Algebraic Group Modelにおける Fiat-Shamir変換

福光 正幸[1,a)]　長谷川 真吾[2,b)]

概要：Fiat-Shamir 型署名の安全性証明については多くの研究がなされているが, ランダムオラクルモデルにおける証明では帰着効率を tight にできないことが知られている. しかしながら, 代表的な Fiat-Shamir 型証明である Schnorr 署名について, Fuchsbauer, Plouviez, Seurin は攻撃アルゴリズムが Algebraic な場合に上記の不可能性を突破し, tight な安全性証明を構築できることを示した. 本論文では彼らの結果が一般の Fiat-Shamir 型署名においても成立することを示す.

キーワード：Fiat-Shamir 署名, Algebraic Group Model, 安全性証明

Fiat-Shamir Transform in Algebraic Group Model

Masayuki Fukumitsu[1,a)]　Shingo Hasegawa[2,b)]

Abstract: There exist many results on the provable security of the Fiat-Shamir (FS)-type signatures. Especially, it is known that the tight security proof for the FS-type signatures cannot be achieved in the random oracle model. However, Fuchsbauer, Plouviez, Seurin overcame the barrier and constructed the tight security proof when the adversary is *algebraic*. In this paper, we aim to generalize their results.

Keywords: Fiat-Shamir Signature, Algebraic Group Model, Provable Security

1. はじめに

Fiat-Shamir (FS) 型署名 FS[ID] は, ID 方式 ID に Fiat-Shamir 変換 [5] を適用して得られるディジタル署名方式であり, Schnorr 署名 [14] などが代表的な方式として知られている. FS 型署名は構成の簡潔さによる効率の良さを持つだけでなく, マルチ署名やグループ署名などの高機能署名における構成要素としても有用である.

FS 型署名の安全性については多くの研究がなされている [1], [2], [6], [9], [11], [12], [13], [15]. 特に, 一般の FS 型署名は tight な安全性を達成できないことが知られている [6], [9], [11], [12], [15]. FS 型署名で tight 安全性を達成するための手法としては, lossiness と呼ばれる性質を持つ方法が存在する [2], [10].

最近, Fuchsbauer, Plouviez, Seurin [8] は, *algebraic group model*(AGM) [7] と呼ばれる, 攻撃アルゴリズムを algebraic な場合に限定した場合, Schnorr 署名が tight 安全性を持つことを示した. ここで, アルゴリズムが algebraic であるとは, 任意の群要素の操作がその群の演算のみで閉じており, 計算過程をトレース可能なもののことをいう.

[8] の結果は, 攻撃アルゴリズムのモデルを制限することで通常のモデルの場合の不可能性を突破できることを示唆している. しかしながら, [8] の対象は Schnorr 署名のみであり, 他の FS 型の署名の場合については言及されていない. そこで, 本論文では [8] の結果を一般の FS 型署名への場合へと拡張し, 同様の結果が得られるか, またそのために必要な条件について考察を行う.

[1] 北海道情報大学 情報メディア学部
Faculty of Information Media, Hokkaido Information University
[2] 東北大学 データ駆動科学・AI 教育研究センター
Center for Data-driven Science and Artificial Intelligence, Tohoku University
[a)] fukumitsu@do-johodai.ac.jp
[b)] shingo.hasegawa.b7@tohoku.ac.jp

© 2021 Information Processing Society of Japan

1.1 結果

本論文では, [8] にて示された AGM における Schnorr 署名の tight 安全性が一般の FS 型署名においても成立するかを検証する. AGM は特定の群に基づく概念であるため, 対象とする方式モデルには何らかの群構造が必要である. そこで, 代数構造を持つ ID 方式である線形 ID 方式 [3] を元に **群ベース *ID* 方式**を導入し, それを FS 変換して得られる署名方式を考察の対象する. 結果として, [8] と同様の結果が成り立つ, すなわち攻撃アルゴリズムを代数的アルゴリズムに制限することで, 既存の tight 安全性に関する不可能性を突破できることを一般の FS 型署名について示した.

2. 準備

$\mathbb{N}$ と $\mathbb{Z}$ で, それぞれ全ての自然数の集合と整数の集合を表す. 2 つの整数 $a \leq b$ について, $[a,b] \subseteq \mathbb{Z}$ は a と b 間の全ての整数の集合である. 任意の $N \in \mathbb{N}$ について, $\mathbb{Z}_N$ と $\mathbb{Z}_N^\times$ は 法 N における剰余環とその単数群である.

確率的アルゴリズム $\mathcal{A}$ について, $y \leftarrow\!\$\, \mathcal{A}(x;\omega)$ で入力 x に対し $\mathcal{A}$ が y を出力することを表す. ここで, ω は $\mathcal{A}$ の内部乱数である. $\mathcal{A}(x)$ は入力 x における $\mathcal{A}$ の出力に対応する確率変数である. 確率分布 D について, $y \leftarrow\!\$\, D$ で y を分布 D に沿って選ぶことを表す . 有限集合 X について, $U(X)$ は X 上の一様分布である. $y \leftarrow\!\$\, X$ は $y \leftarrow\!\$\, U(X)$ と同じ意味である. 任意のアルゴリズム $\mathcal{A}$ (または分布 D) と 入力 x について, $[\mathcal{A}(x)]$ は 入力 x における $\mathcal{A}$ の可能な出力全ての集合を表し, $[\mathcal{A}]$ (および $[D]$) は $\mathcal{A}$ (または D) が出力しうる全ての出力の集合を表す. *DPT* および *PPT* はそれぞれ決定性多項式時間 (Deterministic Polynomial Time) と 確率的多項式時間 (Probabilistic Polynomial Time) の略である.

任意の λ における正関数 ϵ と集合 X_λ 上の確率分布の族 $\{D_\lambda^{(1)}\}$ と $\{D_\lambda^{(2)}\}$ について以下が成り立つとき, $\{D_\lambda^{(1)}\}$ と $\{D_\lambda^{(2)}\}$ は ϵ-*close* であるという: 任意の $\lambda \in \mathbb{N}$ について, $(1/2)\sum_{\overline{x} \in X_\lambda} |\Pr\left[x = \overline{x} \mid x \leftarrow\!\$\, D_\lambda^{(1)}\right] - \Pr\left[x = \overline{x} \mid x \leftarrow\!\$\, D_\lambda^{(2)}\right]| \leq \epsilon(\lambda)$.

2.1 ディジタル署名

署名方式 DS は, 4 項組 $(\mathsf{Pgen}, \mathsf{KGen}, \mathsf{Sig}, \mathsf{Vf})$ で定義される. Pgen は PPT パラメータ生成アルゴリズムであり, 入力のセキュリティパラメータ 1^λ に対し 公開パラメータ K を出力する. KGen は PPT 鍵生成アルゴリズムであり, 入力 K に対し鍵ペア $(\mathsf{sk}, \mathsf{pk})$ を出力する. Sig は PPT 署名アルゴリズムであり, 入力 $(K, \mathsf{sk}, \mathsf{pk}, m)$ に対し署名 σ を出力する. Vf は DPT 検証アルゴリズムであり, 入力 $(K, \mathsf{pk}, m, \sigma)$ に対し, 署名 σ が (pk, m) に対し正当なとき, 1 を出力する.

2.1.1 Completeness

completeness は以下のように定義される: 任意の $\lambda \in \mathbb{N}$, $(\mathsf{sk}, \mathsf{pk}) \leftarrow\!\$\, \mathsf{KGen}(1^\lambda)$, m, $\sigma \leftarrow\!\$\, \mathsf{Sig}(\mathsf{sk}, \mathsf{pk}, m)$ について, $\mathsf{Vf}(\mathsf{pk}, m, \sigma) = 1$ が常に成り立つ.

