Non-Programmable Random Oracle モデル上で安全性証明可能な Fiat-Shamir 型署名

福光 正幸 †　　長谷川 真吾 ‡

† 北海道情報大学
069-8585 北海道江別市西野幌 59-2
fukumitsu@do-johodai.ac.jp

‡ 東北大学
980-8576　仙台市青葉区川内 41
hasegawa@cite.tohoku.ac.jp

あらまし Paillier, Vergnaud は, Schnorr 署名など特定の Fiat-Shamir 型署名（Fiat-Shamir 変換によって得られる署名方式の総称）に対して, 標準モデル上での安全性証明が困難であること, およびこれらが tight secure でないことを表す状況証拠を示した. さらに, 標準モデルと Random Oracle モデルの中間モデルとして知られている NPROM (Non-Programmable Random Oracle Model) 上においても, Fischlin, Fleischhacker が安全性証明の困難性を示している. 本稿では, Catalano, Visconti により提案された Dual-Mode Commitment を用いて, Fiat-Shamir 変換を改良し, DDH 仮定の下でかつ NPROM 上で tight secure な署名方式を構成する.

A Provably Secure Fiat-Shamir-Type Signature in the Non-Programmable Random Oracle Model

Masayuki Fukumitsu†　　Shingo Hasegawa‡

†Hokkaido Information University
Nishi Nopporo 59-2, Ebetsu, Hokkaido, 069-8585, JAPAN
fukumitsu@do-johodai.ac.jp

‡Tohoku University Kawauchi 41, Aoba-ku, Sendai, Miyagi, 980-8576, JAPAN
hasegawa@cite.tohoku.ac.jp

Abstract Paillier and Vergnaud showed the impossibility of proving the security of the Fiat-Shamir(FS) type signatures in the random oracle model. Fischlin and Fleischhacker showed the similar results in the non-programmable random oracle model (NPROM). In this paper, we construct an enhanced variant of the FS transformation, and propose a signatures which can be proven to be tightly secure in the NPROM by adopting the new transformation. To construct our transformation, we employ the *dual-mode commitment* which is introduced by Catalano and Visconti. Our signature is based on the signature given by Katz and Wang (KW signature). By applying the new transformation to the ID scheme corresponding to the KW signature, we obtains a tightly secure signature from the DDH assumption in the NPROM.

1　はじめに

Fiat-Shamir(FS) 変換 [8] は ID スキームから署名を構成する一般的手法であり, 代表的な FS 型署名としては Schnorr 署名 [23] や GQ 署名 [16] などが知られている. FS 型署名の安全性については, Pointcheval, Stern [22] が, 元になる

ID スキームが正当な検証者に対し知識のゼロ知識証明であるとき, ランダムオラクルモデル (ROM) において選択文書攻撃に対し存在的偽造不可 (EUF-CMA) であることを示している. Abdalla, An, Bellare, Namprempre [1] は上記の条件を緩和し, FS 型署名が ROM において EUF-CMA であることと, 元になる ID スキームが受動攻撃に対しなりすまし不可 (imp-pa 安全) であることが等価であることを示した.

暗号方式が tight な安全性証明を持つかは現代暗号における重要なトピックの 1 つである. FS 型署名においては, それについて否定的な結果がいくつか知られている [13, 21, 24]. つまり, いくつかの FS 型署名は代数的帰着により tight な安全性を署名できないというものである. 代数的帰着は安全性証明における妥当な手法と考えられているため [2, 3, 6, 11, 12, 21, 25], FS 型署名は通常の安全性証明のテクニックでは tight な安全性が示せないと考えられる. 一方で, 肯定的な結果も存在する. Micali, Reyzin [18] は, ID スキームから tight な安全性を持つ署名を作成できる変換方法を提案した. しかしながら, 彼らの結果は全ての ID スキームに適用出来る訳ではなく, 例えば Schnorr ID には適用できない. Katz, Wang [14] は, DDH 仮定から tight な安全性を証明できる FS 型署名 (KW 署名) を提案した. KW 署名を一般化することにより, Abdalla, Fouque, Lyubashevsky, Tibouchi は lossyID スキームの概念を提案し, lossyID スキームは tight な安全性を持つ署名に変換可能であることを示した. なお, これらの結果は全て ROM 上におけるものである.

