文字位置の交換を可能とする鍵付き準同型署名方式

小関 義博† 川合 豊†

† 三菱電機株式会社 情報技術総合研究所
247-8501 神奈川県鎌倉市大船 5-1-1
Koseki.Yoshihiro@ak.MitsubishiElectric.co.jp
Kawai.Yutaka@da.MitsubishiElectric.co.jp

あらまし 準同型署名とは，あるメッセージに対して生成された署名から，述語として定義された一定の関係性をもつ別のメッセージに対する署名を秘密鍵を用いることなく生成することが可能な方式である．本稿では，文字列の文字位置の並べ替えを述語として有する準同型署名を扱い，同時に鍵付き準同型署名の概念を提案する．本方式では隣の文字との位置を交換するのに必要となる準同型演算用の鍵が各文字位置毎に生成される．これらの鍵を適切なユーザに配布することによって，準同型演算の権限を制御することが可能となる．本方式は双対ペアリングベクトル空間上に構成され，基底変換の技法を用いることで実現される．

Keyed Homomorphic Signatures for String Permutation

Yoshihiro Koseki† Yutaka Kawai†

†Mitsubishi Electric Information Technology R&D Center
5-1-1, Ofuna, Kamakura City, 247-8501, Japan
Koseki.Yoshihiro@ak.MitsubishiElectric.co.jp
Kawai.Yutaka@da.MitsubishiElectric.co.jp

Abstract In homomorphic signature scheme, signatures for some messages can be used to create a new signature without using secret key as long as the message is related to the original messages under specified rules defined as a predicate. In this paper, we focus on the homomorphic signature scheme for string permutation predicate and we propose a concept of keyed homomorphic signature scheme. In our scheme, homomorphic operation keys are created for each index in the string. Keys are necessary to exchange the index with next character. Distributing these keys to appropriate users, we can control the authority of the homomorphic operation. We constructed scheme over dual paring vector space and used a technique of basis conversion.

1 初めに

背景 近年，クラウドなどの第三者が提供するサーバ上での大規模データの収集とその活用が重要性を増していくとともに，それらのデータを安全に活用するための暗号技術の開発も重要性を増してきている．特に，秘匿性や認証を維持したままデータに対して計算を施すことを可能とする，準同型性を有した暗号方式の研究が盛んに行われている．データに対する認証を維持したまま，計算を行うことを可能とする暗号技術の一つとして準同型署名が存在する．通常の電子署名では，メッセージの完全性を保証するために，一度メッセージに対しての署名が秘

密鍵を用いて生成された後は，メッセージに対していかなる改変を加えた場合であっても，署名が受理されることは無い．つまり一度，認証を行ったデータに対してはいかなる計算も施すことはできない．準同型署名は上記の制約を緩和し，メッセージに対して一定の範囲での改変を可能とし，それによって認証を行ったデータに対しても計算を行うことを可能とする技術である．準同型署名では，メッセージに対して許される改変の種類毎に異なる方式が考えられるため，Jhonson ら [6] によって最初に準同型署名の概念が提案された後，さまざまな方式の研究が行われた [10, 2, 4, 5]．その後，Ahn ら [1] によってこれらの方式を統一的に扱うフレームワークとして方式の有する準同型性を述語 P によって表現することで，さまざまな準同型性を扱う P-準同型署名の概念が提案されるとともに，準同型署名におけるプライバシの概念として文脈秘匿性 (Context Hiding) が提案された．

貢献　応用する対象毎に異なる種類の準同型性が必要となるため，準同型署名ではより多くの種類の述語に対して方式が構成されることが重要となる．本稿では，これまでに実現されていない新たな述語として文字列に対する文字位置交換を述語として有する準同型署名を実現する．また，従来の準同型署名では署名を有する者は自由に準同型演算を実行可能なため，特定の者にのみ準同型演算を許可するといった制御を行うことは出来ない．本稿では従来の P-準同型署名の拡張として準同型演算の実行に必要となる鍵を生成し，それらを適切なユーザに配布することによって準同型演算の権限を制御することのできる鍵付き準同型署名の概念を新たに提案した．そのうえで文字列に対する文字位置の交換を述語として持つ鍵付き準同型署名を実際に構成した．本方式は，鍵付き準同型署名として偽造不可能性を有するとともに，Attrapadung ら [3] によって複数種類定義された文脈秘匿性の内，計算量理論的安全性として最も強い安全性である適応的文脈秘匿性 (Adaptively Context Hiding) を有する．本稿で構成する準同型署名は，岡本-高島によって提案された Dual Paring Vector Space を用いて構成され，文字位置の交換は文献 [8, 9, 7] 等において用いられている基底変換の技法を応用することで実現される．

