Physical Unclonable Functionに基づく認証方式における各認証デバイスの認証精度を考慮した認証モデルに関する一検討

吉田隆弘

1 はじめに

Physical Unclonable Function（PUF，パフ）に基づく認証方式[1, 2, 3]とは，紙やICカード等のハードウェア的な人工物の真正性を判定する技術で，人工物の偽造・複製防止技術として活用できると考えられている．この認証方式では，紙の模様，磁気体の磁力ムラ，LSIにおけるトランジスタや配線の物理特性など，製造時のばらつきによって偶然生じる物理的特徴を各個体固有の認証情報として用いる．製造時のばらつきは製造者でも制御することができないため，人工物の物理的な偽造・複製が困難となる．本稿では，この認証に用いる人工物を認証デバイスと呼ぶ．

本稿では，認証デバイスの定義を従来の定義[2, 3]と同様に，チャレンジと呼ばれる入力全体の集合からレスポンスと呼ばれる出力全体の集合への関数として定義する．認証デバイスを認証するときは，まず認証デバイスの物理的特徴を事前に登録しておいた認証者がチャレンジを送り，そのチャレンジに応じた認証デバイスのレスポンスを受け取る．認証者はこのチャレンジとレスポンスのペア，及び事前登録していた物理的特徴を用いて認証デバイスの真正性を検証する．

PUFに基づく認証方式の安全性を検討する目的で，これまでに様々な攻撃法が提案されている．代表的な攻撃法の一つであるモデリング攻撃[4, 5]は，攻撃者が事前に得たチャレンジ・レスポンスペアを利用し，新たなチャレンジに対するレスポンスを予測することで認証デバイスの偽造を行う攻撃法で，いくつかの認証デバイスに対する有効性が示されている．しかし，これらの研究においては認証方式に対するモデルや性能指標が明確に定められていないため，安全性に対する十分な評価ができていない．実際，従来提案されている全ての攻撃に対して安全な認証方式が提案されても，安全性の指標が明確に定められていないので，今後その認証方式に対して有効な攻撃が提案される可能性が考えられる．

このような問題に対して，PUFに基づく認証方式における認証デバイスを確率モデルとして定義し，このモデルに基づいた認証方式の問題設定を定式化することで認証精度や安全性等の一般的な性能評価が検討されている[6, 7]．しかし，これらの従来研究では一つの認証デバイスに対する認証精度しか考慮していないため，複数の認証デバイスを利用した場合の認証精度に関して何も保証がされていない．

そこで本稿では，複数の認証デバイスを用いる認証方式において，各認証デバイスの認証精度を考慮した統計的モデル化を行い，PUFに基づく認証方式の新たな問題設定を定式化する．次に，この問題設定における最適な認証方式を示し，その安全性評価について検討を行う．

本稿の構成は以下のとおりである．２章では，複数の認証デバイスを用いるPUFに基づく認証モデルを新たに定義する．次に３章では，複数の認証デバイスに対する認証精度を考慮した認証方式の評価基準を導入する．４章では，導入した評価基準を用いて問題設定の定式化を行い，その問題設定に対する漸近的な認証精度と安全性の振る舞いを解析し，最適な認証方式を示す．さらに５章では，最適な認証方式に対する安全性評価について検討する．最後に６章でまとめる．

2 PUFに基づく認証方式

本章では，複数の認証デバイスを用いることを想定した認証モデルを定義する．

2.1 認証デバイスの定義

一般に認証デバイスとして用いる人工物は，同じ製造工程で複数個製造される．そのため製造された複数個の認証デバイスは，その製造工程のばらつきによって物理的特徴がそれぞれ異なったものとなる．また，認証デバイスのレスポンスを観測する際には測定による雑音の混入や測定時の環境の違いにより，認証デバイスへ同じチャレンジを入力しても，異なるレスポンスが観測される．以上の理由から，本稿では認証デバイスを次のような確率モデルとして定義する．

有限集合 $\mathcal{X}$，$\mathcal{Y}$ をそれぞれチャレンジアルファベット，レスポンスアルファベットとし，任意の集合 Θ を物理的特徴全体の集合とする．このとき，用いられる L 個の認証デバイス $\mathrm{F}_1, \mathrm{F}_2, \cdots \mathrm{F}_L$ の物理的特徴をそれぞれ $\theta_j \in \Theta, 1 \leq j \leq L$ とし，それらの集合を $\mathcal{D} = \{\theta_1, \theta_2, \cdots, \theta_L\}$ とおく．ただし，$1 \leq j \leq L$ に対して，$\theta_j \in \Theta$ はそれぞれ独立に Θ 上の確率分布 π に従って発生する．すなわち，$(\Theta_1, \Theta_2, \cdots, \Theta_L)=(\theta_1, \theta_2, \cdots, \theta_L)$ となる確率 $\pi^L(\theta_1, \theta_2, \cdots, \theta_L)$ は

$$\pi^L(\theta_1, \theta_2, \ldots, \theta_L) = \prod_{j=1}^{L} \pi(\theta_i) \tag{1}$$

となる．ここで，θ_j に対する確率変数を Θ_j とした．また，長さ n のチャレンジ系列を $\mathcal{X}^n$ 上の確率変数列 $X^n = X_1X_2 \cdots X_n$ とし，$x^n = x_1x_2 \cdots x_n \in \mathcal{X}^n$ を確率変数列 X^n の実現値とする．ただし，$1 \leq i \leq n$ に対して，$x_i \in \mathcal{X}$ はそれぞれ独立に $\mathcal{X}$ 上の確率分布 P に従って発生する．すなわち，$X^n = x^n$ となる確率 $P^n(x^n)$ は

$$P^n(x^n) = \prod_{i=1}^{n} P(x_i) \tag{2}$$

となる．同様にチャレンジ系列 X^n に対するレスポンス系列を $\mathcal{Y}^n$ 上の確率変数列 $Y^n = Y_1Y_2 \cdots Y_n$ とし，その実現値を $y^n = y_1y_2 \cdots y_n \in \mathcal{Y}^n$ とおく．ただし，$1 \leq i \leq n$ と $1 \leq j \leq L$ に対して，$y_i \in \mathcal{Y}$ は x_i と θ_j のみに依存した $\mathcal{Y}$ 上の条件付き確率分布 W_{θ_j} に従って発生する．すなわち，x^n と θ_j が与えられたもとで $Y^n = y^n$ となる確率 $W^n_{\theta_j}(y^n|x^n)$ は

$$W^n_{\theta_j}(y^n|x^n) = \prod_{i=1}^{n} W_{\theta_j}(y_i|x_i) \tag{3}$$

で与えられる．ここで用いられるチャレンジ系列は，認証者が確率分布 P に従って生成する．一般にチャレンジ系列は対象となる認証デバイスの物理的特徴とは互いに独立に生成されるので，$1 \leq j \leq L$ に対して $X^n = x^n$ かつ $\Theta_j = \theta_j$ となる確率は $P^n(x^n)\pi(\theta_j)$ で与えられる．よって，θ_j が与えられたもとで $(X^n = x^n, Y^n = y^n)$ となる同時確率 $PW^n_{\theta_j}(x^n, y^n)$ は，

$$PW^n_{\theta_j}(x^n, y^n) = W^n_{\theta_j}(y^n|x^n)P^n(x^n) \tag{4}$$

となる．確率分布 π は，認証デバイスの製造工程のばらつきに対応する．本稿では，物理的特徴 θ_j を持つ認証デバイス F_j を条件付き確率分布 W_{θ_j} と等価なものとして定義する．

