SCIS 2012 The 29th Symposium on Cryptography and Information Security
Kanazawa, Japan, Jan. 30- Feb. 2, 2012
The Institute of Electronics, Information and Communication Engineers

バイオメトリック署名を実現する Fuzzy Signature
Fuzzy Signature scheme for Biometric Digital Signature

米山 裕太* 高橋 健太†‡ 本部 栄成** 西垣 正勝§
Yuta Yoneyama Kenta Takahashi Eisei Honbu Masakatsu Nishigaki

あらまし デジタル文書やその著者の正当性を保証する技術であるデジタル署名は，安全な電子商取引を行うために不可欠な技術である．一般的にデジタル署名は「秘密鍵と平文を入力とし，署名を出力する関数（またはアルゴリズム）」として定式化される．ここで，秘密鍵については，通常 IC カード等に格納して保持しておく必要があり，紛失や盗難の危険性，トークン保持による利便性の低下が課題となっている．この問題に対し，生体情報を秘密鍵とすることでトークン保持の必要性をなくし，紛失や盗難の危険性を回避するとともに利便性を向上させる方法が検討されている．しかし，一般的に生体情報はアナログ値のため，取得のたびに読取り誤差が混入し，その値は揺らぐことになる．現在の暗号理論は整数論に基づいているため，秘密鍵の値に誤差を許容するデジタル署名（以下，Fuzzy Signature）を実現することは難しく，「生体情報（秘密鍵に相当）と平文を入力とし，署名を出力する関数」は著者らの知る限り，知られていない．本稿では，格子空間における生体情報のコミットメントと Schnorr 署名を機能的に融合させることによって Fuzzy Signature を構築し，これによってバイオメトリック署名を実現する．

キーワード デジタル署名　バイオメトリクス　テンプレート公開型生体認証基盤

1 はじめに

デジタル署名とは，暗号技術に基づいてデジタル文書やその送信者の正当性を保証する技術であり，安全な電子商取引を行うために不可欠な技術の１つである．デジタル署名は署名者の認証，メッセージの認証，否認防止の機能を備える．日本では 2001 年 4 月に施行された「電子署名及び認証業務に関する法律」[6]によって，デジタル署名は法的にも手書き署名や押印と同等の効力をもつ．

デジタル署名は一般的に，「秘密鍵と平文を入力とし，署名を出力する関数（またはアルゴリズム）」として定式化される．ここで，署名生成用の秘密鍵は，デジタル署名のトラストポイントとなる重要な情報であり，所有者が厳格に管理し，他者に知られないようにしなければならない．このため，秘密鍵は一般に IC カード等に格納されるとともに，暗証番号（又はパスワード）によって秘密鍵をアクティベートするという運用が強いられることになる．しかし，こうした持ち物と暗証番号による秘密鍵の管理においては，IC カードを所持することによる利便性の低下，紛失・盗難による成りすましの危険性が存在する．

そこで，生体情報を秘密鍵とすることで IC カード保持の必要性をなくし，紛失や盗難の危険性を回避するとともに利便性を向上させる方法が検討されている．生体情報は機微情報であるため，生体情報を秘密鍵にできれば，利用者本人が故意に自らの秘密鍵を露出させて事後否認を行うというリスクも抑えられると期待される．しかし，一般的に生体情報はアナログ値のため，たとえ本人のものであったとしても，取得のたびに読取り誤差が混入し，その値は揺らぐことになる．現在の暗号理論は整数論に基づいているため，秘密鍵の値に誤差を許容するデジタル署名（以下，Fuzzy Signature）を実現することは難しい．