2　準備

記法　A が分布であるときに $y \xleftarrow{\mathsf{R}} A$ は y を A からその分布に従ってランダムに選ぶことを指す．A が集合であるときに，$y \xleftarrow{\mathsf{U}} A$ は y を A から一様に選ぶことを指す．位数 q の有限体を $\mathbb{F}_q$ と表し，$\mathbb{F}_q \setminus \{0\}$ を $\mathbb{F}_q^\times$ と表す．$\mathbb{F}_q$ 上のベクトル $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$ を $\vec{x}$ と表記する．二つのベクトル $\vec{x}$ と $\vec{v}$ の内積 $\sum_{i=1}^n x_i v_i$ を $\vec{x} \cdot \vec{v}$ と表す．$\mathbb{F}_q^n$ での零ベクトルを $\mathbf{0}$ と表す．X^{T} は行列 X の転置行列を表し，I_ℓ と 0_ℓ はそれぞれ ℓ 行 ℓ 列の単位行列と零行列を指す．ベクトル空間 $\mathbb{V}$ の要素は $\boldsymbol{x} \in \mathbb{V}$ と表す．$\boldsymbol{b}_i \in \mathbb{V}$ $(i = 1, \ldots, n)$ である時，$\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ によって作られる部分空間は $\mathsf{span}\langle \boldsymbol{b}_1, \ldots, \boldsymbol{b}_n \rangle \subseteq \mathbb{V}$ と表される．また，$\mathbb{B} := (\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n)$ と $\mathbb{B}^* := (\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_n^*)$ に対して，$(x_1, \ldots, x_n)_{\mathbb{B}} := \sum_{i=1}^n x_i \boldsymbol{b}_i$，及び $(y_1, \ldots, y_n)_{\mathbb{B}^*} := \sum_{i=1}^n y_i \boldsymbol{b}_i^*$ と定義する．$\vec{e}_j$ は $(\overbrace{0 \cdots 0}^{j-1}, 1, \overbrace{0 \cdots 0}^{n-j}) \in \mathbb{F}_q^n$ $(j = 1, \ldots, n_t)$ を指す．また，$GL(n, \mathbb{F}_q)$ は次元 n の $\mathbb{F}_q$ 上の一般線形群を指す．

Dual Pairing Vector Spaces (DPVS)

定義 1 (対称ペアリング群)：対称ペアリング群 $(q, \mathbb{G}, \mathbb{G}_T, G, e)$ は素数 q，位数 q の加法的巡回群 $\mathbb{G}$ と乗法的巡回群 $\mathbb{G}_T$ 及び $G \neq 0 \in \mathbb{G}$ と多項式時間で計算可能な非退化性を持つ双線形写像 $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ からなる．セキュリティパラメータ 1^λ を入力として上記対称ペアリング群 $(q, \mathbb{G}, \mathbb{G}_T, G, e)$ を出力するアルゴリズムを $\mathcal{G}_{\mathsf{bpg}}$ と書く．

定義 2 (Dual pairing vector spaces)：$DPVS$ $(q, \mathbb{V}, \mathbb{G}_T, \mathbb{A}, e)$ は位数 q，$\mathbb{F}_q$ 上の N 次元ベクトル空間 $\mathbb{V} := \overbrace{\mathbb{G} \times \cdots \times \mathbb{G}}^{N}$，位数 q の巡回群 $\mathbb{G}_T$，$\mathbb{V}$ の標準基底 $\mathbb{A} := (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_N)$（但し $\boldsymbol{a}_i := (\overbrace{0, \ldots, 0}^{i-1}, G, \overbrace{0, \ldots, 0}^{N-i})$）とペアリング演算 $e : \mathbb{V} \times \mathbb{V} \to \mathbb{G}_T$ から構成される．

ここで，N 次元ベクトル $\boldsymbol{x} := (G_1, \ldots, G_N) \in \mathbb{V}$ と $\boldsymbol{y} := (H_1, \ldots, H_N) \in \mathbb{V}$ のペアリング演算 $e(\boldsymbol{x}, \boldsymbol{y})$ を $e(\boldsymbol{x}, \boldsymbol{y}) := \prod_{i=1}^N e(G_i, H_i) \in \mathbb{G}_T$ と定義する．また，上記演算は非退化性をもつ．$e(G, G) \neq 1 \in \mathbb{G}_T$ であれば任意の i と j に対

して，$e(\boldsymbol{a}_i, \boldsymbol{a}_j) = e(G,G)^{\delta_{i,j}}$ である．ここで $\delta_{i.j}$ は $i = j$ の時に $\delta_{i.j} = 1$ であり，$i \neq j$ の時 $\delta_{i.j} = 0$ である．*DPVS* 生成アルゴリズム $\mathcal{G}_{\mathsf{dpvs}}$ は，セキュリティパラメータ $1^\lambda (\lambda \in \mathbb{N})$ と $\mathbb{V}$ の次元 $N \in \mathbb{N}$ を入力として，$\mathsf{param}'_{\mathbb{V}} := (q, \mathbb{V}, \mathbb{G}_T, \mathbb{A}, e)$ を出力する．このアルゴリズムは $\mathcal{G}_{\mathsf{bpg}}$ から構成することができる．

Dual Orthonormal Basis Generator 以下に，本方式で用いる双対基底生成器（dual orthonormal basis generator）を示す．

$\mathcal{G}_{\mathsf{ob}}(1^\lambda, N_0, N_1)$:
$\mathsf{param}_{\mathbb{G}} := (q, \mathbb{G}, \mathbb{G}_T, G, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{bpg}}(1^\lambda)$,
$\psi \xleftarrow{\mathsf{U}} \mathbb{F}_q^\times, g_T := e(G,G)^\psi$,
for $t = 0, 1$
$\mathsf{param}_{\mathbb{V}_t} := (q, \mathbb{V}_t, \mathbb{G}_T, \mathbb{A}_t, e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{dpvs}}(1^\lambda, N_t)$,
$X_t := (\chi_{t,i,j})_{i,j} \xleftarrow{\mathsf{U}} GL(N_t, \mathbb{F}_q)$,
$(\vartheta_{t,i,j})_{i,j} := \psi \cdot (X_t^{\mathrm{T}})^{-1}$,
$\boldsymbol{b}_{t.i} := \sum_{j=1}^{N_t} \chi_{t,i,j} \boldsymbol{a}_{t,j}, \mathbb{B}_t := (\boldsymbol{b}_{t.1}, \ldots, \boldsymbol{b}_{t.N_t})$,
$\boldsymbol{b}^*_{t.i} := \sum_{j=1}^{N_t} \vartheta_{t,i,j} \boldsymbol{a}_{t,j}, \mathbb{B}^*_t := (\boldsymbol{b}^*_{t.1}, \ldots, \boldsymbol{b}^*_{t.N_t})$,
$\mathsf{param} := (\{\mathsf{param}_{\mathbb{V}_t}\}_{t=0,1}, g_T)$,
return $(\mathsf{param}_{\vec{n}}, g_T, \{\mathbb{B}_t, \mathbb{B}^*_t\}_{t=0,1})$.

