論文 / 著書情報
Article / Book Information

論題(和文)	秘密計算に適する距離の使用によるリモート生体認証
Title	
著者(和文)	永井 慧, 菊池浩明, 尾形わかは, 西垣正勝
Authors	Wakaha Ogata
出典 / Citation	, Vol. , No. , pp. 2B3-3
発行日 / Pub. date	2008, 1
URL	http://search.ieice.org/
権利情報 / Copyright	本著作物の著作権は電子情報通信学会に帰属します。 Copyright (c) 2008 Institute of Electronics, Information and Communication Engineers.

SCIS 2008 The 2008 Symposium on Cryptography and Information Security
Miyazaki, Japan, Jan. 22-25, 2008
The Institute of Electronics, Information and Communication Engineers

秘密計算に適する距離の使用によるリモート生体認証

Remote Biometrics Authentication System Using Secure-Computation Oriented Distance

永井　慧 * 菊池　浩明 * 尾形　わかは † 西垣　正勝 ‡
Kei Nagai Hiroaki Kikuchi Wakaha Ogata Masakatsu Nishigaki

あらまし ゼロ知識証明を適用する事で，検証者に生体情報を漏らさずに生体情報間の距離が小さいことを証明する認証プロトコルが研究されている．一般に生体情報は多次元であるので，十分な精度を得るためにはユークリッド距離の様な距離尺度を用いる必要がある．しかしながら，ゼロ知識証明の観点では，通信コストや計算量の制約条件があり，ユークリッド距離が必ずしも最適とは限らない．そこで，本研究ではユークリッド距離に加えて，コサイン尺度に注目し，秘密計算を用いたリモート生体認証プロトコルを構成する．また，提案プロトコルの実現性の観点から，精度，計算コストの評価を報告する．

キーワード バイオメトリクス，ゼロ知識証明

1 はじめに

パスワードに代わる安全な認証技術として，生体情報を用いた認証が注目されている．従来の認証方式と比べ，秘密情報に関する記憶デバイスを保持する必要も無く，秘密情報の忘却や紛失の危険性が無い．それゆえに，利便性の高い次世代の認証方式として様々な分野で導入が進んでいるが，生体情報の取り扱いにおいて多くの課題が残っている．リモートな環境で認証を行う場合，通信時における生体情報の盗聴や，認証サーバ管理者の不正による生体情報の漏洩が危惧される．特に，生体情報はひとたび漏洩してしまった場合，パスワードと違い変更することが出来ない．そのため，プライバシー情報である生体情報を認証サーバに登録することに抵抗を感じるユーザが多く存在する．

これらの課題を解決するため，Ratha らは予め生体情報にマスクを施した値を登録する事で，情報が漏洩した場合に登録した情報を取り消す事の出来るキャンセラブルバイオメトリクス [1] という概念を導入し，画像ブロック置換，マニューシャ非線形変換などの方式を提案した．また，太田らは虹彩情報に対して回転や歪曲などの変換を施し，変換に使用した乱数を変更する事で登録した生体情報の更新を可能としている [2]．高橋らも指紋情報に対して，生体情報の更新を可能としたキャンセラブル照合方式を提案している [3]．しかし，これらのシステムでは，登録情報の更新に主目的があり，不正なサーバ管理者による情報漏洩については考慮されていない．

一方，尾形らはキャンセラブルバイオメトリクスの概念に加え，非対称暗号プロトコルを利用する事で，サーバが生体情報に関する情報を一切得ることなく，登録情報と認証情報間の「近さ」を証明する秘匿距離評価 [4][5] を提案している．この方式では 2 つの生体情報の近さを，ユークリッド距離を近似した尺度で評価している．しかし，計算コストや通信量が近似精度と生体情報の次元に大きく依存するため，実現は困難であった．