* 静岡大学情報学部，〒432-8011 静岡県浜松市城北 3-5-1, Faculty of Informatics, Shizuoka University, 3-5-1 Johoku, Hamamatsu, Shizuoka, 432-8011
† 日立製作所 横浜研究所，〒244-0817 横浜市戸塚区吉田町 292, Hitach, Ltd., Systems Development Laboratory, 292, Yoshida, Totsuka, Yokohama, Kanagawa, 244-0817
‡ 東京大学大学院情報理工学系研究科，〒113-8656 東京都文京区本郷 7-3-1, Graduate School of Information Science and Technology, The Universe of Tokyo, 7-3-1, Hongo, Bunkyo-ku, Tokyo, 113-8656
** 静岡大学大学院情報学研究科，〒432-8011 静岡県浜松市城北 3-5-1, Faculty of Informatics, Shizuoka University, 3-5-1 Johoku, Hamamatsu, Shizuoka, 432-8011
§ 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, Shizuoka University, 3-5-1 Johoku, Hamamatsu, Shizuoka, 432-8011

この問題に対し，生体情報によって乱数情報のコミットを行うバイオメトリック暗号[7],[8]に基づく生体鍵生成技術が研究されている．バイオメトリック暗号では，乱数をコミットする際に用いた生体情報と十分近い生体情報が入力された場合にのみ，乱数を復元することができる．この乱数を秘密鍵として用いることによって，生体情報によるデジタル署名が実現される．ただしバイオメトリック暗号では，コミットメントから秘密鍵を復元するという原理上，ユーザはデジタル署名を行う際にシステムに対して（生体情報だけでなく）コミットメントを提示することが求められる点に注意が必要である．このためユーザは，コミットメントを IC カード等に入れて所持するか，コミットメントを管理するサーバに問い合わせるといった処理が必要となる．このように，Fuzzy Signature を実現する「生体情報（秘密鍵に相当）と平文のみを入力とし，署名を出力する関数」は著者らの知る限り，知られていない．

そこで本稿では，格子空間における生体情報のコミットメントと Schnorr 署名を機能的に融合させることによって Fuzzy Signature を構築し，これによってバイオメトリック署名を実現する．

本稿の構成は次のとおりである．2 章でデジタル署名とバイオメトリック署名の定義と必要要件をまとめる．3 章ではバイオメトリック署名を実現する暗号プリミティブである Fuzzy Signature を提案し，4 章で評価を行う．最後に 5 章で本稿をまとめ，今後の課題を述べる．

2　デジタル署名とバイオメトリック署名

本章では，デジタル署名とバイオメトリック署名の定義と必要要件を明確にする．

2.1　デジタル署名の定義

デジタル署名は以下の各機能を有する．

認証　検証者は，署名とメッセージが確かに署名者本人から送られてきたものであり，かつ，メッセージに改竄がないことを確かめられる．

否認防止　署名者は，第三者（裁判所など）に対し，そのメッセージを送信した事実を否定できない．

以上の機能を持つデジタル署名は，一般に公開鍵暗号を用いることで実現されている．

公開鍵暗号に基づくデジタル署名の生成は，署名者が秘密鍵を用いて署名対象となるメッセージを暗号化することによって行われる．一方，デジタル署名の検証は，不特定多数の署名検証者が，署名者の公開鍵を利用して署名者による暗号化の正当性を確認することによって行われる．すなわち，秘密鍵が署名生成鍵となり，公開鍵が署名検証鍵に対応する．署名生成鍵を所有する者は署名者ただ一人であるため，生成鍵を署名者が秘密に管理する限り署名者以外の個人がデジタル署名を偽造することは困難である．

デジタル署名方式は以下の 3 つのアルゴリズム(G,S,V)の組で表される．

鍵生成アルゴリズム G： $\boldsymbol{gen}(\mathbf{1}^k) \rightarrow (\boldsymbol{K_s}, \boldsymbol{K_p})$

1^kを入力すると，鍵ペア(K_s, K_p)を生成する．K_pは署名検証鍵であり，公開される．K_sは署名生成鍵であり，署名者が秘密に管理する．kはセキュリティパラメータである．

署名生成アルゴリズム S： $\boldsymbol{sig}(\boldsymbol{K_s}, \boldsymbol{M}) \rightarrow \boldsymbol{\sigma}$

