SCIS 2013 The 30th Symposium on
Cryptography and Information Security
Kyoto, Japan, Jan. 22 - 25, 2013
The Institute of Electronics,
Information and Communication Engineers

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

A Provably Secure Digital Signature with Fuzzy Secret Key and Its Application to Public Biometrics Infrastructure

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

あらまし 従来の暗号理論では一般に，秘密鍵は固定的な情報として扱われる．すなわち 2 つの秘密鍵が僅かでも違えば，異なる鍵と見做される．このため生体情報のように，取得する度に誤差が混入する曖昧な情報を秘密鍵として利用するには，何らかの形で誤差を吸収する必要がある．このように秘密鍵に曖昧さを許容する暗号理論としては Fuzzy Extractor (FE) と呼ばれる，誤り訂正符号を用いた一種の鍵生成関数と，これを利用した暗号，認証，鍵交換プロトコルなどが提案されている．これらのアプローチでは，秘密鍵を用いた処理を行う際に，誤り訂正のための検査符号に相当する情報を補助的に入力する必要がある．一方で，電子署名アルゴリズムは一般に，秘密鍵と平文のみを入力として署名文を出力する関数として定式化される．このため従来のアプローチでは，秘密鍵に曖昧さを許す電子署名を実現できなかった．これに対し我々は SCIS2012 において，整数格子に基づく Fuzzy Commitment と Schnorr 署名を用いた署名方式を提案したが，安全性証明がつかず未完成であった．本稿では SCIS2012 での構成に用いたアプローチを発展させ，Waters Signature と中国人剰余定理を利用することで，秘密鍵に曖昧さを許し，標準モデルで安全性証明可能な電子署名方式 Secure Fuzzy Signature (SFS) を提案する．また生体情報を秘密鍵とする PKI として筆者らが提案している Public Biometrics Infrastructure (PBI) への適用可能性について検討する．

キーワード 電子署名，セキュリティ，バイオメトリクス，PBI

1 はじめに

電子署名とは，電子文書に対してその真正性を保証する技術であり，紙文書に対する印鑑やサインに相当する役割を果たす．具体的には電子文書の作成者や承認者の証明，改ざんや偽造の防止，否認の防止，本人認証などの機能を持ち，電子行政サービスや電子商取引などに広く利用される PKI (Public Key Infrastructure) を実現する，最も基本的な要素技術の一つである．

電子署名方式は，以下の 3 つのアルゴリズムの組 (Gen, Sig, Ver) として定式化される．

Gen :鍵生成
: 1^k (k:セキュリティパラメータ) を入力とし，公開鍵（検証鍵）pk と秘密鍵（署名鍵)sk を出力する確率的多項式時間アルゴリズム (PPTA).

Sig :署名生成
: 秘密鍵 sk およびメッセージ（電子文書）m を入力とし，署名 σ を出力する PPTA.

Ver :検証
: 公開鍵 pk，メッセージ m および署名 σ を入力とし，署名の正当性を検証する PPTA．1(検証成功) または 0(検証失敗) を出力する．

従来，電子署名を含む暗号理論において，秘密鍵や公開鍵，平文といったあらゆる情報は，固定的なデジタルデータとして扱われる．例えば 2 つの秘密鍵が 1 ビットでも異なれば，異なる鍵と見做される．

一方で近年，曖昧で誤差を含む秘密情報に基づく，新たな暗号技術の研究が進められている．具体的には，Fuzzy Extractor (FE) と呼ばれる，誤り訂正符号を用いた一種の鍵生成関数 [1] と，これを利用した暗号，認証，鍵交

* 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-cho, Totsuka-ku, Yokohama-shi, Kanagawa-ken, 244-0817
† 静岡大学大学院 情報学研究科，〒 432-8011，静岡県浜松市中区城北 3-5-1, Graduate school of Informatics, Shizuoka University 3-5-1 Johoku, Naka, Hamamatsu, Shizuoka, 432-8011
‡ 静岡大学創造科学技術大学院，〒 432-8011，静岡県浜松市中区城北 3-5-1, Graduate School of Science and Technology, Shizuoka University 3-5-1 Johoku, Naka, Hamamatsu, Shizuoka, 432-8011

換プロトコルなどが提案されている [2, 3].

こうした技術により，生体情報やPUF (Physically Unclonable Function) といった物理的実体の観測によって得られる，揺らぎを持ったアナログな情報を一種の秘密鍵として用いることが可能となり，鍵管理に伴う様々な実運用上の課題を解決できると期待される．

FE を用いたアプローチでは，鍵生成時に秘密情報 (例えば生体情報) に依存した補助情報 (検査符号に相当) を作成して保存する．認証，暗号，復号など秘密鍵を用いた処理を行う際には，ユーザの秘密情報に含まれる誤差を補助情報を用いて訂正した上で秘密鍵を復元し，一般的な暗号技術を用いて各種の処理を行う．従って FE を用いて電子署名を実現するためには，署名生成アルゴリズム (Sig) の入力として，秘密鍵 sk とメッセージ m に加え，補助情報が必要となる．これは実運用を考えたとき，ユーザが自分の補助情報を IC カード等に入れて所持するか，補助情報が記録されている特定の署名端末に利用を限定するか，補助情報を管理するサーバに問い合わせるか，といった処理が必要となることを意味し，利用環境に制約が生じる．例えば生体情報を秘密鍵とする場合，手ぶらで任意の端末からネットワーク接続を前提とせずに署名を生成する，といった使い方はできない．