そこで，本研究では，ユークリッド距離等の類似度評価方式を用いて，既存の秘匿距離評価と同等の安全性を保ちつつより効率の良い秘匿類似度評価プロトコルを構成する．また，本方式が実現可能であることを示すために，提案プロトコルを用いた指紋認証システムの実装を行い，その精度や処理性能を報告する．

2 既存方式　秘匿距離評価 [4]

登録時にユーザが取得した生体情報 $\boldsymbol{x} = (x_1, \ldots, x_n)$ をサーバに対して秘匿するため，準同型性を持つコミット

* 東海大学大学院工学研究科，259-1292 神奈川県平塚市北金目 1117， Graduate School of Engineering, Tokai University, 1117, Kitakaname, Hiratsuka, Kanagawa, Japan, 1117, string8@cs.dm.u-tokai.ac.jp
† 東京工業大学，183-8512 東京都目黒区大岡山 2-12-1，Tokyo Institute of Technology, 2-12-1, O-okayama, Meguroku, Tokyo, Japan, 152-8550
‡ 静岡大学創造科学技術大学院，432-8011 静岡県浜松市城北 3-5-1，Graduate School of Science and Technology, Shizuoka University, 3-5-1, Johoku, Hamamatsu, Shizuoka, Japan, 432-8011

メント [8] を利用して生体情報のコミットメント $E(x_i, r_i)$ をサーバへ登録する ($i = 1, \ldots, n$)．ここで，r_i は生体情報と同数の次元を持つ乱数とする．

認証時は，抽出した生体情報 $\boldsymbol{x}' = (x'_1, \ldots, x'_n)$ のコミットメント $E(x'_i, r'_i)$ を計算し，$E(x_i, r_i)/E(x'_i, r'_i)$ がある閾値 θ 以内の差にあること，すなわち，$|x_i - x'_i| \leq \theta$ を満たすコミットメントである事をゼロ知識証明 [6][7] により証明する．これを，$i = 1, \ldots, n$ の各次元について行うので，このプロトコルは $O(n)$ で実行が可能である．

ただし，このままでは $\boldsymbol{x}$ が n 次元立方体以内にあることだけを示す荒い近似である．より精度を高めるには，予め定められた係数ベクトル $a_1^{(j)}, \ldots, a_n^{(j)}$ を用いて線形変換し，$|\sum_{i=1}^{n} a_i^{(j)}(\tilde{x}_i - x'_i)| \leq \theta$ を検査すればよい．ただし，変換回数と次元数に比例した回数のゼロ知識証明を行う必要があるため，大きな計算コストを要する．

3 提案方式

ユークリッド距離とコサイン尺度の 2 つの類似度評価関数を用いて先のプロトコルと同様の秘密計算を行い，計算コストの改善を試みる．

3.1 要素技術

3.1.1 ベクトル間類似度

ある二つの n 次元ベクトル $\boldsymbol{A} = (a_1 \ldots, a_n), \boldsymbol{B} = (b_1, \ldots, b_n)$ が与えられた時，この二つの類似性を評価する手法として以下の方式が知られている．

1. コサイン尺度
   ベクトルのなす角を，ベクトル間の類似度 $\cos(\boldsymbol{A}, \boldsymbol{B})$ として次のように与える．

$$\begin{aligned} \cos(\boldsymbol{A}, \boldsymbol{B}) &= \frac{\boldsymbol{A} \cdot \boldsymbol{B}}{\|\boldsymbol{A}\| \, \|\boldsymbol{B}\|} \\ &= \frac{a_1 b_1 + \cdots + a_n b_n}{\sqrt{a_1^2 + \cdots + a_n^2}\sqrt{b_1^2 + \cdots + b_n^2}} \end{aligned}$$

   $\|\boldsymbol{A}\|$ は $\boldsymbol{A}$ のノルムであり，単位ベクトルに正規化することで計算処理を軽減できる．

2. ユークリッド距離
   ベクトル間の類似度として，ユークリッド距離を次のように与える．

$$\|\boldsymbol{A} - \boldsymbol{B}\| = \sqrt{(a_1 - b_1)^2 + \cdots + (a_n - b_n)^2}$$