3 鍵付き準同型署名

本章では，鍵付き準同型署名を定義する．本定義は文献 [1] で定義されている P-準同型署名の定義を基にしており，通常の P-準同型署名における署名鍵，検証鍵に加えて準同型演算に必要となる準同型演算鍵を導入する．

3.1 モデル

まず準同型署名の定義において用いる述語，述語の和，導出可能メッセージについて定義する．

定義 3 (述語，述語の和) :
メッセージ空間 $\mathcal{M}$ 上の述語 P を $P : 2^{\mathcal{M}} \times \mathcal{M} \to \{0,1\}$ と定義する．また，述語 P_1, P_2 に対して述語 $P_1 \cup P_2 : 2^{\mathcal{M}} \times \mathcal{M} \to \{0,1\}$ を $P_1(M,m) = 1$ または $P_2(M,m) = 1$ の場合に $P_1 \cup P_2(M,m) = 1$ となる述語として定義する．同様に要素数 *3* 以上の述語の集合 S に対して，$(\cup_{P_i \in S} P_i) : 2^{\mathcal{M}} \times \mathcal{M} \to \{0,1\}$ を，いずれかの $P_i \in S$ に対して $P_i(M,m) = 1$ となる場合に $(\cup_{P_i \in S} P_i)(M,m) = 1$ となる述語として定義する．

定義 4 (導出可能メッセージ) :
メッセージ空間 $\mathcal{M}$ 上の述語 $P : 2^{\mathcal{M}} \times \mathcal{M} \to \{0,1\}$ に対して，$P(M,m') = 1$ の時，メッセージ m' は $M \subset \mathcal{M}$ から導出されると定義する．$P^i(M)$ を $P^{i-1}(M)$ から導出されるメッセージの集合とし，$P^0(M) := \{m' \in \mathcal{M} | P(M,m') = 1\}$ とする．このとき $P^*(M) := \cup_{i=0}^{\infty} P^i(M)$ を Mに対する導出可能メッセージとして定義する．

次に鍵付き準同型署名について定義する．本稿で提案する鍵付き準同型署名では，通常の準同型署名方式に加えて準同型演算に必要となる準同型演算鍵が生成される．また本稿で定義される方式は，述語集合 S に対して定義され，準同型演算鍵を複数生成し鍵ごとに述語を割り当てることで，各準同型演算鍵ごとに異なる準同型性に対応させる方式として定義される．

定義 5 (鍵付き準同型署名) :
述語集合 S，メッセージ空間 $\mathcal{M}$ に対する鍵付き準同型署名は以下の *4* つのアルゴリズムから構成される．

KeyGen: セキュリティパラメータ 1^k を入力として，検証鍵 vk，署名鍵 sk，準同型演算鍵 $\{\mathsf{hk}_{P_i}\}$ を生成するアルゴリズム．

Sign: 署名鍵 sk と，メッセージ m を入力として，署名 σ を生成するアルゴリズム．

Derive: 準同型演算鍵 hk_{P_i} と，メッセージ・署名ペアの集合 $\{m_i, \sigma_i\}_{m_i \in M}$ と導出メッセージ m' を入力として，$P_i(M,m') = 1$ の場合に導出署名 σ' を，それ以外の場合に $\perp$ を出力するアルゴリズム．

Verify: 検証鍵 vk とメッセージ m，署名 σ を入力として受理ならば *1* を，そうでなければ *0* を出力するアルゴリズム．

正当性 KeyGen によって生成された任意の鍵の組 $\mathsf{vk}, \mathsf{sk}, \{\mathsf{hk}_{P_i}\}$ と，任意の $M \in \mathcal{M}$ と $m' \in \mathcal{M}$ に対して $P_i(M,m') = 1$ のとき，以下の 3 つの条件が成り立つことを要する．

・$\mathsf{Derive}(\mathsf{hk}_{P_i}, \{m_i, \mathsf{Sign}(\mathsf{sk}, m_i)\}, m') \neq \perp$
・$\mathsf{Verify}(vk, m, \mathsf{Sign}(\mathsf{sk}, m)) = 1$
・$\mathsf{Verify}(vk, m', \mathsf{Derive}(\mathsf{hk}_{P_i}, \{m_i, \sigma_i\}, m')) = 1$

3.2 セキュリティ

本章では，鍵付き準同型署名に対する安全性として偽造不可能性 (Unforgeability) と文脈秘匿性 (Context Hiding) を定義する．本稿では複数存在する文脈秘匿性の定義の内，計算量理論的安全性として最も強い定義である適応的文脈秘匿性 (Adaptively Context Hiding) を扱う．

定義 6 (偽造不可能性) 鍵付き準同型署名方式 Π が選択メッセージ攻撃に対する存在的偽造不可能性 (EUF-CMA) を持つとは，いかなる多項式時間攻撃者 $\mathcal{A}$ に対しても下記の EUF-CMA ゲームにおいて，$\mathsf{Succ}(k)$ が k に対して無視できることをいう．

セットアップ: チャレンジャーは $(\mathsf{vk}, \mathsf{sk}, \{\mathsf{hk}_{P_i}\}) \xleftarrow{\mathsf{R}} \mathsf{KeyGen}(1^k)$ を実行し，攻撃者 $\mathcal{A}$ に対して vk を与え，集合 T, Q, R を空にしてセットする．