このように本来，署名生成アルゴリズム (Sig) の入力は上述したように秘密鍵 sk とメッセージ m のみとすべきであり，この意味で従来，秘密鍵に曖昧さを許す電子署名 (Fuzzy Signature) の構成法は，筆者らの知る限り知られていなかった．これに対し筆者らは SCIS2012 において，整数格子に基づく Fuzzy Commitment 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よって Fuzzy Signature の一構成法を提案した [4]．しかしながらその安全性は証明できておらず，電子署名方式として未完成であった．

本稿では，SCIS2012 での構成に用いたアプローチを発展させ，Waters Signature と中国人剰余定理を利用することで，秘密鍵に曖昧さを許し，標準モデルで安全性証明可能な電子署名方式 Secure Fuzzy Signature(SFS) を提案する．また生体情報を秘密鍵とする PKI として筆者らが提案している Public Biometrics Infrastructure (PBI) への適用可能性について検討する．

2 関連研究

2004 年，Dodis らは誤差を含む情報から暗号学的に安全な鍵を生成する方法論として Fuzzy Extractor (FE) の概念を定式化し，その具体的構成法を提案した [1].

2.1 FE のモデル

FE は 鍵生成関数と鍵復元関数 (Gen, Rep) の組として定式化される (図 1)．Gen は，生体情報のように誤差と偏りを持つ情報 x を入力とし，補助情報 h と，鍵空間上で一様分布する鍵 sk を生成する．h から x や sk を推定することはできない．Rep は，x' と h を入力とし，鍵 sk' を復元する．x と x' が，ある距離尺度の下で十分「近い」(以下 $x' \sim x$ と表す) ならば，$sk' = sk$ となる (正しい鍵を復元する).

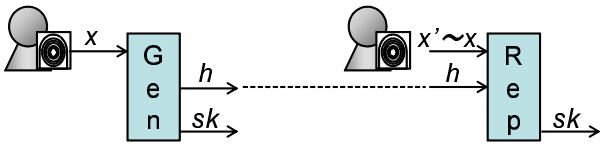

図 1: Fuzzy Extractor

FE は，Secure Sketch と呼ばれるアルゴリズムと，乱数抽出器を組み合わせることで構成できる．Secure Sketch は，x を乱数 r を用いて “安全に” 符号化し s を出力する関数 (SS) と，x', s から誤り訂正によって x を復号するアルゴリズム (Rec) とから構成される．

2.2 Secure Sketch の具体的構成法

Secure Sketch の具体的な構成法としては，Fuzzy Commitment [5], Fuzzy Vault [6], 整数格子に基く Fuzzy Commitment [7] などが知られている．それぞれ秘密情報の誤差を評価する距離関数は，ハミング距離，set difference, L_∞ 距離で与えられる．ここでは一例として Fuzzy Commitment を紹介する．

秘密情報 x の空間を $\mathcal{X} = \{0,1\}^n$ とし，x, x' の間のハミング距離を $d(x, x')$ と表す．また $(n, k, 2t+1)$ 誤り訂正符号アルゴリズム (例えば BCH 符号) を考え，その符号語集合を $\mathcal{C} = \{c_1, c_2, ..., c_N\}$ $(N = 2^k)$ とする．

SS は，x と k ビット乱数 r を入力として受け取ると，$s = x \oplus c_r$ を出力する．

Rec は，x' と s を入力として受け取り，$c' = x' \oplus s$ を計算してこれを誤り訂正符号のデコード関数に入力し，$c_{r'} \in \mathcal{C}$ を得たならば $\hat{x} = s \oplus c_{r'}$ を出力する．デコードに失敗した場合は $\perp$ を出力する．

$c' = x' \oplus s = c_r \oplus (x \oplus x')$ なので，$d(x, x') \leq t$ ならば c' のデコード結果は c_r となり，$\hat{x} = s \oplus c_r = x$ となる．

2.3 Fuzzy Extractor の応用

FE を用いることで，誤差を含む情報を秘密鍵とした共通鍵暗号，鍵交換，認証などが実現できる．例として図 2 に，FE を用いた共通鍵暗号の構成を示す．Enc, Dec はそれぞれ，AES など一般的な共通鍵暗号方式の暗号化，復号化関数を表す．ENC との出力 (暗号文) と補助情報 (C, h) の組を改めて暗号文と見れば，全体として秘密鍵に誤差を許す共通鍵暗号と見ることができる．

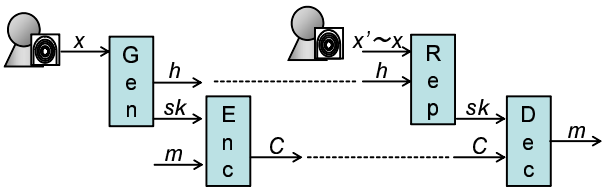

図 2: Fuzzy Extractor を用いた共通鍵暗号

しかしながら前述したように，FE を用いて電子署名を実現しようとすると，署名生成関数 Sig の入力に補助情報 h を追加せざるを得ず，これにより実運用上の制約が生じる．

誤差を含む曖昧な秘密鍵と平文のみを入力として署名生成が可能な電子署名 (Fuzzy Signature) を構成するためには，FE とは本質的に異なるアプローチを採る必要がある．

3 Fuzzy Signature の定義

以下，曖昧さを含む秘密鍵をファジー秘密鍵と呼ぶ事にする．ファジー秘密鍵の空間を $\mathcal{X}$ とし，2 つのファジー秘密鍵 $\boldsymbol{x}, \boldsymbol{x}'$ の間の距離がある距離関数 $d(\cdot,\cdot)$ を用いて評価され，ある閾値 t に対して $d(\boldsymbol{x}, \boldsymbol{x}') < t$ のとき $\boldsymbol{x}, \boldsymbol{x}'$ は「近い」と定義する．

Fuzzy Signature は，以下の 3 つの PPTA の組として定義される．

Gen :鍵生成
: ファジー秘密鍵 $\boldsymbol{x}$ を入力とし，公開鍵 pk を出力する PPTA.

