assumed to be sufficiently large and it has not been considered that genuine biometric information can be easily guessed from a compromised protected template due to the correlation between biometric samples. In this paper, we thus focus on the biometric cryptosystem using a fuzzy commitment scheme and evaluate the security of the protected template with consideration of the correlation between biometric samples. The FCS creates a commitment by binding a biometric bit string, which is generated from biometric samples a user presents, with a codeword of an error-correction code by using a bitwise XOR operator and stores the commitment in the system as a protected template. It is firstly demonstrated in this paper that there is any correlation between bits on a fingerprint bit string by evaluating information content in a fingerprint bit string on the basis of an evaluation method using quadratic Renyi entropy. Additionally, a decodable biometric dictionary attack (DBDA), which is an impersonation attack taking advantage of the correlation, are proposed and the security against the DBDA is theoretically and empirically discussed.

Keywords: biometric authentication based on template protection, fuzzy commitment scheme, guessing attacks, security evaluation

1. はじめに

生体認証は，記憶，所持のわずらわしさから解放されるなどの利便性がある一方，ユーザ，環境条件，運用条件，生体情報，ならびに認証装置などの様々な構成要素において特有の脆弱性が存在する．特に，生体認証においてシステムに保管されている生体情報（以下，テンプレート）は，個人性を多く含む機微情報であり，変更することができないため，情報漏洩に対するリスクが非常に大きい．

このため，ここ 10 年あまりにわたり，生体情報を解読不可能な状態に変換して認証を行うテンプレート保護型生体認証が注目されている．テンプレート保護型生体認証の代表的な研究事例としては，ユーザが提示する生体情報とシステムに保管されている補助情報から一意の秘密鍵を生成するバイオメトリック暗号 [1], [2], [3] と，幾何変形もしくは相関性のあるハッシュ関数などを用いてテンプレートを非可逆に変換するキャンセラブルバイオメトリクス [4], [5] があげられる．特に，Fuzzy Commitment Scheme（FCS）を用いたバイオメトリック暗号は，生体情報の安全性だけでなく，秘密鍵の秘匿性にも優れており，Challenge Handshake Authentication Protocol（CHAP）[6] などの既存の認証プロトコルとの親和性が高く，また他のテンプレート保護技術と比べて実装が容易であることから，近年欧州を中心に活発な議論が展開され，同時に製品化も進んでいる．

FCS は，1999 年に Juels と Wattenberg により提案された誤り訂正符号に基づく暗号方式の一種である．FCS を用いたバイオメトリック暗号では，ユーザの生体情報と任意の秘密鍵から生成された符号語との排他的論理和を計算し，これを補助情報（以下，コミットメント）としてシステムに保管する．このため，生体情報は事前に量子化しておく必要があり，多くの研究者らが揺らぎのある生体情報から一意のビット列（以下，生体ビット列）を抽出する方法を検討している [7], [8], [9], [10]．コミットメントから元の生体ビット列を推定することを困難にするためには，ビット列のすべてのパターンが一様に生起することが望ましい．しかしながら，これまでの検討では，それぞれの提案手法が生体情報間の強い相関性を十分に除去できることを明確に主張できていない．

また，FCS の安全性を情報理論の概念に基づき定式化する試みもある [11], [12], [13]．しかしながら，それらの議論では，生体ビット列の情報量が十分に大きいこと，すなわちビット列の各ビットが i.i.d. であることを前提としており，ビット間の相関性により情報量が減少し，ビット列の推定が容易となる可能性については必ずしも十分に検討されていない．上述したように FCS はすでに実用化のフェーズにあるが，実世界の制約が考慮されていない不十分な評価により安全であると判断された手法が広く普及した場合，想定していなかった危険性が生じる可能性がある．

そこで，本論文では，FCS を用いたバイオメトリック暗号について，生体ビット列のビット間の相関性を考慮してコミットメントの安全性を評価する．まず，ビット間に相関性の残る可能性が高い指紋情報に着目し，筆者らが提案する 2 次の Renyi エントロピーを用いた生体情報の情報量評価手法 [14] に基づき，実際に指紋ビット列のビット間には何らかの相関性があることを明らかにする．次いで，生体ビット列のビット間に相関性があることを利用したなりすましに関する新たな脅威として Decodable Biometric Dictionary Attack（DBDA）を提案し，DBDA に対する安全性を理論的に考察するとともに，シミュレーション結果を交えて定量的に評価する．

2. Fuzzy Commitment Scheme（FCS）を用いたバイオメトリック暗号

Fuzzy Commitment Scheme を用いたバイオメトリック暗号の認証モデルについて概説し，従来の安全性評価の問題点を指摘する．

2.1 認証モデル

Fuzzy Commitment Scheme（FCS）[1] は，1999 年に Juels と Wattenberg により提案された誤り訂正符号に基づく暗号方式の一種であり，生体情報だけでなく秘密鍵の秘匿性にも優れていることから，バイオメトリック暗号への適用が期待されている．**図 1** に，FCS を用いたバイオメトリッ

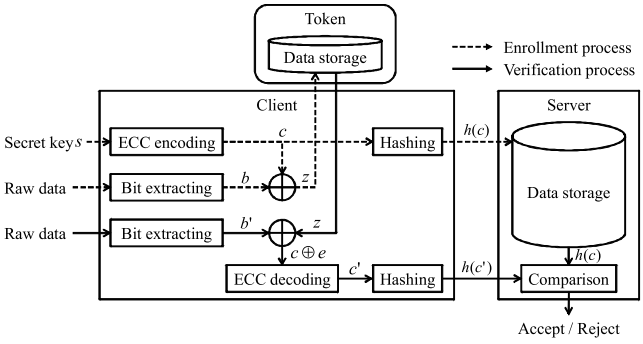

図 1 FCS を用いたバイオメトリック暗号
Fig. 1 Biometric cryptosystem using FCS.