メッセージMと署名生成鍵K_sを入力すると，署名σを出力する．

署名検証アルゴリズム V：

$\boldsymbol{ver}(\boldsymbol{m}, \boldsymbol{K_p}, \boldsymbol{\sigma}) \rightarrow$ **ACCEPT or REJECT**

メッセージM，署名検証鍵K_p，署名σを入力すると，ACCEPT（検証成功）または REJECT（検証失敗）を出力する．

2.2　デジタル署名の必要要件

デジタル署名の要件を満たすためには，主に 3 つの特性が必要とされる．第一に，署名生成鍵K_sで生成された署名は，対応する署名検証鍵K_pによる検証で常に ACCEPT が出力されること，第二に，いかなる攻撃者も署名検証鍵K_pを含む公開情報から有効な署名を生成することは困難であること，第三に，いかなる攻撃者も公開される署名検証鍵K_pおよび署名σから，秘密情報である署名生成鍵K_sを推測することは困難であることである．これらを要件として以下にまとめる．

要件 1：正当性　正当な署名者が生成した署名文は検証を通過する．

要件 2：安全性　検証を通過するのは正当な署名者が生成した署名文に限る．すなわち，選択文書攻撃に対する存在的偽造不能性（CMA-EUF）が証明できる．ここで，安全性を満たすには，公開情報から署名者のみが有する秘密情報が漏れない性質（以下，一方向性）が必要条件となる．

2.3　バイオメトリック署名の定義

本稿では，生体情報を秘密鍵として用いるデジタル署名をバイオメトリック署名と定義する．バイオメトリック署名方式は以下の 3 つのアルゴリズム(BG,BS,BV) の組で表される．

鍵生成アルゴリズム BG： $\boldsymbol{gen_b}(\mathbf{1}^k, \boldsymbol{b}) \rightarrow \boldsymbol{K_p}$

セキュリティパラメータkと署名者の生体情報bを入力とし，生体情報bに対する公開テンプレートK_pを生成する．bが署名生成鍵の役目を果たし，K_pが署名検証鍵に相当する．

署名生成アルゴリズム BS： $\boldsymbol{sig_b}(\boldsymbol{b'}, \boldsymbol{M}) \rightarrow \boldsymbol{\sigma}$

メッセージMと生体情報b'を入力とし，署名σを生成する．生体情報は取得の度に読取り誤差の混入によって揺らぐため，署名生成鍵となる署名生成時の生体情報b'は鍵生成時の生体情報bとはわずかに異なること

に注意されたい.

署名検証アルゴリズム BV：

$ver_b(m, K_p, \sigma) \rightarrow$ **ACCEPTorREJECT**

メッセージM，署名検証鍵K_p，署名σを入力とし，ACCEPT（検証成功）または REJECT（検証失敗）を出力する.

既存技術であるバイオメトリック暗号に基づく生体鍵生成方式との根本的な違いが，署名生成アルゴリズムsig_bである．バイオメトリック暗号では署名生成の際に，署名対象となるメッセージMと秘密鍵の役割を果たす生体情報b'に加えて，生体情報のコミットメントの入力も必要となる．これに対してsig_bでは，Mとb'のみを入力として署名σが生成されるアルゴリズムとなっており，通常のデジタル署名と完全に同じスキーム（デジタル署名において秘密鍵が生体情報に置き換わっただけ）になっている．すなわちバイオメトリック署名では，署名生成の際に（生体情報以外の）ユーザ依存情報は一切不要であり，ユーザは自身の生体情報さえあれば任意のメッセージに署名を付すことができる.

2.4 バイオメトリック署名の必要要件

バイオメトリック署名はデジタル署名の一形態であるため，2.2 節に示したデジタル署名の要件 1：正当性，要件 2：安全性は，バイオメトリック署名においても満たすべき必要要件としてそのまま引き継がれる. ただし，それぞれの要件において，生体情報を署名生成鍵（秘密鍵）として利用することに起因する変更が加わる.

要件 1'：正当性 鍵生成時の生体情報の持ち主が生成した署名文は検証を通過する.