Sig :署名生成
: ファジー秘密鍵 $\boldsymbol{x}'$ およびメッセージ（電子文書）m を入力とし，署名 σ を出力する PPTA.

Ver :検証
: 公開鍵 pk，メッセージ m および署名 σ を入力とし，署名の正当性を検証する PPTA．1(検証成功) または 0(検証失敗) を出力する．

Fuzzy Signature は以下の要件を満たさなくてはならない．

- 正当性
  正当な署名者が生成した署名文と平文の組は検証に成功する．ここで正当な署名者とは，鍵生成の際に入力されたファジー秘密鍵 $\boldsymbol{x}$ と近いファジー秘密鍵 $\boldsymbol{x}'$ を持つ署名者のこと．すなわち

$$\begin{aligned}&\forall m, \sigma, pk;\\ &(\exists \boldsymbol{x}, \boldsymbol{x}'; pk = \mathsf{Gen}(\boldsymbol{x}) \wedge \sigma = \mathsf{Sig}(m, \boldsymbol{x}') \wedge d(\boldsymbol{x}, \boldsymbol{x}') < t)\\ &\quad \rightarrow Pr[\mathsf{Ver}(m, \sigma, pk) = 1] \geq 1 - \epsilon \qquad (1)\end{aligned}$$

  が十分小さな ϵ に対して成立することを要件とする．

- 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．特に，選択文書攻撃に対する存在的偽造不可能性 (EU-CMA) が，妥当な仮定の下に証明できることを要件とする．

4 証明可能安全な Fuzzy Signature の提案

先に述べたとおり，FS を構成するために FE を直接的に利用することはできない．なぜなら FE は，秘密鍵を利用する前に誤り訂正を行うアプローチを採り，このためユーザ固有の補助情報が必要となるためである．そこで我々は FE とは逆のアプローチ，即ち秘密鍵を利用した後 (具体的には署名検証時) に誤差を吸収する方針を採る．しかしながら秘密鍵の誤差を訂正する処理は，その結果として秘密鍵を露呈してしまうことになるため，本来署名検証時には実行できない．我々はこの問題を，一種の線形性を持つ符号化/誤り訂正処理と，符号語 → 秘密鍵 → 公開鍵という一連の写像を準同型性を持たせて構築することで，解決する．

以下では証明可能安全な FS の具体的構成として，Secure Fuzzy Signature (SFS) を提案する．提案方式は，構成要素として整数格子に基づく Fuzzy Commitment [7] と，Waters Signature [8] を利用している．

4.1 準備

4.1.1 ファジー秘密鍵の空間

ファジー秘密鍵の空間は

$$\mathcal{X} = [0, 1)^n \subset \mathbb{R}^n \qquad (2)$$

とし，$\boldsymbol{x}, \boldsymbol{x}' \in \mathcal{X}$ の間の距離関数 d は L_∞ 距離で定義されるものとする．

$$d(\boldsymbol{x}, \boldsymbol{x}') = \max_i |x_i - x'_i|. \qquad (3)$$

ただし x_i, x'_i は，ベクトル $\boldsymbol{x}, \boldsymbol{x}'$ 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 $d(\boldsymbol{x}, \boldsymbol{x}') < t$ のとき $\boldsymbol{x}, \boldsymbol{x}'$ は一致とみなす．

$$k = \lfloor -n \log_2(2t) \rfloor \qquad (4)$$

とし，k は十分大きい (例えば 80 以上) ものとする．k はセキュリティパラメータに相当する．

ファジー秘密鍵 $\boldsymbol{x}$ は $\mathcal{X}$ 上一様分布であるとする．また鍵生成時に入力されるファジー秘密鍵 $\boldsymbol{x}$ に対し，署名生成時に入力されるファジー秘密鍵 $\boldsymbol{x}'$ は，それが正規の鍵であるならば誤差ベクトル

$$\boldsymbol{e} = \boldsymbol{x}' - \boldsymbol{x}$$

は，$\boldsymbol{x}$ には依存しないある誤差分布 $g(\boldsymbol{e})$ (例えば正規分布) に従うものとし，このとき圧倒的確率で $\boldsymbol{e}$ の L_∞ ノルムは t 以下となるものとする．

4.1.2 中国人剰余定理に基く群同型写像

n 個の自然数 $w_1, \cdots, w_n$ を，

$$w_i \approx 1/(2t), \ \ \forall_{i \neq j} GCD(w_i, w_j) = 1 \tag{5}$$

となるよう選び，$W = \prod_{i=1}^{n} w_i$ とおく．整数ベクトル $\boldsymbol{v} = (v_1, \cdots, v_n)$, $\boldsymbol{w} = (w_1, \cdots, w_n)$ に対し，

$$\boldsymbol{v} \bmod \boldsymbol{w} = (v_1 \bmod w_1, \cdots, v_n \bmod w_n) \tag{6}$$

と定義し，

$$\boldsymbol{v}_1 \sim \boldsymbol{v}_2 \Leftrightarrow \boldsymbol{v}_1 \bmod \boldsymbol{w} = \boldsymbol{v}_2 \bmod \boldsymbol{w} \tag{7}$$

なる同値関係 $\sim$ による，群 $(\mathbb{Z}^n, +)$ の剰余類群を $\mathbb{Z}^n_{\boldsymbol{w}}$ と表すことにする．

写像 $f : \mathbb{Z}^n_{\boldsymbol{w}} \to \mathbb{Z}_W$ を以下の通り定義する．$\boldsymbol{v} = (v_1, \cdots, v_n) \in \mathbb{Z}^n_{\boldsymbol{w}}$ に対し，以下の連立合同式を考える．

$$\begin{aligned} V \bmod w_1 &= v_1, \\ &\cdots \\ V \bmod w_n &= v_n. \end{aligned} \tag{8}$$