2.1.2 安全性

本論文では, ディジタル署名の安全性として EUF-CMA 安全性を考える. EUF-CMA 安全性は図 1 に示す EUF-CMA ゲームで定義される. 署名方式 $\mathsf{DS} = (\mathsf{Pgen}, \mathsf{KGen}, \mathsf{Sig}, \mathsf{Vf})$ が (T, ϵ, Q_S)-EUF-CMA 安全であるとは, 時間 T で動作し, 署名オラクルに Q_S 回のクエリを行う任意のアルゴリズム $\mathcal{A}$ に対し, $\mathcal{A}$ が EUF-CMA ゲームに勝つ, すなわち確率 ϵ で $\mathsf{Game}^{\mathsf{EUF\text{-}CMA}}_{Q_S,\mathsf{DS},\mathcal{A}}(\lambda) = 1$ となることをいう. ランダムオラクルモデル (ROM) [4] の場合, (T, ϵ, Q_H, Q_S)-EUF-CMA 安全性は, アルゴリズム $\mathcal{A}$ がランダムオラクルに Q_H 回のクエリを行う (T, ϵ, Q_S)-EUF-CMA 安全性を意味する.

また, 任意の T, ϵ, Q_S について, (T, ϵ, Q_H)-EUF-KOA 安全性を $(T, \epsilon, Q_H, 0)$-EUF-CMA 安全性で定義する.

2.2 ID 方式

ID 方式は証明者 P と検証者 V の間の 2 者間プロトコルである. ID 方式は 6 項組 $(\mathsf{Pgen}, \mathsf{KGen}, P_1, \{\mathcal{CH}_K\}_{K \in [\mathsf{Pgen}]}, P_2, V)$ で構成される [1]. Pgen と KGen はそれぞれ PPT パラメータ生成アルゴリズムと鍵生成アルゴリズムである. P_1 と P_2 は P が実行する PPT アルゴリズムである. $\{\mathcal{CH}_K\}_{K \in [\mathsf{Pgen}]}$ は V が選ぶチャレンジ cha の集合族であり, パラメータ K で決定される. 3 項組 $(K, \mathsf{sk}, \mathsf{pk})$ について, P_1 はステート st とコミットメント cmt のペア $(\mathsf{st}, \mathsf{cmt})$ を出力する. 6 項組 $(K, \mathsf{sk}, \mathsf{pk}, \mathsf{st}, \mathsf{cmt}, \mathsf{cha})$ について, P_2 はレスポンス res を出力する. V は DPT 検証アルゴリズムである. 図 2 にプロトコルの動作を示す.

$\mathsf{ID} = (\mathsf{Pgen}, \mathsf{KGen}, P_1, P_2, \{\mathcal{CH}_K\}_{K \in [\mathsf{Pgen}]}, V)$ を ID 方式とする. 以下に ID 方式の各性質を定義する.

Completeness 任意の $\lambda \in \mathbb{N}$, $(\mathsf{sk}, \mathsf{pk}) \leftarrow\!\$\, \mathsf{KGen}(K)$, $(\mathsf{cmt}, \mathsf{cha}, \mathsf{res}) \leftarrow\!\$\, \mathsf{Tr}(K, \mathsf{sk}, \mathsf{pk})$ について, $V(K, \mathsf{pk}, \mathsf{cmt}, \mathsf{cha}, \mathsf{res}) = 1$ が成り立つ. ここで Tr は Fig. 2 に示す PPT アルゴリズムである.

Special Soundness 以下を満たす DPT アルゴリズム SS が存在する: 任意の $\lambda \in \mathbb{N}$, $K \in [\mathsf{Pgen}]$, $(\mathsf{sk}, \mathsf{pk}) \in [\mathsf{KGen}(K)]$ について, $V(K, \mathsf{pk}, \mathsf{cmt}, \mathsf{cha}, \mathsf{res}) = V(K, \mathsf{pk}, \mathsf{cmt}, \mathsf{cha}', \mathsf{res}') = 1$ かつ $\mathsf{cha} \neq \mathsf{cha}'$ である入力 $(K, \mathsf{pk}, \mathsf{cmt}, \mathsf{cha}, \mathsf{res}, \mathsf{cha}', \mathsf{res}')$ に対し, $(\mathsf{sk}^*, \mathsf{pk}) \in [\mathsf{KGen}(K)]$ となる sk^* を出力する.

ϵ_{HVZK}-honest-verifier-zero-knowledge (ϵ_{HVZK}-HVZK) 以下を満たす PPT アルゴリズム HVZK が存在する: 入力 (K, pk) について $(\mathsf{cmt}, \mathsf{cha}, \mathsf{res})$ を出力する. ただし, 出力の分布が $\mathsf{Tr}(K, \mathsf{sk}, \mathsf{pk})$ の出力分布と ϵ_{HVZK}-close である. ここで, $K \in [\mathsf{Pgen}]$,

$\mathsf{Game}^{\mathsf{EUF\text{-}CMA}}_{Q_S,\mathsf{DS},\mathcal{A}}(\lambda)$

$\mathsf{L} = \emptyset$

$K \leftarrow\!\$\, \mathsf{Pgen}(1^\lambda)$

$(\mathsf{sk}, \mathsf{pk}) \leftarrow\!\$\, \mathsf{KGen}(K)$

$(m^*, \sigma^*) \leftarrow\!\$\, \mathcal{A}^{\mathsf{O}_{\mathsf{Sig}}}(K, \mathsf{pk})$

return 1 **if** $m^* \notin \mathsf{L} \wedge \mathsf{Vf}(K, \mathsf{pk}_{i^*}, m^*, \sigma^*) = 1$

Oracle $\mathsf{O}_{\mathsf{Sig}}(m)$

$\sigma \leftarrow\!\$\, \mathsf{Sig}(K, \mathsf{sk}, \mathsf{pk}, m)$

$\mathsf{L} = \mathsf{L} \cup \{m\}$

return σ

図 1 EUF-CMA ゲームと署名オラクル $\mathsf{O}_{\mathsf{Sig}}$

$\mathsf{P}(K, \mathsf{sk}, \mathsf{pk})$		$\mathsf{V}(K, \mathsf{pk})$	$\mathsf{Tr}(K, \mathsf{sk}, \mathsf{pk})$
			$(\mathsf{st}, \mathsf{cmt}) \leftarrow\!\$\, P_1(K, \mathsf{sk}, \mathsf{pk})$
$(\mathsf{st}, \mathsf{cmt}) \leftarrow\!\$\, P_1(K, \mathsf{sk}, \mathsf{pk})$	$\xrightarrow{\mathsf{cmt}}$		$\mathsf{cha} \leftarrow\!\$\, \mathcal{CH}_K$
	$\xleftarrow{\mathsf{cha}}$	$\mathsf{cha} \leftarrow\!\$\, \mathcal{CH}_K$	$\mathsf{res} \leftarrow\!\$\, P_2(K, \mathsf{sk}, \mathsf{pk}, \mathsf{st}, \mathsf{cmt}, \mathsf{cha})$
			return $(\mathsf{cmt}, \mathsf{cha}, \mathsf{res})$
$\mathsf{res} \leftarrow\!\$\, P_2(K, \mathsf{sk}, \mathsf{pk}, \mathsf{st}, \mathsf{cmt}, \mathsf{cha})$	$\xrightarrow{\mathsf{res}}$	**return** $V(K, \mathsf{pk}, \mathsf{cmt}, \mathsf{cha}, \mathsf{res})$	

図 2 ID 方式 ID と Tr

$(\mathsf{sk}, \mathsf{pk}) \in [\mathsf{KGen}(K)]$ である.

δ-min-entropy 任意の $\lambda \in \mathbb{N}$, $(\mathsf{sk}, \mathsf{pk}) \in [\mathsf{KGen}]$, $\overline{\mathsf{cmt}}$ について, $\Pr[\mathsf{cmt} = \overline{\mathsf{cmt}} \mid (\mathsf{st}, \mathsf{cmt}) \leftarrow\!\$\, P_1(\mathsf{sk}, \mathsf{pk})] \leq 2^{-\delta}$ が成り立つ.