クエリ: 攻撃者 $\mathcal{A}$ は，多項式回のクエリを許される．

署名クエリ: $\mathcal{A}$ がメッセージ $m \in \mathcal{M}$ をクエリしてきたならば，チャレンジャーはユニークなハンドル h を生成し $\mathcal{A}$ に与え，$\sigma \xleftarrow{\mathsf{R}} \mathsf{Sign}(m, \mathsf{sk})$ を計算し，(h, m, σ) を T に保存する．

導出クエリ: $\mathcal{A}$ がハンドルの集合 $\{h_i\}$ とメッセージ $m' \in \mathcal{M}$，述語 $P_i \in S$ をクエリしてきたならば，チャレンジャーは T から (h_i, m_i, σ_i) を取り出す．該当する要素が T に存在しない，あるいは $P_i(\{m_i\}, m') = 0$ ならば $\perp$ を $\mathcal{A}$ に与える．そうでない場合は，ユニークなハンドル h' を生成し $\mathcal{A}$ に与え，$\sigma' \xleftarrow{\mathsf{R}} \mathsf{Derive}(m, \{m_i, \sigma_i\}, \mathsf{hk}_{P_i})$ を計算し，(h', m', σ') を T に保存する．

署名出力クエリ: $\mathcal{A}$ がハンドル h を入力してきたならばチャレンジャーは $(h, m, \sigma) \in T$ を $\mathcal{A}$ に与え，(m, σ) を Q に保存する．このとき h が T に含まれない場合は，$\mathcal{A}$ に $\perp$ を与える．

鍵出力クエリ: $\mathcal{A}$ が述語 $P_i \in S$ を入力してきたならば，hk_{P_i} を $\mathcal{A}$ に与え，P_i を R に保存する．

アウトプット: $\mathcal{A}$ は，(m, σ) を出力する．次の 2 条件が満たされた場合を $\mathcal{A}$ の勝利とし，$\mathcal{A}$ の勝利する確率を $\mathsf{Succ}(k)$ とする．

- $\mathsf{Verify}(\mathsf{vk}, m, \sigma) = 1$
- $m \notin (\cup_{P_i \in R} P_i)^*(\{m | (m, \cdot) \in Q\})$

定義 7 (文脈秘匿性) 鍵付き準同型署名方式 Π が適応的文脈秘匿性を持つ (Adaptively Context Hiding) とは，いかなる多項式時間攻撃者 $\mathcal{A}$ に対しても下記のゲームにおいて $\mathsf{Adv}(k)$ が k に対して無視できることを言う．

セットアップ: チャレンジャーは $(\mathsf{vk}, \mathsf{sk}, \{\mathsf{hk}_{P_i}\}) \xleftarrow{\mathsf{R}} \mathsf{KeyGen}(1^k)$ を実行し，攻撃者 $\mathcal{A}$ に対して $(\mathsf{vk}, \mathsf{sk}, \{\mathsf{hk}_{P_i}\})$ を与える．

チャレンジ: $\mathcal{A}$ は，メッセージの集合 $\{m_i\}$ と，署名の集合 $\{\sigma_i\}$ と署名鍵 hk_{P_i} とメッセージ m' をチャレンジャーに出力する．このとき，もし $P_i(M, m') = 0$ あるいはいずれかの i に対して $\mathsf{Verify}(\mathsf{vk}, m_i, \sigma_i) = 0$ ならばチャレンジャーは $\perp$ を出力してゲームを終了する．そうでない場合，チャレンジャーは $b \xleftarrow{\mathsf{U}} \{0, 1\}$ を選び $b = 0$ なら $\sigma' \xleftarrow{\mathsf{R}} \mathsf{Derive}(\mathsf{hk}_{P_i}, \{m_i, \sigma_i\}, m')$ を計算し，$b = 1$ なら $\sigma' \xleftarrow{\mathsf{R}} \mathsf{Sign}(\mathsf{sk}, m')$ を計算し，σ' を $\mathcal{A}$ に与える．

アウトプット: $\mathcal{A}$ は $b^* \in \{0, 1\}$ を出力する．$b = b'$ の場合を $\mathcal{A}$ の勝利とし，$\mathsf{Adv(k)}$ を $\mathsf{Adv(k)} = |\mathsf{Pr[b = b']} - \frac{1}{2}|$ と定義する．

4 提案方式

本章では，文字列に対する文字位置の交換を述語として有する鍵付き準同型署名の方式を提案する．まず提案方式の構成のアイデアについて記し，図 1 により具体的な構成を示す．その後，安全性証明のアウトラインについて説明する．

4.1 構成のアイデア

提案方式は，文献 [11, 12, 13, 14, 9] における DPVS で作られる双対基底を用いた内積述語暗号を基にしており，内積述語暗号におけるユーザ秘密鍵を署名として用いることで偽造不可能性を実現している．更に文献 [8, 9, 7] において用いられている，DPVS の双対基底を行列によって変換する技法に署名を変換し，準同型性としての文字位置の並べ替えを実現している．同時に，変換に用いる行列を準同型演算鍵として設定することよって鍵付き準同型署名の構成を実現した．最後に署名の再ランダム化に必要となる基底の要素を検証鍵に含めることで適応的文脈秘匿性を実現している．具体的な方式を図 1 に示す．

4.2 安全性

本節では，図 1 で示した方式の安全性証明のアウトラインを示す．初めに安全性証明で用いる補助問題を定義する．

定義 8 (Problem 1) Problem 1 は $(\mathsf{param}, \mathbb{B}_0, \widehat{\mathbb{B}}^*_0, \{\mathbb{B}_t, \widehat{\mathbb{B}}^*_t, W_t\}_{t=1,\ldots,d}, \{\boldsymbol{e}_{\beta,t,1}, \boldsymbol{e}_{t,2}\}_{t=0,\ldots,d}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P1}}_\beta(1^\lambda, d)$ を入力とし β を推定する問題であり，各パラメータは $\beta \xleftarrow{\mathsf{U}} \{0,1\}$ に対して以下のように決定される．