要件 2'：安全性 検証を通過するのは，鍵生成時の生体情報と署名生成時の生体情報が十分に近く，同一人物による署名であることが判断できる場合に限る. 公開テンプレートや署名から署名者の生体情報に関する情報が漏れない性質（一方向性）が必要条件である.

3 Fuzzy Signature

本章では，前章で示したバイオメトリック署名の定義および必要条件を満たす署名方式「Fuzzy Signature」について説明する.

3.1 要素技術

提案方式は，整数格子上の Fuzzy Commitment [1] と，Schnorr 署名[2] を要素技術として利用する.

3.1.1. 整数格子上の Fuzzy Commitment

以下に整数格子上の Fuzzy Commitment を概説する.

登録フェーズ

(1) ユーザの生体情報を取得し，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の整数格子からランダムに格子点Cを選択する. 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.

鍵復元フェーズ

(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，Oから生体特徴ベクトルX'を減算する.

(3) ベクトル$O - X'$を格子間隔δの整数格子空間上で最も近い格子点に写像したものをC'とする. ここで，登録時のXと鍵復元時のX'が$\delta/2$以内であれば，$C' = C$となり，$H(C')$によって秘密鍵K_sが得られる.

3.1.2. Schnorr 署名

以下に Schnorr 署名の手順を説明する.

鍵生成（gen）

(1) 信頼できるセンタ T が，大きな素数p,および位数が大きな素数 q となる$\mathbb{Z}_q^*$の要素gを公開する（すなわち，$g^q = 1 \bmod p$である）.

(2) 証明者はsをランダムに選び，$h = g^{-s} \bmod p$を計算する．ここで，sが秘密鍵，hが公開鍵となる.

署名（sig）

(1) 署名者は秘密鍵s, およびメッセージMを入力とし，以下の計算を行う.

(a) $r \in \mathbb{Z}_q$をランダムに選び$x = g^r \bmod p$を計算する.

(b) $c = H(M, x)$を求める.

(c) $v = r + sc \bmod q$を求める.

(2) 署名文σを(c, v)とする.

検証（ver）

(1) 受信者は，センタと署名者の公開情報(p, q, g, h)，メッセージM，およびその署名文(c, v)を用い，$x = g^v h^c \bmod p$を計算する.

(2) $c = H(M, x)$が成り立てば ACCEPT し，そうでなければ REJECT する.

3.2 Fuzzy Signature の基本原理

整数格子上の Fuzzy Commitment と，Schnorr 署名を機能的に融合させることによって Fuzzy Signature を構築する. 具体的には，Fuzzy Commitment と Schnorr 署名を連結することによって，Fuzzy Commitment における「生体情報のコミットメント」を「バイオメトリック署名の公開テンプレート」へと昇華させる.

Fuzzy Signature 方式の鍵生成フェーズでは，(G1) 生体情報の特徴量をベクトルXで表し，格子空間上のランダムな格子ベクトルYとの合成ベクトル$X + Y$を生成することによって，生体情報をコミットするとともに，(G2) Yを整数変換した値sを$h(s) = g^s \bmod p$（pは大きな素数，gは生成元）の形でコミットする. すなわち，$X + Y$と$h(s)$が Fuzzy Signature 公開テンプレート（署名検証鍵）に相当する.

署名生成フェーズでは, (S1) 生体情報の特徴量をベクトルX'（登録時の生体情報Xとわずかに異なることに注意されたい）で表し，格子空間上のランダムな格子ベクトルY'との合成ベクトル$X'+Y'$を生成した上で, (S2)Y'を整数変換した値s'に対して$h(s')=g^{s'} \bmod p$を求める. (S3) そして，s'を Schnorr 署名の秘密鍵として，メッセージMの Schnorr 署名$\tilde{\sigma}=sig_{schnr}(s',M)$を生成する. すなわち，$(X'+Y', h(s'), M, \tilde{\sigma})$が Fuzzy Signature の署名文となる. ここで, $h(s')$はs'のコミットメントと，Schnorr 署名の公開鍵の両者を兼ねていることに注意されたい.