   単なる類似度として用いるのならば，$\|\boldsymbol{A} - \boldsymbol{B}\|^2$ を取ることで 2 乗根の計算を省略できる．

3.1.2 コミットメント方式

サーバに対して評価値を秘匿するため，加法準同型性を満たすコミットメント方式を用いる．コミットメント $E(m, r)$ は，以下の性質を有する関数とする．

1. $E(m, r)$ から 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' を求める事は困難である．

上記の条件を満たす具体的な構成として，以下に示す藤崎岡本らのコミットメント方式 [8] がある．

N を誰もその素因数を知らない大きな合成数とし，g, h を Z_N の要素とする．誰も h の離散対数 $\log_g h$ を知らないとする．この時，

$$E(m, r) = g^m h^r \bmod N$$

を m のコミットメントとする．ただし，r は十分大きい乱数とする．このコミットメントは，加法準同型性

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

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

を満たす．ただし，Z_N の位数は未知の為，$m + m'$ などは mod 演算ではないことに注意せよ．加法準同型性を利用する事により，上述した各類似度を暗号化したまま計算する．

3.1.3 ゼロ知識証明

コミットされた値を知っていることのゼロ知識証明と，サーバに評価値を与えずにコミットされた値がある範囲に含まれていることを納得させる，区間のゼロ知識証明を用いる．

1. コミットされた値のゼロ知識証明 [8]
   $F = E(m, r)$ とした時，コミットされている値を知っていることの証明を次のように書く．

$$PK\{m \mid F = E(m, r)\} \tag{1}$$

   ここで，$E(m, 0) = g^m$ であることに注意すれば，同プロトコルで，

$$PK\{\alpha \mid F = g^\alpha\}$$

   の証明も実現できる．

2. 区間のゼロ知識証明 [6]
   $F = E(m, r)$ とした時，コミットされている値が $[a, b]$ の範囲にあることの証明を

$$PK\{m \mid F = E(m, r) \wedge m \in [a, b]\}$$

   と書く．この証明には，(1) 式のコミットメントの証明に対して約 5 倍の計算コストと通信量がかかる．

3.2 モデル

提案方式は，生体情報を用いて証明をするユーザ U と認証を行うサーバ S 間のプロトコルである．U は，生体情報 $\boldsymbol{x} = (x_1, \ldots, x_n)$ と乱数 $\boldsymbol{r}$ を用いてコミットメント $E(\boldsymbol{x}, \boldsymbol{r})$ を S に登録する．認証時には，新たに取得する生体情報 $\boldsymbol{y}(\neq \boldsymbol{x})$ が登録されている $\boldsymbol{x}$ に「近い」ことを $\boldsymbol{y}$ を漏らさずに証明する．

ただし，耐タンパーデバイスなどによって守られた $\boldsymbol{x}$ と $\boldsymbol{r}$ のアクセスが許されており，$\boldsymbol{x}$ と $\boldsymbol{y}$ の正確な類似度の計算ができることを仮定する．

3.3 提案方式 1　秘匿コサイン尺度評価

3.3.1 登録

U は生体情報 $\boldsymbol{x} = (x_1, \ldots, x_n)$ と乱数 $\boldsymbol{r} = (r_1, \ldots, r_n)$，$\boldsymbol{x}$ のノルム $c = \|\boldsymbol{x}\|$ を用いて $E_i = E(x_i/c, r_i) = g^{x_i/c} h^{r_i}$ を計算し，$E_1, \ldots, E_n$ をサーバに登録する．

