Vol.2013-CSEC-62 No.45
Vol.2013-SPT-6 No.45
2013/7/19

三角格子における最近傍点探索とその Fuzzy Signature への応用

米山裕太[†]　高橋健太[‡]　西垣正勝[†]

著者らが提案した生体情報を秘密鍵とするディジタル署名 Fuzzy Signature においては，曖昧な生体情報を誤り訂正するために整数格子上の Fuzzy Commitment を用いている．整数格子上の Fuzzy Commitment では，$L\infty$空間における整数格子への丸め処理によって誤り訂正を行っている．しかし，顔認証など，特徴量がユークリッド空間上のベクトルとしてコード化される場合には，Fuzzy Commitment への適用が困難であった．本稿では，三角格子の最近傍探索を用いることで，近似的にユークリッド距離に基づく Fuzzy Commitment および Fuzzy Signature を実現する方法を提案する．

Closest vector problem on triangular lattice and its application to Fuzzy Signature

YUTA YONEYAMA[†]　KENTA TAKAHASHI[‡]　MASAKATSU NISHIGAKI[†]

Fuzzy Signature proposed by the authors is a digital signature scheme using biometric information as a secret key. It uses the Fuzzy Commitment on integer lattice for the error correction of ambiguous biometric information. The principle of error correction of Fuzzy Commitment is rounding to integer lattice in $L\infty$ space. However, in the case of face recognition, the feature value is encoded to a vector in the Euclidean space, and therefore application of Fuzzy Commitment is difficult. In this paper, we propose a method to realize the Fuzzy Commitment and Fuzzy Signature which is approximately based on the Euclidean distance by using the closest vector search on triangular lattice.

1. はじめに

近年，生体情報を用いたユーザ認証の実用化が活発に行われている．また，ユーザ認証だけでなく，生体情報による秘密鍵生成[1]や，それに基づくバイオメトリック暗号の研究も行われている[2][3]．このような動向の中，著者らは秘密鍵に曖昧性を許容するディジタル署名方式 Fuzzy Signature を構築することで，生体情報を秘密鍵とするディジタル署名（以下，バイオメトリック署名）を提案した[4]．これによって，生体情報を用いて PKI（Public Key Infrastructure）と同様の機能を提供することが可能となり，IC カードやパスワードを必要としない個人認証基盤であるテンプレート公開型生体認証基盤 PBI（Public Biometrics Infrastructure）が実現する[5]．

しかし，生体情報の利用には，大きく分けて次の二つの課題がある．1)生体情報は機微情報であるため，システム側にとって登録された生体情報の管理が問題となる．また，生体情報は生涯不変な情報であるため，生体情報が流出してしまった場合に変更できない．これらの問題に対処するため，システムに登録される生体情報を秘匿するテンプレート保護が重要となる．すなわち，生体情報を秘匿したまま生体情報をマッチングする必要がある．2)通常，生体情報の特徴量はベクトルとしてコード化される．しかし，生体情報はアナログ情報であるため，読み取りの度に誤差が混入することになる．そのため，生体情報から常に一定の値を抽出することは困難であり，特徴ベクトルに対し何らかの誤り訂正処理を施す必要がある．たとえば，特徴ベクトルがハミング空間上のベクトルとしてコード化される場合には，ハミング空間における誤り訂正符号が用いられる．

我々が提案したバイオメトリック署名 Fuzzy Signature においては，1)と 2)の問題に対し、生体情報を秘匿したまま誤り訂正を行うために整数格子上の Fuzzy Commitment（以下、格子 Fuzzy Commitment）[6]を利用している．格子 Fuzzy Commitment では，登録時の生体情報と認証時の生体情報をそれぞれユークリッド空間上のn次元実数ベクトルとしてコーディングし，両者の差分ベクトルを格子間隔δの整数格子の最近傍点に丸めることによって秘密情報を復元する．すなわち，$L\infty$空間における$t = \delta/2$の閾値処理により誤り訂正を行っている．これに対し，特徴量がユークリッド空間上のベクトルとしてコード化される顔認証などでは，ユークリッド距離に基づく丸め処理が行われる[7]．そのため，顔などのモダリティに対して格子 Fuzzy Commitment（および Fuzzy Signature）を適用する場合には、ユークリッド距離による閾値処理の代わりに$L\infty$距離による閾値処理を行うことになり，認証精度の劣化を引き起こすことになると考えられる．