もう 1 つの重要なトピックは標準モデル上での証明可能安全性である. FS 型署名の標準モデル上における安全性は既に議論されている. Paillier, Vergnaud [21] は Schnorr 署名の EUF-CMA 安全性が DL 仮定から証明できないことを, OM-DL 仮定 [4] の下で示した. 彼らの結果は GQ 署名にも適用可能である. 一方, Bellare, Shoup[5] は two-tier 署名の概念を提案し, concurrent attack に対し安全 (ss-ca 安全) な ID スキームから two-tier 署名への変換法を与えた. 彼らの変換によって得られる two-tier 署名の安全性は, 標準的な署名の安全性より弱いものの, 標準モデル上で証明可能である.

本稿では, FS 型署名は標準モデル上で tight な安全性証明が可能か, を議論する. [21] の結果より, FS 型署名を標準モデル上で安全性証明することは難しいと考えられる. さらに, Fischlin, Fleischhacker[9] は同様の不可能性が non-programmable random oracle model(NPROM) 上でも成り立つことを示した. NPROM [10, 20] は, ランダムオラクルは ROM と同様にランダムな値を出力するものの, 安全性証明において独立な参加者として扱われるという, ROM よりも弱いモデルである. [9] では, Schnorr 署名が, NPROM 上で single-instance 帰着により DL 仮定から安全性を証明できないことを OM-DL 仮定の下で示している. これらの結果は, オリジナルの FS 型署名は標準モデル, または NPROM 上では安全性証明が難しいことを示唆している. よって, これらのモデル上で (tight な) 安全性証明を行うためには, FS 変換を改良することが必要と考えられる. ここで, FS 変換のメリットは, 変換された署名方式の効率の良さもあるため, それを維持しながらの改良が望ましい. 本稿では, そのような変換方法を構築することを目的とし, その第一歩として NPROM 上で安全性証明が可能な FS 型変換の構成を目指す.

1.1 結果

本稿では, NPROM 上で tight な安全性を持つ署名方式を導く, FS 変換の改良を目的とする. 目的達成のため, dual-mode コミットメントを利用する. dual-mode コミットメントは Catalano, Visconti [7] により提案された, CRS モデルにおいて, CRS の生成アルゴリズムを 2 つ持つコミットメントである. 通常の生成アルゴリズムでは, コミットメントは perfectly binding であり, もう一方の方法では, コミットされた値を任意の値にデコミットすることが可能である. Lindell [17] は, この dual-mode コミットメントを利用して, NPROM 上で Σ プロトコルから非対話ゼロ知識証明の構成を行っている.

上記の dual-mode コミットメントを用いて, FS 変換の改良を行い, その新しい変換を用いて

The EF-CMA game of the signature $\mathfrak{S}$ between a challenger $\mathcal{C}$ and a forger $\mathcal{F}$

Init: $\mathcal{C}$ は $(pk, sk) \leftarrow \mathsf{KGen}(1^k)$ を生成し, pk を $\mathcal{F}$ に送る.

Sign: $\mathcal{F}$ のクエリ m_i に対し, $\mathcal{C}$ は (pk, m_i) に関する署名 σ_i を作成し返答する.

Challenge: $\mathcal{F}$ が (m^*, σ^*) を出力した場合, $\mathcal{C}$ は $m^* \notin \{m_i\}_i \wedge \mathsf{Ver}(pk, m^*, \sigma^*) = 1$ が成り立つとき 1 を出力する.

図 1: EF-CMA ゲームの概要

NPROM 上で tight な安全性証明が可能な署名方式を構築する. 新方式は Katz, Wang[14] による方式 (KW 署名) をベースとする. KW 署名は ROM 上で DDH 仮定から tight な安全性証明が可能な方式であり, 対応する ID スキームである KWID スキームから FS 変換によって構成される. FS 変換に dual-mode コミットメントを組み込み, それを KWID スキームに適用することで, NPROM 上で DDH 仮定より tight な安全性証明が可能な署名方式を構築する.