[1] 早稲田大学理工学術院
Faculty of Science and Engineering, Waseda University, Shinjuku, Tokyo 169–8555, Japan
[2] 産業技術総合研究所セキュアシステム研究部門
Research Institute for Secure Systems, National Institute of Advanced Industrial Science and Technology, Tsukuba, Ibaraki 305–8568, Japan
[3] 株式会社日立製作所横浜研究所
Yokohama Research Laboratory, Hitachi, Ltd., Yokohama, Kanagawa 244–0817, Japan
[a)] hidano@wiz.cs.waseda.ac.jp

本論文の内容は 2011 年 10 月のコンピュータセキュリティシンポジウム 2011（CSS2011）にて報告され，同プログラム委員長により情報処理学会論文誌ジャーナルへの掲載が推薦された論文である．

ク暗号の一例を示す．バイオメトリック暗号では，安全性の観点から，秘密鍵を生成するための補助情報と秘密鍵の正当性を確認するための検証情報は異なるストレージに保管されることが望ましい [15]．そこで，本論文でもこの点に留意して，図 1 のサーバ/クライアントモデルを例に認証方式の概要を説明する．

■ 登録過程

(1) クライアントは，ユーザが提示した生体に関する原情報からビット列 $b \in \mathcal{B} = \{0,1\}^n$ を抽出する．ただし，$|\mathcal{B}| = 2^n$ とする．$|\cdot|$ は集合の要素数を示す．

(2) クライアントは，ランダムに選択した秘密鍵 $s \in \{0,1\}^k$ から誤り訂正符号化により符号語 $c \in \mathcal{C}$ を生成し，b と c との排他的論理和を計算することにより，コミットメント $z = b \oplus c$ を作成する．ただし，本論文では，$\mathcal{C}$ は，符号長 n，情報記号数 k，最小距離 d_{min} の (n, k, d_{min})-線形符号とする．このとき，$|\mathcal{C}| = 2^k$ となり，$t = (d_{min} - 1)/2$ 個以下のビット誤りを訂正できる．

(3) クライアントは，c のハッシュ値 $h(c)$ を計算して認証サーバに送信し，また z をユーザのトークン内に保存する．

(4) 認証サーバは，$h(c)$ を自身のストレージに保管する．

■ 照合過程

(1) クライアントは，登録時と同様に，ユーザが提示した生体に関する原情報から b と同形式の生体情報 $b' \in \mathcal{B}$ を抽出し，また当該ユーザのトークンから z を読みこむ．

(2) クライアントは，b' と z との排他的論理和を計算し，$c \oplus e = b' \oplus z$ から誤り訂正復号化により c' を得る．ただし，$e = b \oplus b'$ とし，$\| e \| \leq t$ のとき，c' は c と一致する．$\|\cdot\|$ はハミング重みを示す．

(3) クライアントは，c' のハッシュ値 $h(c')$ を計算し，$h(c')$ を認証サーバに送信する．

(4) 認証サーバは，$h(c')$ と $h(c)$ を比較し，ユーザの正当性を検証する．

2.2 安全性評価の問題点

バイオメトリック暗号では，補助情報から生体情報もしくは秘密鍵を推定する困難さが安全性の評価項目となる [15], [16]．このため，FCS を用いたバイオメトリック暗号の安全性に関する議論では，漏洩したコミットメント $z = b \oplus c$ から生体ビット列 b もしくは符号語 c を推定する困難さが評価の焦点となり，Tuyls らや Wang らは次の相互情報量により当該評価項目の安全性を定式化している [11], [13]．

$$I(Z; B) = H(B) - H(B|Z) = n - k \quad (1)$$

$$I(Z; S) = H(S) - H(S|Z) = 0 \quad (2)$$

ただし，Z，B，S はそれぞれ z，b，s をとりうる値とする確率変数を示し，$H(\cdot)$ は Shannon エントロピーを示す．さらに，Tuyls らは，式 (1) より，$H(B|Z) = H(B) - (n - k)$ を導出し，$H(B) = n$ として，生体ビット列の推定困難性を $H(B|Z) = k$ に帰着させている [8]．しかしながら，b を生成する際に生体情報間の強い相関性を除去できなかった場合，あるビットが生起したときに必ず生起するビットが混入するなど，ビット間にも何らかの相関性が残る．このとき，各ビットは i.i.d. でなくなり，B は一様分布に従わなくなる．また，ある離散確率変数の Shannon エントロピーは，その確率変数が一様分布に従うときに最大値をとり，それ以外のときは最大値より小さい値をとる．したがって，ビット間に何らかの相関性がある場合，$H(B)$ は n より小さい値をとり，$H(B|Z)$ も同様に k より減少すると考えられる．式 (2) についても，ビット間に何らかの相関性がある場合，$H(S|Z)$ は k より小さい値をとる可能性があり，必ずしも等号が成立するとは限らない．したがって，生体ビット列のビット間に何らかの相関性がある場合，コミットメントが漏洩した際の生体ビット列および秘密鍵の推定はともに従来評価よりも容易になる可能性がある．このため，1 章で述べたように，すべてのパターンが一様に生起するビット列を作成できない限り，従来の安全性評価は妥当ではないと考えられる．

3. 指紋ビット列の情報量評価

本章では，生体情報の中でも隆線の連続性などからビット間に相関性の残る可能性が高い指紋情報に着目し，筆者らが提案する 2 次の Renyi エントロピーを用いた生体情報の情報量評価手法 [14] に基づき，指紋ビット列の情報量を定量的に評価する．そして，その評価結果より，指紋ビット列のビット間には何らかの相関性があることを明らかにする．まず，3.1 節において，生体情報の情報量評価手法を紹介し，次いで，3.2 節において，本評価手法の指紋ビット列を用いた FCS への適用方法を示す．そして，3.3 節において，実際に指紋画像のデータベースを用いて指紋ビット列の 2 次の Renyi エントロピーを算出する．