そこで本稿では，正三角格子（以下，三角格子）上の各格子点におけるボロノイ領域が，整数格子上の各格子点におけるボロノイ領域よりも球に近くなることに着目し，三角格子上の各格子点への丸め処理によって、近似的にユークリッド距離に基づく格子 Fuzzy Commitment を構築する．これにより，近似的にユークリッド距離に基づく Fuzzy

[†] 静岡大学大学院情報学研究科
Faculty of Informatics, Shizuoka University
[‡] (株)日立製作所 横浜研究所
Hitach, Ltd., Systems Development Laboratory

Signature も実現可能となる．ここで，任意の格子基底による最近傍点探索を効率的に行うことは一般的に困難であるが，三角格子の場合は効率的に最近傍点探索を行う手順が存在し、提案方式では，$O(n^2)$の計算量で三角格子上での丸め処理を行うことができる．

また，本稿では，提案方式の有効性を確認するために，提案方式（$L\infty$空間における三角格子への丸め処理）と格子 Fuzzy Commitment（$L\infty$空間における整数格子への丸め処理）の認証精度を、ユークリッド距離に基づく誤り訂正を行った際の認証精度比較するためのシミュレーション実験を行った．

本稿の構成は次の通りである．まず，2 章で我々の提案した Fuzzy Signature について概説する．3 章では，三角格子について述べ，4 章で三角格子を利用して Fuzzy Commitment および Fuzzy Signature の改良を行う．5 章でシミュレーション実験による提案方式の評価を行い，6 章でまとめる．

2. Fuzzy Signature

2.1 節で Fuzzy Signature の要素技術である格子 Fuzzy Commitment（整数格子上の Fuzzy Commitment）について説明し，2.2 節で Fuzzy Signature について説明する．

2.1 格子 Fuzzy Commitment

格子 Fuzzy Commitment はバイオメトリック暗号の一方式である．登録フェーズでは、生体情報を用いて秘密情報をコミットする。認証フェーズでは、登録情報と十分に近い生体情報を所持しているユーザのみが、コミットメントから秘密情報を復元することができる．

登録フェーズ

(1) ユーザの生体情報を取得し，n次元実数空間上の特徴ベクトルXとしてコード化する．

(2) 格子間隔δのn次元整数格子を構成する。ここで、すべての格子点には異なる整数が割り振られている。格子からランダムに格子点Cを選択する．格子点Cに割り振られている整数をcとする。公開ハッシュ$H(\cdot)$を用いて$H(c)$を計算し，これを秘密鍵K_sとする．

(3) 格子点Cと生体特徴ベクトルXの合成ベクトルOをコミットメントとして登録する．

認証フェーズ

(1) ユーザの生体特徴ベクトルX'を取得する．

(2) サーバからコミットメントOを取得し，ベクトル$O - X'$を求める．

(3) 差分ベクトル$O - X'$に対応するn次元実数空間上の点を、格子間隔δの整数格子上で最も近い格子点に丸める。その格子点をC'とし、C'に割り振られている整数をc'とする．登録時のXと認証時のX'との$L\infty$距離が$\delta/2$以内であれば，$C' = C$（すなわち、$c' = c$）となり，$H(c')$によって秘密鍵K_sが得られる．

認証フェーズにおいて，ある格子点に丸められる点の集合は，整数格子におけるボロノイ領域となる．図 1 に 2 次の整数格子と，そのボロノイ領域を示す．

2.2 Fuzzy Signature の基本原理

Fuzzy Signature は鍵生成，署名生成，署名検証の三つのアルゴリズムから構成される．文献[5]では，拡張型 Waters 署名[8]を用いて安全性証明可能な Secure Fuzzy Signature を構築しているが、本稿では簡単のため、Fuzzy Signature の基本形[4]について説明する．

準備

$int(\cdot)$をベクトルから整数への変換関数とする．秘密鍵sに対する公開鍵$p = PK(s)$とする。アルゴリズム$\{Gen, Sig, Ver\}$を，準同型性$PK(s_1 + s_2) = PK(s_1) * PK(s_2)$を満たすディジタル署名アルゴリズムとする。ここで、'$*$'は任意の演算であり、このような準同型性を有するディジタル署名アルゴリズムは一般に知られている．