3.3.2 認証

1. U は新たに生体情報 $\boldsymbol{y} = (y_1, \ldots, y_n)$ とノルム $c' = \|\boldsymbol{y}\|$ を用いて，登録コミットメント E_i について求めた $G_i = E_i^{\frac{y_i}{c'}}$ とその計算の正当性の証明 $PK_1 =$

$$PK\left\{\frac{y_i}{c'} \,\middle|\, G_i = E_i^{\frac{y_i}{c'}}\right\} \tag{2}$$

を $i = 1, \ldots, n$ について S へ送る．

2. S は，$G_1, \ldots, G_n$ から $\boldsymbol{x}$ と $\boldsymbol{y}$ のコサイン尺度 $d_C = \cos(\boldsymbol{x}, \boldsymbol{y})$ のコミットメント D_C を

$$\begin{aligned} D_C &= \prod_{i=1}^{n} G_i \\ &= g^{\sum \frac{x_i y_i}{cc'}} h^{R_C} \\ &= E(d_C, R_C) \end{aligned}$$

により求める．ただし，$R_C = \Sigma_{i=1}^{n} \frac{r_i y_i}{c'}$ とする．

3. U は，登録情報にアクセスして，d_C,R_C を求め，それが閾値 τ_1 以上であることを $PK_2 =$

$$PK\left\{d_C, R_C \,\middle|\, D_C = E(d_C, R_C) \wedge d_C \in [\tau_1, 1]\right\}$$

により証明する．

4. S は，PK_1 と PK_2 を検証し，全て真であれば U を認証する．

これらの流れを図 1 に示す．

	U		S
登録			
	$\boldsymbol{x} = (x_1, \ldots, x_n)$		
	$c = \|\boldsymbol{x}\|$		
	$E_i = E(x_i/c, r_i)$	$E_1, \ldots, E_n$	
		$\longrightarrow$	$E_1, \ldots, E_n$
認証			
1.	$\boldsymbol{y} = (y_1, \ldots, y_n)$,		
	$c' = \|\boldsymbol{y}\|$		
	$G_i = E_i^{\frac{y_i}{c'}}$	$G_1, \ldots, G_n$,	
		PK_1	
		$\longrightarrow$	2. $D_C = \prod_{i=1}^{n} G_i$
			Verify PK_1
3.	$d_C = cos(\boldsymbol{x}, \boldsymbol{y})$		
	$R_C = \sum_{i=1}^{n} r_i \frac{y_i}{c'}$	PK_2	
		$\longrightarrow$	4. Verify PK_2

図 1: 秘匿コサイン尺度評価プロトコル

3.4 提案方式 2　秘匿ユークリッド距離評価

3.4.1 登録

U は生体情報 $\boldsymbol{x} = (x_1, \ldots, x_n)$ に加えてそれらの平方値 $x_1^2, \ldots, x_d^2$ のコミットメント $E_i = g^{x_i} h^{r_i}$，$\tilde{E}_i = g^{x_i^2} h^{r_i x_i}$ を作成し，E_i と $\tilde{E}_i$ が正しい 2 乗の関係になっていることの証明 $PK_3 =$

$$PK\left\{x_i, r_i \,\middle|\, \tilde{E}_i = E_i^{x_i} \wedge E_i = E(x_i, r_i)\right\}$$

を S に対して実行する．S は PK_3 を検証し，正しければ U を登録する．

3.4.2 認証

1. U は新たに生体情報 $\boldsymbol{y} = (y_1, \ldots, y_n)$ と平方値 $y_1^2, \ldots, y_n^2$ を用いて，コミットメント $F_i = g^{y_i} h^{r_i'}$，$\tilde{F}_i = g^{y_i^2} h^{r_i' y_i}$，登録コミットメント E_i を用いて $G_i = E_i^{y_i}$ を計算する．更に，U は F_i と $\tilde{F}_i$ が正しい関係にあり，G_i が正しくコミットメントから計算されていることを $PK_4 =$

$$PK\left\{y_i, r_i' \,\middle|\, \tilde{F}_i = F_i^{y_i} \wedge F_i = E(y_i, r_i') \wedge G_i = E_i^{y_i}\right\}$$