2.2 認証モデルの定義

PUFに基づく認証方式の参加者は，L 個の認証デバイス F_j，$1 \leq j \leq L$ の各利用者，及び認証デバイスの真正性を検証する認証者で構成される．ここで，L 人の利用者には公開のID情報 $1 \leq j \leq L$ がそれぞれ与えられているとする．認証デバイスは認証者が製造し，関数 $\varphi_n : \{1, 2, \cdots, L\} \times \mathcal{X}^n \times \mathcal{Y}^n \times \Theta \to \{0, 1\}$ を用いて検証を行う．本稿では物理的特徴を利用した認証方式を，次の公開情報と4つのフェーズによって構成さ

れる認証方式として定義する.

公開情報：3つの集合 $\mathcal{X}, \mathcal{Y}, \Theta$，2つの確率分布 P, π, 関数 φ_n，及び確率分布のクラス

$$\mathcal{W}(\mathcal{X}, \mathcal{Y}, \Theta) = \{W_\theta \mid \theta \in \Theta\} \tag{5}$$

を公開情報とする.

認証デバイス生成フェーズ：$1 \leq j \leq L$ に対して，認証者は認証デバイス F_j を生成し，利用者 j へそれぞれ配布する．このとき，条件付き確率分布 W_{θ_j} は，Θ 上の確率分布 π に従って定まる．また，認証者は生成した L 個の認証デバイスの物理的特徴である $\mathcal{D}$ を安全に保管しておく.

チャレンジ生成フェーズ：$1 \leq j \leq L$ に対して認証デバイス F_j を持つ利用者 j は，認証者へID情報 j を送る．次に，認証者は確率分布 P^n に従ってチャレンジ系列 $x^n \in \mathcal{X}^n$ を生成し，安全な通信路で利用者 j に送る.

レスポンス生成フェーズ：利用者 j は，送られてきたチャレンジ系列 x^n を認証デバイス F_j に入力し，条件付き確率分布 $W_{\theta_j}^n$ に従ったレスポンス系列 $y^n \in \mathcal{Y}^n$ を観測する．このレスポンス系列 y^n を，安全な通信路で認証者に送る.

検証フェーズ：認証者は送られてきたID情報 j，レスポンス系列 y^n，チャレンジ生成フェーズで生成したチャレンジ系列 x^n，記憶しておいた物理的特徴 θ_j に対して，関数 φ_n を用いて検証を行う．$\varphi_n(j, x^n, y^n, \theta_j) = 0$ のときは正しい認証デバイスからのレスポンス系列であると受理し，$\varphi_n(j, x^n, y^n, \theta_j) = 1$ のときは受理しない.

3 PUFに基づく認証方式の評価基準の導入

次に，2章で定義したモデルに基づいて，認証精度と安全性の評価基準を導入する．

3.1 攻撃者の仮定

ここで，PUFに基づく認証方式に対する安全性を評価するために，攻撃者に関する仮定を置く．

まず攻撃目標を，認証デバイス F_j，$1 \leq j \leq L$ の一つを複製することとする．すなわち，F_j の物理的特徴 θ_j に関する情報を得ることが攻撃目標となる．また，攻撃者は攻撃対象である認証デバイス F_j の物理的特徴 θ_j を知らない第三者とする．攻撃者が利用できる情報は認証デバイス F_j に対する長さ m のチャレンジ系列とレスポンス系列の対 $(\tilde{x}^m, \tilde{y}^m) \in \mathcal{X}^m \times \mathcal{Y}^m$，及び公開情報とする．

この仮定は，認証者が認証デバイス生成フェーズで認証デバイスを利用者に送る際，攻撃者が何らかの方法で認証デバイスを奪い，一定期間チャレンジとレスポンスを観測し，その観測結果を利用して認証デバイスを偽造する攻撃等を想定していることになる．したがって，攻撃者は認証デバイスを偽造するために，$(\tilde{x}^m, \tilde{y}^m)$ から W_{θ_j} に近い条件付き確率分布 V を決定することが目標となる．また，系列の長さ m が大きいほど攻撃者にとって有利な条件となるので，攻撃者の能力を表すパラメータの一つとして用いることができる．

3.2 認証精度の評価基準

本稿では，認証方式の認証精度を測る評価基準として，以下で定義する誤拒否率と誤受理率を導入する．

誤拒否率は，L 個の認証デバイスに対する物理的特徴の集合 $\mathcal{D}$，チャ

レンジの分布 P, 及び関数 φ_n に対して定義される確率である.

定義1 集合 $\mathcal{D}$, 分布 P, 及び関数 φ_n に対して, 誤拒否率 $\alpha_{\mathcal{D}}^{(n)}$を

$$\alpha_{\mathcal{D}}^{(n)} = \max_{j:\theta_j \in \mathcal{D}} \alpha_j^{(n)} \tag{6}$$

と定義する. ここで, $\alpha_j^{(n)}$ を

$$\alpha_j^{(n)} = \sum_{x^n \in \mathcal{X}^n} \sum_{y^n \in \mathcal{Y}^n} PW_{\theta_j}^n(x^n, y^n) \varphi_n(j, x^n, y^n, \theta_j) \tag{7}$$

とおいた. □

誤拒否率 $\alpha_{\mathcal{D}}^{(n)}$ は, 認証デバイス F_j から得られたレスポンス系列 y^n が受理されない確率 $\alpha_j^{(n)}$ の $\mathcal{D}$ に関する最大値となる.

また, 誤受理率も誤拒否率と同様に, L 個の認証デバイスに対する物理的特徴の集合 $\mathcal{D}$, チャレンジの分布 P, 及び関数 φ_n に対して定義される確率である.

定義2 集合 $\mathcal{D}$, 分布 P, 及び関数 φ_n に対して, 誤受理率 $\beta_{\mathcal{D}}^{(n)}$ を

$$\beta_{\mathcal{D}}^{(n)} = \max_{(i,j):\theta_i, \theta_j \in \mathcal{D}, i \neq j} \beta_{i,j}^{(n)} \tag{8}$$

と定義する. ここで, $\beta_{i,j}^{(n)}$ を

$$\beta_{i,j}^{(n)} = \sum_{x^n \in \mathcal{X}^n} \sum_{y^n \in \mathcal{Y}^n} PW_{\theta_i}^n(x^n, y^n) \left(1 - \varphi_n(j, x^n, y^n, \theta_j)\right) \tag{9}$$

とおいた. □

誤受理率 $\beta_{\mathcal{D}}^{(n)}$ は, 認証デバイス F_i から得られたレスポンス系列 y^n が認証デバイス F_j として受理されてしまう確率 $\beta_{i,j}^{(n)}$ の $\theta_i, \theta_j \in \mathcal{D}, i \neq j$ に関する最大値となる.