鍵生成$BGen$

入力：生体特徴ベクトルX　出力：公開テンプレートT

(G1) n次元整数格子上のベクトルYをランダムに選択する．

(G2) Yを整数変換した値$s = int(Y)$を秘密鍵とし，対応する公開鍵$h = PK(s)$を計算する．

(G3) n次元実数ベクトルXに対して、$C = X + 2t \cdot Y$を計算し，公開テンプレート$T = (h, C)$を出力する．

署名生成$BSig$

入力：生体特徴ベクトルX'、メッセージ（平文）M

出力：署名σ

(S1) n次元整数格子上のベクトルY'をランダムに選択する．

(S2) Y'を整数変換した値$s' = int(Y')$を秘密鍵とし，対応する公開鍵$h' = PK(s')$を計算する．

(S3) s'を秘密鍵とするMの署名文$\tilde{\sigma} = Sig(s', M)$を生成する．ここで，$h$が$\tilde{\sigma}$を検証するための公開鍵となる．

(S4) n次元実数ベクトルX'に対し、$C' = X' + 2t \cdot Y'$を計算し，$\sigma = (\tilde{\sigma}, h', C')$を Fuzzy Signature の署名文とする．

署名検証$BVer$

入力：メッセージM，公開テンプレートT，署名文σ

出力：ACCEPT（成功）または REJECT（失敗）

(V1) $Ver(h', M)$によって$\tilde{\sigma}$を検証し，成功なら V2 に進み，失敗なら REJECT を出力して終了する．

(V2) CとC'を用い，以下の計算を行いs_dを求める。

$$s_d = int\left(\left\lfloor \frac{1}{2t} \cdot (C - C' + t \cdot \mathbf{1}) \right\rfloor\right)$$

(V3) 以下の通りh_dを計算する．

$$h_d = h * h'^{-1}$$

(V4) $h_d = PK(s_d)$が成り立つなら ACCEPT，そうでないなら REJECT を出力する．

ステップ V2 において，生体特徴ベクトルの距離$d(X,X')=L_\infty||x_i-x_i'||<t$である場合にのみ、$s_d=s-s'$が成り立つ。このため，ステップ V4 において，$PK(s_d)$が$h_d$と一致することを確かめることで、$X$と$X'$の一致（近似）が確認でき，かつ，ステップ V1 の検査によってメッセージMの署名検証が可能となる．図 2 に Fuzzy Signature の各アルゴリズムを図示する．

2.3 Fuzzy Signature の課題

検証アルゴリズムのステップ V2 では，コミットメントの差分$C-C'$に対し，整数格子の最近傍点への丸め処理を行っている．すなわち、Fuzzy Signature は、格子 Fuzzy Commitment と同様，$L\infty$空間における閾値処理によって誤り訂正を行っている．これに対し，生体情報の特徴量がユークリッド空間上の実数ベクトルとしてコード化される顔認証などでは，差分ベクトルがユークリッド距離によって評価されることになる．そのため，顔などのモダリティに対して Fuzzy Signature を適用した場合には，ユークリッド距離によって行われるべき閾値処理が$L\infty$距離によって代用されることになり，署名検証精度が低下すると考えられる．