署名検証フェーズでは，公開鍵$\big(X+Y, h(s)\big)$と署名文$(X'+Y', h(s'), M, \tilde{\sigma})$から，(V1) $h(s'), M$を用いて Schnorr 署名$\tilde{\sigma}=sig_{schnr}(s',M)$の正当性を検査するとともに, (V2) 生体情報のコミットメントに関する差分ベクトル$(X+Y)-(X'-Y')$を生成し，(V3) その正当性を$h(s)-h(s')=g^{s-s'} \bmod p$によって検査する．$X$と$X'$が十分に近いときにのみ，ステップ V2 における差分ベクトルの最近傍格子点が$Y-Y'$に一致することになる. $Y-Y'$を整数変換した値が$s-s'$であることから，ステップ V3 の検査によって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の署名検証が成功する.

3.3 Fuzzy Signature の手順

以下では，提案方式の鍵生成から署名検証までの手順を説明する（図 1）.

準備

P1 生体情報の空間βはn次元実数ベクトル空間$\mathbb{R}^n$の部分集合とし，$X,\ X' \in \beta$の間の距離関数dはL_∞距離で定義されるものとする:

$$d(X,X') = \max_i |\, x_i - x_i' \,|$$

ただしx_i, x_i'は，ベクトル$X,\ X'$のi番目の要素とする（$i=0,1,\cdots,n-1$）. あるしきい値$t \in \mathbb{R}$ に対して$d(X,X')<t$のとき$X,\ X'$は一致するとみなす.

P2 セキュリティパラメータkに対し, kビットの素数qと, $p = |q-1$なる素数pを選ぶ. また$g \in Z_p^*$を，位数がqとなるよう選ぶ. qに対し，整数Kを以下のように定める:

$$K = \left\lfloor \frac{q^{\frac{1}{n}} - 1}{2} \right\rfloor$$

kを適切に設定することで, Kは任意の生体情報$X \in \beta$の各要素の絶対値$|x_i|$がとり得る最大値より十分大きくなるようにしておく.

P3 (t,p,q,g,K)をシステム共通のパラメータとする.

P4 Kに対して格子点集合 $\mathcal{L}(K)$を,

$$\mathcal{L}(K) = \{Y=(y_0,\cdots,y_n-1) | y_i \in \mathbb{Z}, 0 \le y_i < K\}$$

とし，格子点Yを整数に対応させる関数$int: \mathcal{L} \to \mathbb{Z}$を

$$int(Y) = \sum_{i=0}^{n-1} y_i (2K+1)^i$$

と定義する．$int(Y)$ は，整数ベクトルYを$2K+1$進数とみなした整数値である.

P5 $\mathbb{Z}_q$の元を出力するハッシュ関数$H(\cdot)$を用意する.

鍵生成（gen）

入力: 生体情報X.
出力: 公開テンプレートT.

G1 $Y \in \mathcal{L}(K)$をランダムに選ぶ.

G2 $s=int(Y), h=g^{-s} \bmod p$とする.
このとき，Yの各要素y_iは 0 以上K未満のため
$0 \le s = int(2Y)/2 < (2K+1)^n/2 < q/2$
であることに注意する.

G3 $C=X+2t \cdot Y$とする.

G4 $T=(h,C)$を出力する.

署名生成（sig）

入力: 平文M, 生体情報X'.
出力: 署名文σ.

S1 $Y' \in \mathcal{L}(K)$をランダムに選ぶ.

S2 $s'=int(Y'), h'=g^{-s'} \bmod p$とする

S3 s'を秘密鍵として, Mに対する Schnorr 署名文$\tilde{\sigma}$を生成する.
(a) $r \in \mathbb{Z}_q$をランダムに選び，$a=g^r \bmod p$を計算する.
(b) $c=H(M,a)$を求める.
(c) $v=r-sa \bmod q$を計算する.
(d) $\tilde{\sigma}=(c,v)$とする.

S4 $C'=X'+2t \cdot Y'$とする.