により S に証明する．

2. S は，平方ユークリッド距離 $d_E = \|\boldsymbol{x} - \boldsymbol{y}\|^2$ のコミットメント $D_E = E(d_E, R_E) = g^{d_E} h^{R_E}$ を次のようにして計算する．ただし，$R_E = \Sigma(r_i x_i - 2 r_i y_i + r_i' y_i)$ とする．

$$D_E = \prod_{i=1}^{n} \tilde{E}_i \tilde{F}_i / G_i^2$$

$$= g^{\Sigma(x_i^2-2x_iy_i+y_i^2)}h^{\Sigma(r_ix_i-2r_iy_i+r'_iy_i)}$$
$$= g^{d_E}h^{R_E}$$

3. U は登録情報から d_E，R_E を求め，D_E にコミットされた d_E が閾値 τ_2 以内であることのゼロ知識証明 $PK_5 =$

$$PK\left\{d_E, R_E \,\middle|\, D_E = E(d_E, R_E) \wedge d_E \in [0, \tau_2]\right\}$$

により S に証明する．

4. S は，PK_4，PK_5 を検証し，真であれば U を認証する．

これらの一連の流れを図 2 に示す．

$\underline{U}$		$\underline{S}$
登録		
$\boldsymbol{x} = (x_1, \ldots, x_n)$		
$x_1^2, \ldots, x_n^2$		
$E_i = g^{x_i}h^{r'_i}$		
$\tilde{E}_i = g^{x_i^2}h^{\tilde{r}'_i}$	$E_1, \ldots, E_n,$	
	$\tilde{E}_1, \ldots, \tilde{E}_n,$	
	PK_3	
	$\longrightarrow$	$E_1, \ldots, E_n$
		$\tilde{E}_1, \ldots, \tilde{E}_n$
		Verify PK_3
認証		
1. $\boldsymbol{y} = (y_1, \ldots, y_n),$		
$y_1^2, \ldots, y_n^2$		
$F_i = g^{y_i}r'_i$		
$\tilde{F}_i = g^{y_i^2}\tilde{r}'_i$		
$G_i = E_i^{y_i}$	$\tilde{F}_1, \ldots, \tilde{F}_n,$	
	$G_1, \ldots, G_n,$	
	PK_4	
	$\longrightarrow$	2. $D_E = \prod_{i=1}^{n} \frac{\tilde{E}_i\tilde{F}_i}{G_n^2}$
		Verify PK_4
3. $d_E = \|\boldsymbol{x} - \boldsymbol{y}\|^2$	PK_5	
	$\longrightarrow$	4. Verify PK_5

図 2: 秘匿ユークリッド距離評価プロトコル

4 評価

秘密計算を行う際の計算及び通信コストは，ゼロ知識証明のオーダーに依存する．また，方式毎にサーバが保管する情報も異なるため，実際の各方式の処理量は自明ではない．そこで，各類似度による提案方式を指紋認証に適用し，実装に基づいた評価を行う．

4.1 精度

ユークリッド距離およびコサイン尺度の使用についての妥当性を示すため，各類似度評価方式の持つ識別能力を明らかにする．本実験では，300×300[pixel] の指紋画像を 18×18 ブロックに分割し，ブロックごとの平均隆線角度を生体情報として用いた．

しかしながら，分割された各ブロック内には隆線が全くない部分が存在する．そこで，ブロックの中心から $n = L^2$ 次元分のブロックを入力とする．ただし，L は $2 \leq L \leq 18$ であり，適切な L の決定については 4.3 節で議論する．