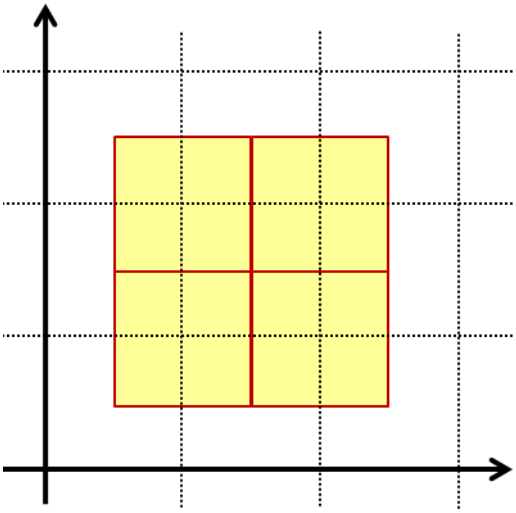

図 1：整数格子と格子点のボロノイ領域

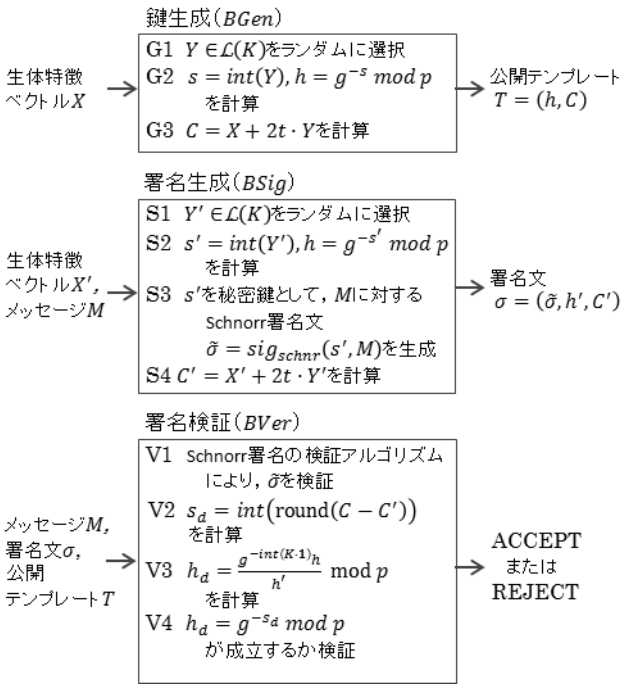

図 2：Fuzzy Signature の各アルゴリズム

3. 三角格子

3.1 三角格子とそのボロノイ領域

n次元三角格子とは，任意の基底$\boldsymbol{b_i}\in\mathbb{R}^n$（$i=1,\dots,n$）において，他のすべての基底$\boldsymbol{b}_{j\neq i}$とのなす角が$\pi/3$ [rad]となる基底

$$\boldsymbol{B}_T=[\boldsymbol{b_1},\dots,\boldsymbol{b_n}],|\boldsymbol{b}_i|=1\,,\boldsymbol{b}_i\cdot\boldsymbol{b}_j=\cos\left(\frac{\pi}{3}\right)\ \text{for all}\ i\neq j$$

によって張られる格子

$$L(\boldsymbol{B}_T)=\{\boldsymbol{B}_T\boldsymbol{x}|\boldsymbol{x}\in\mathbb{Z}^n\}$$

である．

図 3 に 2 次の三角格子を示す．2 次の三角格子では，各格子点のボロノイ領域が正六角形となる．

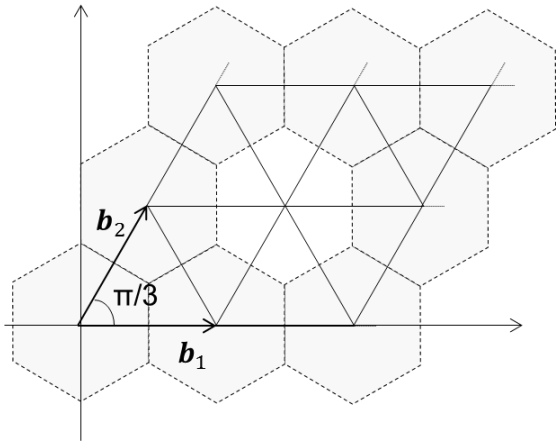

図 3：正三角格子と各格子点のボロノイ領域

3.2 最近傍ベクトル問題

最近傍ベクトル問題 CVP（Closest Vector Problem）とは，基底$\boldsymbol{B} \in \mathbb{R}^{n\times m}$とターゲットベクトル$\boldsymbol{t} \in \mathbb{R}^n$が与えられたとき，$\boldsymbol{B}$で張られる格子$L(\boldsymbol{B})$の中でターゲットベクトル$\boldsymbol{t} \in \mathbb{R}^n$に最も近い格子ベクトル$B\boldsymbol{x}$（$\boldsymbol{x} \in \mathbb{Z}^n$）を求める問題である．一般的に CVP は NP 困難であることが証明されており[8]，現在でも，任意の基底$\boldsymbol{B}$に対して CVP を多項式時間で解くアルゴリズムは発見されていない．

n次元三角格子の CVP は、同様に、任意の点$\boldsymbol{x} \in \mathbb{R}^n$と$n$次正三角格子の格子点集合$Y = \{\boldsymbol{y}_j | \boldsymbol{y}_j \in \mathbb{R}^n, j = 1, \dots, 2^n\}$が与えられたときに，最も近い格子点$\boldsymbol{y}$を求める問題として定式化される．愚直な方法では，ターゲットベクトル$\boldsymbol{x}$の周囲の2^n個すべての格子点$\boldsymbol{y}_j$との距離を求める必要がある．この方法は指数時間アルゴリズムであり，現実的ではない．しかし、三角格子の場合は効率的に最近傍点探索を行う手順が存在する。4.2 節では，$O(n^2)$の計算量で三角格子の CVP 求解アルゴリズムを説明する．