Random-Self-Reducibility 以下を満たす PPT アルゴリズム Rand と DPT アルゴリズム DRand が存在する:

(a) 任意の $\lambda \in \mathbb{N}$, $K \leftarrow\!\$\, \mathsf{Pgen}(1^\lambda)$, $(\mathsf{sk}, \mathsf{pk}) \leftarrow\!\$\, \mathsf{KGen}(K)$ について, $(r, \mathsf{pk}') \leftarrow\!\$\, \mathsf{Rand}(K, \mathsf{pk})$ である pk' の分布が, pk の分布と一致する.

(b) 任意の $\lambda \in \mathbb{N}$, $K \in [\mathsf{Pgen}]$, $(\mathsf{sk}, \mathsf{pk}) \in [\mathsf{KGen}(K)]$, $(r, \mathsf{pk}') \in [\mathsf{Rand}(K, \mathsf{pk})]$ について, sk' が $(\mathsf{sk}', \mathsf{pk}') \in [\mathsf{KGen}(K)]$ を満たすとき, $\mathsf{sk}^* = \mathsf{DRand}(K, \mathsf{pk}, \mathsf{sk}', \mathsf{pk}', r)$ である sk^* について $(\mathsf{sk}^*, \mathsf{pk}) \in [\mathsf{KGen}(K)]$ が成り立つ.

2.2.1 ID 方式の安全性

ID 方式の安全性は [1], [11] に従う. $\mathsf{ID} = (\mathsf{Pgen}, \mathsf{KGen}, P_1, \{\mathcal{CH}_K\}_{K \in [\mathsf{Pgen}]}, P_2, V)$ とする. KR-KOA 安全性および PIMP-KOA 安全性は図 3 に示す KR-KOA ゲームおよび PIMP-KOA ゲームで定義される. ID が (T, ϵ)-KR-KOA 安全であるとは, 時間 T で動作する任意のアルゴリズム $\mathcal{A}$ に対し, $\mathcal{A}$ が KR-KOA に勝つ, すなわち確率 ϵ で $\mathsf{Game}^{\mathsf{KR\text{-}KOA}}_{\mathsf{ID},\mathcal{A}}(\lambda) = 1$ となることをいう. 同様に, ID が $(T, \epsilon, Q_{\mathsf{cha}})$-PIMP-KOA 安全であるとは, 時間 T で動作し, $\mathsf{O}_{\mathsf{cha}}$ オラクルに Q_{cha} 回のクエリを行う任意のアルゴリズム $\mathcal{A}$ に対し, $\mathcal{A}$ が PIMP-KOA ゲームに勝つ, すなわち確率 ϵ で $\mathsf{Game}^{\mathsf{PIMP\text{-}KOA}}_{Q_{\mathsf{cha}},\mathsf{ID},\mathcal{A}}(\lambda) = 1$ となることをいう. また, (T, ϵ)-IMP-KOA 安全性は $(T, \epsilon, 1)$-PIMP-KOA 安全性を意味する.

2.3 Fiat-Shamir 署名

Fiat-Shamir 変換 [5] は, ID 方式から署名方式を作る一般的手法である. $\mathsf{ID} = (\mathsf{Pgen}, \mathsf{KGen}, P_1, \{\mathcal{CH}_K\}_{K \in [\mathsf{Pgen}]}, P_2, V)$ を ID 方式, ℓ_m を λ の多項式, $\{H_K : \{0,1\}^* \to \mathcal{CH}_K\}_{K \in [\mathsf{Pgen}]}$ をハッシュ関数 H_K の族とする. ID を元にする Fiat-Shamir 型署名 $\mathsf{FS}[\mathsf{ID}] = (\mathsf{Pgen}, \mathsf{KGen}, \mathsf{Sig}, \mathsf{Vf})$ は, 次のように定義される:

Pgen と KGen : ID のものと同じ.

$\mathsf{Sig}(K, \mathsf{sk}, \mathsf{pk}, m)$: メッセージ $m \in \{0,1\}^{\ell_m}$ の署名 $\sigma = (\mathsf{cmt}, \mathsf{res})$ を次のように計算する: $(\mathsf{st}, \mathsf{cmt}) \leftarrow\!\$\, P_1(K, \mathsf{sk}, \mathsf{pk})$, $\mathsf{cha} = H_K(\mathsf{cmt}, m)$, $\mathsf{res} \leftarrow\!\$\, P_2(K, \mathsf{sk}, \mathsf{pk}, \mathsf{st}, \mathsf{cmt}, \mathsf{cha})$.

$\mathsf{Vf}(K, \mathsf{pk}, m, (\mathsf{cmt}, \mathsf{res}))$: $V(K, \mathsf{pk}, \mathsf{cmt}, c, \mathsf{res})$ を出力. ただし, $c = H_K(\mathsf{cmt}, m)$.

2.4 Algebraic Group Model と Algebraic Reduction

族 $\{\mathbb{G}_K\}_K$ に関する *algebraic group model* および *algebraic reduction* は, 代数的アルゴリズム $\mathcal{A}$ [12] により定義される. 代数的アルゴリズムとは, 直感的には $\mathcal{A}$ が $\mathbb{G}_K$ の元を計算するときに $\mathbb{G}_K$ 上の演算のみを使用するということである. Paillier と Vergnaud はこの概念を以下のように定義した: $\mathcal{A}$ が入力される M 個の群要素 $a_1, \ldots, a_M \in \mathbb{G}_K$ とパラメータ K に対し $w \in \mathbb{G}_K$ を出力するとき, $w = \sum_{k=1}^{M} \alpha_k a_k$ となる $(\alpha_1, \ldots, \alpha_M) \in \mathbb{Z}^M$ が存在し, $\mathcal{A}$ は w とともに $(\alpha_1, \ldots, \alpha_M)$ を出力する. ここで, $(\alpha_1, \ldots, \alpha_M)$ は基底 $(a_1, \ldots, a_M)$ における w の係数ベクトルと呼ばれる.

任意の $M \in \mathbb{N}$, $\boldsymbol{a} = (a_1, \ldots, a_M) \in \mathbb{G}_K^M$, $\boldsymbol{\alpha} =$

$\mathsf{Game}^{\mathsf{KR\text{-}KOA}}_{\mathsf{ID},\mathcal{A}}(\lambda)$

$K \leftarrow\!\$\ \mathsf{Pgen}(1^\lambda)$

$(\mathsf{sk},\mathsf{pk}) \leftarrow\!\$\ \mathsf{KGen}(K)$

$\mathsf{sk}^* \leftarrow\!\$\ \mathcal{A}(K,\mathsf{pk})$

return 1 **if** $(\mathsf{sk}^*,\mathsf{pk}) \in [\mathsf{KGen}(K)]$

$\mathsf{Game}^{\mathsf{PIMP\text{-}KOA}(\lambda)}_{Q_{\mathsf{cha}},\mathsf{ID},\mathcal{A}}$

$\mathsf{L} = \emptyset$

$i = 1$

$K \leftarrow\!\$\ \mathsf{Pgen}(1^\lambda)$

$(\mathsf{sk},\mathsf{pk}) \leftarrow\!\$\ \mathsf{KGen}(K)$

$(i^*,\mathsf{res}^*) \leftarrow\!\$\ \mathcal{A}^{\mathsf{O}_{\mathsf{cha}}}(K,\mathsf{pk})$

$(\mathsf{cmt}^*,\mathsf{cha}^*) \leftarrow \mathsf{L}[i^*]$

return $V(K,\mathsf{pk},\mathsf{cmt}^*,\mathsf{cha}^*,\mathsf{res}^*)$

Oracle $\mathsf{O}_{\mathsf{cha}}(\mathsf{cmt})$

$\mathsf{cha} \leftarrow\!\$\ \mathcal{CH}_K$

$\mathsf{L}[i] \leftarrow (\mathsf{cmt},\mathsf{cha})$

$i = i+1$

return cha

図 3 KR-KOA ゲーム, PIMP-KOA ゲームとオラクル $\mathsf{O}_{\mathsf{cha}}$

$(\alpha_1,\ldots,\alpha_M) \in \mathbb{Z}^M$ について, $\langle \boldsymbol{a},\boldsymbol{\alpha}\rangle = w = \sum_{k=1}^M \alpha_k a_k$ とする. $w_{\{\langle \boldsymbol{a},\boldsymbol{\alpha}\rangle\}}$ で, $w \in \mathbb{G}_K$ およびその $(a_1,\ldots,a_M)$ における係数ベクトル $(\alpha_1,\ldots,\alpha_M) \in \mathbb{Z}^M$ のペア $(w,(\alpha_1,\ldots,\alpha_M))$ を表す. すなわち, $w = \langle \boldsymbol{a},\boldsymbol{\alpha}\rangle$ である.