3.1 生体情報の情報量評価手法

生体ビット列のビット間の相関性の有無を情報量の概念に基づき定量的に評価するためには，情報量の評価尺度として，ビット間の相関性の有無に応じて異なる値をとり，また推定結果に対する信頼性が高いものを選定する必要がある．2.2 節で述べたように，ビット間に相関性がない場合，生体ビット列空間上の離散確率変数は一様分布に従い，ビット間に何らかの相関性がある場合，一様分布とは異なる分布に従う．このため，評価尺度は，一様分布のときに最大値をとり，それ以外のときに最大値より小さい値をとるものが望ましく，この条件を満たす代表的な情報量評価

尺度としては，Shannon エントロピーや 2 次の Renyi エントロピーがあげられる．しかしながら，生体ビット列空間は高次元な空間であるため，生体ビット列の確率分布の推定には膨大なサンプルが必要となり，分布推定が容易ではない．このため，生体ビット列の確率分布から導出される Shannon エントロピーは評価尺度として適さない．一方，2 次の Renyi エントロピーは，一般的には，生体ビット列の確率分布から導出されるが，筆者らにより生体情報の距離分布を用いて導出する方法が提案されている．生体認証において生体情報間の距離は生体ビット列よりも低次元な情報であるため，生体ビット列の確率分布よりも推定が容易である．また，距離分布の推定については，生体認証の標準的な精度評価方法 [17] の中で信頼性の高い分布推定方法が定められていることから，その分布から導出される情報量に対する信頼性は高いと考えられる．そこで，本論文では，2 次の Renyi エントロピーを情報量の評価尺度として採用する．以下，筆者らが提案している 2 次の Renyi エントロピーを用いた生体情報の情報量評価手法について述べる．

まず，生体情報 b の空間 $\mathcal{B}$ 上の離散確率変数を B（以下，確率変数はすべて離散確率変数としてあつかう），B の確率関数を $p_B(b)$ とすると，生体情報の 2 次の Renyi エントロピー $H_2(B)$ は次式で定義される [18]．

$$H_2(B) = -\log_2 \sum_{b\in\mathcal{B}} p_B(b)^2 \tag{3}$$

生体情報 b，$b' \in \mathcal{B}$ の間の距離 $d \in \mathbb{R}$ をとりうる値とする確率変数 D の確率関数 $p_D(d)$ は，$\mathcal{B}$ 上の i.i.d. な 2 つの確率変数 B と B'，およびスコア関数 $g : \mathcal{B} \times \mathcal{B} \to \mathbb{R}$ を用いて，次式で表せる．

$$\begin{aligned} p_D(d) &= P(g(B,B') = d) && (4)\\ &= \sum_{\substack{b,b'\in\mathcal{B},\\ g(b,b')=d}} P(B=b, B'=b') && (5)\\ &= \sum_{\substack{b,b'\in\mathcal{B},\\ g(b,b')=d}} p_B(b)p_B(b') && (6) \end{aligned}$$

このとき，距離の公理の 1 つである非退化性：$b = b' \Leftrightarrow g(b,b') = 0$ より，2 つの生体情報が一致する確率 $p_D(0)$ は次式で与えられる．

$$\begin{aligned} p_D(0) &= \sum_{\substack{b,b'\in\mathcal{B},\\ b=b'}} p_B(b)p_B(b') && (7)\\ &= \sum_{b\in\mathcal{B}} p_B(b)^2 && (8) \end{aligned}$$

したがって，$H_2(B)$ は，$p_D(0)$ を用いて，次式で表せる．

$$H_2(B) = -\log_2 p_D(0) \tag{9}$$

$p_D(0)$ はきわめて小さい値であると考えられるが，$p_D(d)$ が既知であれば容易に導出できる．また，$p_D(d)$ は，b のサンプルを用いた照合実験をとおして得られる d のサンプルを学習データとして推定でき，b のサンプルの収集および照合を生体認証の標準的な精度評価方法 [17] に従うことにより，信頼性の高い分布推定が可能となる．このため，本評価手法では，式 (9) を用いて $H_2(B)$ を評価することを提案している．ただし，生体認証の精度評価では，本人間の照合結果が必要となるため，一般的な生体情報のデータベースには意図的に同一の生体から取得した複数の情報が収録されている．$\mathcal{B}$ は高次元な空間であるため，2 つの生体ビット列間の距離の値が小さくなる確率はきわめて小さいものであるが，本人間の照合結果を利用した場合，値の小さい d のサンプルが不自然に増加し，適切に分布推定を行えない可能性がある．このため，$p_D(d)$ の推定には，異なる生体どうしでの照合結果のみを利用する．$p_D(d)$ の推定に関しては，Daugman の虹彩認証 [19] のように $p_D(d)$ の形状が十分に検討された認証モデルであれば，$p_D(d)$ のモデルに基づき d のサンプルからパラメトリックに推定する [20]．一方，$p_D(d)$ の形状が未知でモデル化が困難な場合には，分布の形状を仮定せずにデータに依存して推定するノンパラメトリックな手法を用いる．

3.2 指紋ビット列の 2 次の Renyi エントロピー

2.1 節で示したように，FCS を用いたバイオメトリック暗号では，生体情報 b は符号長 n のビット列 $\mathcal{B} = \{0,1\}^n$ で記述され，2 つの生体ビット列 b，$b' \in \mathcal{B}$ の間の距離 d は次式で表せる．

$$d = \frac{\| b \oplus b' \|}{n} \tag{10}$$

このとき，d をとりうる値とする確率変数 D の確率関数 $p_D(d)$ は，生体ビット列のすべてのパターンが $\mathcal{B}$ 上に一様に分布するとき，各ビットの一致確率を θ とすると，$\theta = 0.5$ の二項分布 $Bi(0.5, n)$ でモデル化できる [19]．しかしながら，指紋の形状は，5 種類程度のパターンに分類できるため，隆線の位置と角度には強い相関性があり，指紋画像の部分的な領域における隆線の角度情報のみから隆線の連続性を利用して元の指紋画像を復元できることが知られている [21]．また，既存の指紋ビット列生成手法の多くは，マニューシャ情報や隆線の角度マップなど，指紋画像の部分的な領域における隆線の角度情報に基づく特徴量からビット列を生成しているが，特徴量を抽出する際に，指紋の形状に関する情報を過不足なく抽出するための最適な次元数などについてはまったく配慮していない．指紋特徴量が必要以上に多くの次元で構成された場合，一部の次元だけで元の指紋画像を完全に復元できる可能性があり，残りの次元は指紋の形状にまったく寄与しないと考えられる．そのような特徴量からビット列を生成した場合，同様に指紋の形状に関する情報をまったく持たないビットが混入する可