3.3 安全性の評価基準

本稿では，安全性の評価基準として複製成功確率を導入する．$1 \leq j \leq L$ に対して，認証デバイス F_j に対応する分布 $W_{\theta_j}^n$ とは異なる分布

$$V^n(y^n|x^n) = \prod_{i=1}^{n} V(y_i|x_i),\ (x^n, y^n) \in \mathcal{X}^n \times \mathcal{Y}^n \tag{10}$$

から得られたレスポンス系列 y^n が認証者に受理される確率を複製成功確率として定義する．

定義3 任意の $\theta \in \Theta$ と P，及び任意の条件付き確率分布 V に対して，複製成功確率 $\gamma_{\mathcal{D}}^{(n)}$ を

$$\gamma_{\mathcal{D}}^{(n)} = \max_{j:\theta_j \in \mathcal{D}} \gamma_j^{(n)}, \tag{11}$$

$$\gamma_j^{(n)} = \sum_{x^n \in \mathcal{X}^n} \sum_{y^n \in \mathcal{Y}^n} PV^n(x^n, y^n)\,(1 - \varphi_n(j, x^n, y^n, \theta_j)) \tag{12}$$

として定義する．ここで，

$$PV^n(x^n, y^n) = V^n(y^n|x^n)P^n(x^n) \tag{13}$$

とした． □

4 誤受理率と複製成功確率の漸近的性質

本稿ではチャレンジとレスポンスの系列長 n が大きくなるにつれて誤拒否率 $\alpha_{\mathcal{D}}^{(n)}$ がいくらでも0に近づけることができるという条件のもと，誤受理率 $\beta_{\mathcal{D}}^{(n)}$ と複製成功確率 $\gamma_{\mathcal{D}}^{(n)}$ をできる限り小さくするような関数 φ_n を選ぶ問題を考える．

本章では，PUFに基づく認証方式における問題設定の定式化を行い，その問題における誤受理率と複製成功確率の指数部の漸近的な振る舞いに

ついて検討する.

4.1 問題の定式化

本稿では，誤拒否率 $\alpha_{\mathcal{D}}^{(n)}$ が，$\alpha_{\mathcal{D}}^{(n)} \to 0$ となるとき，誤受理率 $\beta_{\mathcal{D}}^{(n)} = e^{-nR_1}$ と複製成功確率 $\gamma_{\mathcal{D}}^{(n)} = e^{-nR_2}$ の指数部のレート R_1, R_2 をどこまで大きくできるかを考える．本稿では，このような問題を次のように定式化する.

定義4 任意の θ, P, V に対して，以下の条件を満たす関数 φ_n が存在するとき，レートの組 $R = (R_1, R_2)$ が達成可能であるという.

$$\lim_{n\to\infty} \alpha_{\mathcal{D}}^{(n)} = 0, \tag{14}$$

$$\liminf_{n\to\infty} \frac{1}{n} \log \frac{1}{\beta_{\mathcal{D}}^{(n)}} \geq R_1, \tag{15}$$

$$\liminf_{n\to\infty} \frac{1}{n} \log \frac{1}{\gamma_{\mathcal{D}}^{(n)}} \geq R_2 \tag{16}$$

以下，本稿では対数の底は e とする.

また，次のように定義される $E_1(P, \mathcal{D})$ と $E_2(P, V, \mathcal{D})$ を，それぞれ最大許容誤受理率指数，最大許容複製確率指数と呼ぶ.

$$E_1(P, \mathcal{D}) = \sup\{R_1 \mid R\text{が達成可能}\}, \tag{17}$$

$$E_2(P, V, \mathcal{D}) = \sup\{R_2 \mid R\text{が達成可能}\}. \tag{18}$$

□

ここで定義した認証方式の問題は，認証者が観測したチャレンジ系列とレスポンス系列の対 (x^n, y^n) が，認証者にとって既知となる分布 $PW_{\theta_i}^n$ に従うか異なる分布 $PW_{\theta_i}^n$, $i \neq j$ に従うかを検定する問題，及び未知の分

布 PV^n に従うかを検定する問題となる．前者は2値仮説検定問題として考えることができ，誤拒否率が第一種過誤，誤受理率が第二種過誤に対応する．また，後者はユニバーサル2値仮説検定問題[8, 9, 10]の一つとして考えることができ，誤拒否率が第一種過誤，複製成功確率が第二種過誤に対応する．Hoeffding[8]による問題設定は，本稿の問題設定においてチャレンジ系列を用いない場合の認証方式に対応する．また，メッセージ認証方式において定義4と同様の定式化が行われており，その問題に対する最大許容誤受理率指数が示されている[11]．

4.2 最大許容誤受理率指数と最大許容複製確率指数の導出

本節では，定義4で定義した最大許容誤受理率指数と最大許容複製確率指数の導出を行う．

4.2.1 系列のタイプとその性質

まず，導出する際に用いるタイプ，条件付きタイプ，及びその系列が持つ基本的な性質[12]を紹介する．

$x^n \in \mathcal{X}^n$ に対して，$N(x|x^n)$ を x^n における $x \in \mathcal{X}$ の出現個数とし，

$$P_{x^n}(x) = \frac{1}{n} N(x|x^n),\ x \in \mathcal{X} \tag{19}$$

で与えられる確率分布 P_{x^n} を系列 x^n のタイプという．長さ n の系列 x^n によって与えられるタイプ全体の集合を $P_n(\mathcal{X})$ で表し，タイプが $\overline{P} \in P_n(\mathcal{X})$ となる系列全体の集合を

$$T^n(\bar{P}) = \left\{ x^n \in \mathcal{X}^n \mid \bar{P} = P_{x^n} \right\} \tag{20}$$

で表す．$(x^n, y^n) \in \mathcal{X}^n \times \mathcal{Y}^n$ に対しても同様に，$N(x, y|x^n, y^n)$ を (x^n, y^n) における (x, y) の出現個数とし，

$$PW_{x^n y^n}(x,y) = \frac{1}{n} N(x,y \mid x^n, y^n), (x,y) \in \mathcal{X} \times \mathcal{Y} \tag{21}$$

で与えられる確率分布 $PW_{x^n y^n}$ を系列 (x^n, y^n) の同時タイプという．

また，x^n が与えられたもとでの y^n の条件付きタイプを

$$W_{y^n|x^n}(y|x) = \frac{PW_{x^n y^n}(x,y)}{P_{x^n}(x)}, \ (x,y) \in \mathcal{X} \times \mathcal{Y} \tag{22}$$