この方程式の解 V は，W を法として唯一つ存在する (中国人剰余定理)．そこで $f(\boldsymbol{v}) = V$ として，写像 f を定義する．

明らかに，

$$f(\boldsymbol{v}_1 + \boldsymbol{v}_2) = f(\boldsymbol{v}_1) + f(\boldsymbol{v}_2) \tag{9}$$

が成立する (f の同型性)．

4.1.3 ファジー秘密鍵の符号化と誤り訂正

$\mathbb{Z}^n_{\boldsymbol{w}}$ と同様に，実数ベクトルの加法に関する群 $(\mathbb{R}^n, +)$ に対して式 (6)(7) で定義される同値類に関する剰余類群を $\mathbb{R}^n_{\boldsymbol{w}}$ とおく．ただし実数 y に対し，$r = y \bmod w_i$ は以下の条件を満たす実数と定義する．

$$\exists k \in \mathbb{Z}; y = kw_i + r, \ \ 0 \leq r < w_i. \tag{10}$$

関数 ϕ を以下の通り定義する．

$$\phi(\boldsymbol{x}) = (w_1 x_1, \cdots, w_n x_n) \in \mathbb{R}^n_{\boldsymbol{w}}. \tag{11}$$

ここで，$\phi(\boldsymbol{x} + \boldsymbol{e}) = \phi(\boldsymbol{x}) + \phi(\boldsymbol{e})$ が成立することに注意する．ϕ はある種の線形な符号化処理と見ることができる．

更に関数 $\psi : \mathbb{R}^n \to \mathbb{Z}^n$ を以下の通り定義する．

$$\psi((y_1, \cdots, y_n)) = (\lfloor y_1 + 0.5 \rfloor, \cdots, \lfloor y_n + 0.5 \rfloor) \tag{12}$$

ψ はある種の誤り訂正処理と見なすことができる．

$\boldsymbol{x}, \boldsymbol{x}' \in \mathcal{X}$ に対し $d(\boldsymbol{x}, \boldsymbol{x}') < t$ ならば

$$||\phi(\boldsymbol{x}) - \phi(\boldsymbol{x}')||_\infty < \max\{w_i\} t \approx \frac{1}{2}$$

(式 (5) より) なので，圧倒的確率で

$$\psi(\phi(\boldsymbol{x}) - \phi(\boldsymbol{x}')) = \boldsymbol{0}.$$

また $\boldsymbol{x} \in \mathbb{R}^n$, $\boldsymbol{s} \in \mathbb{Z}^n$ に対して

$$\psi(\boldsymbol{x} + \boldsymbol{s}) = \psi(\boldsymbol{x}) + \boldsymbol{s}$$

が成立する．

4.1.4 Modified Waters Signature

Waters Signature (WS) [8] は，標準モデルの下で選択文書攻撃に対する存在的偽造不能性 (EU-CMA) が証明可能な，効率的な電子署名方式として知られている．ここでは SFS の構成要素として，Waters Signature を僅かに修正した Modified Waters Signature (MWS) を用いる．以下 MWS の概要を説明する．

Setting

前述の整数 W(およそ k ビット) に対し，$W \mid p-1$ となる最小の素数 p を選ぶ．$\mathbb{G} = \langle g \rangle, \mathbb{G}_T$ をそれぞれ位数が p の巡回群とし，

$$e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$$

を双線形写像とする．$h \in \mathbb{Z}_p^\times$ を位数 W の元とし，

$$g_2, u' \in_R \mathbb{G}, \ \ U = \{u_1, \cdots, u_l\} \in_R \mathbb{G}^l$$

をそれぞれランダムに選択する．(h, g, g_2, u', U) を公開パラメータとする．

MWS における鍵生成，署名生成，検証アルゴリズムは以下の通り．

Gen_{MWS} : 鍵生成

$\beta \in_R \mathbb{Z}_W$ をランダムに選択して秘密鍵とし，$\alpha = h^\beta \in \mathbb{Z}_p^\times$, $g_1 = g^\alpha \in \mathbb{G}$ を計算し，g_1 を公開鍵とする．

Sig_{MWS} : 署名生成

メッセージ m のビット表現を $m = (m_1, \cdots, m_l)$ とし，$\mathcal{M} = \{i \mid m_i = 1\}$ とする．$r \in \mathbb{Z}_p^\times$ をランダムに選択し，署名 σ を以下の通り計算する．

$$\sigma = (\sigma_1, \sigma_2) = (g_2^{h^\beta} (u' \prod_{i \in \mathcal{M}} u_i)^r, g^r)$$

Ver_{MWS} : 検証

以下の等式の成立を検証する．

$$e(\sigma_1, g) = e(\sigma_2, u' \prod_{i \in \mathcal{M}} u_i) \cdot e(g_1, g_2).$$

Remark 1.

MWS において，β の代わりに $\alpha = h^\beta \in \mathbb{Z}_p^\times$ を秘密鍵としてもよい．この場合，WS と MWS の唯一の違いは，秘密鍵の選択方法にある．WS では $\alpha \in_R \mathbb{Z}_p$ を秘密鍵とするのに対し，MWS では 一旦 $\beta \in_R \mathbb{Z}_W$ を選択してから $\alpha = h^\beta$ を計算し，秘密鍵とする．このため MWS の秘密鍵空間は，WS の秘密鍵空間の部分集合となり，その割合は W/p である．従って MWS の EU-CMA を確率 ϵ_{MWS} で破るアルゴリズムがあれば，これを用いて WS の EU-CMA を確率

$$\epsilon_{WS} \geq \frac{W}{p}\epsilon_{MWS}$$

で破ることができる．つまり MWS の安全性は WS の安全性に帰着され，帰着効率は p/W である．p は $W|p-1$ なる最小の素数であり，また素数定理より整数 z 付近における素数の密度は凡そ $1/\ln z$ で評価できることから，$iW+1$ $(i = 1, 2.\cdots)$ が素数となる確率は i が W に対して十分小さいとき凡そ $1/\ln W$ で評価でき，帰着効率 p/W は平均的に $O(\ln W) = O(k)$ と考えられる．

Remark 2.