4. 三角格子 Fuzzy Signature

我々は，三角格子においては各格子点のボロノイ領域が，整数格子のボロノイ領域よりも球に近くなることに着目した．これを利用して，L∞空間における三角格子への丸め処理を行うことで，近似的にユークリッド距離に基づく誤り訂正が実現できると期待できる．

ここで、三角格子への丸め処理は、三角格子における最近傍ベクトル問題 CVP を解くことと等価になる。我々は，三角格子の対称性を利用することによって，計算量が$O(n^2)$である三角格子上の CVP 求解アルゴリズムを構成し，効率的な最近傍格子点への丸め処理を実現する．そして、これを利用し，三角格子を用いた Fuzzy Commitment および Fuzzy Signature を構築する．

4.1 三角格子空間における最近傍点探索

n次元三角格子上の CVP 求解アルゴリズムを説明する．

n次元三角格子の基底ベクトルを$\boldsymbol{B}_T = (\boldsymbol{b_1}, \dots, \boldsymbol{b_n})$としたとき，ターゲットベクトル$\boldsymbol{x} = x_1\boldsymbol{b}_1 + \dots + x_n\boldsymbol{b}_n (x_i \in \mathbb{R})$に最も近くなる最近傍格子を$\boldsymbol{y} = y_1\boldsymbol{b}_1 + \cdots y_n\boldsymbol{b}_n$（$\boldsymbol{y}_i = 0\ or\ 1$)とする．ここでは，説明を簡単にするため，ターゲットベクトル$\boldsymbol{x}$は単位ベクトルより小さい（$0 \le x_i < 1$）とする．

このとき，任意のi, jにおいて，

$$x_i < x_j \Rightarrow (y_i, y_j) = (0,0)\ or\ (0,1)\ or\ (1,1),\quad x_i > x_j \Rightarrow (y_i, y_j) = (0,0)\ or\ (1,0)\ or\ (1,1) \tag{1}$$

が成り立つ．これは，ターゲットベクトルの各要素x_iの大きさの大小関係と対応する最近傍格子の各要素y_iの大小関係は逆転することはないということを表している．すなわち，式(1)は，

$$x_i < x_j \Rightarrow y_i \leqq y_j,\ x_i > x_j \Rightarrow y_i \geqq y_j \tag{2}$$

と書き直すことができる．この事実を用い，x_iの昇順に対応するようにy_iを並び替え，y_i^*とすると，

$$y_1^* \leqq y_2^* \leqq \cdots \leqq y_n^* \tag{3}$$

が成立する．y_iの取り得る値は 0 または 1 なので，式(3)を満たす$\{y_i^*\}$は途中まで 0 が連続し，以後 1 が連続する数列となる．数列$\{y_i^*\}$の前からk番目まで 0 が連続するとした場合，kの取り得る範囲は$k = 0,1,\dots,n$の$n+1$通りとなる．よって，式(3)を満たす$\{y_i^*\}$によって定まる$n+1$個の格子点ベクトル $\boldsymbol{y}_k$とターゲットベクトル$\boldsymbol{x}$の距離を求めることで，最近傍格子点を決定することができる．

具体的なアルゴリズムを以下に示す．

1 三角格子基底 B_T を用い，ターゲットベクトル$\boldsymbol{x}$を$\boldsymbol{x} = x_1b_1 + \dots + x_nb_n (x_i \in \mathbb{R})$と分解する．
2 x_iを$x_i = z_i + r_i (z_i \in \mathbb{Z}, 0 \le R_i < 1)$と分解する．
3 $\{r_1, \dots, r_n\}$を昇順にソートし，$\{r_1', \dots, r_n'\}$を得る．このときのインデックスの置換を$\sigma(\cdot)$，逆置換を$\tau(\cdot) = \sigma^{-1}(\cdot)$とする．すなわち、$r_i = x'_{\sigma(i)} \Leftrightarrow x_i' = x_{\tau(i)}$である．
4 $k \in \mathbb{Z}$に対し，$y_{\tau(j)} = 0\ (j \le k), y_{\tau(j)} = 1\ (j > k)$である数列$(y_1, \dots, y_n)$を作成し，$y(k) = y_1b_1 + \cdots y_nb_n$とする．$k = 0, 1, \dots, n$に対し$y(k)$を作成し，$Y = \{y(0), \dots, y(n)\}$を候補格子点集合とする．
5 Yの各格子点に対して$\boldsymbol{x}$との距離を求め，最も近い格子点を$\boldsymbol{y}_{min}$とする．
6 $\boldsymbol{y}_{min}$と各$z_i\boldsymbol{b}_i$を加算したベクトル$\boldsymbol{y} = \boldsymbol{y}_{min} + \sum z_i\boldsymbol{b}_i$が最近傍格子点となる．