$\mathcal{A}$ にブラックボックスアクセスを行う帰着 $\mathcal{R}$ を考える. $\{\mathbb{G}_K\}_K$ に関する *algebraic group model (AGM)* [7] とは, $\mathcal{A}$ が $\{\mathbb{G}_K\}_K$ に関し代数的アルゴリズムであることをいう. 同様に, $\{\mathbb{G}_K\}_K$ に関する *algebraic reduction* [12] とは, $\mathcal{R}$ が $\{\mathbb{G}_K\}_K$ に関し代数的アルゴリズムであることをいう.

3. 群ベース ID 方式

本節では, 本論文が対象とする群ベース ID 方式とその性質を導入する.

3.1 定義

本論文では, ID 方式の特別な形である群ベース ID 方式を取り扱う. これは線形 ID 方式 LID [3] の一種であり, 準同型関数の族を元に定義される. [3] に習い, 準同型関数の族および群ベース ID 方式は以下で定義される.

定義 1 (準同型関数)**.** 準同型関数の族 HF は 以下を満たす $(\mathsf{Pgen},\{L_K:\mathfrak{D}_K \to \mathfrak{R}_K\}_{K\in[\mathsf{Pgen}]})$ で定義される*:*

- Pgen は入力 1^λ に対しパラメータ K を出力する PPT パラメータ生成アルゴリズムである.
- $\{L_K:\mathfrak{D}_K \to \mathfrak{R}_K\}_{K\in[\mathsf{Pgen}]}$ は添え字集合 $K \in [\mathsf{Pgen}]$ で規定され, 任意の $K \in [\mathsf{Pgen}]$ について以下を満たす*:*
  - $\mathfrak{D}_K$ と $\mathfrak{R}_K$ が群.
  - $L_K : \mathfrak{D}_K \to \mathfrak{R}_K$ が準同型. すなわち, 任意の $c,d \in \mathbb{Z}$, $x,y \in \mathfrak{D}_K$ について,

$$L_K(x\cdot c + y\cdot d) = L_K(x)\cdot c + L_K(y)\cdot d.$$

定義 2 (群ベース ID 方式)**.** 群ベース *ID* 方式 GID は ペア $\left(\mathsf{HF},\{(\mathcal{CH}_K,D^{\mathsf{sk}}_K,D^{\mathsf{st}}_K)\}_{K\in[\mathsf{Pgen}]}\right)$ で構成される.

- $\mathsf{HF} = (\mathsf{Pgen},\{L_K:\mathfrak{D}_K \to \mathfrak{R}_K\}_{K\in[\mathsf{Pgen}]})$ は準同型関数の族.
- $\{(\mathcal{CH}_K,D^{\mathsf{sk}}_K,D^{\mathsf{st}}_K)\}_{K\in[\mathsf{Pgen}]}$ は添え字集合 $K \in [\mathsf{Pgen}]$ で規定され, 任意の $K \in [\mathsf{Pgen}]$ について以下を満たす*:*
  - $\mathcal{CH}_K \subseteq \mathbb{Z}$.
  - D^{sk}_K と D^{st}_K は多項式時間サンプリング可能な $\mathfrak{D}_K$ 上の分布.

群ベース *ID* 方式 GID により, *ID* 方式 $(\mathsf{Pgen},\mathsf{KGen},P_1,\{\mathcal{CH}_K\}_{K\in[\mathsf{Pgen}]},P_2,V)$ は以下のように構成される*:*

Pgen *:* GID の HF のものと同一.

$\mathsf{KGen}(K)$ *:* $\mathsf{sk} \leftarrow\!\$\ D^{\mathsf{sk}}_K$, $\mathsf{pk} = L_K(\mathsf{sk})$ とし, 秘密鍵 sk と公開鍵 pk を出力.

$P_1(K,\mathsf{sk},\mathsf{pk})$ *:* $\mathsf{st} \leftarrow\!\$\ D^{\mathsf{st}}_K$, $\mathsf{cmt} = L_K(\mathsf{st})$ とし, ステート st と コミットメント cmt を出力.

$\{\mathcal{CH}_K\}_{K\in[\mathsf{Pgen}]}$ *:* GID のものと同一.

$P_2(K,\mathsf{sk},\mathsf{pk},\mathsf{st},\mathsf{cmt},\mathsf{cha})$ *:* レスポンス $\mathsf{res} = \mathsf{st} + \mathsf{sk}\cdot\mathsf{cha}$ を出力.

$V(K,\mathsf{pk},\mathsf{cmt},\mathsf{cha},\mathsf{res})$ *:* $L_K(\mathsf{res}) = \mathsf{cmt} + \mathsf{pk}\cdot\mathsf{cha}$ のとき, 1 を出力.

3.2 Linear Representability

GID のパラメータ $K \in [\mathsf{Pgen}]$ について, $(a_1,\ldots,a_M,\mathsf{aux}) \in \mathfrak{R}_K^M \times \{0,1\}^*$ の形とする. linear representability とは, 任意の $w = \sum_{k=1}^M a_k\alpha_k \in \mathfrak{R}_K$ ($(\alpha_1,\ldots,\alpha_M) \in \mathbb{Z}^M$) について, w の表現 $(\alpha_1,\ldots,\alpha_M)$ が

図 4 AGM における群ベース ID 方式 GID の安全性と FS 型署名 FS[GID] の安全性の関係

効率的に $w = L_K(\alpha)$ となる $\alpha \in \mathfrak{D}_K$ に変換 (および逆変換) できることである. 詳細な定義は以下の通りである.

定義 3 (Linear Representability)**.** 群ベース *ID* 方式を $\mathsf{GID} = (\mathsf{HF}, \{(\mathcal{CH}_K, D_K^{\mathsf{sk}}, D_K^{\mathsf{st}})\}_{K\in[\mathsf{Pgen}]})$ とする. 任意の $K \in [\mathsf{Pgen}]$ について, $K = (a_1, \ldots, a_M, \mathsf{aux}) \in \mathfrak{R}_K^M \times \{0,1\}^*$ の形とする. 以下を満たす *DPT* アルゴリズム Rep と IRep が存在するとき, GID は linearly representable であるという*:*

- Rep *:* $K = (a_1, \ldots, a_M, \mathsf{aux}) \in \mathfrak{R}_K^M \times \{0,1\}^*$ と $w = \sum_{k=1}^M a_k\alpha_k$ を満たす入力 $(K, w, \alpha_1, \ldots, \alpha_M)$ に対し, $w = L_K(\alpha)$ となる $\alpha \in \mathfrak{D}_K$ を出力.
- IRep *:* $K = (a_1, \ldots, a_M, \mathsf{aux}) \in \mathfrak{R}_K^M \times \{0,1\}^*$ と $w = L_K(\alpha)$ を満たす入力 (K, w, α) に対し, $w = \sum_{k=1}^M a_k\alpha_k$ となる $(\alpha_1, \ldots, \alpha_M) \in \mathbb{Z}^M$ を出力.

