Vol.2012-CSEC-58 No.43
Vol.2012-SPT-4 No.43
2012/7/20

# 生体情報を用いた認印型デジタル署名:Lazy Signature

米山裕太[†]　高橋健太[†††‡]　本部栄成[†]　西垣正勝[†††]

現在のデジタル署名は，実印における印鑑登録制度を電子文書に対して実現しているものである．ただし，実社会においては実印の使用は稀で，認印がより広く使用されている．認印は，本人が押印したことが認められれば法的効力においては実印と差がなく，事前登録が不要で手軽に利用できる．この認印のシステムを電子的に実現できれば，認証局へ事前登録不要な利便性の高いデジタル署名としての利用が期待できる．しかし，従来のデジタル署名を事前登録無しで運用するだけでは，事後否認を防止することができない．そこで本稿では，個人に固有な生体情報を用いることで事後否認を防止でき，事前登録が不要という認印のメリットを持つデジタル署名方式:Lazy Signature を提案する．

キーワード:　デジタル署名　バイオメトリクス　認印

# Lazy Signature:
# A non-registered Digital Signature Using Biometrics

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

The conventional digital signature is implemented and operated as the function of registered stamp or signature for digital documents. In the real world, however, it is rare to use registered stamps or signatures, and non-registered ones are more used often. If it is possible to apply non-registered stamp/signature system to digital world, it is expected that digital signature will become more useful and effective. To achieve this, it is vital to ensure that “the signing key is not registered, but still repudiation is prevented”. So, we propose to combine digital signature and biometric signature to connect signing key and signer with each other. Thus, a non-registered digital signature, Lazy Signature, is realized in this paper.

Key words: Digital signature, Biometrics, Non-registered signature

## 1. はじめに

現在のデジタル署名は，実印における印鑑登録制度を電子文書に対して実現しているものである．実印を利用するにはまず，市や区役所等に実印を持参して本人と印影の紐付けを保証してもらい，その証拠として印鑑登録証明書を発行してもらう．これにより，文書の押印が実印所持者本人によるものであることに対する信頼性が得られ，契約不履行の根本的な原因となる否認を防ぐことが可能である．デジタル署名も同様に，認証局に公開鍵を届け出て公開鍵証明書を発行してもらうことによって，署名が付されている電子文書の本人性や真正性を保証する仕組みとなっている．デジタル署名も実印と同様の法的効力が認められており[1]，事後否認が大きな問題となるような契約では，電子文書に対してデジタル署名が用いられている．

しかしながら，我々の生活において実印の使用場面を考えてみると，土地や住宅などの売買，遺産相続など，比較的高額な契約時に限定されており，その他の日常的な契約においては，ほとんど認印が使用されている．認印とは，実印登録を行っていない印鑑のことを示す．実社会においては，押印された紙が物理的に存在することによって，契約の事実が（ある程度の信頼度で）確認できる．また，必要に応じて，対面で契約書を取り交わすなどの措置を講ずることによって，その契約を（ある程度の信頼度で）保証することができる．このため，認印であっても契約における否認防止の要件が満たされることが社会的に認められており，認印の押印行為は国内で法的な効力を持つ[2]．このことから，契約において重要なことは，実印であるか認印であるかに依るのではなく，契約の当事者間で信頼が構築できるかどうかであることがわかる．すなわち，当事者間の信頼を担保することができれば，印鑑の事前登録は必ずしも必要となるわけではないと考えられる．

これに対し，電子社会におけるオンライン契約においては，印鑑や契約書に相当する電子データは容易にコピーが可能であること，非対面でのやりとりとなることなどの制約が存在する．このため，事前登録によるトラストアンカを用いなければ当事者間の信頼を構築することが難しく，認印型のデジタル署名が実現できていなかった．

そこで本稿では，生体情報を秘密鍵としてデジタル署名を生成することにより，署名と個人の紐付けを実現することで，認証局への事前登録がない状態でも署名の信用が得られる認印型デジタル署名 Lazy Signature を提案する．た