S5 $\sigma=(\tilde{\sigma}, h', C')$を出力する.

署名検証（ver）

入力: 平文M, 署名文$\sigma=(\tilde{\sigma}, h', C')$,
公開テンプレート$T=(h,C)$.
出力: ACCEPT or REJECT.

V1 Schnorr 署名の検証アルゴリズムにより，$\tilde{\sigma}=(c,v)$を検証する.
(a) $a=g^v h'^c \bmod p$を計算する.
(b) $c=H(M,a)$が成立しなければ REJECT を出力して停止する.

V2 以下の通りs_dを計算する.

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

ここで，$V = (v_0, \cdots, v_n) \in \mathbb{R}^n$に対して$\lfloor V \rfloor = (\lfloor v_0 \rfloor, \cdots, \lfloor v_n \rfloor) \in \mathbb{Z}^n$とする．また$\mathbf{1} = (1, 1, \cdots, 1)$とする．

V3　以下の通りh_dを計算する．

$$h_d = \frac{g^{-int(K \cdot \mathbf{1})} h}{h'} \bmod p$$

V4　$h_d = g^{-s_d} \bmod p$が成立すればACCEPT, 成立しなければREJECTを出力する．

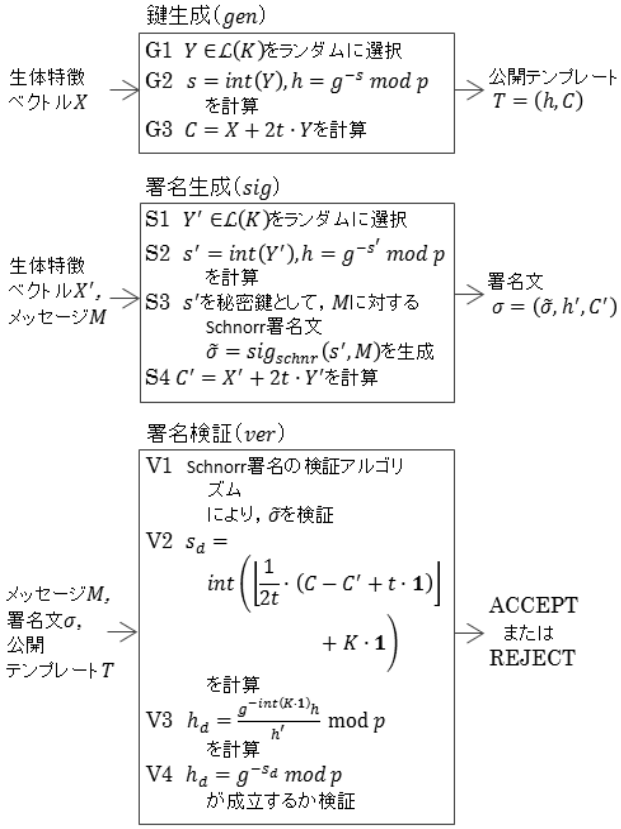

図 1:Fuzzy Signature の手順

3.4　Remarks

ステップV2において，$d(X, X') < t$ならば，またそのときに限って以下が成立する．

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

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

$$= int(Y - Y' + K \cdot \mathbf{1})$$

$$= int(Y) - int(Y') + int(K \cdot \mathbf{1})$$

このとき，$0 \le int(Y), int(Y') \le int(K \cdot \mathbf{1}) < q/2$なので，$0 \le s_d < q$であることに注意する．$\frac{1}{2t}(X - X')$に対して床関数をとる操作は，生体情報間の誤差を訂正する一種の誤り訂正とみなすことができる．一方，ステップV3において，以下が成立する．

$$h_d = \frac{g^{-int(K \cdot \mathbf{1})} g^{-int(Y)}}{g^{-int(Y')}} \bmod p$$

$$= g^{-\left(int(Y) - int(Y') + int(K \cdot \mathbf{1})\right)} \bmod p$$

すなわち，$d(X, X') < t$である場合に限って，ステップV2のs_dがステップV3のh_dの指数部と一致することになる．したがって，ステップV4は$d(X, X') < t$のときにACCEPTを出力し，そうでなければREJECTを出力する．

