L-023

Fuzzy Commitment Scheme における生体情報の推定困難性に関する一考察

A Study on Difficulty of Estimation of Biometric Information in Fuzzy Commitment Scheme

披田野 清良 † **市野 将嗣** ‡ **小松 尚久** † **高橋 健太** §
Seira HIDANO Masatsugu ICHINO Naohisa KOMATSU Kenta TAKAHASHI

1. まえがき

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，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，近年，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，生体情報の相関性により当該情報量が減少し，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検討されていない．そこで，本稿では，Fuzzy Commitment Scheme（以下，FCS）を用いたバイオメトリック暗号に着目し，生体情報空間の大きさを利用した生体情報推定に関する脅威を明らかにすると共に，指紋認証を一例として，それらの脅威に対する安全性を定量的に評価する．

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

Fuzzy Commitment Scheme は，1999 年に Juels らにより提案された誤り訂正符号を用いた暗号方式の一種である [1]．図 1 に，サーバ/クライアントモデルにおける FCS を用いたバイオメトリック暗号の概要を示す．

登録過程

1. クライアントは，ユーザが提示する生体情報からビット列 $B \in \mathcal{B} \subseteq \{0,1\}^n$ を抽出する．ただし，$|\mathcal{B}| = 2^l$ $(l \leq n)$ とする．
2. クライアントは，ランダムに選択した秘密情報 $S \in \{0,1\}^k$ から誤り訂正符号化により符号語 $W \in \mathcal{W}$ を生成し，B と W の排他的論理和によりコミットメント $C = B \oplus W$ を作成する．ただし，本稿では，$\mathcal{W}$ は，符号長 n，情報記号数 k，最小距離 d の (n,k,d)-線形符号とする．
3. クライアントは，S のハッシュ値 $h(S)$ を計算し，C と $h(S)$ の組 $(C, h(S))$ を認証サーバに送信する．
4. 認証サーバは $(C, h(S))$ をストレージに保管する．

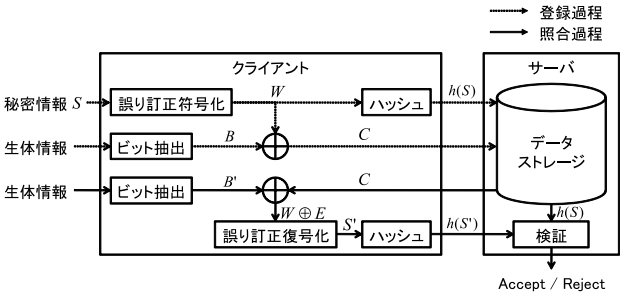

図 1: FCS を用いたバイオメトリック暗号

照合過程

1. クライアントは，登録時と同様に，ユーザが提示する生体情報からビット列 B' を抽出し，当該ユーザの C を認証サーバーから取り寄せる．
2. クライアントは，B' と C の排他的論理和を計算し，$W \oplus E = B' \oplus C$ から誤り訂正復号化により S' を得る．ただし，$E = B \oplus B'$ とし，E のハミング重みが $(d-1)/2$ 以内のとき，S' は S と一致する．
3. クライアントは，S' のハッシュ値 $h(S')$ を計算し，$h(S')$ を認証サーバに送信する．
4. 認証サーバは，$h(S')$ と $h(S)$ を比較し，ユーザの正当性を検証する．

3. 生体情報推定攻撃

FCS を用いたバイオメトリック暗号では，生体情報から抽出したビット列 B は，n 個のビットで記述される．しかし，ビット抽出の際に生体情報の相関性を完全に除去できなかった場合，識別に有効ではないビットが混入する可能性がある．このとき，B の空間の大きさ $|\mathcal{B}|$ は 2^n から大きく減少し，B の推定が容易になると考えられる．そこで，本章では，生体情報推定攻撃として，通常運用時における $|\mathcal{B}|$ を利用した Bits Estimation Attack (以下，BEA) と，あるユーザのコミットメント C が漏洩した際の $|\mathcal{B}|$ と符号語 W の空間の大きさ $|\mathcal{W}|$ を利用した Strong BEA (以下，SBEA) ついて述べる．

まず，BEA の攻撃手順を以下に示す．

1. 対象となるモダリティの生体情報データベースを用意する．
2. 生体情報をデータベースからランダムに選択し，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，選択した生体情報をクライアントに入力する．

ただし，通常運用時は，$|\mathcal{W}|$ のみを利用した Codeword Estimation Attack (CEA) も考えられる．具体的には，

† 早稲田大学, Waseda University
‡ 電気通信大学, The University of Electro-Communications
§ 東京大学, The University of Tokyo

$\mathcal{W}$ が (n,k,d)-線形符号の場合に，2^k 個の $h(S)$ の中からランダムに一つを選択し，照合過程の手順 3 において，それを認証サーバに送信する．CEA の攻撃成功確率が BEA より高い場合，CEA を用いて攻撃する．