† 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
‡ 東京大学大学院情報理工学系研究科
Graduate School of Information Science and Technology, The Universe of Tokyo
††† 静岡大学創造科学技術大学院
Graduate School of Science and Technology, Shizuoka University

だし，生体情報はアナログ情報であるため，入力誤差などの混入によってその値が揺らぐことになる．このため，生体情報から秘密鍵を生成するにあたっては，生体情報の曖昧性に対する対処が必要となる．これを実現する技術として，著者らによる Fuzzy Signature [3]がある．本稿では，Fuzzy Signature を基に，Lazy Signature を構築する．

## 2. 認印型デジタル署名

### 2.1 現在のデジタル署名の限界

実印と認印の違いが印鑑の事前登録の有無にあることから鑑みるに，現在のデジタル署名と認印型デジタル署名の違いは「公開鍵の認証局への登録を行うか否か」という運用の違いに帰着すると考えることができる．すなわち，認印型デジタル署名の構成要素となる鍵生成，署名生成，署名検証の 3 つのアルゴリズム自体は，現在のデジタル署名のそれらと同じである．現在のデジタル署名と認印型デジタル署名の運用手順を図 1 と図 2 に示す．

現在のデジタル署名の運用手順（図 1）は次のとおりである．①鍵生成・登録：署名者は，秘密鍵-公開鍵のペアを生成した後，公開鍵を認証局に登録する．認証局は，署名者の本人性を確認し，公開鍵証明書を発行する．署名者は，秘密鍵を秘密に保持する．②署名生成：署名者は自身の秘密鍵を用いて，平文に対するデジタル署名を生成する．署名文とともに公開鍵証明書を受信者に送信する．③署名検証：検証者は，公開鍵証明書の正当性を確認したのち，その公開鍵で署名文を検証する．

これに対し，認印型デジタル署名の運用手順（図 2）は次のようになる．①鍵生成：署名者は，秘密鍵-公開鍵のペアを生成した後，秘密鍵を自身で秘密に保管する．公開鍵は認証局に登録しない．②署名生成：署名者は，自身の秘密鍵を用いて平文に対するデジタル署名を生成する．署名文とともに公開鍵そのものを受信者に送信する．③署名検証：検証者は，署名文とともに送られてきた公開鍵を用いて署名文を検証する．

しかし，図 2 の運用においては，公開鍵の事前登録がないため，署名者と公開鍵の紐付けが保証されていない．したがって，署名は，署名生成時に使用した秘密鍵を故意に消失させることによって，容易に署名文を否認することが可能である．1 章で述べたように，電子社会におけるオンライン契約においては，電子データは容易にコピーが可能であること，非対面でのやりとりであるため当事者間の信頼が希薄となることなどから，図 2 の運用における否認防止性の欠落を別の方法で補うことが難しい．このため，現在まで認印型のデジタル署名が実現できていなかった．