ステップG2における(s, h)は，Schnorr署名における秘密鍵と公開鍵のペアである．またステップG3は，生体情報Xを，秘密鍵sに対応するベクトルYでマスクして秘匿する操作（コミット）とみなすことができる．すなわちsは，生体情報Xをマスクするための乱数とSchnorr署名の（一時的な）秘密鍵を兼ねている．一方，ステップV2のs_dは，登録時のsと署名生成時s'との「差」に相当しており，h_dがs_dに対応するSchnorr署名の公開鍵となっている．このように，提案方式においては，生体情報X, X'を秘密鍵に対応するベクトルY, Y'でマスクして秘匿する操作（ベクトルの加算）の線形性と，Schnorr署名の公開鍵$h = g^{-s} \bmod p$が秘密鍵sの加法に対して持つ準同型性を利用し，両者を効果的に融合している．なお，ElGamal署名[4]やDSA署名[5]，さらにそれらの楕円曲線版署名方式の公開鍵においても同様の準同型性を持つため，Schnorr署名の代わりに用いることができる．

4　評価

本章では，提案方式がバイオメトリック署名の必要要件を満たしているか検討を行う．なお，一方向性についても安全性とは別に検討する．

4.1　要件 1'：正当性

署名者が公開テンプレートを有する本人であれば，公開テンプレートとしてコミットされている生体特徴ベクトルXと署名生成時に用いられた生体特徴ベクトルX'のL_∞距離$d(X, X')$がt未満であると期待できる．したがって，公開テンプレートの持ち主が生成した署名者であれば，ステップV2で正しいs_dを生成することができ，ステップV4の検証を通過できる．

ただし，本人であれば，$d(X, X') < t$となる生体特徴

ベクトルX'が得られるか否かについては，評価実験を通じて実際の FRR を調査する必要がある．

4.2 要件 2'：安全性

正当な署名者以外の人物が任意のメッセージに対する署名を偽造するには，Schnorr 署名$c = H(M, a)$を偽造するか，または，生体情報のコミットメント$C' = X' + 2t \cdot Y'$を偽造する必要がある．ここで，Schnorr 署名はランダムオラクル仮定と離散対数問題の困難性の仮定のもとで CMA-EUF であると証明されているため[3]，生体情報のコミットメントを偽造する方法のみが残される．

生体情報のコミットメントC'の偽造については，攻撃者は，C'から Schnorr 署名の秘密鍵s'を取り出して不正メッセージに対する Schnorr 署名文を偽造する方法と，不正な Schnorr 署名文と辻褄の合うC'を偽造する方法が考えられる．

前者の方法に対しては，C'においてランダムベクトルY'が生体特徴ベクトルX'でマスクされた形になっているため，X'（正確には，XまたはX'に十分近いベクトル）を所持していない攻撃者はC'からX', Y'を取り出すことは困難である．また，公開テンプレートと署名から$C - C' = (X - X') + 2t \cdot (Y - Y') \fallingdotseq 2t \cdot (Y - Y')$を計算することができるが，$X'$（正確には，$X$または$X'$に十分近いベクトル）を所持していない攻撃者にとっては，$C - C'$からY'を取り出すことも同様に難しい．このため，署名者以外がY'を整数変換した値であるs'を推測することは困難であるといえる．後者の方法に対しても，X'（正確には，XまたはX'に十分近いベクトル）を所持していない攻撃者にとっては，自らが選んだ不正な Schnorr 秘密鍵$\tilde{s'}$に対応するY'をX'を用いてマスクすることは基本的に不可能である．したがって，不正な Schnorr 秘密鍵$\tilde{s'}$と辻褄の合うコミットメントC'を偽造することも困難である．

以上より，提案方式は CMA-EUF であるといえる．

ただし，他人であっても，FAR の確率で$d(X, X') < t$となる生体特徴ベクトルX'が得られる．このため，評価実験を通じて実際の FAR を調査する必要がある．