能性がある．

その結果，照合の際に識別に有効なビット数は減少する．したがって，指紋ビット列の $p_D(d)$ は，識別に有効なビット数を $\hat{n}$ とし，次式に示す二項分布でモデル化できると仮定する．

$$p_D(d) = \frac{\hat{n}!}{(\hat{n}d)!(\hat{n}(1-d))!}\theta^{\hat{n}(1-d)}(1-\theta)^{\hat{n}d} \tag{11}$$

ただし，既存のビット列生成手法は，どのビットも 0 と 1 が生起する確率が一様となるように配慮しているため，θ は理想的な場合と同様にほぼ 0.5 に近い値をとると考えられる．

このとき，D の平均 $E(D)$ および分散 $V(D)$ は，それぞれ次のように表せる．

$$E(D) = 1 - \theta \tag{12}$$

$$V(D) = \frac{\theta(1-\theta)}{\hat{n}} \tag{13}$$

式 (11) より，$p_D(0) = \theta^{\hat{n}}$ となり，指紋ビット列の 2 次の Renyi エントロピー $H_2(B)$ は次式で表せる．

$$H_2(B) = -\log_2 \theta^{\hat{n}} \tag{14}$$

θ と $\hat{n}$ の値は，生体ビット列のサンプルを用いた他人間照合実験を通して得られる距離のサンプルの平均および分散と式 (12)，式 (13) より実験的に推定し，指紋ビット列の 2 次の Renyi エントロピーはそれらの推定値と式 (14) より算出する．

3.3 情報量評価実験

本実験では，FCS の指紋認証への適用例として，Tuyls らの指紋ビット列を用いたバイオメトリック暗号 [8] を評価対象とした．Tuyls らのビット列生成手法では，まず，指紋の中心点を基準に指紋画像を 16×16 の格子に分割し，Jain らの提案する 4 種の Gabor フィルタを用いた手法 [22] により 1,024 次元，Bazen らの Squared Directional Field [23] を用いた手法により 512 次元，計 1,536 次元の特徴ベクトルを生成する．次に，指紋画像のデータベースを用いて次元ごとに特徴量の平均を計算し，平均値より小さい値の次元には 0 を，大きい値の次元には 1 を割り当て 1,536 次元のビット列を作成する．そして，同一指から取得した複数枚の指紋画像を利用して信頼性の高いビットのみを選択し，符号長 n（≤1,536）の指紋ビット列を生成する．

指紋画像のデータベースとしては，FVC2002 DB1 のセット A に収録されている異なる 100 指から 8 枚ずつ取得した計 800 枚の画像を使用した．ただし，それぞれの指について 6 枚を登録用，残りの 2 枚を照合用とし，符号長 $n = 127$ の指紋ビット列を生成して異なる指どうしで照合を行った．

図 2 に異なる指どうしで照合を行った際の実験結果を示す．水平軸は式 (10) を用いて算出した距離を表し，垂直軸は距離の各値の生起確率を表す．このとき，指紋ビット列間の距離の平均は 0.498，分散は 0.00565 であった．式 (12) および式 (13) より，各ビットの一致確率 θ の推定値は 0.502，有効ビット数 $\hat{n}$ の推定値は 44 となり，図 2 にはこれらの推定値と式 (11) から算出した推定分布を示している．推定分布がほぼ実験値と一致することから，指紋ビット列の距離分布は式 (11) の二項分布で近似でき，指紋ビット列の 2 次の Renyi エントロピー $H_2(B)$ は式 (14) を用いて十分に推定可能であるといえる．上記の推定値と式 (14) より，$H_2(B)$ は 44 bits であった．また，およそ $\theta = 0.5$ の二項分布で近似できることから，指紋ビット列空間には 2^{44} 個のパターンが存在すると考えられる．符号長 127 の生体ビット列の場合，理想的には 2^{127} 個のパターンが生起するため，ビット間の相関性により，とりうるパターン数が大きく減少してしまったことがうかがえる．

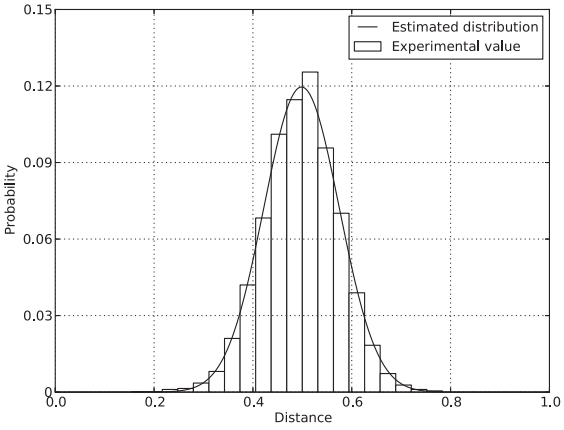

図 2 他人間照合実験結果
Fig. 2 Distribution of distance scores.