この CVP 求解アルゴリズムの計算量は次のように見積もられる。手順 3 のソートが $O(n \log n)$である。手順 5 においては，候補格子点 1 点とターゲットベクトルの距離計算が$O(n)$であり、これが候補格子点の数だけ（$n+1$回）行われるため、計算量は$O(n^2)$となる．全体の計算量は n^2に支配されるため，アルゴリズム全体で$O(n^2)$となる．

4.2 三角格子上の Fuzzy Commitment

4.1 節の CVP 求解アルゴリズムを用い，三角格子上の Fuzzy Commitment を構成する．

登録フェーズ

(1) ユーザの生体情報を取得し，n次元実数空間上の特徴ベクトルXとしてコード化する．
(2) 格子間隔δのn次元三角格子$L(\boldsymbol{B}_T)$を構成する。ここで、すべての格子点には異なる整数が割り振られている。格子からランダムに格子点Cを選択する．格子点Cに割り振られている整数をcとする。公開ハッシュ$H(\cdot)$を用いて$H(c)$を計算し，これを秘密鍵K_sとする．
(3) 格子点Cと生体特徴ベクトルXの合成ベクトルOをコミットメントとして登録する．

認証フェーズ

(1) ユーザの生体特徴ベクトルX'を取得する．
(2) サーバからコミットメントOを取得し，ベクトル$O - X'$を求める．
(3) 4.1 節の CVP 求解アルゴリズムを用いて、差分ベクトル

$O-X'$に対応するn次元実数空間上の点を、格子間隔δの三角格子上で最も近い格子点に丸める。その格子点をC'とし、C'に割り振られている整数をc'とする．登録時のXと認証時のX'との$L\infty$距離が$\delta/2$以内であれば，$C' = C$（すなわち、$c' = c$）となり，$H(c')$によって秘密鍵K_sが得られる．

2.1 節の格子 Fuzzy Commitment からの変更点は，整数格子の代わりに三角格子を用いるようにするのみである．

4.3 三角格子上の Fuzzy Signature

2.2 節の Fuzzy Signature に対しても，鍵生成，署名生成アルゴリズムにおける整数格子を三角格子$L(\boldsymbol{B}_T)$に変更するのみで、三角格子上の Fuzzy Signature を構築することができる．以下では，その検証アルゴリズムのみ示す．

署名検証$BVer$

入力：メッセージM，公開テンプレートT，署名文σ

出力：ACCEPT（成功）または REJECT（失敗）

(V1) $ver(h', M)$によって$\tilde{\sigma}$を検証し，成功なら V2 に進み，失敗なら REJECT を出力して終了する．

(V2) コミットメントの差分であるベクトル$C - C'$に対し，4.1 節の CVP 求解アルゴリズムを適用し，最近傍格子点$\boldsymbol{y}$を求める．

(V3) $s_d = int(\boldsymbol{y})$を計算する．

(V4) 以下の通りh_dを計算する．

$$h_d = h * h'^{-1}$$

(V5) $h_d = PK(s_d)$が成り立つなら ACCEPT，そうでないなら REJECT を出力する．

5. 評価実験

5.1 実験内容

提案方式を評価するため，生体特徴ベクトルを想定したデータに対し，提案方式（$L\infty$空間における三角格子への丸め処理）、整数格子方式（$L\infty$空間における整数格子への丸め処理）、ユークリッド距離方式（ユークリッド空間における超求の中心への丸め処理）のそれぞれの認証精度を比較するシミュレーション実験を行った．