4. AGM における Fiat-Shamir 型署名の安全性

本節では, AGM における, 群ベース ID 方式 GID の安全性と GID を元に構成される Fiat-Shamir 型署名 FS[GID] の安全性の関係を考察する. 結果のまとめを図 4 に示す. 以下それぞれの定理および証明を記述するが, 定理 2 の証明についてはスペースの都合により省略する.

定理 1 (KR-KOA $\to$ PIMP-KOA in AGM)**.** GID を *linear representability* と *special soundness* を持つ群ベース *ID* 方式とする. GID が $\{\mathfrak{R}_K\}_{K\in[\mathsf{Pgen}]}$ に関する代数的アルゴリズム に対し, (T, ϵ)-KR-KOA 安全であるとする. このとき, 任意の $Q'_{\mathsf{cha}} \geq 1$ について, GID は $\{\mathfrak{R}_K\}_{K\in[\mathsf{Pgen}]}$ に関する代数的アルゴリズム に対し, $(T', \epsilon', Q'_{\mathsf{cha}})$-PIMP-KOA 安全である. ただし,

$$T' \approx T, \quad and \quad \epsilon' \leq \epsilon + \frac{1}{|\mathcal{CH}_K|}.$$

証明. $\mathcal{A}$ を GID に対する PIMP-KOA 代数的アルゴリズムとする. この $\mathcal{A}$ を利用する KR-KOA アルゴリズム $\mathcal{B}$ を構成する. $\mathcal{B}$ の目標は入力された pk に対応する sk^* の計算である. $\mathcal{B}$ の基本的な戦略は $\mathcal{A}$ の出力を利用して GID の special soundness を使用することである. $\mathcal{A}$ は PIMP-KOA アルゴリズムであるため, $V(K, \mathsf{pk}, \mathsf{cmt}^*, \mathsf{cha}^*, \mathsf{res}^*) = 1$, $(\mathsf{cmt}^*, \mathsf{res}^*) = \mathsf{L}[i^*]$ となる (i^*, res^*) を出力する. 一方, $\mathcal{A}$ は $\{\mathfrak{R}_K\}_{K\in[\mathsf{Pgen}]}$ に関する代数的アルゴリズムなので, $\mathcal{A}$ の動作中に $\mathcal{A}$ から出力された $\mathsf{cmt}^* \in \mathfrak{R}_K$ には係数ベクトルが付随している. この係数ベクトルから, $V(K, \mathsf{pk}, \mathsf{cmt}^*, \mathsf{cha}', \mathsf{res}') = 1$ となる $(\mathsf{cmt}^*, \mathsf{cha}', \mathsf{res}')$ を作成することができる. すなわち, $\mathcal{A}$ の一度の起動で special soundness の条件を満たす $(K, \mathsf{pk}, \mathsf{cmt}^*, \mathsf{cha}^*, \mathsf{res}^*, \mathsf{cha}', \mathsf{res}')$ を得られるため, sk^* の計算が可能になる.

以上の戦略による $\mathcal{B}$ の構成を図 5 に示す. $\mathsf{O}_{\mathsf{cha}}^{\mathsf{alg}}$ は $\mathcal{B}$ による $\mathcal{A}$ が利用するチャレンジオラクルのシミュレーションである.

チャレンジオラクルのシミュレーション $\mathsf{O}_{\mathsf{cha}}^{\mathsf{alg}}$**.** $\mathsf{O}_{\mathsf{cha}}^{\mathsf{alg}}$ へのクエリ $(\mathsf{cmt}_{\{\langle \boldsymbol{a},\boldsymbol{\alpha}\rangle+\mathsf{pk}\cdot\beta\}})$ について, $\mathsf{cha} \leftarrow\!\!\$\, \mathcal{CH}_K$ を選び, リスト L に格納する. また, $\mathcal{A}$ は代数的アルゴリズムなので, $\mathcal{A}$ は cmt の係数ベクトル $(\boldsymbol{\alpha}, \beta)$ も同時にクエリする. そこで, これをリスト $\mathsf{L}_{\mathsf{alg}}$ に格納し, cha を $\mathcal{A}$ への返答とする.

sk^* の計算. 図 5 における $\mathcal{B}$ の動作には, $\mathcal{B}$ が停止する場合が 5 行目と 7 行目に存在する. $\mathcal{B}$ が停止せず, かつ $\mathcal{A}$ が (i^*, res^*) を出力した場合, $\mathcal{B}$ が sk^* を計算できることを示す.

5 行目で $\mathcal{B}$ が停止しない場合, $\mathcal{A}$ が検証式をパスする (i^*, res^*) $((\mathsf{cmt}^*, \mathsf{cha}^*) = \mathsf{L}[i^*])$ を出力していることを意味する. ここで $\mathsf{O}_{\mathsf{cha}}^{\mathsf{alg}}$ の定義より, リスト $\mathsf{L}_{\mathsf{alg}}$ から cmt^* の基底 $(a_1, \ldots, a_M, \mathsf{pk}) = (\boldsymbol{a}, \mathsf{pk}) \in \mathfrak{R}_K^{M+1}$ における 係数ベクトル $(\alpha_1^*, \ldots, \alpha_M^*, \beta^*) = (\boldsymbol{\alpha}^*, \beta^*) \in \mathbb{Z}^{M+1}$ を, $(\boldsymbol{\alpha}^*, \beta^*) = \mathsf{L}_{\mathsf{alg}}[\mathsf{cmt}^*]$ として取り出すことができる. これは $\mathcal{A}$ が入力として $\mathfrak{R}_K$ の元 $a_1, \ldots, a_M$ と pk を取る代数的アルゴリズムであり, チャレンジオラクルに $\mathsf{cmt}^* = \langle \boldsymbol{a}, \boldsymbol{\alpha}^*\rangle + \mathsf{pk}\cdot\beta^* = \sum_{k=1}^M a_k \cdot \alpha_k^* + \mathsf{pk}\cdot\beta^*$ をクエリするときには $(\boldsymbol{\alpha}^*, \beta^*)$ を同時に出力しなければならないためである.

ここで $w^* = \sum_{k=1}^M a_k\alpha_k^*$ について, linear representability により $w^* = L_K(\alpha^*)$ となる $\alpha^* \in \mathfrak{D}_K$ が存在する. よって,

$$\begin{aligned}\mathsf{cmt}^* &= \sum_{k=1}^M a_k \cdot \alpha_k^* + \mathsf{pk}\cdot\beta^* \\ &= w^* + \mathsf{pk}\cdot\beta^* = L_K(\alpha^*) + \mathsf{pk}\cdot\beta^* \qquad (1)\end{aligned}$$

が成り立つ.

式 (1) と GID の定義より, $V(K, \mathsf{pk}, \mathsf{cmt}^*, -\beta^*, \alpha^*) = 1$ が従う. また, 7 行目で $\mathcal{B}$ が停止しない場合, $\mathsf{cha}^* \neq -\beta^*$ となるため, $(K, \mathsf{pk}, \mathsf{cmt}^*, \mathsf{cha}^*, \mathsf{res}^*, -\beta^*, \alpha^*)$ は SS が $(\mathsf{sk}^*, \mathsf{pk}) \in [\mathsf{KGen}(K)]$ となる sk^* を出力するための条件を満たす. 以上より, $\mathcal{B}$ が停止せず, かつ $\mathcal{A}$ が (i^*, res^*) を出力するならば, $\mathcal{B}$ は 正しく sk を計算する, すなわち KR-KOA ゲームに勝利できる.