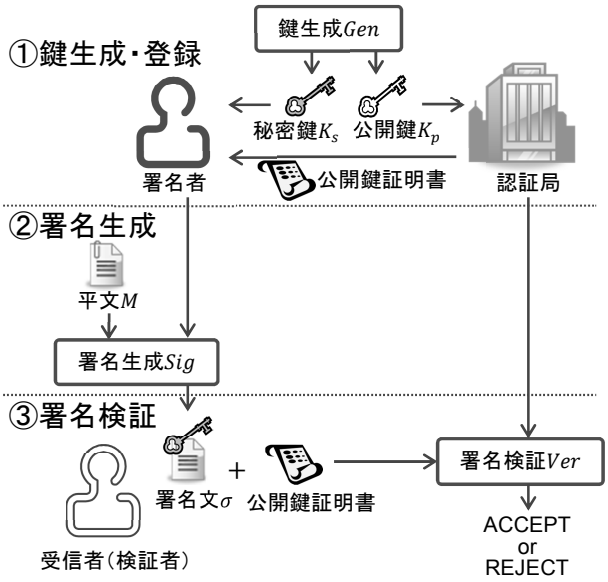


図 1：現在のデジタル署名の運用手順

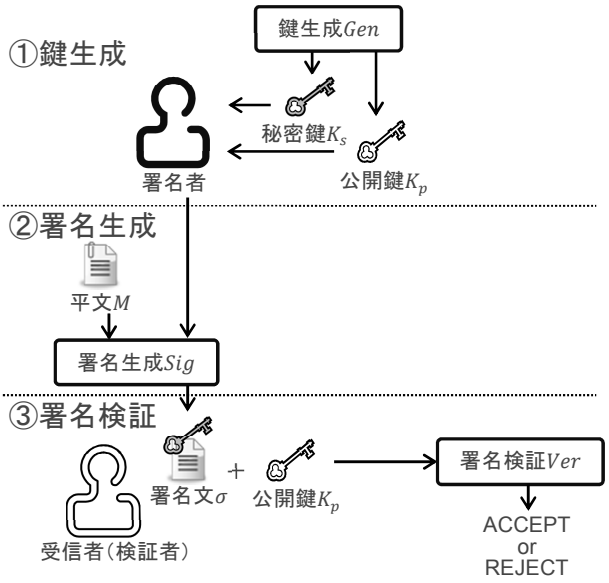


図 2：認印型デジタル署名の運用手順

### 2.2 バイオメトリック署名による認印型デジタル署名

生体情報を秘密鍵としてデジタル署名を生成することにより，署名と個人の紐付けを実現することで，認証局への事前登録がない状態でも署名文に対する信用が担保される．すなわち，認印として拇印を用いることによって，認印型デジタル署名が実現できると期待される．

生体情報は個人に固有な情報であり，生涯不変な情報であるため，署名文が署名者の生体情報に基づくものであるならば，認証局への事前登録なしであっても，その署名文の本人によって作られたものであることが保障できる．また，生体情報は機微情報であるため，自ら生体情報を他人に暴露することは考えにくい．以上より，契約文書の本人性，真正性，否認不可性が確認できると考えられる．さら

に，生体情報のみでデジタル署名が生成できることで，トークンやパスワードが不要となることによる利便性の向上や，トークンの紛失やパスワードの忘却といったリスクの回避も期待できる．

ただし，生体情報はアナログ情報であるため，入力誤差などの混入によってその値が揺らぐことになる．このため，生体情報から秘密鍵を生成するにあたっては，生体情報の曖昧性に対する対処が必要となる．これを実現する技術として，著者らが提案しているバイオメトリック署名[3]がある．本稿では，バイオメトリック署名を用いて認印型デジタル署名を実装していく．

バイオメトリック署名のアルゴリズムを以下に示す．

**鍵生成$BGen(1^k, b) \rightarrow K_p$**

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$BSig(b', M) \rightarrow \sigma$**

メッセージ$M$と生体情報$b'$を入力とし，署名$\sigma$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$BVer(m, K_p, \sigma) \rightarrow$ ACCEPTorREJECT**

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

また，バイオメトリック署名の必要要件は以下のとおりである．

**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．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．

### 2.3 Lazy Signature

バイオメトリック署名を用いた認印型デジタル署名を Lazy Signature と呼称する．Lazy Signature の運用手順（図 3）は次のようになる．①鍵生成：署名者は，$BGen$によって自身の生体情報$b$に対する公開テンプレート$K_p$（公開鍵に相当）を生成する．公開テンプレート$K_p$は認証局に登録しない．②署名生成：署名者は，$BSig$によって自身の生体情報$b'$を用いて平文$M$に対するデジタル署名$\sigma$を生成する．署名文$\sigma$とともに公開テンプレート$K_p$を受信者に送信する．③署名検証：検証者は，署名文$\sigma$と公開テンプレート$K_p$を用いて署名文$\sigma$を検証する．

署名文に対して何らかの疑義が生じた場合には，下記の④をオフラインで実行することよって，署名文$\sigma$の信頼性を確認することができる．④調停：検証者は，署名者に検証者の目前で$BGen(1^k, b'') \rightarrow K'_p$を実行してもらい，その公開テンプレート$K'_p$で署名$\sigma$の検証を行う．ここで，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，この時点の生体情報$b''$は，$b$および$b'$とはわずかに異なる．しかし，署名者本人の生体情報であれば$b$，$b'$，$b''$は十分に類似しているため，バイオメトリック署名の要件 2 から，$b'$によって生成された署名文$\sigma$の正当性を，$b''$から生成された公開テンプレート$K'_p$によって検証できることが保証される．なお，④においても認証局が介在しないことに留意されたい．