と定義する．条件付きタイプ全体の集合を $\mathcal{W}_n(\mathcal{Y}|x^n)$ で表し，x^n が与えられたもとでの条件付きタイプが $\bar{W} \in \mathcal{W}_n(\mathcal{Y}|x^n)$ となる系列全体の集合を

$$T^n(\bar{W} \mid x^n) = \left\{ y^n \in \mathcal{Y}^n \mid \bar{W} = W_{y^n|x^n} \right\} \tag{23}$$

で表す．

タイプの数 $|\mathcal{P}_n(\mathcal{X})|$，及び x^n が与えられたもとでの条件付きタイプの数 $|\mathcal{W}_n(\mathcal{Y}|x^n)|$ は，

$$|\mathcal{P}_n(\mathcal{X})| \ \leq \ (n+1)^{|\mathcal{X}|}, \tag{24}$$

$$|\mathcal{W}_n(\mathcal{Y} \mid x^n)| \ \leq \ (n+1)^{|\mathcal{X}||\mathcal{Y}|} \tag{25}$$

を満たす．ここで，$|\cdot|$ は集合のサイズを表す．

任意のタイプ $\bar{P} \in \mathcal{P}_n(\mathcal{X})$ に対して，

$$(n+1)^{-|\mathcal{X}|} \exp\left\{ nH(\bar{P}) \right\} \leq |T^n(\bar{P})| \leq \exp\left\{ nH(\bar{P}) \right\} \tag{26}$$

が成り立ち，全ての $x^n \in T^n(\bar{P})$ 対して，

$$P^n(x^n) = \exp\left\{ -n \left[H(\bar{P}) + D(\bar{P}||P) \right] \right\} \tag{27}$$

が成り立つ．ここで，$H(\bar{P})$ は分布 $\bar{P}$ に関するエントロピー

$$H(\bar{P}) = -\sum_{x\in\mathcal{X}} \bar{P}(x)\log \bar{P}(x) \tag{28}$$

とし，$D(\overline{P}\|P)$ は分布 $\overline{P}$ と P に関するダイバージェンス

$$D(\bar{P}||P) = \sum_{x\in\mathcal{X}} \bar{P}(x)\log\frac{\bar{P}(x)}{P(x)} \tag{29}$$

とした．

同様に，任意タイプ $\overline{P}\in P_n(\mathcal{X})$ を持つ $x^n \in T^n(\overline{P})$ が与えられたもとでの任意の条件付きタイプ $\overline{W}\in \mathcal{W}_n(\mathcal{Y}|x^n)$ に対して，

$$(n+1)^{-|\mathcal{X}||\mathcal{Y}|}\exp\left\{nH(\bar{W}|\bar{P})\right\} \le |T^n(\bar{W}\mid x^n)| \le \exp\left\{nH(\bar{W}|\bar{P})\right\} \tag{30}$$

が成り立ち，全ての $y^n \in T^n(\overline{W}|x^n)$ に対して，

$$W_\theta^n(y^n|x^n) = \exp\left\{-n\left[H(\bar{W}|\bar{P})+D(\bar{W}||W_\theta|\bar{P})\right]\right\} \tag{31}$$

が成り立つ．ここで，$H(\overline{W}|\overline{P})$ は分布 $\overline{P}$ と $\overline{W}$ に関する条件付きエントロピー

$$H(\bar{W}|\bar{P}) = -\sum_{x\in\mathcal{X}}\bar{P}(x)\sum_{y\in\mathcal{Y}}\bar{W}(y\mid x)\log\bar{W}(y\mid x) \tag{32}$$

とし，$D(\overline{W}\|W_\theta|\overline{P})$ は分布 $\overline{P}$，$\overline{W}$，W_θ, $\theta\in\Theta$ に関する条件付きダイバージェンス

$$D(\bar{W}||W_\theta|\bar{P}) = \sum_{x\in\mathcal{X}}\bar{P}(x)\sum_{y\in\mathcal{Y}}\bar{W}(y|x)\log\frac{\bar{W}(x|y)}{W_\theta(y|x)} \tag{33}$$

とした．

4.2.2 最大許容誤受理率指数と最大許容複製成功確率指数

次に，前述した系列のタイプに関する基本的性質を用いて，最大許容誤受理率指数 $E_1(P,\mathcal{D})$ と最大許容複製成功確率指数 $E_2(P,V,\mathcal{D})$ を導出する．

定理 1　任意の確率分布 P, V, 及び $\mathcal{D}$ に対して,

$$E_1(P,\mathcal{D}) = \min_{(i,j):\theta_i,\theta_j\in\mathcal{D},i\neq j} D(W_{\theta_j}||W_{\theta_i}|P), \tag{34}$$

$$E_2(P,V,\mathcal{D}) = \min_{j:\theta_j\in\mathcal{D}} D(W_{\theta_j}||V|P). \tag{35}$$

が成立する. □

(証明) まず,

$$E_1(P,\mathcal{D}) \geq \min_{(i,j):\theta_i,\theta_j\in\mathcal{D},i\neq j} D(W_{\theta_j}||W_{\theta_i}|P), \tag{36}$$

$$E_2(P,V,\mathcal{D}) \geq \min_{j:\theta_j\in\mathcal{D}} D(W_{\theta_j}||V|P) \tag{37}$$

を証明する.

ここで任意の $\lambda\in(0,1)$ に対してタイプの集合 $\mathcal{P}_n^{(\lambda)}$ を,

$$\mathcal{P}_n^{(\lambda)} = \left\{\bar{P}\in\mathcal{P}_n(\mathcal{X})|D(\bar{P}||P)\leq n^{-\lambda}\right\} \tag{38}$$

とおき, 同様に任意の $\lambda\in(0,1)$, $\theta_j\in\mathcal{D}$, $x^n\in\mathcal{X}$ に対して条件付きタイプの集合 $\mathcal{W}_n^{(\theta_j,\lambda)}(x^n)$ を,

$$\mathcal{W}_n^{(\theta_j,\lambda)}(x^n) = \left\{\bar{W}\in\mathcal{W}_n(\mathcal{Y}|x^n)|D(\bar{W}||W_{\theta_j}|P_{x^n})\leq n^{-\lambda}\right\} \tag{39}$$

とおく. また, これらの集合に属するタイプ及び条件付きタイプとなる系列全体の集合を, それぞれ,

$$\mathcal{X}^n(\lambda) = \sum_{\bar{P}\in\mathcal{P}_n^{(\lambda)}} T^n(\bar{P}), \tag{40}$$

$$\mathcal{Y}^n(\theta_j,\lambda,x^n) = \sum_{\bar{W}\in\mathcal{W}_n^{(\theta_j,\lambda)}(x^n)} T^n(\bar{W}\mid x^n) \tag{41}$$

とし, 以下の集合 $\mathcal{A}^n(\theta_j,\lambda)$ を定義する.