$\mathcal{B}$ の勝利確率. $\mathcal{A}$ は $(T', \epsilon', Q'_{\mathsf{cha}})$-PIMP-KOA アルゴリズムなので, オラクル $\mathsf{O}_{\mathsf{cha}}^{\mathsf{alg}}$ からの $(\mathsf{cmt}^*, \mathsf{cha}^*)$ に対し確率 ϵ' で $V(K, \mathsf{pk}, \mathsf{cmt}^*, \mathsf{cha}^*, \mathsf{res}^*) = 1$, $(\mathsf{cmt}^*, \mathsf{res}^*) = \mathsf{L}[i^*]$ と

$\mathcal{B}(K, \mathsf{pk})$

1: $\mathsf{L} = \mathsf{L}_{\mathsf{alg}} = \emptyset$
2: $i = 1$
3: $(i^*, \mathsf{res}^*) \leftarrow\$\, \mathcal{A}^{\mathsf{O}^{\mathsf{alg}}_{\mathsf{cha}}}(K, \mathsf{pk})$
4: $(\mathsf{cmt}^*, \mathsf{cha}^*) = \mathsf{L}[i^*]$
5: **abort if** $V(K, \mathsf{pk}, \mathsf{cmt}^*, \mathsf{cha}^*, \mathsf{res}^*) \neq 1$
6: $(\alpha_1^*, \ldots, \alpha_M^*, \beta^*) = \mathsf{L}_{\mathsf{alg}}[\mathsf{cmt}^*]$
7: **abort if** $\mathsf{cha}^* = -\beta^*$
8: $w^* = \sum_{k=1}^{M} a_k \alpha_k^*$
9: $\alpha^* = \mathsf{Rep}(K, w^*, \alpha_1^*, \ldots, \alpha_M^*)$
10: **return** $\mathsf{SS}(K, \mathsf{pk}, \mathsf{cmt}^*, \mathsf{cha}^*, \mathsf{res}^*, -\beta^*, \alpha^*)$

$\mathsf{O}^{\mathsf{alg}}_{\mathsf{cha}}(\mathsf{cmt}_{\{\langle \boldsymbol{a}, \boldsymbol{\alpha} \rangle + \mathsf{pk} \cdot \beta\}})$

1: $\mathsf{cha} \leftarrow\$\, \mathcal{CH}_K$
2: $\mathsf{L}[i] = (\mathsf{cmt}, \mathsf{cha})$
3: $i = i + 1$
4: $\mathsf{L}_{\mathsf{alg}}[\mathsf{cmt}] = (\alpha_1, \ldots, \alpha_M, \beta)$
5: **return** cha

図 5 KR-KOA アルゴリズム $\mathcal{B}$, チャレンジオラクルのシミュレーション $\mathsf{O}^{\mathsf{alg}}_{\mathsf{cha}}$

なる (i^*, res^*) を出力する．よって, $\mathcal{B}$ は確率 ϵ' で 5 行目の停止条件を回避できる．

続いて, 任意のコミットメント cmt^* と β^* について, $\mathcal{B}$ は β^* と独立に $\mathsf{cha}^* \leftarrow\$\, \mathcal{CH}_K$ を選ぶため, $\mathsf{cha}^* = -\beta^*$ となる確率は $1/|\mathcal{CH}_K|$ である．よって, $\mathcal{B}$ は確率 $1/|\mathcal{CH}_K|$ で 7 行目の停止条件を回避できる．以上より $\epsilon \geq \epsilon' - 1/|\mathcal{CH}_K|$ となるため, $\mathcal{B}$ は (T, ϵ)-KR-KOA アルゴリズムである． □

定理 2 (PIMP-KOA $\rightarrow$ EUF-KOA in AGM)**.** GID を群ベース *ID* 方式とする．GID が $\{\mathfrak{R}_K\}_{K \in [\mathsf{Pgen}]}$ に関する代数的アルゴリズム に対し, $(T, \epsilon, Q_{\mathsf{cha}})$-PIMP-KOA 安全であるとする．このとき, 任意の $Q'_{\mathsf{cha}} \geq 1$ について, FS[GID] は $\{\mathfrak{R}_K\}_{K \in [\mathsf{Pgen}]}$ に関する代数的アルゴリズムに対し, *ROM* において (T', ϵ', Q_H)-EUF-KOA 安全である．ただし,

$$T' \approx T,\ \epsilon' = \epsilon,\quad \textit{and}\ \ Q_H = Q_{\mathsf{cha}} - 1.$$

定理 3 (EUF-KOA $\rightarrow$ EUF-CMA in AGM)**.** GID を *linear representability*, ϵ_{HVZK}*-HVZK*, δ*-min-entropy* を持つ群ベース *ID* 方式とする．FS[GID] が $\{\mathfrak{R}_K\}_{K \in [\mathsf{Pgen}]}$ に関する代数的アルゴリズム に対し, (T, ϵ, Q_H)-EUF-KOA 安全であるとする．このとき, FS[GID] は $\{\mathfrak{R}_K\}_{K \in [\mathsf{Pgen}]}$ に関する代数的アルゴリズム に対し, *ROM* において $(T', \epsilon', Q_H, Q_S)$-EUF-CMA 安全である．ただし,

$$T' = T - O(M + Q_S),\quad \textit{and}$$
$$\epsilon' \leq \epsilon + \frac{(Q_H + Q_S)^2}{2^\delta} + Q_S \cdot \epsilon_{\mathsf{HVZK}}.$$

証明. EUF-CMA 代数的アルゴリズム $\mathcal{A}$ を利用する EUF-KOA 代数的アルゴリズム $\mathcal{B}$ を構成する．$\mathcal{B}$ の構成にあたっての基本的なアイディアは, $\mathcal{B}$ と $\mathcal{A}$ はともに EUF の達成を目的とするアルゴリズムなため, $\mathcal{A}$ が出力した偽造をそのまま $\mathcal{B}$ の出力とするものである．しかしながら, $\mathcal{A}$ は EUF-CMA アルゴリズムなので, $\mathcal{A}$ に偽造を出力させるためには $\mathcal{A}$ によるランダムオラクルと署名オラクルへのクエリに対応しなければならない．$\mathcal{B}$ は EUF-KOA アルゴリズムなので, $\mathcal{A}$ のランダムオラクルクエリに対しては, 自身が利用できるランダムオラクルを利用して返答することができる．しかし, 署名オラクルクエリに対してはそうではないため, 何らかの手段で署名オラクルクエリに対する返答をしなければならない．よって, $\mathcal{B}$ が GID の HVZK を利用し署名オラクルをシミュレートすることで, $\mathcal{A}$ に偽造 $(m^*, (\mathsf{cmt}^*, \mathsf{res}^*))$ を出力させることを目標とする．$\mathcal{A}$ が出力した偽造をそのまま $\mathcal{B}$ の出力とすることで, $\mathcal{B}$ は EUF-KOA ゲームに勝利可能である．

以上の戦略による $\mathcal{B}$ の構成を図 6 に示す．$\mathsf{O}^{\mathsf{alg}}_H$ は $\mathcal{B}$ によるランダムオラクルの, $\mathsf{O}^{\mathsf{alg}}_{\mathsf{Sig}}$ は署名オラクルのそれぞれシミュレーションである．

ランダムオラクルのシミュレーション $\mathsf{O}^{\mathsf{alg}}_H$**.** $\mathsf{O}^{\mathsf{alg}}_H$ へのクエリ (cmt, m) について, $\mathcal{B}$ は O_H に $(\mathsf{cmt}_{\{\mathsf{cmt} \cdot 1\}}, m)$ をクエリし, その返答をそのまま $\mathsf{O}^{\mathsf{alg}}_H$ の回答とする．