近年，Feng らにより，1 枚の指紋画像に含まれる全マニューシャのうち約 6 割のマニューシャがあれば，元の指紋画像をほぼ完全に復元できることが示唆されている [24]．本実験で用いた指紋画像のデータベースの場合，1 枚の指紋画像に含まれるマニューシャ数の平均が 31 個であったため，およそ 19 個のマニューシャのみで指紋画像を復元できるといえる．Tuyls らの指紋ビット列生成手法では，特徴量としてマニューシャ情報を用いているわけではないが，Squared Directional Field を用いた手法により生成される角度情報はマニューシャ情報の角度情報と類似しており，マニューシャを含む分割領域であればマニューシャの位置に関する情報も保持できるため，その領域はマニューシャ 1 つと同等の情報量を持つと考えられる．Squared Directional Field を用いた手法では，それぞれの分割領域の角度情報が x 軸方向と y 軸方向の 2 次元の特徴量で表されるため，上記の議論より計 38 次元の情報があれば指紋画像を十分に復元できる可能性があるといえる．また，Tuyls らの手法により生成された指紋ビット列は，その約

7 割が，Squared Directional Field を用いた手法により生成されたビットであるため，上記の 38 次元の特徴量に関するビットが選択されている可能性が高い．このとき，残りのビットは指紋に関する情報を持たずに一意に決まるため，指紋ビット列は約 38 bits 程度の情報量を持つと考えられる．本節で得られた 44 bits はおおむねこの値に近い値であるため，たしかに上記の 38 次元の特徴量に関するビットが選択されていることがうかがえる．ただし，Feng らの手法では，平均 6 個の分割領域において復元に失敗することが分かっているため，指紋画像を一意に決定するには，別にそれらの失敗する領域に関する情報を持つビットが必要となる．このため，本節で得られた指紋ビット列の情報量は 38 bits よりもわずかに大きい値になったと考えられる．したがって，44 bits という値は妥当な値であるといえる．

ビット間に相関性を残さないためには，指紋特徴量からビット列を生成する際に，次元間の関係や適切な次元数について十分に議論する必要があるが，Tuyls ら以外の指紋情報に適用可能な他のビット列生成手法においても，この点については必ずしも十分に配慮されていないため，同様にビット間に相関性が残る可能性が高い．ビット間の相関性により生体ビット列として実際にとりうるパターン数が減少する場合，4 章および 5 章で詳述するが，FCS の安全性を著しく低下させるなりすましに関する脅威が存在する．

4. FCS に対する攻撃

本章では，FCS を用いたバイオメトリック暗号においてコミットメントが漏洩した際に起こりうる，ビット間の相関性により生体ビット列としてとりうるパターン数が減少することを利用した当該システムへのなりすましに関する新たな脅威について述べる．ただし，本論文では，異なるシステムに保管されている同一の生体から作成された複数のコミットメントを利用した攻撃 [12], [25] は対象とせず，単一のシステムに対する攻撃のみについて言及する．したがって，漏洩したコミットメントから元の生体ビット列を完全に復元することは目的とせず，対象システムへのなりすましに成功することが可能な生体ビット列の推定を目的とする．また，攻撃時にコミットメントの破棄および再作成は行われていないものとする．まず，本章で提案する新たな攻撃方法との比較のために，FCS に対する一般的な総当たり攻撃として，4.1 節において，生体ビット列空間の大きさを利用した Biometric Dictionary Attack（BDA）を示し，4.2 節において，符号語空間の大きさを利用した Exhaustive Codeword Search Attack（ECSA）を示す．そして，4.3 節において，新たな攻撃方法として，ビット間の相関性により生体ビット列のすべてのパターンが生起しない場合に生体ビット列空間に含まれる何らかの符号語に誤り訂正可能な語の数が減少することを利用した Decodable Biometric Dictionary Attack（DBDA）を提案する．

4.1 Biometric Dictionary Attack（BDA）

BDA の攻撃手順を以下に示す．

(1) システムで利用されているモダリティの生体情報データベース $DB = \{f_1, \ldots, f_N\}$ を用意し，DB からランダムに 1 つを攻撃用生体情報 f^* として選択する．
(2) 2.1 節で示した照合過程の手順 1 において，攻撃対象ユーザになりすまし，f^* をクライアントに入力する．
(3) 照合過程の手順 4 において，認証サーバが Accept を返せば攻撃成功とする．

4.2 Exhaustive Codeword Search Attack（ECSA）

ECSA の攻撃手順を以下に示す．ただし，攻撃者は誤り訂正符号に関する各パラメータと生成多項式を知っているものとする．

(1) 2^k 個の符号語空間 $\mathcal{C}$ からランダムに 1 つを攻撃用符号語 c^* として選択する．
(2) 照合過程の手順 3 において，クライアント内の c' を c^* に改ざんするか，もしくは c^* のハッシュ値 $h(c^*)$ を不正に認証サーバに送信する．
(3) 照合過程の手順 4 において，認証サーバが Accept を返せば攻撃成功とする．

4.3 Decodable Biometric Dictionary Attack（DBDA）

あるユーザのコミットメント $z = b \oplus c$ が漏洩した際の DBDA の攻撃手順を以下に示す．

(1) BDA と同様にシステムで利用されているモダリティの生体情報データベース $DB = \{f_1, \ldots, f_N\}$ を用意する．
(2) $f_i \in DB$ からビット列 b_i を生成し，b_i と取得した z との排他的論理和 $b_i \oplus z$ に対して誤り訂正復号化処理を施す．このとき，$b_i \oplus z$ は何らかの符号語に復元される場合と復号化に失敗して何も復元されない場合がある．
(3) 手順 2 において，$b_i \oplus z$ が何らかの符号語に復元された場合，f_i を新たな攻撃用生体情報データベース $\overline{DB}$ に加える．手順 2 および手順 3 はすべての f_i について行う．
(4) $\overline{DB}$ からランダムに 1 つを攻撃用生体情報 f^* として選択して，照合過程の手順 1 において，z が盗まれたユーザになりすまし，f^* をクライアントに入力する．
(5) 照合過程の手順 4 において，認証サーバが Accept を返せば攻撃成功とする．

Simoens らや Kelkboom らは，同一の生体から作成された複数のコミットメントの識別困難性の評価において，DBDA と類似の概念に基づくクロスマッチング型の Decod-

ability Attack に着目して議論を展開している [12], [25]. 特に，Kelkboom らは，当該攻撃への対策として，コミットメントを作成する前に生体ビット列に対してビット置換を施す方法を提案している．しかしながら，攻撃者がビット置換を行うための変換行列を知っている場合，Kelkboom らの方法では DBDA を防ぐことはできない．

5. セキュリティ分析

4 章で示したそれぞれの脅威に対する安全性について，まず，5.1 節において，攻撃の成功確率を理論的に考察し，次いで，5.2 節において，シミュレーション結果を交えて定量的に評価する．