$$\mathcal{A}^n(\theta_j,\lambda)=\{(x^n,y^n)|x^n\in\mathcal{X}^n(\lambda),y^n\in\mathcal{Y}^n(\theta_j,\lambda,x^n)\}. \tag{42}$$

この集合に対して定められる関数 φ_n^* を

$$\varphi_n^*(j,x^n,y^n,\theta_j)=\begin{cases}0 & \text{if } (x^n,y^n)\in\mathcal{A}^n(\theta_j,\lambda)\\ 1 & \text{otherwise}\end{cases} \tag{43}$$

と定義すると，式(6)の誤拒否率 $\alpha_{\mathcal{D}}^{(n)}$ の定義，及び式(38)-(43)の各集合と関数の定義より，

$$\begin{aligned}
\alpha_{\mathcal{D}}^{(n)} &= \max_{j:\theta_j\in\mathcal{D}}\alpha_j^{(n)}\\
&= \max_{j:\theta_j\in\mathcal{D}}\sum_{(x^n,y^n)\in\overline{\mathcal{A}^n(\theta_j,\lambda)}}PW_{\theta_j}^n(x^n,y^n)\\
&= \max_{j:\theta_j\in\mathcal{D}}\left\{\sum_{x^n\in\overline{\mathcal{X}^n(\lambda)}}P^n(x^n)\sum_{y^n\in\mathcal{Y}^n}W_{\theta_j}^n(y^n|x^n)+\sum_{x^n\in\mathcal{X}^n(\lambda)}P^n(x^n)\sum_{y^n\in\overline{\mathcal{Y}^n(\theta_j,\lambda,\bar{P})}}W_{\theta_j}^n(y^n|x^n)\right\}\\
&\le \max_{j:\theta_j\in\mathcal{D}}\left\{\sum_{\overline{\mathcal{X}^n(\lambda)}}P^n(x^n)+\sum_{\mathcal{X}^n(\lambda)}P^n(x^n)\sum_{\overline{\mathcal{Y}^n(\theta_j,\lambda,\bar{P})}}W_{\theta_j}^n(y^n|x^n)\right\}\\
&= \max_{j:\theta_j\in\mathcal{D}}\left\{\sum_{\bar{P}\in\overline{\mathcal{P}_n^{(\lambda)}}}\sum_{x^n\in T^n(\bar{P})}P^n(x^n)+\sum_{\mathcal{X}^n(\lambda)}P^n(x^n)\sum_{\bar{W}\in\overline{\mathcal{W}_n^{(\theta_j,\lambda)}(x^n)}}\sum_{y^n\in T^n(\bar{W}|x^n)}W_{\theta_j}^n(y^n|x^n)\right\}
\end{aligned} \tag{44}$$

が成り立つ．ここで，集合 $\mathcal{A}$ に対する補集合を $\overline{\mathcal{A}}$ とした．また，式(24)，(26)，(27)より，

$$\sum_{\bar{P}\in\overline{\mathcal{P}_n^{(\lambda)}}}\sum_{x^n\in T^n(\bar{P})}P^n(x^n)\le(n+1)^{|\mathcal{X}|}\exp\left\{-n\min_{\bar{P}:\bar{P}\in\overline{\mathcal{P}_n^{(\lambda)}}}D(\bar{P}||P)\right\} \tag{45}$$

が成立し，式(25)，(30)，(31)より，

$$\begin{aligned}
&\sum_{x^n\in\mathcal{X}^n(\lambda)}P^n(x^n)\sum_{\bar{W}\in\overline{\mathcal{W}_n^{(\theta_j,\lambda)}(x^n)}}\sum_{y^n\in T^n(\bar{W}|x^n)}W_{\theta_j}^n(y^n|x^n)\\
&\le (n+1)^{|\mathcal{X}||\mathcal{Y}|}\sum_{\mathcal{X}^n(\lambda)}P^n(x^n)\exp\left\{-n\min_{\bar{W}:\bar{W}\in\overline{\mathcal{W}_n^{(\theta_j,\lambda)}(x^n)}}D(\bar{W}||W_{\theta_j}|P_{x^n})\right\}
\end{aligned} \tag{46}$$

が成立するので，$\mathcal{P}_n^{(\lambda)}$ と $\mathcal{W}_n^{(\theta,\lambda)}(x^n)$ の定義，及び式(44)-(46)より，

$$\alpha_{\mathcal{D}}^{(n)} \leq 2(n+1)^{|\mathcal{X}||\mathcal{Y}|} \exp\left\{-n^{1-\lambda}\right\} \tag{47}$$

を得る．したがって，式(14)を得る．

誤受理率 $\beta_{\mathcal{D}}^{(n)}$ に対しても同様に展開すると，

$$\begin{aligned}
\beta_{\theta}^{(n)} &= \max_{(i,j):\theta_i,\theta_j\in\mathcal{D},i\neq j} \beta_{i,j}^{(n)} \\
&= \max_{(i,j):\theta_i,\theta_j\in\mathcal{D},i\neq j} \sum_{(x^n,y^n)\in A^n(\theta_j,\lambda)} PW_{\theta_i}^n(x^n,y^n) \\
&\leq \max_{(i,j):\theta_i,\theta_j\in\mathcal{D},i\neq j} (n+1)^{|\mathcal{X}||\mathcal{Y}|} \exp\left\{-n \min_{\mathcal{P}_n^{(\lambda)}} \min_{\mathcal{W}_n^{(\theta_j,\lambda)}(\bar{P})} \left[D(\bar{P}||P) + D(\bar{W}||W_{\theta_i}|\bar{P})\right]\right\}
\end{aligned} \tag{48}$$

が得られる．同様に複製成功確率に対して，

$$\begin{aligned}
\gamma_{\mathcal{D}}^{(n)} &= \max_{j:\theta_j\in\mathcal{D}} \gamma_j^{(n)} \\
&\leq \max_{j:\theta_j\in\mathcal{D}} (n+1)^{|\mathcal{X}||\mathcal{Y}|} \exp\left\{-n \min_{\mathcal{P}_n^{(\lambda)}} \min_{\mathcal{W}_n^{(\theta_j,\lambda)}(\bar{P})} \left[D(\bar{P}||P) + D(\bar{W}||V|\bar{P})\right]\right\}
\end{aligned} \tag{49}$$