この時，本人 (genuine)50 指，他人 (imposter)450 指についての精度を算出するが，この際にテンプレートとして登録する生体情報に偏りがあった場合，正しい精度を得ることが出来ない．そのため，本人の集合 $A = (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{51})$ の代表点をテンプレート $\boldsymbol{x}_i$ として用いる必要がある．この時，各 $\boldsymbol{x}_j \in A \setminus \{\boldsymbol{x}_i\}$ を求め，それらの分散 $\mathrm{Var}(d_E^{(j)})$ を算出した．次元 $n = 2^2, \ldots, 18^2$ におけるユークリッド距離の分散を図 3 にまとめる．

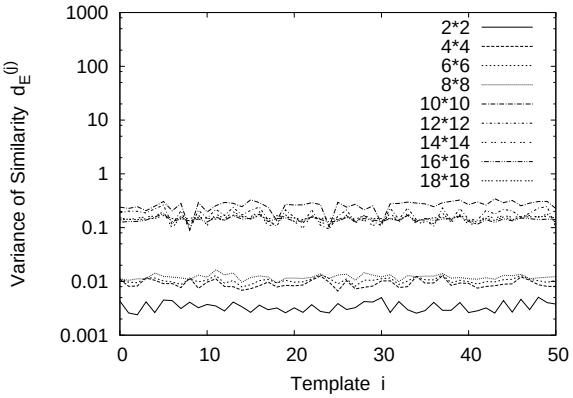

図 3: 本人間ユークリッド距離の分散

各次元の平均値を算出し，最小値 0.068 をとったインデックス $i = 9$ 番目の指紋画像をテンプレートとして用いることとする．この上で，本人，他人間についての各類似度 d_C, d_E を算出した．次元 $n = 8^2$ における各類似度の分布を図 4，5 に示す．

図 4，5 より，2 つの分布は十分に離れているので，適切に閾値を設定する事で両者ともに FAR，FRR を小さく抑える事が可能であることが分かった．

また，$n = 12^2$ において，閾値 τ_1, τ_2 を変化させた際の誤り率を図 6 に示す．FAR，FRR 共にユークリッド距離の精度が高く，例えば FAR=0.2[%] の時，コサイン尺度の FRR は 12[%] であるのに対して，ユークリッド距離は 2[%] におさまっている．他の次元についてもユークリッド距離の精度が高い，もしくは同等であったため，精度についてはユークリッド距離が優れていると

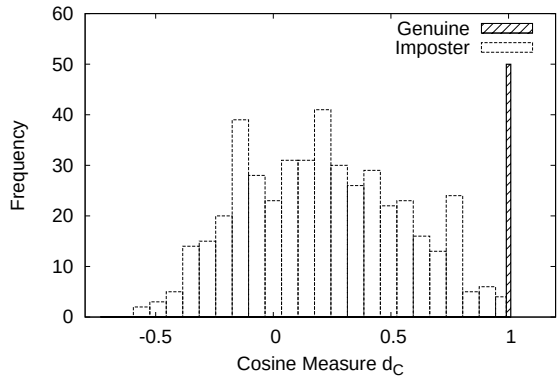

図 4: コサイン尺度 d_C のヒストグラム

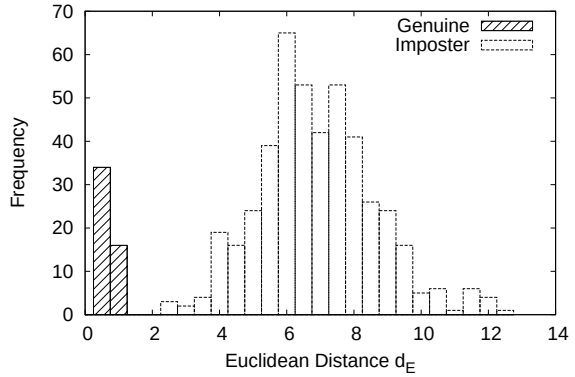

図 5: ユークリッド距離 d_E のヒストグラム

言える．

4.2 コスト

通信コスト，計算量と，サーバ，ユーザが持つ情報を表 1 にまとめる．

計算量は，主要な処理である U と S が計算したコミットメントと，ゼロ知識証明に用いた回数を表している．通信コストは U から S への通信のみを見積もり，他は簡略化した．なお，支配的な要素であるコミットメントのサイズ（1024[bit] 程度）を ℓ で表している．