5.1 理論的考察

本節では，生体情報間の相関性の影響の 1 つとして，生体ビット列のすべてのパターンが $\mathcal{B} = \{0,1\}^n$ 上に一様に分布せずに，生起確率がきわめて低いパターンが存在する場合を考える．

■ BDA

BDA の攻撃成功確率は，生体認証の標準的な精度評価尺度の 1 つである False Accept Rate（FAR）と一致する [26]. ここで，$\mathcal{B}$ 上の確率変数の従う確率関数 $p_B(b)$ を用いて，$\mathcal{B}$ の部分集合 $\bar{\mathcal{B}} = \{b \mid p_B(b) > \epsilon, b \in \mathcal{B}\}$ を考える．生体ビット列間の相関性が大きいとき，$|\bar{\mathcal{B}}| = 2^{\hat{n}}$ は $|\mathcal{B}| = 2^n$ より小さい値をとる．ただし，$\bar{\mathcal{B}}$ 上の確率変数は一様分布に従うと仮定する．このとき，FAR は，$\{0,1\}^n$ からランダムに選択した語 x を用いて，次式で表せる．

$$FAR = \frac{|\bar{\mathcal{B}}_t(b)|}{2^n \cdot P(x \in \bar{\mathcal{B}})} \tag{15}$$

$$= \frac{|\bar{\mathcal{B}}_t(b)|}{|\bar{\mathcal{B}}|} \tag{16}$$

$\bar{\mathcal{B}}_t(b)$ は，b を中心とする半径 t の超球の内側にある生体ビット列の集合，すなわち，$\bar{\mathcal{B}}_t(b) = \{b' | \parallel b \oplus b' \parallel \leq t, b' \in \bar{\mathcal{B}}\}$ とする．

■ ECSA

ECSA の攻撃成功確率 P_{ECSA} は，符号語空間 $\mathcal{C}$ の大きさ $|\mathcal{C}| = 2^k$ を用いて，次式で表せる．

$$P_{ECSA} = \frac{1}{2^n \cdot P(x \in \mathcal{C})} \tag{17}$$

$$= \frac{1}{|\mathcal{C}|} = \frac{1}{2^k} \tag{18}$$

■ DBDA

$\mathcal{C}_t(c)$ をある符号語 $c \in \mathcal{C}$ について誤り訂正可能な語の集合，すなわち，$\mathcal{C}_t(c) = \{x | \parallel c \oplus x \parallel \leq t, x \in \{0,1\}^n\}$ とすると，DBDA の攻撃成功確率 P_{DBDA} は次式で表せる．

$$P_{DBDA} = \frac{|\bar{\mathcal{B}}_t(b)|}{2^n \cdot P(x \oplus z \in \bigcup_{c \in \mathcal{C}} \mathcal{C}_t(c), x \in \bar{\mathcal{B}})} \tag{19}$$

$$\approx \frac{|\bar{\mathcal{B}}_t(b)|}{2^n \cdot P(x \in \bigcup_{c \in \mathcal{C}} \mathcal{C}_t(c) \cap \bar{\mathcal{B}})} \tag{20}$$

ただし，式 (20) は，線形符号の性質により，$\bar{\mathcal{B}}$ と $\bar{\mathcal{B}}$ を z だけ平行移動した空間において，何らかの符号語に誤り訂正可能な語の空間の占める割合がほぼ等しくなることを仮定している [13]．ここで，BDA および ECSA との安全性に関する関係を明らかにするために，FAR および P_{ECSA} の導出に用いたパラメータに着目する．ただし，議論を簡単にするために，$\bar{\mathcal{B}}$ に含まれる $2^{\hat{n}}$ 個のすべてのパターンが $\mathcal{B}$ の部分空間 $\{0,1\}^{\hat{n}}$ 上に存在すると仮定する．このとき，$\bar{\mathcal{B}}$ に含まれる c の個数を $2^{\hat{k}}$ $(\hat{k} \leq k)$ とすると，式 (16) および式 (18) より，P_{DBDA} は次式で表せる．

$$P_{DBDA} \approx FAR \cdot \frac{|\bar{\mathcal{B}}|}{|\bar{\mathcal{B}}_t(b)| \cdot 2^{\hat{k}}} \tag{21}$$

$$\approx (P_{ECSA})^{\frac{\hat{k}}{k}} \tag{22}$$

式 (21) の $|\bar{\mathcal{B}}_t(b)| \cdot 2^{\hat{k}}$ は，生体ビット列空間と誤り訂正可能な語の空間が重なる領域の大きさを示しており，$\bar{\mathcal{B}}$ 上にどの符号語にも復元されない語が存在する場合，$|\bar{\mathcal{B}}|$ よりも小さくなることは明らかである．筆者らの知る限り，FCS を用いたバイオメトリック暗号において，認証精度を保ちつつ，生体ビット列のすべてのパターンを何らかの符号語に誤り訂正可能な最適な復号方法は存在しない．したがって，式 (21) より，P_{DBDA} はビット間の相関性にかかわらず，FAR よりも必ず高くなることが分かる．また，式 (22) より，ビット間に相関性がないときは，DBDA の有効性は ECSA と同程度であるが，ビット間の相関性により生体ビット列空間の大きさが小さくなり，$\bar{\mathcal{B}}$ に含まれる c の数が減少するにつれて増大することが分かる．式 (22) の $\hat{k}/k$ は，$\bar{\mathcal{B}}$ と $\mathcal{B}$ に含まれる何らかの符号語に誤り訂正可能な語の空間の大きさの比とも解釈できる．このため，$\bar{\mathcal{B}}$ が部分空間 $\{0,1\}^{\hat{n}}$ と一致しないような複雑な空間構造の場合においても，生体ビット列空間の大きさが小さくなり，$\bar{\mathcal{B}}$ に含まれる何らかの符号語に誤り訂正可能な語の空間の大きさが小さくなれば，DBDA の有効性は ECSA よりも高くなるといえる．以上より，ビット間の相関性により，生体ビット列として実際にとりうるパターン数が減少する場合，FCS の安全性は，DBDA により，従来の BDA や ECSA と比較して，さらに低下すると考えられる．

5.2 安全性評価実験

FCS を用いたバイオメトリック暗号を指紋認証に適用し，4 章で示した脅威に対する安全性を定量的に評価する．

本実験では，3.3 節の情報量評価実験と同様に，Tuyls らの指紋ビット列を用いたバイオメトリック暗号 [8] を評価対象とした．また，(n, k, d_{min})-線形符号として符号長 $n = 127$ の BCH 符号を使用し，情報記号数 k は 8, 15 と変化させた．

表 1 に，BCH 符号の各パラメータ値における FAR, P_{ECSA}，ならびに P_{DBDA} の値を示す．また，参考値とし

表 1 攻撃成功確率
Table 1 Success probabilities of attacks.