$\mathcal{G}^{\mathsf{P1}}_\beta(1^\lambda, d)$:
$(\mathsf{param}, (\mathbb{B}_0, \mathbb{B}^*_0), (\mathbb{B}_1, \mathbb{B}^*_1)) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, N_0 := 5, N_1 := 7)$,
for $i = 1, \ldots, d-1$
$W_i \xleftarrow{\mathsf{U}} GL(N_1, \mathbb{F}_q)$, $W^*_i := (W_i^{\mathrm{T}})^{-1}$
$\mathbb{B}_{i+1} := \mathbb{B}_i W_i$, $\mathbb{B}^*_{i+1} := \mathbb{B}^*_i W^*_i$
$\widehat{\mathbb{B}}^*_0 := (\boldsymbol{b}^*_{0,1}, \boldsymbol{b}^*_{0,2}, \boldsymbol{b}^*_{0,4})$,
$\widehat{\mathbb{B}}^*_i := (\boldsymbol{b}^*_{i,1}, \boldsymbol{b}^*_{i,2}, \boldsymbol{b}^*_{i,5}, \boldsymbol{b}_{i,6})$
$\varphi_0, \omega \xleftarrow{\mathsf{U}} \mathbb{F}_q, \tau \xleftarrow{\mathsf{U}} \mathbb{F}^\times_q$,
$\boldsymbol{e}_{0,0} := (0, \omega, 0, 0, \varphi_0)_{\mathbb{B}_0}$,
$\boldsymbol{e}_{1,0} := (0, \omega, \tau, 0, \varphi_0)_{\mathbb{B}_0}$,
for $t = 1, \ldots, d$,
$\vec{\psi}_t, \vec{\phi}_t \xleftarrow{\mathsf{U}} \mathbb{F}^2_q$
$\boldsymbol{e}_{0,t,1} := (\ \omega,\ 0,\ 0^2,\ 0^2,\ \vec{\phi}_t)_{\mathbb{B}_t}$,
$\boldsymbol{e}_{1,t,1} := (\ \omega,\ 0,\ \vec{\psi}_t,\ 0^2,\ \vec{\phi}_t)_{\mathbb{B}_t}$,
$\boldsymbol{e}_{t,2} := \omega \boldsymbol{b}_{t,2}$
return $(\mathsf{param}, \mathbb{B}_0, \widehat{\mathbb{B}}^*_0, \{\mathbb{B}_t, \widehat{\mathbb{B}}^*_t, W_t\}_{t=1,\ldots,d}, \{\boldsymbol{e}_{\beta,t,1}, \boldsymbol{e}_{t,2}\}_{t=0,\ldots,d})$.

任意の確率的アルゴリズム $\mathcal{B}$ に対して，$\mathsf{Adv}^{\mathsf{P1}}_{\mathcal{B}}(\lambda) := \left|\mathsf{Pr}\left[1 \leftarrow \mathcal{B}(1^\lambda, \varrho) \middle| \varrho \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P1}}_0(1^\lambda, \mathsf{d})\right] - \mathsf{Pr}\left[1 \leftarrow \mathcal{B}(1^\lambda, \varrho) \middle| \varrho \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P1}}_1(1^\lambda, d)\right]\right|$ を $\mathcal{B}$ のアドバンテージとして定義する．

定義 9 (Problem 2) Problem 2 は $(\mathsf{param}, \widehat{\mathbb{B}}_0, \widehat{\mathbb{B}}^*_0, \{\widehat{\mathbb{B}}_t, \widehat{\mathbb{B}}^*_t\}_{t=1,\ldots,d}, \{\boldsymbol{h}^*_{\beta,t,i}, \boldsymbol{e}_{t,i}\}_{t=1,\ldots,d,i=1,2}) \xleftarrow{\mathsf{R}} \mathcal{G}^{\mathsf{P2}}_\beta(1^\lambda, d)$ を入力とし β を推定する問題であり，各パラメータは $\beta \xleftarrow{\mathsf{U}} \{0,1\}$ に対して以下のように決定される．

$\mathcal{G}^{\mathsf{P2}}_\beta(1^\lambda, d)$:
$(\mathsf{param}, (\mathbb{B}_0, \mathbb{B}^*_0), (\mathbb{B}_1, \mathbb{B}^*_1)) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, N_0 := 5, N_1 := 7)$
for $i = 1, \ldots, d-1$,
$W_i \xleftarrow{\mathsf{U}} GL(N_1, \mathbb{F}_q)$, $W^*_i := (W_i^{\mathrm{T}})^{-1}$
$\mathbb{B}_{i+1} := \mathbb{B}_i W_i$, $\mathbb{B}^*_{i+1} := \mathbb{B}^*_i W^*_i$
$\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,2}, \boldsymbol{b}_{0,5})$,
$\widehat{\mathbb{B}}_i := (\boldsymbol{b}_{i,1}, \boldsymbol{b}_{i,2}, \boldsymbol{b}_{i,7})$
$\delta, \omega, \eta_0, \phi_0, \tau, u_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q, z_0 := u_0^{-1}$
$\boldsymbol{h}^*_{0,0} := (0, \delta, 0, \eta_0, 0)_{\mathbb{B}^*_0}, \boldsymbol{h}^*_{1,0} := (0, \delta, u_0, \eta_0, 0)_{\mathbb{B}^*_0}$
$\boldsymbol{e}_0 := (0, \omega, \tau z_0, 0, \phi_0)_{\mathbb{B}_0}$,
$\vec{e}_1 := (1, 0)$, $\vec{e}_2 := (0, 1) \in \mathbb{F}^2_q$,
for $t = 1, \ldots, d, i = 1, 2$;
$Z_t \xleftarrow{\mathsf{U}} GL(2, \mathbb{F}_q), U_t \xleftarrow{\mathsf{U}} (Z_t^{-1})^{\mathrm{T}}, \vec{\eta}_t \xleftarrow{\mathsf{U}} \mathbb{F}^2_q, \phi_t \xleftarrow{\mathsf{U}} \mathbb{F}_q$
$\boldsymbol{h}^*_{0,t,i} := (\ \delta \vec{e}_i,\ 0^2,\ \vec{\eta}_t,\ 0^2\ )_{\mathbb{B}^*_t}$
$\boldsymbol{h}^*_{1,t,i} := (\ \delta \vec{e}_i,\ \vec{e}_i U_t,\ \vec{\eta}_t,\ 0^2\ )_{\mathbb{B}^*_t}$
$\boldsymbol{e}_{t,i} := (\ \omega \vec{e}_i,\ \tau \vec{e}_i Z_t,\ 0^2,\ \phi_t\ )_{\mathbb{B}_t}$
return $(\mathsf{param}, \widehat{\mathbb{B}}_0, \mathbb{B}^*_0, \{\widehat{\mathbb{B}}_t, \mathbb{B}^*_t, W_t\}_{t=1,\ldots,d}, \boldsymbol{h}_{\beta,0}, \boldsymbol{e}_0, \{\boldsymbol{h}^*_{\beta,t,i}, \boldsymbol{e}_{t,i}\}_{t=1,\ldots,d,i=1,2})$