$\sigma = (\sigma_1, \sigma_2)$ に対して，$\sigma^r = (\sigma_1^r, \sigma_2^r)$ と書くことにする．このとき $(g_2^{h^\beta})^{h^{\beta_d}} = g_2^{h^{\beta+\beta_d}}$ より，$\sigma^{h^{\beta_d}}$ は $\beta' = \beta + \beta_d$ を秘密鍵とする m への正しい署名となっている．

4.2 アルゴリズム

Secure Fuzzy Signature のアルゴリズム $\Sigma = (\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$ は以下の通り．

4.2.1 鍵生成 (Gen)

入力: ファジー秘密鍵 $\boldsymbol{x} \in \mathcal{X}$， 出力: 公開鍵 pk

G1. $\boldsymbol{s} \in \mathbb{Z}_{\boldsymbol{w}}^n$ をランダムに選ぶ.

G2. $\beta = f(\boldsymbol{s})$, $g_1 = g^{h^\beta}$ とする.

G3. $\boldsymbol{c} = \phi(\boldsymbol{x}) + \boldsymbol{s} \bmod \boldsymbol{w} \in \mathbb{R}_{\boldsymbol{w}}^n$ とする.

G4. $pk = (g_1, \boldsymbol{c})$ を出力する.

ステップ G3 は，ファジー秘密鍵 $\boldsymbol{x}$ を，MWS の秘密鍵 β に対応するベクトル $\boldsymbol{s}$ でマスクして秘匿する操作 (あるいは逆に $\boldsymbol{s}$ を $\boldsymbol{x}$ でマスクする操作) とみなすことができる．

4.2.2 署名生成 (Sig)

入力: 平文 m, ファジー秘密鍵 $\boldsymbol{x}'$， 出力: 署名文 σ

S1. $\boldsymbol{s}' \in \mathbb{Z}_{\boldsymbol{w}}^n$ をランダムに選ぶ.

S2. $\beta' = f(\boldsymbol{s}')$, $g_1' = g^{h^{\beta'}}$ とする.

S3. $\tilde{\sigma} = \mathsf{Sig}_{MWS}(m, \beta')$

S4. $\boldsymbol{c}' = \phi(\boldsymbol{x}') + \boldsymbol{s}' \bmod \boldsymbol{w}$ とする.

S5. $\sigma = (\tilde{\sigma}, g_1', \boldsymbol{c}')$ を出力する.

4.2.3 検証 (Ver)

入力: 平文 m, 署名文 $\sigma = (\tilde{\sigma}, g_1', \boldsymbol{c}')$,
公開鍵 $pk = (g_1, \boldsymbol{c})$.
出力: 1(成功) or 0(失敗).

V1. $\mathsf{Ver}_{MWS}(m, \sigma, g_1') = 0$ なら 0 を出力して停止する.

V2. 以下の通り S_d を計算する.

$$\beta_d = f(\psi(\boldsymbol{c} - \boldsymbol{c}') \bmod \boldsymbol{w}) \tag{13}$$

V3. 以下の成立を検証する.

$$g_1 = (g_1')^{h^{\beta_d}}. \tag{14}$$

成立すれば 1，成立しなければ 0 を出力する.

4.3 正当性

ステップ V2 において，$d(\boldsymbol{x}, \boldsymbol{x}') < t$ ならば，またそのときに限って圧倒的確率で以下が成立する.

$$\begin{aligned}
\beta_d &= f(\psi((\boldsymbol{s} - \boldsymbol{s}') + (\boldsymbol{x} - \boldsymbol{x}')) \bmod \boldsymbol{w}) \\
&= f(\boldsymbol{s} - \boldsymbol{s}' + \psi(\boldsymbol{x} - \boldsymbol{x}') \bmod \boldsymbol{w}) \\
&= f(\boldsymbol{s} - \boldsymbol{s}' \bmod \boldsymbol{w}) \\
&= f(\boldsymbol{s}) - f(\boldsymbol{s}') \bmod W \\
&= \beta - \beta' \bmod W.
\end{aligned}$$

従って $d(\boldsymbol{x}, \boldsymbol{x}') < t$ ならば，ステップ V3 において以下が成立する.

$$\begin{aligned}
(g_1')^{h^{\beta_d}} &= (g^{h^{\beta'}})^{h^{\beta_d}} = g^{h^{\beta'} h^{\beta_d}} = g^{h^{\beta'+\beta_d}} \\
&= g^{h^\beta} = g_1.
\end{aligned}$$

従って Ver は，$d(\boldsymbol{x}, \boldsymbol{x}') < t$ のとき圧倒的確率で 1 を出力し，それ以外のとき圧倒的確率で 0 を出力する.

β を MWS の秘密鍵と見なすと，β_d は，登録時の秘密鍵と署名生成時に一時的にランダムに生成した秘密鍵との「差」に相当する．SFS の検証アルゴリズムは，ファジー秘密鍵 $\boldsymbol{x}, \boldsymbol{x}'$ を秘密鍵に対応するベクトル $\boldsymbol{s}, \boldsymbol{s}'$ でマスクして秘匿する操作 (ベクトルの加算) の線形性と，ベクトル $\boldsymbol{s}, \boldsymbol{s}'$ を MWS の秘密鍵 β, β' へ対応させる写像 f の同型性，MWS の公開鍵 $g_1 = g^{h^\beta} \bmod p$ が秘密鍵 β の加法に対して持つ準同型性を利用している.