2 準備

本稿では必要な用語や記号の定義を行う. λ を空文字列とする. $x \in_{\mathrm{U}} D$ で, x が集合 D から一様ランダムに選ばれることを表す. $x := y$ で, x が y で定義または置き換えられることを表す. アルゴリズム $\mathcal{A}$ について, $y \leftarrow \mathcal{A}(x)$ は入力 x に対し y を出力することを表す. $\mathcal{A}$ が確率的なふるまいをする場合, $\mathcal{A}(x)$ は入力 x に対する出力の確率変数を意味する. ただし, 確率は $\mathcal{A}$ の内部乱数に従う. 特に, $y \leftarrow \mathcal{A}(x; r)$ と書くときは乱数として r を使用していることを表す.

関数 $\nu(k)$ が**無視できる**とは, 任意の多項式 μ について定数 k_0 が存在し, 全ての $k \geq k_0$ に対して $\nu(k) < 1/\mu(k)$ であることをいう. negl をなんらかの無視できる関数を表すものとする. k はセキュリティパラメータである.

X と Y を集合 D 上の確率変数とし, $\mathcal{X} = \{X_k\}_k$ と $\mathcal{Y} = \{Y_k\}_k$ を集合 D_k 上に定義される確率変数 X_k, Y_k の族とする. $\mathcal{X}$ が $\mathcal{Y}$ と**計算量的に識別できない**とは, 任意の確率的多項式時間 (PPT) 機械 $\mathcal{A}$ について, $|\Pr[\mathcal{A}(1^k, X_k) = 1] - \Pr[\mathcal{A}(1^k, Y_k) = 1]| = \mathrm{negl}(k)$ が成り立つことをいう. X と Y の統計的距離を $\Delta(X, Y) := 1/2 \sum_{v \in D} |\Pr[X = v] - \Pr[Y = v]|$ で定義する.

補題 1 ([19]) X と Y を集合 D 上の確率変数とし, R を集合, $f : D \to R$ を関数とする. このとき, $\Delta(f(X), f(Y)) \leq \Delta(X, Y)$ が成り立つ.

2.1 署名

署名方式$\mathfrak{S}$ は 3 つのアルゴリズム $(\mathsf{KGen}, \mathsf{Sign}, \mathsf{Ver})$ から成る. 鍵生成アルゴリズム KGen は入力のセキュリティパラメータ 1^k に対し公開鍵 pk と秘密鍵 sk を出力する. 署名アルゴリズム Sign は入力 (pk, sk, m) に対し署名 σ を出力する. 検証アルゴリズム Ver は入力 (pk, m, σ) に対し署名 σ が公開鍵 pk におけるメッセージ m 署名であるとき, またそのときに限り 1 を出力する.

選択文書攻撃に対する存在的偽造 *(EUF-CMA)* [15] の定義を行う. $\mathfrak{S} = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Ver})$ を署名方式とする. 図 1 に, $\mathfrak{S}$ に対する選択文書攻撃による存在的偽造ゲーム (EF-CMA ゲーム) の概要を表す. 偽造者 $\mathcal{F}$ が *EF-CMA* **ゲームに勝つ**とは, 挑戦者 $\mathcal{C}$ が EF-CMA ゲームにおいて 1 を出力することをいう. 署名方式 $\mathfrak{S}$ が *EUF-CMA* であるとは, 任意の多項式時間偽造者 $\mathcal{F}$ について, $\mathcal{F}$ が EF-CMA ゲームに勝つ確率が k において無視できることである. なお, 確率の全空間は $\mathcal{C}$ と $\mathcal{F}$ の内部乱数である. また, 署名方式 $\mathfrak{S}$ が (T, ϵ, q_S, q_H)-*EUF-CMA* であるとは, 任意の時間 T で動作し, **Sign** フェイズにおいて q_S 回の署名クエリと q_H 回のハッシュクエリを行う偽造者 $\mathcal{F}$ について, $\mathcal{F}$ が EF-CMA ゲームに勝つ確率が高々 ϵ であることである.