任意の確率的アルゴリズム $\mathcal{B}$ に対して，$\mathcal{B}$ のアドバンテージ $\mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}}(\lambda)$ は定義 8 と同様に定義される．

偽造不可能性　本節では，提案方式の偽造不可能性の証明のアウトラインについて記述する．

定理 1 *Problem1,2* の困難性の下で，提案方式は選択メッセージ攻撃に対する偽造不可能性（*EUF-CMA* 安全性）を持つ．

上記定理を証明するために以下の $(\nu+4)$ 個のゲームからなるゲーム列を考える．ここで ν は署名クエリの最大回数とする．Game 0 において，四角で囲まれた係数はのちの Game で変形する係数を示しており，それ以降の他の Game において，四角で囲まれた係数はひとつ前の Game から変化した係数を示す．

Game 0: 通常の EUF-CMA ゲーム．よって ℓ 回目の署名クエリに対しては，以下のように署名を生成する．

$$\begin{aligned}\sigma_0 &:= (1, -\delta_0, \boxed{0}, \eta_0, 0)_{\mathbb{B}_0^*}\\ \sigma_i &:= (\delta_i + \theta_i m_i, -\theta_i, \boxed{0,0}, \eta_{1,i}, \eta_{2,i}, 0)_{\mathbb{B}_i^*}\end{aligned}$$

また検証アルゴリズムにおいては c_0, c_i を以下の様に生成する．

$$\begin{aligned}c_0 &:= (\boxed{\lambda}, \omega, \boxed{0}, 0, \phi_0)_{\mathbb{B}_0}\\ c_i &:= (\omega(1, m_i), \boxed{0,0}, 0, 0, \phi_i)_{\mathbb{B}_i}\end{aligned}$$

Game 1: Game 1 では，署名クエリに対して，ハンドルではなく生成した署名を直接返答し (m, σ) を Q に保存する．導出クエリ，署名出力クエリに対しては $\perp$ を出力する．

Game 2: Game 2 は検証アルゴリズムで以下の様に c_0, c_i を生成する点を除いて Game 1 と同じである．

$$\begin{aligned}c_0 &:= (\lambda, \omega, \boxed{\psi_0}, 0, \phi_0)_{\mathbb{B}_0}\\ c_i &:= (\omega(1, m_i), \boxed{\psi_{1,i}, \psi_{2,i}}, 0, 0, \phi_i)_{\mathbb{B}_i}\end{aligned}$$

ここで，$\psi_0, \psi_{1,i}, \psi_{2,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ である．

Game 3-ℓ $(\ell = 1, \ldots, \nu)$: Game 3-0 は Game 2 を指す．Game 3-ℓ は ℓ 回目の署名クエリに対して以下の様に返答する点を除いて Game 3-$(\ell-1)$ と同じである

$$\begin{aligned}\sigma_0 &:= (1, -\delta_0, \boxed{\gamma_0}, \eta_0, 0)_{\mathbb{B}_0^*}\\ \sigma_i &:= (\delta_i + \theta_i m_i, -\theta_i, \boxed{\gamma_{1,i}, \gamma_{2,i}}, \eta_{1,i}, \eta_{2,i}, 0)_{\mathbb{B}_i^*}\end{aligned}$$

ここで，$\gamma_0, \gamma_{1,i}, \gamma_{2,i} \xleftarrow{\mathsf{U}} \mathbb{F}_q$ である．

Game 4: Game 4 は検証アルゴリズムで以下の様に c_0, c_i, ζ' を生成する点を除いて Game 3-ν と同じである．

$$\begin{aligned}c_0 &:= (\boxed{\lambda'}, \omega, \psi_0, 0, \phi_0)_{\mathbb{B}_0}\\ c_i &:= (\omega(1, m_i), \psi_{1,i}, \psi_{2,i}, 0, 0, \phi_i)_{\mathbb{B}_i}\\ \zeta' &:= g_T^{\lambda}\end{aligned}$$

以下の補題 1-5 より，Game 4 における攻撃者の勝利する確率が無視できるほど小さく，各 Game の間での攻撃者の勝利する確率の差が無視できるほど小さいことを示し，Game 0 すなわち通常の EUF-CMA ゲームにおける攻撃者の勝利する確率が無視できるほど小さいことを示す．ここで $\mathsf{Succ}^{(0)}(k)$，$\mathsf{Succ}^{(1)}(k)$，$\mathsf{Succ}^{(2)}(k)$，$\mathsf{Succ}^{(3\text{-}\ell)}(k)$，$\mathsf{Succ}^{(4)}(k)$ は Game 0, 1, 2, 3-ℓ, 4 において攻撃者が勝利する確率を表す．