(n, k, d_{min})	(127, 8, 63)	(127, 15, 55)
FRR	0.0118	0.0296
FAR	0.00180	0.000360
P_{ECSA}	0.00391	3.05×10^{-5}
P_{DBDA}	0.207	0.0496

て，生体認証の標準的な精度評価尺度の 1 つである False Reject Rate（FRR）を併記する [26]．どちらのパラメータ値においても P_{DBDA} の値は FAR と P_{ECSA} の値を大きく上回る結果となった．したがって，5.1 節で示したように，ビット間の相関性により，実際に生体ビット列としてとりうるパターン数が減少する場合，FCS の安全性は，DBDA により，従来の BDA や ECSA と比較して，著しく低下するといえる．また，3.3 節の実験結果より，指紋ビット列空間には 2^{44} 個のパターンが存在すると考えられる．このため，それらのパターンが存在する実際の空間上に，$2^{\hat{k}=44k/127}$ 個の符号語が存在すると仮定した場合，P_{DBDA} は，5.1 節の式 (22) より，$(n, k, d_{min}) = (127, 8, 63)$ のときは 0.147，$(n, k, d_{min}) = (127, 15, 55)$ のときは 0.0273 となる．どちらのパラメータの場合も，表 1 の値から大きく外れるものではないが，実験値の方がやや大きい値となった．これは，2^{44} 個のすべてのパターンが必ずしも指紋ビット列空間の部分空間 $\{0, 1\}^{44}$ 上に存在するわけではなく，より符号語を含みにくい空間構造の中に存在するためと考えられる．ただし，その複雑な空間を推定することは容易ではないため，実際に DBDA に対する FCS の安全性を評価する際は，従来の安全性評価のようにすべてを理論評価に頼るのではなく，FRR や FAR の評価と同様に本節の実験評価を実施すべきであるといえる．

6. おわりに

本論文では，テンプレート保護型生体認証の一方式である Fuzzy Commitment Scheme（FCS）を用いたバイオメトリック暗号に着目し，生体情報間の相関性を考慮して保護テンプレートの安全性を定量的に評価した．FCS を用いたバイオメトリック暗号では，生体情報からビット列を生成し，誤り訂正符号の符号語との排他的論理和を計算することにより，安全性を確保している．そこで，本論文では，まず，ビット間に相関性の残る可能性が高い指紋情報に着目し，指紋ビット列の 2 次の Renyi エントロピーを定量的に評価することにより，既存のビット列生成手法では指紋情報の持つ強い相関性を十分に除去できずに指紋ビット列空間の大きさが理想的な場合よりも小さくなることを明らかにした．次いで，生体ビット列空間の大きさが小さくなる場合に有効ななりすましに関する新たな脅威として，Decodable Biometric Dictioary Attack（DBDA）を提案し，それらの脅威に対する安全性を理論的に考察するとともに，シミュレーション結果を交えて定量的に評価した．その結果，ビット間の相関性により生体ビット列空間の大きさが理想的なときよりも小さくなる場合，FCS の安全性は，DBDA により，従来の FCS に対する一般的な攻撃方法と比較して，著しく低下するという知見を得ている．

また，本論文では誤り訂正符号として線形符号を対象としているが，非線形符号を用いた FCS もいくつか提案されている [27]．今後は，本論文の議論を非線形符号を用いた場合に拡張し，同様に，生体ビット列間の相関性が及ぼす影響や DBDA に対する安全性を明らかにしていく．

参考文献

[1] Juels, A. and Wattenberg, M.: A fuzzy commitment scheme, *Proc. 6th ACM Conference on Computer and Communications Security* (*CCS99*), pp.28–36 (1999).

[2] Juels, A. and Sudan, M.: A fuzzy vault scheme, *Proc. IEEE International Symposium on Information Theory* (*ISIT2002*), p.408 (2002).

[3] Dodis, Y., Ostrovsky, R., Reyzin, L. and Smith, A.: Fuzzy extractors: How to generate strong keys from biometrics and other noisy data, *SIAM Journal on Computing*, Vol.38, No.1, pp.97–139 (2008).

[4] Ratha, N.K., Connell, J.H. and Bolle, R.M.: Enhancing security and privacy in biometrics-based authentication systems, *IBM Systems Journal*, Vol.40, No.3, pp.614–634 (2001).

[5] Takahashi, K.: Unconditionally provably secure cancelable biometrics based on a quotient polynomial ring, *Proc. 2011 IEEE International Joint Conference on Biometrics* (*IJCB2011*), pp.1–8 (2011).

[6] The Internet Engineering Task Force: PPP challenge handshake authentication protocol (CHAP), available from ⟨http://www.ietf.org/rfc/rfc1994.txt⟩.

[7] Chang, Y., Zhang, W. and Chen, T.: Biometrics-based cryptographic key generation, *Proc. 2004 IEEE International Conference on Multimedia and Expo* (*ICME2004*), Vol.3, pp.2203–2206 (2004).

[8] Tuyls, P., Akkermans, A.H.M., Kevenaar, T.A.M., Schrijen, G.J., Bazen, A.M. and Veldhuis, R.N.J.: Practical biometric authentication with template protection, *Proc. 5th International Conference on Audio- and Video-Based Biometric Person Authentication* (*AVBPA2005*), pp.436–446 (2005).