4.3 一方向性

生体情報のコミットメントCおよびCは，（前節で説明したように，ランダムベクトルYおよびY'が生体特徴ベクトルXまたはX'でマスクされた形になっているわけだが，XおよびX'とYおよびY'の役割を入れ替えて）生体特徴ベクトルXおよびX'がランダムベクトルYまたはY'でマスクされた形になっていると考えることもできる．このため，XまたはX'に十分近いベクトルを所持していない攻撃者は，CまたはC'から生体特徴ベクトルXまたはX'に関する情報を逆算することは難しい．

ただし，一方向性を満たすためには，生体情報のエントロピは十分大きくなくてはならないことに注意が必要である．なぜなら，バイオメトリック暗号では，攻撃者は公開テンプレートを用いて生体情報に対する総当り攻撃をオフラインで実行することが可能であるためである．一般に，単独の生体情報（例えば 1 本の指の指紋）のエントロピの大きさは限られるため，複数の生体情報を組み合わせることが必須と考えられる．

5 まとめと今後の課題

本稿では，格子空間における生体情報のコミットメントと Schnorr 署名を機能的に融合させることによって，曖昧性を有する生体情報を秘密鍵として使用することができるデジタル署名方式である Fuzzy Signature を構築し，これによってバイオメトリック署名を実現した．

提案方式には，以下の課題が残る．

第一に，検証ステップ V2 の計算の制約上$(int^{-1}(s_d)$の各ビットが$[0, 2K + 1)$の範囲に収まるようにするために），Schnorr 秘密鍵sおよびs'をn桁の$(2K + 1)$進数の取り得る空間から一様に選ぶことができない．セキュリティパラメータkを大きく取ることで安全性を高めることができるが，この構造の制約による脆弱性がないか検討する必要がある．

第二に，攻撃者が同一署名者による複数の署名を集めると，生体情報のコミットメントの総和をとることによってランダムベクトル（YやY'）の値がキャンセルされ，生体特徴ベクトル（XまたはX'）が抽出されてしまう．単純な対策としては，ランダムベクトルY'の空間を十分に大きくとる方法が考えられるが，安全性について詳細な検討が必要である．

第三に，生体情報の近さを評価する距離関数としてハミング距離を用いることができない．提案方式稿では，生体情報をマスクする情報であるY, Y'が Schnorr 秘密鍵の役割を兼ねるため，ベクトルY, Y'を数値に変換した上で用いている．このため，Y, Y'生体特徴ベクトルの誤差をL_∞距離として定義せざるを得ない．実際の生体情報の誤差はハミング距離として与えられるものが多いと考えられるため，提案方式を，ハミング距離を利用可能な方法に改良していく方法を検討していく必要がある．

今後は，以上の課題について検討を掘り進めるとともに，提案方式を実装し，実験を通して検証精度（FAR,FRR）の評価を行う予定である．

参考文献

[1] 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.

[2] C. P. Schnorr. “Efficient identification and signatures for smart cards”, CRYPTO’89, LNCS 435, pp. 239–252. Springer-Verlag, 1990.

[3] Pointcheval D. and J. Stern, “Security proofs for signature schemes,” Proceedings of EUROCRYPT ’96, LNCS 1070, pp. 387-398, Springer-Verlag, 1996.
[4] T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms”, IEEE Trans. Inform. Theory, 31 (1985), 469-472.
[5] National Institute of Standards and Technology (NIST), “DigitalSignature Standard”, FIPS Publication 186, May 1994.
[6] 法務省, “電子署名及び認証業務に関する法律に基づく特定認証業務の認定にかかる指針”, http://www.moj.go.jp/MINJI/minji32-3.html
[7] A. Juels and M. Sudan, “A Fuzzy Vault Scheme”, IEEE International Symposium on Information Theory, pp. 408, 2002.
[8] A. Jules and M. Wattenberg, “A fuzzy commitment scheme”, In Proc. ACM Conf. Computer and Communication Security, pages 28–36, 1999.