補題 1 任意の多項式時間攻撃者 $\mathcal{A}$ と任意のセキュリティパラメータ k に対して，$\mathsf{Succ}^{(0)}(k) = \mathsf{Succ}^{(1)}(k)$ である．

補題 2 任意の多項式時間攻撃者 $\mathcal{A}$ と任意のセキュリティパラメータ k に対して，$|\mathsf{Succ}^{(1)}(k) - \mathsf{Succ}^{(2)}(k)| \leq \mathsf{Adv}^{\mathsf{P1}}_{\mathcal{B}_1}(k)$ となる確率的アルゴリズム $\mathcal{B}_1$ が存在する．

補題 3 任意の多項式時間攻撃者 $\mathcal{A}$ と任意のセキュリティパラメータ k に対して，$|\mathsf{Succ}^{(3\text{-}\ell)}(k) - \mathsf{Succ}^{(3\text{-}(\ell-1))}(k)| \leq \mathsf{Adv}^{\mathsf{P2}}_{\mathcal{B}_{2\text{-}\ell}}(k) + 1/q$ となる確率的アルゴリズム $\mathcal{B}_{2\text{-}\ell}$ が存在する．ここで $\mathcal{B}_{2\text{-}\ell} := \mathcal{B}_2(\ell, \cdot)$ である．

補題 4 任意の多項式時間攻撃者 $\mathcal{A}$ と任意のセキュリティパラメータ k に対して，$\mathsf{Succ}^{(4)}(k) = \mathsf{Succ}^{(3\text{-}\nu)}(k)$ である．

補題 5 任意の多項式時間攻撃者 $\mathcal{A}$ と任意のセキュリティパラメータ k に対して，$\mathsf{Succ}^{(4)}(k) = 0$ である．

文脈秘匿性　本節では，提案方式の文脈秘匿性の証明のアウトラインについて記述する．まず，提案方式は検証鍵に含まれる基底を用いることによって準同型演算時に署名が完全に再ランダム化される．そのため，本方式に対して適応的文脈秘匿性ゲームにおける攻撃者が勝利するためには，$\mathbb{B}_0^*$ の 3 次元目あるい $\mathbb{B}_i^*$ の 3, 4 次元目が非ゼロの署名を生成するほかない．しかし，Problem 1 よりそのような攻撃者は存在しないことから適応的文脈秘匿性が証明される．

参考文献

[1] J. H. Ahn, D. Boneh, J. Camenisch, S. Hohenberger, A. Shelat, and B. Waters. Computing on authenticated data. In *Theory of Cryptography - TCC 2012*, volume 7194 of *LNCS*, pages 1–20, 2012.

[2] G. Ateniese, D. H. Chou, B. de Medeiros, and G. Tsudik. Sanitizable signatures. In *Computer Security - ESORICS 2005*, volume 3679 of *LNCS*, pages 159–177, 2005.

[3] N. Attrapadung, B. Libert, and T. Peters. Computing on authenticated data: New privacy definitions and constructions. In *Advances in Cryptology - Asiacrypt 2012*, volume 7658 of *LNCS*, pages 367–385, 2012.

[4] D. Boneh, D. M. Freeman, J. Katz, and B. Waters. Signing a linear subspace: Signature schemes for network coding. In *Public Key Cryptography - PKC 2009*, volume 5443 of *LNCS*, pages 68–87, 2009.

[5] C. Brzuska, H. Busch, Ö. Dagdelen, M. Fischlin, M. Franz, S. Katzenbeisser, M. Manulis, C. Onete, A. Peter, B. Poettering, and D. Schröder. Redactable signatures for tree-structured data: Definitions and constructions. In *Applied Cryptography and Network Security - ACNS 2010*, volume 6123 of *LNCS*, pages 87–104, 2010.

[6] R. Johnson, D. Molnar, D. X. Song, and D. Wagner. Homomorphic signature schemes. In *Topics in Cryptology - CT-RSA 2002*, volume 2271 of *LNCS*, pages 244–262, 2002.

[7] Y. Kawai and T. Hirano. Toward efficient searchable encryption with partial matching. In *Symposium on Cryptography and Information Security - SCIS 2014*, 2014.

[8] Y. Kawai and K. Takashima. Fully Anonymous Functional Proxy Re Encryption. http://eprint.iacr.org/2011/543, 2013.

[9] Y. Kawai and K. Takashima. Predicate- and attribute-hiding inner product encryption in a public key setting. In *Pairing Based Cryptography - Pairing 2013*, volume 8365 of *LNCS*, pages 113–130, 2013.

[10] S. Micali and R. L. Rivest. Transitive signature schemes. In *Topics in Cryptology - CT-RSA 2002*, volume 2271 of *LNCS*, pages 236–243, 2002.

[11] T. Okamoto and K. Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In *Advances in Cryptology - CRYPTO 2010*, volume 6223 of *LNCS*, pages 191–208, 2010. Full version is available at http://eprint.iacr.org/2010/563.

[12] T. Okamoto and K. Takashima. Achieving short ciphertexts or short secret-keys for adaptively secure general inner-product encryption. In *Cryptology and Network Security - CANS 2011*, volume 7092 of *LNCS*, pages 138–159, 2011. Full version is available at http://eprint.iacr.org/2011/648.

[13] T. Okamoto and K. Takashima. Adaptively attribute-hiding (hierarchical) inner product encryption. In *Advances in Cryptology - Eurocrypt 2012*, volume 7237 of *LNCS*, pages 591–608, 2012. Full version is available at http://eprint.iacr.org/2011/543.