		コサイン	ユークリッド
計算量	1. PK_1/PK_4	$3n$	$11n$
	3. PK_2/PK_5	19×2	19×2
	計	$3n + 38$	$11n + 38$
通信コスト	1. $G/G, \tilde{F}$	$n\ell$	$2n\ell$
	PK_1/PK_4	$n\ell$	$3n\ell$
	3. PK_2/PK_5	$5\ell \times 2$	$5\ell \times 2$
	計	$\ell(2n + 10)$	$\ell(5n + 10)$

表 1: 各方式の必要なコスト

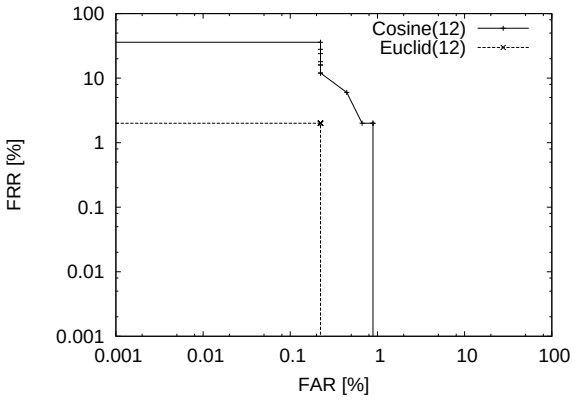

図 6: 次元 $n = 12^2$ における誤認証率

また，PK_1 や PK_4 の証明は次元数 n に比例するが，PK_2，PK_5 の区間の証明は定数である事に注意されたい．

4.3 次元による評価

上で議論したように，精度はユークリッド距離が高く，コストはコサイン尺度が小さい．では，最適な次元 n はあるだろうか．

ここでは，次元 n を $2^2, \ldots, 18^2$ まで変化させた時の精度を EER（Equal Error Rate）で図 7 に示す．

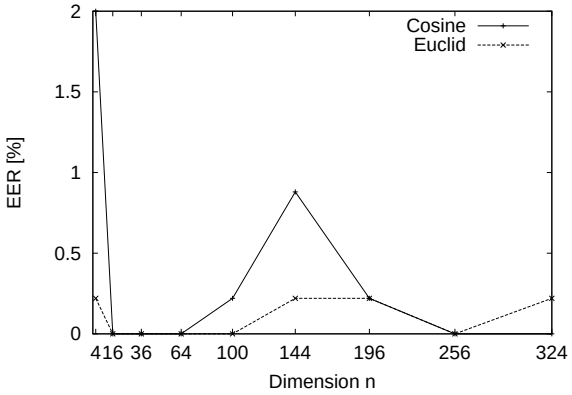

図 7: 次元 n における各方式の認証精度

$4^2 \leq n \leq 8^2$ の範囲では EER が 0，すなわち，誤認証が生じなかった．

また，表 1 にまとめたコストが実際にどの程度の処理時間を要するかを明らかにするために，提案プロトコルの試験実装を行った．実装環境を表 2 に示す．

処理時間と次元の関係を図 8 に示す．ただし，CeleronM, 1.00GHz，512MB のマシン環境，PK のセキュリティパラメータ $t = 160$[bit] として実験を行った．

$n = 8^2$ とした時，秘匿コサイン尺度評価は $3,218$[ms]，秘匿ユークリッド距離評価は $8,078$[ms] で実行が可能であった．

このことより，次元 n を $4^2 \leq n \leq 8^2$ の範囲に限定すると，コサイン尺度とユークリッド距離は同等の精度を

表 2: 実装環境

ツール	仕様
指紋リーダー	Digital Persona U.are.U4000
開発ソフト	Digital Persona Gold SDK 2.5.0 Java version 1.5.0_06 NIST NFIS2[10]