4.4 安全性

Theorem 1. *Waters Signature* が *EU-CMA* 安全ならば，*Secure Fuzzy Signature* Σ も *EU-CMA* 安全.

Proof. 前記 MWS の Remark 1 より，MWS の安全性は WS の安全性に帰着される．そこで以下では SFS Σ の安全性を MWS の安全性に帰着させる事を目標に，SFS の EU-CMA を破る攻撃者 $\mathcal{A}$ を用いて，MWS の EU-CMA を破る挑戦者 $\mathcal{C}$ を構成する.

初期設定: MWS の公開パラメータを (h, g, g_2, u', U) とし，公開鍵を $g_1 = g^{h^\beta} \in \mathbb{G}$，秘密鍵を $\beta \in \mathbb{Z}_W$ とする．β は挑戦者 $\mathcal{C}$ には知らされない．$\mathcal{C}$ は

$$\boldsymbol{c} \in_R \mathbb{R}^n_{\boldsymbol{w}}$$

をランダムに選択し，$pk = (g_1, \boldsymbol{c})$ を公開鍵として，上記パラメータとともに攻撃者 $\mathcal{A}$ に入力する．ここで，

$$\boldsymbol{x} = \phi^{-1}(\boldsymbol{c} - f^{-1}(\beta))$$

とおくと，pk は $\boldsymbol{x}$ をファジー秘密鍵，β を登録時の MWS 秘密鍵とする Σ の公開鍵であり，$\boldsymbol{x}$ は $\mathcal{X}$ 上一様分布（真のファジー秘密鍵の分布に一致）であることに注意する．

質問フェーズ: $\mathcal{A}$ が Σ 署名オラクルに対してメッセージ m_j を聞いたら，$\mathcal{C}$ はまず MWS 署名オラクルに m_j を問い合わせ，署名 $\hat{\sigma}_j$ を得る．

次に $\beta_d \in_R \mathbb{Z}_W$ をランダムに選び，$\boldsymbol{e}$ を誤差分布 $g()$ に従ってランダムに生成する．

$$\sigma_j = (\tilde{\sigma}, g_1', \boldsymbol{c}') = ((\hat{\sigma}_j)^{h^{\beta_d}}, g_1^{h^{\beta_d}}, \boldsymbol{c} + f(\beta_d) + \phi(\boldsymbol{e}) \bmod \boldsymbol{w})$$

を計算し，m_j に対する署名として $\mathcal{A}$ に返す．

ここで σ_j は，

$$\boldsymbol{x'} = \boldsymbol{x} + \boldsymbol{e}$$

を署名時のファジー秘密鍵とし，$\beta' = \beta + \beta_d \bmod W$ を署名時の秘密鍵とする，Σ の正しい署名となる．

回答: $\mathcal{A}$ が $(m^*, \sigma^* = (\tilde{\sigma}^*, g_1^*, \boldsymbol{c}^*))$ を出力したら，$\mathcal{C}$ は

$$\beta_d^* = f(\psi(\boldsymbol{c} - \boldsymbol{c}^*) \bmod \boldsymbol{w})$$

を計算する．$\beta^* = \beta - \beta_d^*$ とすると，$\tilde{\sigma}^*$ は m^* に対する秘密鍵 β^* による正しい署名となっている．

従って上記 MWS の Remark 2 より，

$$\hat{\sigma}^* = (\tilde{\sigma}^*)^{h^{\beta_d^*}}$$

は，m^* に対する秘密鍵 β による正しい署名となっている．そこで $\mathcal{C}$ は，$(m^*, \hat{\sigma}^*)$ を出力する． □

5 PBI への適用可能性

筆者らは SCIS2012 において，IC カードなどの所有物や，暗証番号・パスワードのような記憶を必要としない，生体認証に基づく個人認証基盤として，PBI (Public Biometrics Infrastructure) の概念を提案し，その機能要件を整理した．

5.1 PBI モデル

PBI のシステムモデルを図 3 に示す．PBI システムは，バイオメトリック認証局 (BCA: Biometric Certificate Authority) とリポジトリから構成される．本モデルは，

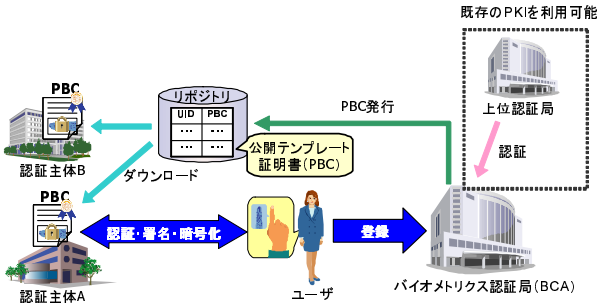

図 3: PBI モデル

PKI における秘密鍵の代わりに生体情報，公開鍵の代わりに公開テンプレートを用いることを除けば，PKI と同様である．登録，認証，暗号，署名の各処理の流れは以下の通りである．

登録

- BCA はユーザの本人確認を行った上で生体情報 $\boldsymbol{x}$ を取得し，これに基づいて公開テンプレート pk を作成する
- BCA は pk とユーザ ID(UID)，有効期限等の情報の組に対して署名を付与し，公開テンプレート証明書 (PBC: Public Biometric Certificate) として発行する．
- BCA は PBC をリポジトリに登録し，公開する．