$\mathbf{Exp}^{\mathsf{DDH}}_{\mathsf{Samp}_{\mathsf{DDH}},\mathcal{A}}(k)$	$\mathbf{Exp}^{\mathsf{DDH}}_{\mathsf{Samp}_{\mathsf{rand}},\mathcal{A}}(k)$
1. $(D, w) \leftarrow \mathsf{Samp}_{\mathsf{DDH}}(1^k)$; and	1. $(D, w) \leftarrow \mathsf{Samp}_{\mathsf{rand}}(1^k)$; and
2. return $\mathcal{A}(D)$	2. return $\mathcal{A}(D)$

$\mathsf{Samp}_{\mathsf{DDH}}(1^k)$	$\mathsf{Samp}_{\mathsf{rand}}(1^k)$
1. $(\mathbb{G}, p, g) \leftarrow \mathsf{IGen}(1^k)$, $h \in_{\mathrm{U}} \mathbb{G}$;	1. $(\mathbb{G}, p, g) \leftarrow \mathsf{IGen}(1^k)$, $h \in_{\mathrm{U}} \mathbb{G}$;
2. $x \in_{\mathrm{U}} \mathbb{Z}_p$;	2. $x_1, x_2 \in_{\mathrm{U}} \mathbb{Z}_p$; and
3. $y_1 := g^x$, $y_2 := h^x$;	3. $y_1 := g^{x_1}$, $y_2 := h^{x_2}$; and
4. $D := (\mathbb{G}, p, g, h, y_1, y_2)$, $w := x$ and	4. $D := (\mathbb{G}, p, g, h, y_1, y_2)$, $w := (x_1, x_2)$ and
5. return (D, w).	5. return (D, w).

図 2: $\mathbf{Exp}^{\mathsf{DDH}}_{\mathsf{Samp}_{\mathsf{DDH}},\mathcal{A}}$ と $\mathbf{Exp}^{\mathsf{DDH}}_{\mathsf{Samp}_{\mathsf{rand}},\mathcal{A}}$ の概要

2.2 DDH 仮定 [14]

$\mathbb{G}$ を生成元 g を持つ素数位数 p の群とする. IGen を群生成器とする. 入力 1^k について, IGen は群 $\mathbb{G}$, 素数 p, 生成元 g の組 $(\mathbb{G}, p, g)$ を出力する. $D := (\mathbb{G}, p, g, h, y_1, y_2)$ を *DDH* **インスタンス**と呼ぶ. 特に, ある $x \in \mathbb{Z}_p$ について $y_1 = g^x$, $y_2 = h^x$ が成り立つとき, *DDH* **タプル**と呼ぶ. x を D の**証拠**と呼ぶ. アルゴリズム $\mathcal{A}$ が *DDH* **問題**を解くとは, 与えられた DDH タプルに対し 1 を出力することである. *DDH* **仮定が成り立つ**とは, 任意の PPT アルゴリズム $\mathcal{A}$ に対し,

$$\begin{aligned}&\mathsf{Adv}^{\mathsf{DDH}}_{\mathcal{A}}(k)\\ &:= \Big|\Pr\Big[\mathbf{Exp}^{\mathsf{DDH}}_{\mathsf{Samp}_{\mathsf{DDH}},\mathcal{A}}(k) = 1\Big]\\ &\quad - \Pr\Big[\mathbf{Exp}^{\mathsf{DDH}}_{\mathsf{Samp}_{\mathsf{rand}},\mathcal{A}}(k) = 1\Big]\Big| = \mathrm{negl}(k),\end{aligned}$$

が成り立つことである. ここで, $\mathbf{Exp}^{\mathsf{DDH}}_{\mathsf{Samp}_{\mathsf{DDH}},\mathcal{A}}$ と $\mathbf{Exp}^{\mathsf{DDH}}_{\mathsf{Samp}_{\mathsf{rand}},\mathcal{A}}$ は図 2 に示すとおりである.