次に，SBEA の攻撃手順を以下に示す．

1. 対象となるモダリティの生体情報データベースを用意し，登録過程の手順 1 と同様の方法によりビット抽出を行い，ビット列の集合 $\{B_1,\ldots,B_N\}$ を作成する．
2. 取得した C と $\{B_1,\ldots,B_N\}$ の各ビット列との排他的論理和を計算し，集合 $\{C\oplus B_1,\ldots,C\oplus B_N\}$ のそれぞれの情報に対して誤り訂正復号化処理を施す．
3. 手順 2 において何らかの情報が復元された場合，復元に用いた生体情報を手順 1 のデータベースより選択し，照合過程の手順 1 において，C が盗まれたユーザになりすまし，選択した生体情報をクライアントに入力する．

4. セキュリティ分析

3 章で示した脅威に対する安全性を理論的に考察する．

まず，CEA の攻撃成功 CAP は，$\{0,1\}^n$ 上の一様分布に従う確率変数を X とすると，符号語 W の空間の大きさ $|\mathcal{W}|=1/2^k$ を用いて，次式で表せる．

$$CAP = \frac{1}{2^n\cdot P(X\in\mathcal{W})} \quad (1)$$

$$= \frac{1}{|\mathcal{W}|}=\frac{1}{2^k} \quad (2)$$

次に，BEA の攻撃成功確率は，生体認証の標準的な精度評価尺度の一つである FMR と一致し，ビット列 B の空間の大きさ $|\mathcal{B}|=1/2^l$ を用いて，次式で表せる．

$$FMR = \frac{M}{2^n\cdot P(X\in\mathcal{B})} \quad (3)$$

$$= \frac{M}{|\mathcal{B}|}=\frac{M}{2^l} \quad (4)$$

ただし，簡単のため，B は $\mathcal{B}$ 上の一様分布に従うと仮定し，また $M=\sum_{i=0}^{(d-1)/2}{}_l\mathrm{C}_i$ とする．

以上より，通常運用時におけるなりまし攻撃の最大成功確率 SAP は次式で表せる．

$$SAP = max(CAP, FMR) \quad (5)$$

ただし，$max(a,b)$ は a と b の大きい値を返す．

そして，$SBEA$ の攻撃成功確率 $\overline{SAP}$ は次式で表せる．

$$\overline{SAP} = \frac{M}{2^n\cdot P(X\oplus C\in\mathcal{W}\cap X\in\mathcal{B})} \quad (6)$$

$$\approx \frac{M}{2^n\cdot P(X\in\mathcal{W}\cap\mathcal{B})} \quad (7)$$

$$\approx \frac{M}{2^n\cdot P(X\in\mathcal{W})P(X\in\mathcal{B})} \quad (8)$$

このとき，(1) 式，(3) 式より，$\overline{SAP}$ は次式で表せる．

$$\overline{SAP} = CAP\cdot\frac{M}{P(X\in\mathcal{B})} \quad (9)$$

$$= FMR\cdot\frac{1}{P(X\in\mathcal{W})} \quad (10)$$

表 1: 実験結果

(n,k,d)	$FNMR$	FMR	$\overline{SAP}$
(127,8,57)	0.06	0.042	0.856
(127,15,55)	0.065	0.0361	0.824
(127,22,47)	0.12	0.0186	0.742

(4) 式より，生体情報推定攻撃に対する安全性は $|\mathcal{B}|$ により大きく変化すると考えられる．また，(9) 式，(10) 式より，コミットメント C が漏洩した場合，安全性は，通常運用時に比べて明らかに低下すると言える．

5. 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，3 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，Tuyls らの指紋コードを用いたバイオメトリック暗号 [2] を評価対象とし，(n,k,d)-線形符号として BCH 符号を用いた．また，指紋データベースとして 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 127 の指紋コードを生成して照合を行った．

BCH 符号に関する各パラメータを変化させたときの $FNMR$ および FMR，$\overline{SAP}$ を表 1 に示す．$(n,k,d)=(127,22,47)$ のとき，FMR の理論値は，(4) 式において $l=127$ とすると，8.48×10^{-14} となる．しかし，表 1 において，$(n,k,d)=(127,22,47)$ のときの FMR の値に注目すると，理論値とは大きく異なるため，指紋コードのビット間に何らかの相関があることがうかがえる．また，どのパラメータ値においても $\overline{SAP}$ は FMR より著しく減少していることから，4 章で理論的に示したように，コミットメント漏洩時の安全性は通常運用時に比べて低下すると言える．

6. まとめと今後の課題

本稿では，まず，FCS を用いたバイオメトリック暗号における生体情報の相関性を利用した脅威として，生体情報推定攻撃を示した．そして，それらの脅威に対する安全性を理論的に考察すると共に，指紋認証を例にして，当該安全性を定量的に評価した．その結果，コミットメント漏洩時に安全性が著しく低下するという知見を得た．今後は，5 章で得られた結果と同様の結果を 4 章の考察と生体情報の情報量に基づき理論的に評価する方法を検討する．

参考文献

[1] A. Juels and M. Wattenberg,“ A fuzzy commitment scheme, ”Proc. the 6th ACM Conference on Computer and Communications Security, pp.28-36, 1999.

[2] P. Tuyls et al.,“ Practical Biometric Authentication with Template Protection, ”Proc. the 5th International Conference on Audio- and Video-Based Personal Authentication, pp.436-446, 2005.