[14] T. Okamoto and K. Takashima. Fully secure unbounded inner-product and attribute-based encryption. In *Advances in Cryptology - Asiacrypt 2012*, volume 7658 of *LNCS*, pages 349–366, 2012. Full version is available at http://eprint.iacr.org/2011/671.

$\mathsf{KeyGen}(1^k, N)$:

$(\mathsf{param}, (\mathbb{B}_0, \mathbb{B}_0^*), (\mathbb{B}_1, \mathbb{B}_1^*)) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^\lambda, N_0 = 5, N_1 = 7)$

For $i = 1, \ldots, N-1$

$W_i \xleftarrow{\mathsf{U}} GL(N_1, \mathbb{F}_q), W_i^* := (W_i^{\mathrm{T}})^{-1}$, $\mathbb{B}_{i+1} := \mathbb{B}_i W_i$, $\mathbb{B}_{i+1}^* := \mathbb{B}_i^* W_i^*$

$\widehat{\mathbb{B}}_0 := (\boldsymbol{b}_{0,1}, \boldsymbol{b}_{0,2}, \boldsymbol{b}_{0,5})$, $\widehat{\mathbb{B}}_i := (\boldsymbol{b}_{i,1}, \boldsymbol{b}_{i,2}, \boldsymbol{b}_{i,7})$,

$\widehat{\mathbb{B}}_0^* := (\boldsymbol{b}_{0,2}^*, \boldsymbol{b}_{0,4}^*)$, $\widehat{\mathbb{B}}_i^* := (\boldsymbol{b}_{i,1}^*, \boldsymbol{b}_{i,2}^*, \boldsymbol{b}_{i,5}^*, \boldsymbol{b}_{i,6}^*)$

return $\mathsf{vk} := (\mathsf{param}, \{\widehat{\mathbb{B}}_i\}_{i=0,\ldots,N}, \{\widehat{\mathbb{B}}_i^*\}_{i=0,\ldots,N})$, $\mathsf{sk} := (\boldsymbol{b}_{0,1}^*, \mathsf{vk})$, $\mathsf{hk}_i := (W_i, \mathsf{vk})$.

$\mathsf{Sign}(\mathsf{sk}, m)$:

$\delta_1, \ldots, \delta_N \xleftarrow{\mathsf{U}} \mathbb{F}_q^N, \delta_0 = \Sigma_{i=1}^N \delta_i, \eta_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q, \eta_{1,1}, \ldots, \eta_{1,N} \xleftarrow{\mathsf{U}} \mathbb{F}_q^N, \eta_{2,1}, \ldots, \eta_{2,N} \xleftarrow{\mathsf{U}} \mathbb{F}_q^N,$

$\theta_1 \ldots, \theta_N \xleftarrow{\mathsf{U}} \mathbb{F}_q^N$

$\sigma_0 = (1, -\delta_0, 0, \eta_0, 0)_{\mathbb{B}_0^*}$

For $i = 1, \ldots, N$

$\sigma_i := (\delta_i + \theta_i m_i, -\theta_i, 0, 0, \eta_{1,i}, \eta_{2,i}, 0)_{\mathbb{B}_i^*}$

return $\sigma := (\sigma_0, \ldots, \sigma_N)$.

$\mathsf{Derive}(\mathsf{hk}_j, (m, \sigma), m')$:

$\hat{\sigma}_j := \sigma_{j+1} W_j^{-1}, \hat{\sigma}_{j+1} := \sigma_j W_j$

$\delta'_1, \ldots, \delta'_N \xleftarrow{\mathsf{U}} \mathbb{F}_q^N, \delta'_0 = \Sigma_{i=1}^N \delta'_i, \eta'_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q, \eta'_{1,1}, \ldots, \eta'_{1,N} \xleftarrow{\mathsf{U}} \mathbb{F}_q^N, \eta'_{2,1}, \ldots, \eta'_{2,N} \xleftarrow{\mathsf{U}} \mathbb{F}_q^N,$

$\theta'_1 \ldots, \theta'_N \xleftarrow{\mathsf{U}} \mathbb{F}_q^N$

$\tau := (0, -\delta'_0, 0, \eta'_0, 0)_{\mathbb{B}_0^*}$

For $i = 1, \ldots, N$

$\tau_i := (\delta'_i + \theta'_i m_i, -\theta'_i, 0, 0, \eta'_{1,i}, \eta'_{2,i}, 0)_{\mathbb{B}_i^*}$

$\sigma'_1 := \sigma_1 \tau_1, \ldots, \sigma'_{j-1} := \sigma_{j-1} \tau_{j-1},$

$\sigma'_j := \hat{\sigma}_j \tau_{j+1}, \sigma'_{j+1} := \hat{\sigma}_{j+1} \tau_j,$

$\sigma'_{j+2} := \sigma_{j+2} \tau_{j+2}, \ldots, \sigma'_N := \sigma_N \tau_N$

return $(\sigma'_1, \ldots, \sigma'_N)$.

$\mathsf{Verify}(\mathsf{vk}, m, \sigma)$:

$\lambda \xleftarrow{\mathsf{U}} \mathbb{F}_q, \omega \xleftarrow{\mathsf{U}} \mathbb{F}_q, \phi_0, \ldots, \phi_N \xleftarrow{\mathsf{U}} \mathbb{F}_q^N$

$c_0 := (\lambda, \omega, 0, 0, \phi_0)_{\mathbb{B}_0}$

$c_i := (\omega(1, m_i), 0, 0, 0, 0, \phi_i)_{\mathbb{B}_i}$

$\zeta := \Pi_{i=0}^N e(c_i, \sigma_i), \zeta' := g_T^\lambda$

If $\zeta = \zeta'$ return 1, otherwise return 0.

図 1: 提案方式