認証

- ユーザが認証端末を介して認証主体に UID と認証要求を送る．
- 認証主体は，UID をキーとしてリポジトリから PBC を取得し，署名検証と有効期限等のチェックを行う．
- 認証主体はユーザ（の認証端末）と対話的通信（チャレンジレスポンス）を行い，ユーザが確かに $\boldsymbol{x}$ に十分近い生体情報 $\boldsymbol{x}'$ を持っていることを，pk を用いて確認する．

暗号

- 送信者は，リポジトリから受信者の PBC を取得し，署名検証と有効期限等のチェックを行う．
- 送信者は，pk を用いて平文 m を暗号化し，受信者へ送信する．
- 受信者は自分の生体情報 $\boldsymbol{x}'$ を用いて暗号文を復号化する．

署名

- 署名作成者は，平文 m に対して自分の生体情報 $\boldsymbol{x}'$ を用いて署名文 σ を作成する．
- 署名検証者は，リポジトリから署名作成者の PBC

を取得し，署名検証と有効期限等のチェックを行う．

- 署名検証者は，pk を用いて平文と署名文の組 (m, σ) を検証する．

なお BCA や更にその上位の CA による証明書の階層構造には，従来の公開鍵暗号と PKI の仕組みを用いることができる．

5.2 各機能の要件

PBI の主目的は，PKI における秘密鍵を生体情報で置き換えることにより，エンドユーザによる秘密鍵の管理を不要とし，IC カードやパスワードが不要なセキュリティ基盤を実現することにある．このため PBI の認証，暗号，署名機能は以下の要件を満たさなくてはならない．

なお以下では，生体情報 $\boldsymbol{x}, \boldsymbol{x}'$ の間の距離がある距離関数 $d(\cdot,\cdot)$ を用いて評価され，ある閾値 t に対して $d(\boldsymbol{x}, \boldsymbol{x}') < t$ のとき $\boldsymbol{x}, \boldsymbol{x}'$ は「一致」（同一ユーザの生体情報）と判定すべきものとする．

登録機能要件

(R1) 登録機能は，生体情報 $\boldsymbol{x}$ を入力とし，公開テンプレート pk を出力する PPTA $pk = \mathsf{Gen}(\boldsymbol{x})$ で表現できること．

(R2) pk から $\boldsymbol{x}$ が復元あるいは推定できないこと．

認証機能要件

(R3) 認証機能は，生体情報 $\boldsymbol{x}'$ を入力とするユーザ側の PPTA P と，pk を入力とし 1(受理) 又は 0(拒否) を出力する認証主体側の PPTA V から成るプロトコル $<\mathsf{P}(\boldsymbol{x}'), \mathsf{V}(pk)>$ として表現できること．

(R4) (完全性:) V は，$^{\exists}\boldsymbol{x}; pk = \mathsf{Gen}(\boldsymbol{x}) \wedge d(\boldsymbol{x}, \boldsymbol{x}') < t$ のとき十分高い確率（圧倒的確率）で 1 を出力すること．

(R5) (健全性:) V は，$\neg(^{\exists}\boldsymbol{x}; pk = \mathsf{Gen}(\boldsymbol{x}) \wedge d(\boldsymbol{x}, \boldsymbol{x}') < t)$ のとき圧倒的確率で 0 を出力すること．なお攻撃者の条件に関しては従来の認証プロトコルの安全性モデルに準じるものとする．

暗号機能要件

(R6) 暗号化機能は，平文 m と公開テンプレート pk を入力とし，暗号文 c を出力する PPTA $c = \mathsf{Enc}(m, pk)$ で表現できること．

(R7) 復号化機能は，暗号文 c と生体情報 $\boldsymbol{x}'$ を入力とし，平文 m' を出力する PPTA $m' = \mathsf{Dec}(c, \boldsymbol{x}')$ で表現できること．

(R8) (正当性:) $^{\exists}\boldsymbol{x}; pk = \mathsf{Gen}(\boldsymbol{x}) \wedge d(\boldsymbol{x}, \boldsymbol{x}') < t$ のとき圧倒的確率で $m' = m$ となること．

(R9) (秘匿性:) $^{\exists}\boldsymbol{x}; pk = \mathsf{Gen}(\boldsymbol{x}) \wedge d(\boldsymbol{x}, \boldsymbol{x}') < t$ なる $\boldsymbol{x}'$ を知らない攻撃者は，$c = \mathsf{Enc}(m, pk)$ から m の部分情報を得ることができないこと．なお攻撃者の条件や目的など安全性モデルの詳細は従来の公開鍵暗号に準じるものとする．

署名機能要件

(R10) 署名作成機能は，平文 m と生体情報 $\boldsymbol{x}'$ を入力とし，署名文 σ を出力する PPTA $\sigma = \mathsf{Sig}(m, \boldsymbol{x}')$ で表現できること．

(R11) 署名検証機能は，平文 m, 署名文 σ, 公開テンプレート pk を入力とし，1(成功) 又は 0(失敗) を出力する PPTA $\mathsf{Ver}(m, \sigma, pk)$ で表現できること．

(R12) (正当性:) $^{\exists}\boldsymbol{x}; pk = \mathsf{Gen}(\boldsymbol{x}) \wedge d(\boldsymbol{x}, \boldsymbol{x}') < t$ のとき圧倒的確率で $\mathsf{Ver}(m, \sigma, pk) = 1$ となること．

(R13) (安全性:) $\neg(^{\exists}\boldsymbol{x}; pk = \mathsf{Gen}(\boldsymbol{x}) \wedge d(\boldsymbol{x}, \boldsymbol{x}') < t)$ のとき圧倒的確率で $\mathsf{Ver}(m, \sigma, pk) = 0$ となること．なお攻撃者の条件や目的など安全性モデルの詳細は従来の電子署名に準じるものとする．