今回は，N人のユーザ$u_i(i = 0, \dots, N)$を仮定し，次の手順によって、u_iごとにM個のn次元生体特徴実数ベクトル$d_j \in n(j = 0, \dots, M)$を生成することによって、認証実験のデータを用意した．まず、生体特徴ベクトルの個人間変動を「平均 0，標準偏差d_uの正規分布」でモデル化し、この正規分布に従う乱数を自動生成することによって各ユーザu_iの特徴ベクトルの分布中心c_iを決定する．次に，生体特徴ベクトルの個人内変動を「ユーザu_iそれぞれの分布中心c_iを平均とし，標準偏差d_dの正規分布」でモデル化し，この正規分布に従う乱数を自動生成することによって各ユーザu_iのM個の特徴ベクトルデータ$d_{i,j}(j = 0, \dots, M)$を生成する．

実験手順は次の通りである．今回の実験では、誤り訂正能力の比較が目的であるため，生体情報の登録フェーズにおいては理想的な状況を想定し、各ユーザu_iの登録情報は各々の特徴ベクトルの分布平均c_iとした．そして，全ユーザの$\{d_{i,j} \mid i = 0, \dots, N, j = 0, \dots, M\}$を認証情報として、それぞれの方式に対して認証試行を行う．認証閾値（提案方式および整数格子方式における閾値は，格子間隔をδとしたときの$\delta/2$である）を調整し、本人拒否率（FRR）と他人受入率（FAR）が一致した時点の認証精度 EER を求める．次数nを変化させていき，nに対する EER の変化を調査する．

今回は、データ数$M = 20$，他人間標準偏差$d_u = 1000$については固定し，ユーザ数$N = 100, 200, 300$，個人内標準偏差$d_d = 500, 900$とした場合についてそれぞれ実験を行う．なお、生体情報$\{d_{i,j}\}$の生成は乱数に支配されるため、今回はそれぞれのパラメータに対して 5 回ずつ$\{d_{i,j}\}$を生成し、その平均値を実験結果とする．

5.2 実験結果と評価

図 4 に、$N = 100, d_d = 500$の場合の次元nの増加に対する EER の変化のグラフを示す．同様に、図 5 に$N = 300, d_d = 500$の場合，図 6 に$N = 100, d_d = 900$の場合，図 7 に$N = 300, d_d = 900$の場合を示す．

提案方式と整数格子方式を比較すると，図 4 から図 7 のいずれの結果においても提案方式のほうがユークリッド距離方式の結果に近くなっていることがわかる．提案方式による認証精度の向上の効果が認められた結果となっている。