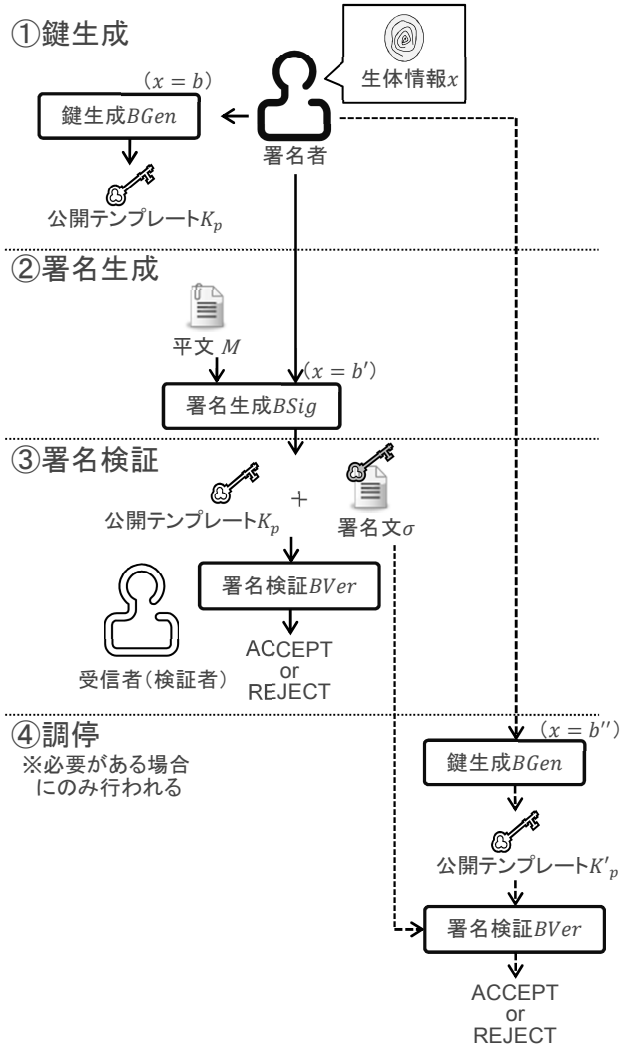


図 3：Lazy Signature

バイオメトリック署名においては，$BGen$と$BSig$の実施順序に制約はない（$BSig$→$BGen$→$BVer$の順序でも署名検証が可能である）．この性質を利用すれば，Lazy Signature を事後検証型の手順で運用することもできる．事後検証型 Lazy Signature の運用手順（図 4）は次のようになる．①署名生成：署名者は，自身の生体情報を用いて平文に対するデジタル署名を生成する．②署名ロギング：受信者は署名

文を保存する．この時点では署名文の検証は行わない．③署名検証：②で保存された署名の検証が必要となった時に初めて，検証者は署名者から公開テンプレートを入手し，署名文の検証を行う．