署名オラクルのシミュレーション $\mathsf{O}^{\mathsf{alg}}_{\mathsf{Sig}}$**.** $\mathcal{A}$ による署名オラクル $\mathsf{O}^{\mathsf{alg}}_{\mathsf{Sig}}$ への t 回目のクエリ m_t については, HVZK を使い $(\mathsf{cmt}_t, \mathsf{cha}_t, \mathsf{res}_t)$ を計算し, cha_t を (cmt_t, m_t) におけるランダムオラクルの出力としてプログラムする．ここで, 既に $\mathsf{L}_H[\mathsf{cmt}_t, m_t]$ が定義されていた場合は動作を停止するが, GID の δ-min-entropy によりその確率は $(t + Q_H)/2^\delta$ でおさえられる．クエリされた m_t に対する署名は $(\mathsf{cmt}_t, \mathsf{res}_t)$ であるが, ここで $\mathcal{B}$ は $\{\mathfrak{R}_K\}_{K \in [\mathsf{Pgen}]}$ に関する代数的アルゴリズムであり, また $\mathsf{cmt}_t \in \mathfrak{R}_K$ であるため, $(\mathsf{cmt}_t, \mathsf{res}_t)$ の出力の際は cmt_t の係数ベクトルを同時に出力しなければならない．$\mathcal{B}$ への入力は (K, pk) であり, いま K は $(\boldsymbol{a}, \mathsf{aux}) \in \mathfrak{R}_K^M \times \{0,1\}^*$ の形であるため, 基底 $(\boldsymbol{a}, \mathsf{pk})$ における係数ベクトルを以下のように計算する．HVZK の性質より, $(\mathsf{cmt}_t, \mathsf{cha}_t, \mathsf{res}_t)$ について $L_K(\mathsf{res}_t) = \mathsf{cmt}_t + \mathsf{pk} \cdot \mathsf{cha}_t$ となる．GID の linear repre-

$\mathcal{B}^{\mathsf{O}_H}(K, \mathsf{pk})$

1 : $\mathsf{L}_H = \mathsf{L} = \emptyset$

2 : $i = 1$

3 : $(m^*, (\mathsf{cmt}^*_{\{\langle \boldsymbol{a}, \boldsymbol{\alpha}_{\mathsf{cmt}^*}\rangle + \mathsf{pk}\cdot\beta_{\mathsf{cmt}^*} + \langle \mathbf{cmt}, \boldsymbol{\gamma}_{\mathbf{cmt}^*}\rangle\}}, \mathsf{res}^*)) \leftarrow\$ \mathcal{A}^{\mathsf{O}_H^{\mathsf{alg}}, \mathsf{O}_{\mathsf{Sig}}^{\mathsf{alg}}}(K, \mathsf{pk})$

4 : $\mathsf{cha}^* \leftarrow \mathsf{O}_H^{\mathsf{alg}}(\mathsf{cmt}^*_{\{\mathsf{cmt}^*\cdot 1\}}, m^*)$

5 : **abort if** $m^* \in \mathsf{L} \vee L_K(\mathsf{res}^*) \neq \mathsf{cmt}^* + \mathsf{pk}\cdot\mathsf{cha}^*$

6 : **return** $(m^*, (\mathsf{cmt}^*_{\{\mathsf{cmt}^*\cdot 1\}}, \mathsf{res}^*))$

$\mathsf{O}_H^{\mathsf{alg}}(\mathsf{cmt}_{\{\langle \boldsymbol{a}, \overline{\boldsymbol{\alpha}}\rangle + \mathsf{pk}\cdot\overline{\beta} + \langle \mathbf{cmt}, \overline{\boldsymbol{\gamma}}\rangle\}}, m)$

$\mathsf{L}_H[\mathsf{cmt}, m] \leftarrow \mathsf{O}_H(\mathsf{cmt}_{\{\mathsf{cmt}\cdot 1\}}, m) \quad$ **if** $\mathsf{L}_H[\mathsf{cmt}, m] = \bot$

return $\mathsf{L}_H[\mathsf{cmt}, m]$

$\mathsf{O}_{\mathsf{Sig}}^{\mathsf{alg}}(m_t)$

$\mathsf{L} = \mathsf{L} \cup \{m_t\}$

$(\mathsf{cmt}_t, \mathsf{cha}_t, \mathsf{res}_t) \leftarrow\$ \mathsf{HVZK}(K, \mathsf{pk})$

abort if $\mathsf{L}_H[\mathsf{cmt}_t, m_t] \notin \{\mathsf{cha}_t, \bot\}$

$\mathsf{L}_H[\mathsf{cmt}_t, m_t] \leftarrow \mathsf{cha}_t$

$\boldsymbol{\alpha}_{t,\mathsf{cmt}} = \mathsf{IRep}(K, L_K(\mathsf{res}_t), \mathsf{res}_t)$

return $(m_t, ((\mathsf{cmt}_t)_{\{\langle \boldsymbol{a}, \boldsymbol{\alpha}_{t,\mathsf{cmt}}\rangle - \mathsf{pk}\cdot\mathsf{cha}_t\}}, \mathsf{res}_t))$

図 6 EUF-KOA 代数的アルゴリズム $\mathcal{B}$, ランダムオラクルのシミュレーション $\mathsf{O}_H^{\mathsf{alg}}$, 署名オラクルのシミュレーション $\mathsf{O}_{\mathsf{Sig}}^{\mathsf{alg}}$

sentability より $L_K(\mathsf{res}_t) = \langle \boldsymbol{a}, \boldsymbol{\alpha}_{t,\mathsf{cmt}}\rangle$ となる $\boldsymbol{\alpha}_{t,\mathsf{cmt}} \in \mathbb{Z}^M$ が IRep により得られるため, $\mathsf{cmt}_t = \langle \boldsymbol{a}, \boldsymbol{\alpha}_{t,\mathsf{cmt}}\rangle - \mathsf{pk}\cdot\mathsf{cha}_t$ となる. これは cmt_t の $(\boldsymbol{a}, \mathsf{pk})$ における係数ベクトルが $(\boldsymbol{\alpha}_{t,\mathsf{cmt}}, -\mathsf{cha}_t)$ であることを意味する. よって, $((\mathsf{cmt}_t)_{\{\langle \boldsymbol{a}, \boldsymbol{\alpha}_{t,\mathsf{cmt}}\rangle - \mathsf{pk}\cdot\mathsf{cha}_t\}}, \mathsf{res}_t)$ がクエリ m_t における署名オラクルの返答となる.

偽造の出力. $\mathcal{A}$ が偽造の作成に成功した場合, $(m^*, (\mathsf{cmt}^*_{\{\langle \boldsymbol{a}, \boldsymbol{\alpha}_{\mathsf{cmt}^*}\rangle + \mathsf{pk}\cdot\beta_{\mathsf{cmt}^*} + \langle \mathbf{cmt}, \boldsymbol{\gamma}_{\mathbf{cmt}^*}\rangle\}}, \mathsf{res}^*))$ を出力する. ここで **cmt** は $\mathcal{A}$ が署名オラクルへのクエリで得た cmt_t を要素とするベクトルである. 各 cmt_t も $\mathfrak{R}_K$ の元であるため, cmt^* には基底 $(\boldsymbol{a}, \mathsf{pk}, \mathbf{cmt})$ における係数ベクトル $(\boldsymbol{\alpha}_{\mathsf{cmt}^*}, \beta_{\mathsf{cmt}^*}, \boldsymbol{\gamma}_{\mathbf{cmt}^*})$ が付随している. ここで cmt^* 自体も $\mathfrak{R}_K$ の元であるため, 代数的アルゴリズムの定義より, cmt^* を新たな基底としてとることができる. すなわち基底 $(\boldsymbol{a}, \mathsf{pk}, \mathbf{cmt}, \mathsf{cmt}^*)$, 係数ベクトルが $(\mathbf{0}, 0, \mathbf{0}, 1)$ である $\mathsf{cmt}^*_{\{\mathsf{cmt}^*\cdot 1\}}$ を出力に含められるため, $(m^*, (\mathsf{cmt}^*_{\{\mathsf{cmt}^*\cdot 1\}}, \mathsf{res}^*))$ を $\mathcal{B}$ の出力とでき, $\mathcal{B}$ は EUF-KOA ゲームに勝利できる.