なお前述の認証機能は，署名機能を用いて実現することができる．具体的には V がランダムな平文 m（チャレンジ）を P へ送信し，P は $\sigma = \mathsf{Sig}(m, \boldsymbol{x}')$ を作成して送り返す（レスポンス）．V は $\mathsf{Ver}(m, \sigma, pk)$ を出力する．つまり署名検証に成功したら認証を受理，そうでなければ拒否する．

更に，生体情報は，その統計的性質として以下の要件を満たさなくてはならない．

生体情報の要件

(R14) 生体情報 $\boldsymbol{x}, \boldsymbol{x}'$ が同一の生体から取得されたものであるとき，これが一致しない確率

$$FRR = \Pr(d(\boldsymbol{x}, \boldsymbol{x}') \geq t \mid \boldsymbol{x}, \boldsymbol{x}'\text{は同一生体})$$

が十分小さいこと．

(R15) 生体情報 $\boldsymbol{x}, \boldsymbol{x}'$ が異なる生体から取得されたものであるとき，これが一致する確率

$$FAR = \Pr(d(\boldsymbol{x}, \boldsymbol{x}') < t \mid \boldsymbol{x}, \boldsymbol{x}'\text{は異なる生体})$$

が十分小さいこと．

なお PBI を実現する場合，FAR は一般的な生体認証において要求される値よりも遥かに小さく (例えば $FAR < 2^{-80}$) なくてはならない．なぜなら PBI ではテンプレート pk が公開されるため，攻撃者は適当な生体情報 $\boldsymbol{x}'$ と pk を入力として認証機能を実行し，失敗したら別の生体情報 $\boldsymbol{x}''$ を試す，という試行を繰り返す単純な総当り攻撃 (FAR 攻撃) を実行することが可能であり，その 1 回あたりの攻撃成功確率は FAR となるためである．

従来の生体認証システムは FAR 攻撃に対して，一定回数連続して認証失敗した場合にアカウントをロックするといったシステム的対策によって対処可能である．し

かし PBI では攻撃者はシステムに対して認証要求を出すことなく（オフラインで）FAR 攻撃を実行することが可能であることに注意が必要である．

(R14)(R15) を満たすことは，単独の生体情報 (例えば 1 本の指の指紋) を用いる限り極めて困難であり，従って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．

5.3 Secure Fuzzy Signature の適用可能性

前章で提案した SFS は，生体特徴量をファジー秘密鍵とし，公開鍵を公開テンプレートとして用いることで，PBI の登録機能要件 (R1)(R2) および署名機能要件 (R10) (R11) (R12) (R13) を全て満たし，PBI を実現する要素技術として利用可能である．ただし署名の安全性要件 (R13) に関しては，前章で述べた Secure Fuzzy Signature のファジー秘密鍵に関する前提条件が満たされることが必要である．特に，(1) ファジー秘密鍵が $\mathcal{X}$ 上一様分布であること，(2) ファジー秘密鍵間の距離が L_∞ で計算できること (更にその場合に本人拒否率を実用的なレベルまで小さくできること)，(3) セキュリティパラメータ k が十分な大きさを持つこと，が重要である．

一般に生体情報の特徴量は，特徴量空間上で一様分布するとは限らず，また距離が L_∞ で定義されるとは限らない．このため特徴量に何らかの変換を施すことで，ある別の空間 $\mathcal{X}$ 上で一様分布となり，かつ距離を L_∞ で定義しても本人拒否率が十分小さくなり，更にセキュリティパラメータ k が十分な大きさを保つようにする必要がある．個々のモダリティ(指紋，静脈など) に対して，こうした特徴量変換の具体的なアルゴリズムを与えることは，今後の課題である．特に (3) の前提条件を満たすためには，生体情報自体のエントロピーが十分に大きい必要があり，複数の生体情報（例えば複数指の指紋）を組合わせるなどの方策を採る必要があると考える．

なお SFS を用いて PBI における電子署名が実現できれば，認証も容易に実現できる．また FE を用いることで原理的には PBI における公開鍵暗号も実現可能であり，SFS とあわせて PBI の全ての機能を実現可能になると考えられる．

6 まとめ

本稿では，整数格子に基づく Fuzzy Commitment と Waters Signature，中国人剰余定理を利用することで，秘密鍵に曖昧さを許す電子署名方式 Secure Fuzzy Signature (SFS) を構築し，その安全性を Waters Signature の安全性へ帰着することで，標準モデルの下での安全性証明を与えた．また生体情報を秘密鍵とする PKI として筆者らが提案している Public Biometrics Infrastructure (PBI) への適用可能性を検討し，SFS が PBI の登録機能要件，署名機能要件を満たすことを明らかにした．ただし生体情報を秘密鍵とした SFS の安全性を保証するためには，生体特徴量をファジー秘密鍵へ変換する関数であって，(1) ファジー秘密鍵が $\mathcal{X}$ 上一様分布であること，(2) 特徴量間の距離が L_∞ で計算できること，(3) セキュリティパラメータ k が十分な大きさを持つこと，を満たすものを構成する必要がある．指紋，静脈など具体的なモダリティに対してこうしたアルゴリズムを構成することが今後の課題である．

謝辞

本成果の一部は総務省委託研究「災害に備えたクラウド移行促進セキュリティ技術の研究開発」によるものです．

参考文献

[1] Y. Dodis, L. Reyzin, and A. Smith. Fuzzy extractors: how to generate strong keys. In *Eurocrypt 2004*, 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: ACM Press, 2004.

[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] A. Juels and M. Wattenberg. A fuzzy commitment scheme. In *Proc. ACM CCS1999*, pp. 28–36, 1999.

[6] A. Juels and M. Sudan. A fuzzy vault scheme. In *Proc. IEEE Int. Symposium on. International Symposium on Information Theory (ISIT)*, 2002.

[7] 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.

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