が成り立つ．また，任意の $\theta_j \in \mathcal{D}$ に対して，$\mathcal{P}_n^{(\lambda)}$ と $\mathcal{W}_n^{(\theta_j,\lambda)}(P_{x^n})$ の定義より，それぞれの集合は P と W_{θ_j} の近傍に収束するので，n が大きくなると，式(48)，(49)のダイバージェンス $D(\overline{P}||P)$ は0に近づき，条件付きダイバージェンス $D(\overline{W}||W_{\theta_i}|\overline{P})$，$D(\overline{W}||V|\overline{P})$ は，それぞれ $D(W_{\theta_i}||W_{\theta_i}|P)$，$D(W_{\theta_i}||V|P)$ に近づく．したがって，

$$R_1 = \min_{(i,j):\theta_i,\theta_j\in\mathcal{D},i\neq j} D(W_{\theta_j}||W_{\theta_i}|P), \tag{50}$$

$$R_2 = \min_{j:\theta_j\in\mathcal{D}} D(W_{\theta_j}||V|P) \tag{51}$$

としたとき，式(15)，(16)がそれぞれ成り立つ．以上より，式(36)，(37)が証明された．

次に，式(36)，(37)の逆向きの不等式

$$E_1(P,\mathcal{D}) \leq \min_{(i,j):\theta_i,\theta_j\in\mathcal{D},i\neq j} D(W_{\theta_j}||W_{\theta_i}|P), \tag{52}$$

$$E_2(P,V,\mathcal{D}) \leq \min_{j:\theta_j\in\mathcal{D}} D(W_{\theta_j}||V|P) \tag{53}$$

が示されれば定理が証明できる．式(52)，(53)の証明は，式(14)と

$$\liminf_{n\to\infty}\frac{1}{n}\log\frac{1}{\beta_{\mathcal{D}}^{(n)}} > \min_{(i,j):\theta_i,\theta_j\in\mathcal{D},i\neq j} D(W_{\theta_j}||W_{\theta_i}|P), \tag{54}$$

$$\liminf_{n\to\infty}\frac{1}{n}\log\frac{1}{\gamma_{\mathcal{D}}^{(n)}} > \min_{j:\theta_j\in\mathcal{D}} D(W_{\theta_j}||V|P) \tag{55}$$

を満たす関数 φ_n が存在すると仮定し，矛盾を導くことができればよい．式(54)，(55)より，任意の j に対して

$$\frac{1}{n_l}\log\frac{1}{\beta_{\mathcal{D}}^{(n_l)}} \geq \min_{(i,j):\theta_i,\theta_j\in\mathcal{D},i\neq j} D(W_{\theta_j}||W_{\theta_i}|P)+\epsilon,\ \lim_{l\to\infty} n_l=\infty, \tag{56}$$

$$\frac{1}{n'_l}\log\frac{1}{\gamma_{\mathcal{D}}^{(n'_l)}} \geq \min_{j:\theta_j\in\mathcal{D}} D(W_{\theta_j}||V|P)+\epsilon',\ \lim_{l\to\infty} n'_l=\infty \tag{57}$$

を満たす部分列 $\{n_l\}_{l=1}^{\infty}$, $\{n'_l\}_{l=1}^{\infty}$ 及び $\epsilon,\epsilon'>0$ が存在する．ここで，

$$(i^*,j^*) = \arg\max_{(i,j):\theta_i,\theta_j\in\mathcal{D},i\neq j} \beta_{i,j}^{(n)} \tag{58}$$

とおき，$PW_{\theta_{j^*}}^n$ を帰無仮説，$PW_{\theta_{i^*}}^n$ を対立仮説としたときの2値仮説検定を考える．このときの第一種過誤と第二種過誤は，それぞれ $\alpha_{j^*}^{(n)}$，$\beta_{i^*,j^*}^{(n)} = \beta_{\mathcal{D}}^{(n)}$ となる．仮定より $\alpha_{\theta_{j^*}}^{(n)}\to 0$ を満たすので，このような仮説検定に対して，

$$\begin{aligned}\alpha_{\theta_{j^*}}^{(n)}\log\frac{\alpha_{\theta_{j^*}}^{(n)}}{1-\beta_{\mathcal{D}}^{(n)}}+(1-\alpha_{\theta_{j^*}}^{(n)})\log\frac{1-\alpha_{\theta_{j^*}}^{(n)}}{\beta_{\mathcal{D}}^{(n)}} &\leq D\left(PW_{\theta_{j^*}}^n||PW_{\theta_{i^*}}^n\right)\\ &= nD\left(W_{\theta_{j^*}}||W_{\theta_{i^*}}|P\right)\end{aligned} \tag{59}$$

が成立する[11, 13]．等号は，ダイバージェンスと条件付きダイバージェンスの定義を用いた．

また，

$$j^{**} = \arg\max_{j:\theta_j \in \mathcal{D}} \gamma_k^{(n)} \tag{60}$$

とおき，$PW_{\theta j^{**}}^n$ を帰無仮説，PV^n を対立仮説としたときの2値仮説検定における第一種過誤と第二種過誤をそれぞれ $\tilde{\alpha}_{\theta_{j^{**}}}^{(n)}$，$\tilde{\gamma}_{\theta_{j^{**}}}^{(n)}$ とする．このとき，$\alpha_{\mathcal{D}}^{(n)} \to 0$ となる任意の φ_n における $\gamma_{\theta_{j^{**}}}^{(n)} = \gamma_{\mathcal{D}}^{(n)}$ に対し，$\tilde{\gamma}_{\theta_{j^{**}}}^{(n)} \leq \gamma_{\mathcal{D}}^{(n)}$ かつ $\tilde{\alpha}_{\theta_{j^{**}}}^{(n)} \to 0$ を満たす仮説検定が存在する．式(59)と同様に，このような仮説検定に対して，

$$\tilde{\alpha}_{\theta_{j^{**}}}^{(n)} \log \frac{\tilde{\alpha}_{\theta_{j^{**}}}^{(n)}}{1-\tilde{\gamma}_{\theta_{j^{**}}}^{(n)}} + (1-\tilde{\alpha}_{\theta_{j^{**}}}^{(n)}) \log \frac{1-\tilde{\alpha}_{\theta_{j^{**}}}^{(n)}}{\tilde{\gamma}_{\theta_{j^{**}}}^{(n)}} \leq nD\left(W_{\theta_{j^{**}}} || V|P\right) \tag{61}$$

が成立する．

一方，

$$h(\alpha_{\theta_{j^*}}^{(n)}) = -\alpha_{\theta_{j^*}}^{(n)} \log \alpha_{\theta_{j^*}}^{(n)} - (1-\alpha_{\theta_{j^*}}^{(n)}) \log(1-\alpha_{\theta_{j^*}}^{(n)}) \tag{62}$$

とおくと，式(59)の左辺に対して，

$$\begin{aligned}
&\alpha_{\theta_{j^*}}^{(n)} \log \frac{\alpha_{\theta_{j^*}}^{(n)}}{1-\beta_{\mathcal{D}}^{(n)}} + (1-\alpha_{\theta_{j^*}}^{(n)}) \log \frac{1-\alpha_{\theta_{j^*}}^{(n)}}{\beta_{\mathcal{D}}^{(n)}} \\
&= -h(\alpha_{\theta_{j^*}}^{(n)}) + \alpha_{\theta_{j^*}}^{(n)} \log \frac{1}{1-\beta_{\mathcal{D}}^{(n)}} + (1-\alpha_{\theta_{j^*}}^{(n)}) \log \frac{1}{\beta_{\mathcal{D}}^{(n)}} \\
&\geq -1 + (1-\alpha_{\theta_{j^*}}^{(n)}) \log \frac{1}{\beta_{\mathcal{D}}^{(n)}}
\end{aligned} \tag{63}$$