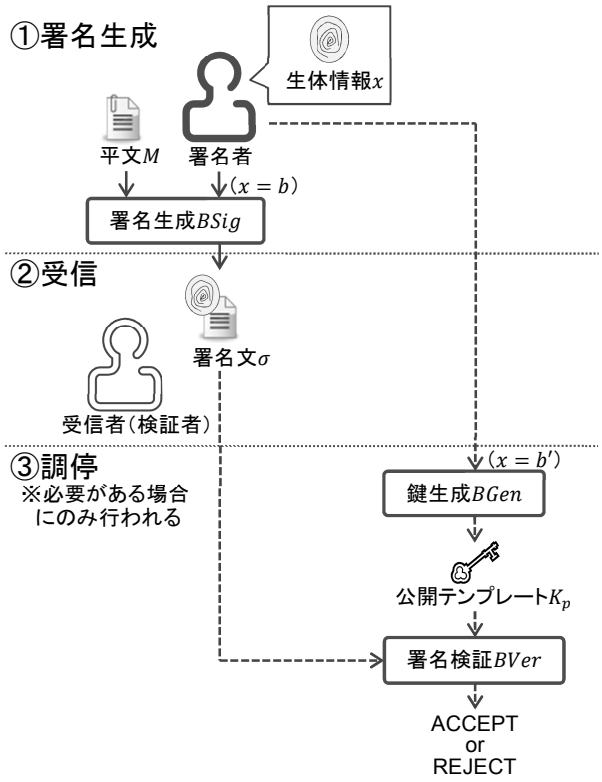


図 4：事後検証型 Lazy Signature

図 4 の運用方法は，事前登録不要でユーザの生体情報のみで容易に署名が生成できるため，ライフログ管理やデジタルフォレンジック等の用途に向いていると考えられる．例えば，平素からユーザの入退室ログを公開テンプレートなしの認印型デジタル署名によって所得しておけば，万一の有事の際にユーザから公開テンプレートを提出してもらうことによって，その時刻にその部屋に居たユーザ（署名者）を同定できる．

## 3. Fuzzy Signature

前章で示したように，本稿では，バイオメトリック署名のビルディングブロックである$BGen$，$BSig$，$BVer$を用いて認印型デジタル署名 Lazy Signature を構築している．バイオメトリック署名の具体的な実現手法の一つが Fuzzy Signature [3]である．本章では，Fuzzy Signature の詳細について説明する．

### 3.1 要素技術

提案方式は，整数格子上の Fuzzy Commitment [4] と，Schnorr 署名[5] 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$\delta$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$\delta$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$\sigma$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 3）．

**準備**

P1　生体情報の空間$\beta$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$L_\infty$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 L($K$)を，

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

とし，格子点$Y$を整数に対応させる関数$int$:L→ $\mathbb{Z}$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（$BGen$）**

入力: 生体情報$X$.
出力: 公開テンプレート$T$.

G1　$Y$ ∈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（$BSig$）**

入力: 平文$M$, 生体情報$X'$.
出力: 署名文$\sigma$.

S1　$Y'$ ∈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) $v = r + sc \bmod q$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（$BVer$）**

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　以下のとおり$s_d$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　以下のとおり$h_d$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．