$\mathcal{B}$ の勝利確率. 既に見たように, t 回目の署名オラクルクエリにおける停止確率は $(t + Q_H)/2^\delta$ でおさえられる. よって, 署名オラクルシミュレーション全体の停止確率は $\sum_{t=1}^{Q_S}(t + Q_H)/2^\delta \leq (Q_S + Q_H)^2/2^\delta$ となる. また, ϵ_{HVZK}-HVZK により, $\mathsf{O}_{\mathsf{Sig}}^{\mathsf{alg}}$ が停止しない限り, $\mathsf{O}_{\mathsf{Sig}}^{\mathsf{alg}}$ の出力分布は Sig の出力分布と ϵ_{HVZK}-close であることが保証される. $\mathcal{A}$ は $(T', \epsilon', Q_H, Q_S)$-EUF-CMA 代数的アルゴリズム, すなわち確率 ϵ' で偽造を出力するため, $\mathcal{B}$ は少なくとも確率 $\epsilon' - (Q_S + Q_H)^2/2^\delta - Q_S\cdot\epsilon_{\mathsf{HVZK}}$ で EUF-KOA に勝利できる. □

注意. 定理 3 の証明において, $\mathcal{B}$ の最終的な出力を $(m^*, (\mathsf{cmt}^*_{\{\mathsf{cmt}^*\cdot 1\}}, \mathsf{res}^*))$ とした. これは入力で与えられた $\mathfrak{R}_K$ の元だけでなく, $\mathcal{B}$ の動作中に得られた $\mathfrak{R}_K$ の元も基底として加えることができるためである. しかしながら, cmt^* は $\mathcal{A}$ より $\mathsf{cmt}^*_{\{\langle \boldsymbol{a}, \boldsymbol{\alpha}_{\mathsf{cmt}^*}\rangle + \mathsf{pk}\cdot\beta_{\mathsf{cmt}^*} + \langle \mathbf{cmt}, \boldsymbol{\gamma}_{\mathbf{cmt}^*}\rangle\}}$ の形で与えられ, **cmt** の各要素についても署名オラクルシミュレーションの途中で基底 $(\boldsymbol{a}, \mathsf{pk})$ における係数ベクトルが得られている. よって適切な基底変換を行うことで cmt^* の基底 $(\boldsymbol{a}, \mathsf{pk})$ における係数ベクトルを計算できる, すなわち $\mathcal{B}$ へと入力された $(\boldsymbol{a}, \mathsf{pk})$ のみを使用する形で cmt^* を出力することも可能である.

5. おわりに

本論文では, [8] で示された代数的アルゴリズムを用いた攻撃モデルによる Schnorr 署名の tight 安全性について, 一般の FS 型署名への適用可能性を考察した. 代数的アルゴリズムは特定の群に基づく概念であるため, 群ベース ID 方式を導入し, それを FS 変換して得られる署名方式を考察の対象とした. 結果として, [8] と同様の結果, すなわち攻撃アルゴリズムを代数的アルゴリズムに制限することで, 既存の tight 安全性に関する不可能性を突破できることを一般の FS 型署名について示した.

本論文では FS 型署名の安全性証明可能性について, tight 安全性および肯定的な結果にのみ注目したが, [11] では Non-programmable ROM における不可能性の結果についても言及されている. 今回用いた手法を用いて, 他の不可能性の結果を回避することができるかを今後の課題とする.

謝辞 本研究は JSPS 科研費 JP18K11288, JP19K20272 の助成を受けたものです.

参考文献

[1] Abdalla, M., An, J. H., Bellare, M. and Namprempre, C.: From Identification to Signatures Via the Fiat-Shamir Transform: Necessary and Sufficient Conditions for Security and Forward-Security, *Information Theory, IEEE Transactions on*, Vol. 54, No. 8, pp. 3631–3646 (2008).

[2] Abdalla, M., Fouque, P.-A., Lyubashevsky, V. and Tibouchi, M.: Tightly Secure Signatures From Lossy Identification Schemes, *Journal of Cryptology*, Vol. 29, No. 3, pp. 597–631 (online), DOI: 10.1007/s00145-015-9203-7 (2016).

[3] Backendal, M., Bellare, M., Sorrell, J. and Sun, J.: The Fiat-Shamir Zoo: Relating the Security of Different Signature Variants, *Secure IT Systems* (Gruschka, N., ed.), Cham, Springer International Publishing, pp. 154–170 (2018).

[4] Bellare, M. and Rogaway, P.: Random Oracles Are Practical: A Paradigm for Designing Efficient Protocols, *Proceedings of the 1st ACM Conference on Computer and Communications Security*, CCS '93, New York, NY, USA, ACM, pp. 62–73 (online), available from ⟨http://doi.acm.org/10.1145/168588.168596⟩ (1993).

[5] Fiat, A. and Shamir, A.: How To Prove Yourself: Practical Solutions to Identification and Signature Problems, *Advances in Cryptology — CRYPTO' 86* (Odlyzko, A. M., ed.), Berlin, Heidelberg, Springer Berlin Heidelberg, pp. 186–194 (1987).

[6] Fleischhacker, N., Jager, T. and Schröder, D.: On Tight Security Proofs for Schnorr Signatures, *ASIACRYPT 2014* (Sarkar, P. and Iwata, T., eds.), LNCS, Vol. 8873, Springer, Heidelberg, pp. 512–531 (online), DOI: 10.1007/978-3-662-45611-8_27 (2014).

[7] Fuchsbauer, G., Kiltz, E. and Loss, J.: The Algebraic Group Model and its Applications, *Advances in Cryptology – CRYPTO 2018* (Shacham, H. and Boldyreva, A., eds.), Cham, Springer International Publishing, pp. 33–62 (2018).

[8] Fuchsbauer, G., Plouviez, A. and Seurin, Y.: Blind Schnorr Signatures and Signed ElGamal Encryption in the Algebraic Group Model, *Advances in Cryptology – EUROCRYPT 2020* (Canteaut, A. and Ishai, Y., eds.), Cham, Springer International Publishing, pp. 63–95 (2020).

[9] Garg, S., Bhaskar, R. and Lokam, S. V.: Improved Bounds on Security Reductions for Discrete Log Based Signatures, *Advances in Cryptology – CRYPTO 2008* (Wagner, D., ed.), Springer Berlin Heidelberg, pp. 93–107 (2008).

[10] Katz, J. and Wang, N.: Efficiency Improvements for Signature Schemes with Tight Security Reductions, *Proceedings of the 10th ACM Conference on Computer and Communications Security*, CCS '03, New York, NY, USA, ACM, pp. 155–164 (online), DOI: 10.1145/948109.948132 (2003).

[11] Kiltz, E., Masny, D. and Pan, J.: Optimal Security Proofs for Signatures from Identification Schemes, *Advances in Cryptology – CRYPTO 2016* (Robshaw, M. and Katz, J., eds.), Berlin, Heidelberg, Springer Berlin Heidelberg, pp. 33–61 (2016).

[12] Paillier, P. and Vergnaud, D.: Discrete-Log-Based Signatures May Not Be Equivalent to Discrete Log, *Advances in Cryptology - ASIACRYPT 2005* (Roy, B., ed.), Springer Berlin Heidelberg, pp. 1–20 (2005).

[13] Pointcheval, D. and Stern, J.: Security Arguments for Digital Signatures and Blind Signatures, *Journal of Cryptology*, Vol. 13, No. 3, pp. 361–396 (online), available from ⟨https://doi.org/10.1007/s001450010003⟩ (2000).

[14] Schnorr, C. P.: Efficient signature generation by smart cards, *Journal of Cryptology*, Vol. 4, No. 3, pp. 161–174 (online), available from ⟨https://doi.org/10.1007/BF00196725⟩ (1991).

[15] Seurin, Y.: On the Exact Security of Schnorr-Type Signatures in the Random Oracle Model, *Advances in Cryptology – EUROCRYPT 2012* (Pointcheval, D. and Johansson, T., eds.), Springer Berlin Heidelberg, pp. 554–571 (2012).