が成り立つ．不等号は，$h(\alpha_{\theta_{j^*}}^{(n)}) \leq 1$ と $-\alpha_{\theta_{j^*}}^{(n)} \log(1-\beta_{\mathcal{D}}^{(n)}) \geq 0$ を用いた．よって，式(57)，(59)，(63)より，

$$-1 + n_l(1-\alpha_{\theta_{j^*}}^{(n_l)}) \left[D\left(W_{\theta_{j^*}} || W_{\theta_{i^*}}|P\right) + \epsilon\right] \leq n_l D\left(W_{\theta_{j^*}} || W_{\theta_{i^*}}|P\right) \tag{64}$$

が成立する．この不等式を整理すると，

$$\alpha_{\theta_{j^*}}^{(n_l)} \geq \frac{\epsilon - 1/n_l}{D\left(W_{\theta_{j^*}} || W_{\theta_{i^*}}|P\right) + \epsilon} \tag{65}$$

を得る．

同様に，

$$h(\tilde{\alpha}^{(n)}_{\theta_{j^{**}}}) = -\tilde{\alpha}^{(n)}_{\theta_{j^{**}}} \log \tilde{\alpha}^{(n)}_{\theta_{j^{**}}} - (1-\tilde{\alpha}^{(n)}_{\theta_{j^{**}}}) \log(1-\tilde{\alpha}^{(n)}_{\theta_{j^{**}}}) \tag{66}$$

とおくと，式(61)の左辺に対して，

$$\begin{aligned}
&\tilde{\alpha}^{(n)}_{\theta_{j^{**}}} \log \frac{\tilde{\alpha}^{(n)}_{\theta_{j^{**}}}}{1-\tilde{\gamma}^{(n)}_{\theta_{j^{**}}}} + (1-\tilde{\alpha}^{(n)}_{\theta_{j^{**}}}) \log \frac{1-\tilde{\alpha}^{(n)}_{\theta_{j^{**}}}}{\tilde{\gamma}^{(n)}_{\theta_{j^{**}}}} \\
&= -h(\tilde{\alpha}^{(n)}_{\theta_{j^{**}}}) + \tilde{\alpha}^{(n)}_{\theta_{j^{**}}} \log \frac{1}{1-\tilde{\gamma}^{(n)}_{\theta_{j^{**}}}} + (1-\tilde{\alpha}^{(n)}_{\theta_{j^{**}}}) \log \frac{1}{\tilde{\gamma}^{(n)}_{\theta_{j^{**}}}} \\
&\geq -1 + (1-\tilde{\alpha}^{(n)}_{\theta_{j^{**}}}) \log \frac{1}{\tilde{\gamma}^{(n)}_{\theta_{j^{**}}}}
\end{aligned} \tag{67}$$

が成り立つ．よって，$\tilde{\gamma}^{(n)}_{\theta_{j^{**}}} \leq \gamma^{(n)}_{\mathcal{D}}$ と式(57)，(61)，(67)より，

$$-1 + n'_l(1-\tilde{\alpha}^{(n'_l)}_{\theta_{j^{**}}}) \left[D\left(W_{\theta_{j^{**}}} || V|P\right) + \epsilon' \right] \leq n'_l D\left(W_{\theta_{j^{**}}} || V|P\right)$$

が成立する．この不等式を整理すると，

$$\tilde{\alpha}^{(n'_l)}_{\theta_{j^{**}}} \geq \frac{\epsilon' - 1/n'_l}{D\left(W_{\theta_{j^{**}}} || V|P\right) + \epsilon'} \tag{68}$$

を得る．

式(65)と式(68)より $\alpha^{(n_l)}_{\theta_{j^*}}$ と $\tilde{\alpha}^{(n'_l)}_{\theta_{j^{**}}}$ が0に収束しないので，仮定に矛盾する．したがって，式(52)，(53)が成立する． □

この定理によって関数 φ^*_n を用いる認証方式が，任意の集合 $\mathcal{D}$ と条件付き確率分布 V に対して誤受理率と複製成功確率の指数部 R_1, R_2 を最大にする最適な認証方式の一つであることが示された．しかし，V が攻撃者以外には未知となるため，この定理だけでは最適な認証方式に対する定量的な安全性の保証ができない．次章では，最大許容複製成功確率指数を達成する最適な認証方式に対する安全性について検討する．

5．最適な認証方式の安全性評価

定理1によって最大許容複製成功確率指数が導出されたが，攻撃者によって決定される V が未知であるため定理1では，どの程度の安全性が保証されているのかは定量的に定められない．そこで本稿では，まず3. 1節で仮定した攻撃を統計的決定理論に基づき定式化し，ベイズ基準のもとで最適な攻撃法を示す．次に，この攻撃法に対する最大許容複製成功確率指数を達成する認証方式の安全性について検討する．

攻撃者は攻撃対象となる認証デバイス F_j に対する長さ m のチャレンジ系列とレスポンス系列 $(\tilde{x}^m, \tilde{y}^m) \in \mathcal{X}^m \times \mathcal{Y}^m$ が観測できる．また，攻撃者は F_j に対応する条件付き確率分布 W_{θ_j} を推定することが目標となるので，$(\tilde{x}^m, \tilde{y}^m)$ が与えられたもとでの W_{θ_j} の推定値を $\hat{W}_{\theta_j}(\tilde{x}^m, \tilde{y}^m)$ と定義する．この推定値 $\hat{W}_{\theta_j}$ に対する評価基準となる損失関数として，以下で定義される対数損失を考える．

$$L(\theta_j, \hat{W}_{\theta_j}, \tilde{x}^m, \tilde{y}^m) = \sum_{x\in\mathcal{X}} \sum_{y\in\mathcal{Y}} PW_{\theta_j}(x,y) \log \frac{W_{\theta_j}(y|x)}{\hat{W}_{\theta_j}(\tilde{x}^m, \tilde{y}^m)}. \tag{69}$$

この損失関数は式(33)の条件付きダイバージェンスの定義より，

$$L(\theta_j, \hat{W}_{\theta_j}, \tilde{x}^m, \tilde{y}^m) = D(W_{\theta_j} || \hat{W}_{\theta_j} | P) \tag{70}$$

となり，定義4で定義した問題において $V = \hat{W}_{\theta_j}$ とした場合の，最大許容複製成功確率指数 $E_2(P, \hat{W}_{\theta_j}, \mathcal{D})$ が損失関数 $L(\theta_j, \hat{W}_{\theta_j}, \tilde{x}^m, \tilde{y}^m)$ 以下となる．すなわち，

$$E_2(P, \hat{W}_{\theta_j}, \mathcal{D}) \leq L(\theta_j, \hat{W}_{\theta_j}, \tilde{x}^m, \tilde{y}^m) \tag{71}$$