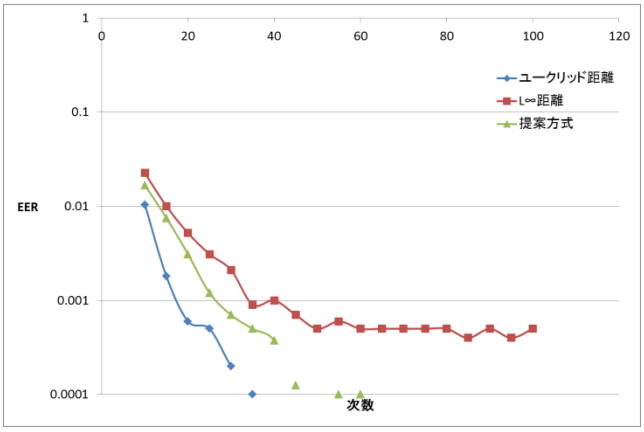

図 4：EER の変化（$N = 100, d_d = 500$）

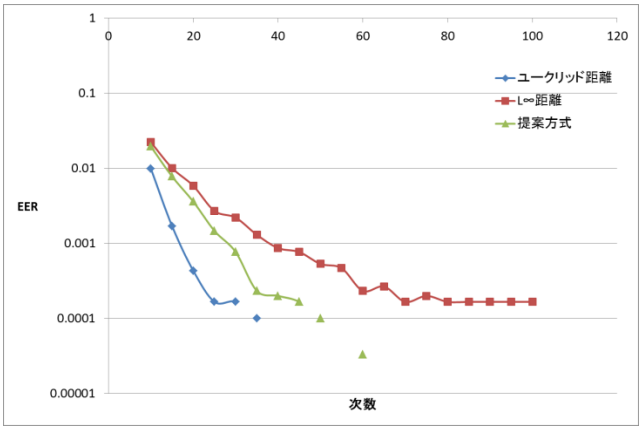

図 5：EER の変化（$N = 300, d_d = 500$）

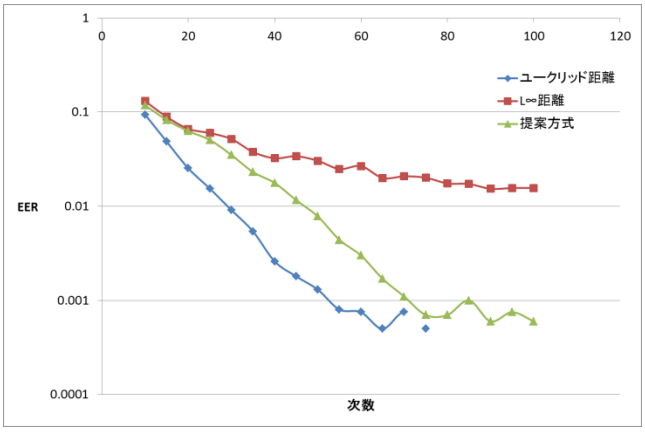

図 6：EER の変化（$N = 100, d_d = 900$）

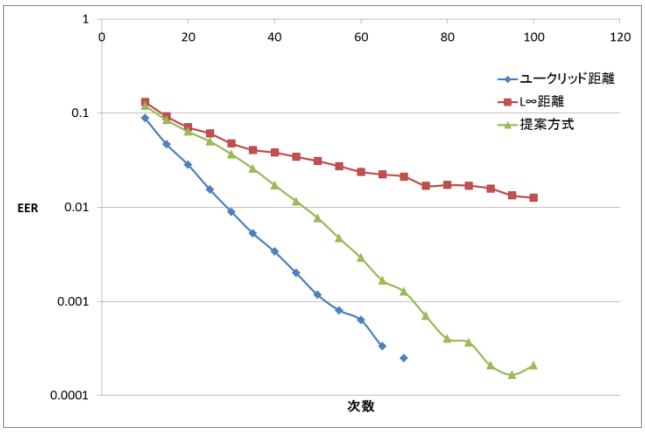

図 7：EER の変化（$N = 300, d_d = 900$）

6. まとめと今後の課題

本稿では，三角格子における効率的な最近傍点探索アルゴリズムを構成し，$L\infty$空間における三角格子への丸め処理によって読み取り誤差を含む曖昧な生体情報に対する誤り訂正を行うことで，近似的にユークリッド距離に基づく Fuzzy Commitment および Fuzzy Signature を構築した．正規分布に従う人工的な生体情報データに対するシミュレーション結果より，提案方式においては、従来の整数格子による誤り訂正よりも高い認証精度が得られることが確かめられた．

今後は提案方式とユークリッド距離方式との認証精度の差を定性的に評価する必要がある．また，今回のシミュレーションは正規分布に従うデータを仮定したが，実際の生体特徴ベクトルの分布には偏りがあると考えられる．そのため，生体情報の公開データセットを用いるなどしてより実用的な評価実験を行っていきたい．

参考文献

1) Y. Dodis, L. Reyzin, and A. Smith. Fuzzy extractors: how to generate strong keys. In Eurocrypt2004, Vol. 3027 of LNCS, pp. 523–540, 2004.

2) X. Boyen. Reusable cryptographic fuzzy extractors.In ACM Conference on Computer and Communications Security—CCS 2004, pp. 82–91. New-York:

3) Y. Dodis, B. Kanukurthi, J. Katz, L. Reyzin, and Adam Smith. Robust fuzzy extractors and authenticated key agreement from close secrets. In Advances in Cryptology – CRYPTO 2006, 2006.

4) 米山裕太，高橋健太，本部栄成，西垣正勝． バイオメトリック署名を実現する fuzzy signature. 2012 年暗号とセキュリティシンポジウム(SCIS2012), 2012.

5) 高橋健太，米山裕太，本部栄成，西垣正勝．秘密鍵に曖昧さを許す証明可能安全な電子署名と，テンプレート公開型生体認証基盤への応用. 2013 年暗号とセキュリティシンポジウム(SCIS2013), 2013.

6) G. Zheng, W. Li, and C. Zhan. Cryptographic key generation from biometric data using lattice mapping. In 18th International Conference on Pattern Recognition (ICPR2006), 2006.

7) M Turk, A Pentland - Journal of cognitive neuroscience, 1991 - MIT Press

8) B. Waters, Efficient identity based encryption without random oracles. In EUROCRYPT 2005, Vol.3494 of LNCS, pp. 114–127, 2005.

9) D.Micciancio S.Goldwassr, 暗号理論のための格子の数学, SpringerJapan, 2006