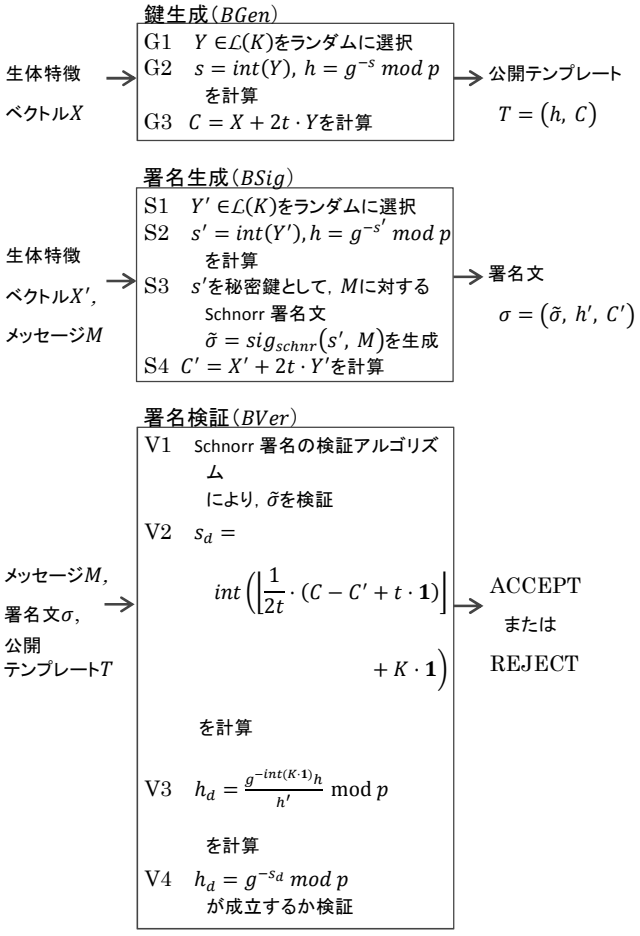


図 5：Fuzzy Signature の各アルゴリズム

### 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．

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

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

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

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

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．

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

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

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$\boldsymbol{X}$を，秘密鍵$\boldsymbol{s}$に対応するベクトル$\boldsymbol{Y}$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$\boldsymbol{s}$は，生体情報$\boldsymbol{X}$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[6]や DSA 署名[7]，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．

### 3.5 評価

2.2 節に示したバイオメトリック署名の 2 つの要件である正当性，安全性について，Fuzzy Signature がこれを満たすことを説明する．

#### 3.5.1 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$L_\infty$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．

#### 3.5.2 要件 2：安全性

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[8]，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，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．攻撃者が，$C'$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 署名文の偽造を試みても，$C'$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．不正な Schnorr 署名文と辻褄の合う$C'$を偽造する方法に対しても，$X'$（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，Fuzzy Signature は CMA-EUF であるといえる．

ただし，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，安全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．

## 4. おわりに

本稿では，曖昧性を有する生体情報を秘密鍵とするデジタル署名である Fuzzy Signature を用い，実世界における認印に対応するデジタル署名方式 Lazy Signature を構築した．Lazy Signature は事前登録不要で否認防止を実現するデジタル署名であり，実世界において大勢を占める認印ベースの契約のオンライン化を実現するたけでなく，ライフログやデジタルフォレンジックの分野にも適用可能であると期待される．

提案方式は以下の課題を残している．今後は，これらの課題の解決に努めるとともに，提案方式の実装，実験を通じて検証精度（FAR，FRR）の評価を行う予定である．

- 署名者が, 生体情報をスキャナに入力する際に故意に生体情報を歪ませたような場合, 生成された署名は署名者の正しい生体情報によって検証をすることができない．ただし，この問題は認印型デジタル署名に限らず，生体認証全般に当てはまる問題であり，本稿の範疇を超える．
- 提案方式は，事後否認等の問題が発生した場合には，オフラインにて当事者どうしで署名の本人性や真正性を確認することができる（図 3 における④）が，金銭の授受などが行われた後で問題が発生した場合には，対処が遅れることになる．すなわち提案方式は，被害を未然に防ぐことはできない. 実社会における実印，認印と同様に，通常のデジタル署名と認印型デジタル署名も場面に応じた使い分けが必要となる．
- 提案方式のビルディングブロックになっている Fuzzy Signature には, いくつかの技術的な課題が存在している．提案方式もそれらの課題を引き継ぐ．

**謝辞**　本稿を執筆するにあたり，静岡大学情報学部原田伸一朗先生から，法律的観点からのご助言をいただきました．心より感謝申し上げます．

## 参考文献

1) 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
2) 法テラス, 法律関連用語集 http://www.houterasu.or.jp/houritsu_yougoshuu/yougo_mi/mi_5.html
3) 米山裕太, 高橋健太, 他, “バイオメトリック署名を実現する Fuzzy Signature”, SCIS2012, 2012
4) G. Zheng, W. Li, and C. Zhan. “Cryptographic keygeneration from biometric data using lattice Mapping”, In 18th International Conference on Pattern Recognition (ICPR2006), 2006.
5) C. P. Schnorr. “Efficient identification andsignatures for smart cards”, CRYPTO’89, LNCS 435, pp. 239–252. Springer-Verlag, 1990.
6) T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms”, IEEE Trans. Inform. Theory, 31 (1985), 469-472.
7) National Institute of Standards and Technology(NIST), “DigitalSignature Standard”, FIPS Publication 186, May 1994.
8) Pointcheval D. and J. Stern, “Security proofs for signature schemes,” Proceedings of EUROCRYPT ’96, LNCS 1070, pp. 387-398, Springer-Verlag, 1996.