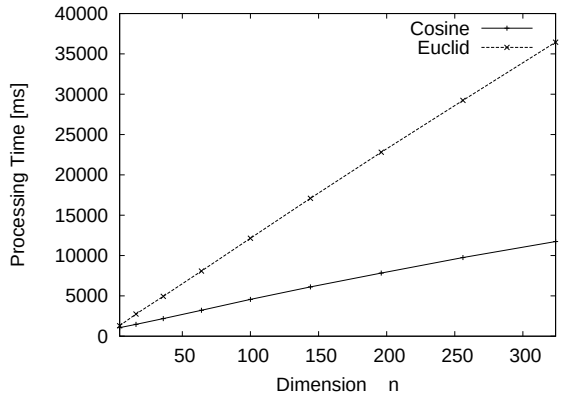

図 8: 次元 n における各方式における処理時間

持つため，コストの小さいコサイン尺度が秘密計算に適していると言える．

4.4 安全性

提案プロトコルは先に提案されている秘匿距離評価と同等の安全性が保たれるが，不正なユーザが登録情報に近いユークリッド距離やコサイン尺度を偽造する攻撃に対する安全性を検討する必要がある．しかしながら，PK_2 や PK_5 が偽造できる確率は，R_C や R_E の大きさ（セキュリティパラメータ）に対して無視できるほど小さい．

5 おわりに

類似度評価尺度を秘密にしたまま安全に認証を行うための秘密計算プロトコルを提案した．また，提案方式の有意性を明らかにするため，マニューシャの隆線角度を用いて提案プロトコルの試験実装を行い，2 つの秘匿類似度評価プロトコルを指紋認証に適用した．

入力が小さい次元に限定されている場合は各手法の精度が同等であることから秘匿コサイン尺度評価が優れていると言えるが，いずれの方式も生体情報が持つ次元数に依存した計算コストを要することが分かった．

謝辞

本研究は文部科学省科学研究費補助金「ゼロ知識証明を用いた非対称なリモートバイオメトリクス利用者認証」の支援を受けている．

参考文献

[1] N. K. Ratha, J. H. Connell and R. M. Bolle, “Enhancing Security and Privacy in Biometrics-based Authentication Systems”, IBM Systems Journal, Vol. 40, No. 3, 2001.

[2] 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.

[3] 高橋健太，三村昌広，“キャンセラブル指紋照合方式の提案,” コンピュータセキュリティシンポジウム CSS2005，pp. 379-384, 2005.

[4] 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,” 第 29 回情報理論とその応用シンポジウム予稿集，SITA2006，pp. 319-322, 2006.

[5] 尾形わかは, 菊池浩明, 西垣正勝, “区間の ZKIP を用いた生体認証方式の改良,” 第 30 回情報理論とその応用シンポジウム予稿集，SITA2007，pp. 689-693, 2007.

[6] F. Boudot, “Efficient Proofs that a Committed Number Lies in an Interval,” Proc. EUROCRYPT 2000, LNCS 1807, pp. 431-444, Springer, 2000.

[7] A. Chan, Y. Frankel and Y. Tsiounis, “Easy Come – Easy Go Divisible Cash,” Proc. EUROCRYPT ’87, LNCS vol. 304, pp. 127-141, 1998.

[8] E. Fujisaki and T. Okamoto, “Statistical Zero Knowledge Protocols to Prove Modular Polynomial Relations,” Proc. CRYPTO ’97, LNCS 1294, pp. 16-30, Springer, 1997.

[9] D. Maltoni, D. Maio, A. K. Jain and S. Prabhakar, “Handbook of Fingerprint Recognition,” Springer Sccience + Buisiness Media，2003.

[10] “NIST FINGERPRINT IMAGE SOFTWARE 2 (NFIS2)”, http://fingerprint.nist.gov/NFIS/