が成り立つ．これは，最適な認証方式が式(69)の損失関数を最小にする攻撃を受けたとしても，このときの複製成功確率の指数部のレートが最大許容複製成功確率指数 $E_2(P, \hat{W}_{\theta_j}, \mathcal{D})$ より大きくなることを意味するの

で，最適な認証方式の定量的な安全性指標として用いることができる．しかし，損失関数 $L(\theta_j, \hat{W}_{\theta_j}, \tilde{x}^m, \tilde{y}^m)$ は長さ m の系列 $(\tilde{x}^m, \tilde{y}^m)$，及び θ_j の関数なので，実際得られた系列によって損失関数の値が変化して評価が難しく，かつ任意の θ_j に対し損失関数を最小化する推定値が存在するとは限らない．そこで，式(69)の損失関数を $(\tilde{X}^m, \tilde{Y}^m)$ と Θ に関して期待値をとったベイズリスク関数の最小化を考える．ベイズリスク関数 $BR(\hat{W}_{\theta_j})$ は以下で与えられる．

$$BR(\hat{W}_{\theta_j}) = \int_{\theta_j \in \Theta} \sum_{\tilde{x}^m} \sum_{\tilde{y}^m} PW_{\theta_j}^m(\tilde{x}^m, \tilde{y}^m) L(\theta_j, \hat{W}_{\theta_j}, \tilde{x}^m, \tilde{y}^m) \pi(\theta_j) d\theta_j. \quad (72)$$

このベイズリスク関数を最小にする推定値 $\hat{W}_{\theta_j}^B$ がベイズ基準のもとで最適な推定値となり，W_{θ_j} を事後分布 $\pi(\theta_j|\tilde{x}^m, \tilde{y}^m)$ で重み付けた予測分布

$$\hat{W}_{\theta_j}^B(\tilde{x}^m, \tilde{y}^m) = \int_{\theta_j \in \Theta} W_{\theta_j}(y|x) \pi(\theta_j|\tilde{x}^m, \tilde{y}^m) d\theta_j, \ (x, y) \in \mathcal{X} \times \mathcal{Y} \quad (73)$$

で与えられる[14]．式(73)の予測分布 $\hat{W}_{\theta_j}^B$ を認証デバイスの偽造に用いた場合の損失関数は，式(69)より，

$$\begin{aligned} L(\theta_j, \hat{W}_{\theta_j}^B, \tilde{x}^m, \tilde{y}^m) &= \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} PW_{\theta_j}(x, y) \log \frac{W_{\theta_j}(y|x)}{\hat{W}_{\theta_j}^B(y|x, \tilde{x}^m, \tilde{y}^m)} \\ &= D(W_{\theta_j} || \hat{W}_{\theta_j}^B | P) \end{aligned} \quad (74)$$

となり，式(74)の $\mathcal{D}$ に関する最小値は

$$\begin{aligned} \min_{j:\theta_j \in \mathcal{D}} L(\theta_j, \hat{W}_{\theta_j}^B, \tilde{x}^m, \tilde{y}^m) &= \min_{j:\theta_j \in \mathcal{D}} D(W_{\theta_j} || \hat{W}_{\theta_j}^B | P) \\ &= E_2(P, \hat{W}_{\theta_j}^B, \mathcal{D}) \end{aligned} \quad (75)$$

となり，$V = \hat{W}_{\theta_j}^B$ とした場合の，最大許容複製成功確率指数 $E_2(P, \hat{W}_{\theta_j}, \mathcal{D})$ と一致する．この量は最適な認証方式に対し，ベイズ基準のもとで最適な攻撃を行ったときの誤受理率の指数部のレートとなるので，認証方式の安全性指標の一つとして用いることができる．

6. まとめ

本稿では，PUFに基づく認証方式における各認証デバイスの認証精度を考慮したモデルと問題設定を定義し，最大許容誤受理率指数と最大許容複製成功確率指数を導出した．これらの指数はそれぞれ認証精度と安全性の評価基準として用いることができる．次に，これらの指数を達成する最適な認証方式の安全性評価を行い，PUFに基づく認証方式の安全性指標の一つを示した．

謝辞

本研究の一部は，横浜商科大学学術研究会助成金の援助による．

参考文献

[1] 松本弘之，宇根正志，松本勉，岩下直行，菅原嗣高，“人工物メトリクスの評価における現状と課題，” 金融研究，第23巻，別冊１号，pp.61-140, 2004.

[2] S. R. Pappu, “Physical one-way functions,” Ph.D thesis, Massachusetts Institute of Technology, Mar. 2001.

[3] B. Gassend, D. Clarke, M. Van Dijk, and S. Devadas, “Silicon physical random functions,” In Proceedings of the 9th ACM Conference on Computer and Communications Security, pp.148-160, Nov. 2002.

[4] M. Majzoobi, F. Koushanfar, and M. Potkonjak, “Testing techniques for hardware security,” In Proceedings of the International Test Conference (ITC), pp.1-10, Oct. 2008.

[5] U. Ruhrmair, F. Sehnke, J. Solter, G. Dror, S. Devadas, and J. Schmidhuber, “Modeling attacks on physical unclonable functions,” In Proceedings of the 17th ACM conference on Computer and communications security, pp.237-249, Oct. 2010.

[6] 石井智，吉田隆弘，堀井俊佑，松嶋敏泰，“PUF を利用した認証に対する統計的モデル化に関する一考察，” 電子情報通信学会技術報告，vol.111, no.142, IT2011-13, pp.19-24, July 2011.

[7] 吉田隆弘，地主創，松嶋敏泰，“物理的特徴を用いた認証方式の統計的モデ

ル化と安全性評価に関する一検討," 第34回情報理論とその応用シンポジウム予稿集, pp.246-251, Nov. 2011.

[8] W. Hoeffding, "Asymptotically optimal tests for multinomial distributions," Ann. Math. Stat., vol.36, pp.369-401, 1965.

[9] O. Zeitouni, and M. Gutman, "On universal hypotheses testing via large deviations," IEEE Trans. Information Theory, vol.37, no.2, pp.285-290, Mar. 1991.

[10] R. Ahlswedea, E. Aloyanb, and E. Haroutunian, "On Logarithmically asymptotically optimal hypothesis testing for arbitrarily varying source with side information," General Theory of Information Transfer and Combinatorics, Lecture Notes in Computer Science, vol.4123, pp.547-552, 2006.

[11] H. Koga and H. Yamamoto, "Coding theorems for secret-key authentication systems," IEICE, trans. Fundamentals, vol.E83-A, no.8, pp.1691-1703, Aug. 2000.

[12] I. Csiszár and J. Kőrner, Information Theory : Coding Theorems for Discrete Memoryless Systems, Academic Press, 1981.

[13] R. E. Blahut, Principles and Practice of Information Theory, Addison Wesley, 1987.

[14] J. O. Berger, Statistical Decision Theory and Bayesian Analysis, Springer-Verlag, New York, 1985.