[9] Sutcu, Y., Rane, S., Yedidia, J., Draper, S. and Vetro, A.: Feature transformation of biometric templates for secure biometric systems based on error correcting codes, *Proc. 2008 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops* (*CVPRW2008*), pp.1–6 (2008).

[10] Chen, C. and Veldhuis, R.: Binary biometric representation through pairwise polar quantization, *Proc. 3rd IAPR/IEEE International Conference on Biometrics* (*ICB2009*), pp.72–81 (2009).

[11] Tuyls, P. and Goseling, J.: Capacity and examples of template-protecting biometric authentication systems, *Proc. International Biometric Authentication Workshop* (*BioAW2004*), pp.158–170 (2004).

[12] Simoens, K., Tuyls, P. and Preneel, B.: Privacy weaknesses in biometric sketches, *Proc. 2009 IEEE Sympo-*

sium on Security and Privacy, pp.188–203 (2009).
[13] Wang, Y., Rane, S., Draper, S.C. and Ishwar, P.: An information-theoretic analysis of revocability and reusability in secure biometrics, *Proc. 2011 Information Theory and Applications Workshop* (*ITA2011*), pp.1–10 (2011).
[14] 披田野清良，赤尾直彦，小松尚久，高橋健太：Renyi エントロピーを用いた虹彩情報の情報量評価手法，情報処理学会論文誌，Vol.52, No.9, pp.2631–2640 (2011).
[15] ITU-T SG17 Recommendation X.1091: A guideline for evaluating telebiometric template protection techniques.
[16] Jain, A.K., Nandakumar, K. and Nagar, A.: Biometric template security, *EURASIP Journal on Advances in Signal Processing* (2008).
[17] Mansfield, A.J. and Wayman, J.L.: Best practices in testing and reporting performance of biometric devices: Version 2.01, Technical Report, Center for Mathematics and Scientific Computing, National Physical Laboratory (2002).
[18] Renyi, A.: On measures of entropy and information, *Proc. 4th Berkeley Symposium on Mathematical Statistics and Probability*, Vol.1, pp.547–561 (1960).
[19] Daugman, J.: The Importance of being random: Statistical principles of iris recognition, *Pattern Recognition*, Vol.36, No.2, pp.279–291 (2003).
[20] Bishop, C.M.: *Pattern Recognition and Machine Learning*, Springer (2006).
[21] Maltoni, D., Maio, D., Jain, A.K. and Prabhakar, S.: *Handbook of Fingerprint Recognition*, Springer (2003).
[22] Jain, A., Prabhakar, S., Hong, L. and Pankanti, S.: Filterbank-based fingerprint matching, *IEEE Trans. Image Processing*, Vol.9, No.5, pp.846–859 (2000).
[23] Bazen, A. and Veldhuis, R.: Detection of cores in fingerprints with improved dimension reduction, *Proc. 4th IEEE Benelux Signal Processing Symposium* (*SPS2004*), pp.41–44 (2004).
[24] Feng, J. and Jain, A.K.: Fingerprint reconstruction: From minutiae to phase, *IEEE Trans. Pattern Analysis and Machine Intelligence*, Vol.33, No.2, pp.209–223 (2011).
[25] Kelkboom, E.J.C., Breebaart, J., Kevenaar, T.A.M., Buhan, I. and Veldhuis, R.N.J.: Preventing the decodability attack based cross-matching in a fuzzy commitment scheme, *IEEE Trans. Information Forensics and Security*, Vol.6, No.1, pp.107–121 (2011).
[26] Li, S.Z. and Jain, A.: *Encyclopedia of Biometrics*, Springer (2009).
[27] Nandakumar, K.: A fingerprint cryptosystem based on minutiae phase spectrum, *Proc. 2nd IEEE International Workshop on Information Forensics and Security* (*WIFS2010*), pp.1–6 (2010).

推薦文

本論文では，Fuzzy Commitment Scheme（FCS）を用いたバイオメトリック暗号の安全性の再評価を行っている．まず，著者らが以前に発表している 2 次の Renyi エントロピーを用いた情報量評価手法に基づき，具体的に指紋情報の情報量を定量的に評価して，生体情報間に強い相関性があることを示している．また，FCS を用いたバイオメトリック暗号において，上記の相関性を利用したなりすまし攻撃に対する安全性を理論的立場と上記の指紋情報の情報量データに適用したシミュレーションの立場から示している．本論文の結果は，FCS を用いたバイオメトリック暗号の安全性の向上に貢献すると考え，推薦論文として推薦する．

（コンピュータセキュリティシンポジウム 2011
プログラム委員長　四方順司）

披田野 清良　（正会員）

2007 年早稲田大学理工学部コンピュータ・ネットワーク工学科卒業．2012 年同大学理工学術院基幹理工学研究科博士後期課程修了．博士（工学）．2010 年日本学術振興会特別研究員．2011 年早稲田大学理工学術院基幹理工学部助手．2013 年 KDDI（株）入社．在学中は，生体認証のテンプレート保護技術に関する研究に従事．

大木 哲史　（正会員）

2002 年早稲田大学理工学部電子・情報通信学科卒業．2010 年同大学大学院理工学研究科博士後期課程修了．博士（工学）．2007 年同大学理工学研究所嘱託研究員．2010 年同客員研究員．2011 年同次席研究員．2013 年 5 月産業技術総合研究所特別研究員として現在に至る．バイオメトリクス等を用いた個人認証技術とネットワークへの応用に関する研究に従事．電子情報通信学会会員．

高橋 健太　（正会員）

1998 年東京大学理学部卒業．2000 年同大学大学院理学系研究科修士課程修了．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）にてバイオメトリクスおよび情報セキュリティの研究開発に従事．2012 年東京大学大学院情報理工学系研究科博士後期課程修了．2001 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．2008 年度情報処理学会論文賞受賞．電子情報通信学会会員．博士（情報理工学）．