また,$(T_{\mathsf{DDH}}, \epsilon_{\mathsf{DDH}})$-DDH 仮定が成り立つとは, 任意の時間 T_{DDH} で動作する偽造者 $\mathcal{A}$ について, $\mathsf{Adv}^{\mathsf{DDH}}_{\mathcal{A}}(k) \leq \epsilon_{\mathsf{DDH}}$ が成り立つことである.

DDH 仮定について, 次の補題が成り立つ.

補題 2 $\mathsf{Samp}_{\mathsf{rand}}(1^k)$ が生成する $(\mathbb{G}, p, g, h, y_1, y_2)$ が *DDH* タプルである確率は $1/p$ である.

補題 3 ([14]) $(\mathbb{G}, p, g, h, y_1, y_2)$ が *DDH* タプルでないと仮定する. このとき, 任意の $A, B \in \mathbb{G}$ について, 高々*1* つの $\mathsf{cha}^+ \in \mathbb{Z}_p$ が存在し, ある $\mathsf{res} \in \mathbb{Z}_p$ について $A = g^{\mathsf{res}} y_1^{\mathsf{cha}^+}$, $B = h^{\mathsf{res}} y_2^{\mathsf{cha}^+}$ が成り立つ.

2.3 Dual-Mode コミットメント

dual-mode コミットメント $\mathfrak{D}$ は 3 つのアルゴリズム $(\mathsf{GenCRS}, \mathsf{Com}, \mathsf{S}_{\mathsf{com}})$ から成る. CRS 生成アルゴリズム GenCRS は入力のセキュリティパラメータ 1^k に対し CRSϱ を出力する. コミットメント作成アルゴリズム Com_ϱ は入力のメッセージ M と CRSϱ に対しコミットメント cmt を出力する. $\mathsf{S}_{\mathsf{com}}$ は以下の 3 つのモードを持つ: (1) 入力の 1^k に対し CRS とトラップドアのペア (ϱ, td) を出力する, (2) 入力の (ϱ, td) に対し cmt を出力する, (3) 入力の $(\varrho, \mathsf{td}, \mathsf{cmt}, M)$ に対し $r \in \{0,1\}^{\ell_{\mathsf{rand}}}$ を出力する, ただし ℓ_{rand} は k の多項式である.

dual-mode コミットメントは以下の性質を持つ:

Perfectly Binding $(\mathsf{GenCRS}, \mathsf{Com})$ について, $\varrho \leftarrow \mathsf{GenCRS}(1^k)$ の場合 $\mathsf{Com}_\varrho(M; r)$ は非対話かつ perfectly-binding なコミットメントである.

Correct Simulation k, $(\varrho, \mathsf{td}) \leftarrow \mathsf{S}_{\mathsf{com}}(1^k)$, $\mathsf{cmt} \leftarrow \mathsf{S}_{\mathsf{com}}(\varrho, \mathsf{td})$ について, $r \leftarrow \mathsf{S}_{\mathsf{com}}(\varrho, \mathsf{td}, \mathsf{cmt}, M)$ に対し $\mathsf{cmt} = \mathsf{Com}_\varrho(M, r)$.

$(q_{\mathfrak{D}}, \epsilon_{\mathfrak{D}})$**-DM-indistinguishability** $(\mathsf{Com}, \mathsf{S}_{\mathsf{com}})$

$\mathbf{Exp}^{\mathsf{DM}}_{\mathsf{Com},\mathcal{A}}(k)$	$\mathbf{Exp}^{\mathsf{DM}}_{\mathsf{S_{com}},\mathcal{A}}(1^k)$
1. $\varrho \leftarrow \mathsf{GenCRS}(1^k)$	1. $(\varrho, \mathsf{td}) \leftarrow \mathsf{S_{com}}(1^k)$
2. $\boldsymbol{c} := \emptyset, \boldsymbol{r} := \emptyset$	2. $\boldsymbol{c} := \emptyset, \boldsymbol{r} := \emptyset$
3. for $i = 1$ to $q_{\mathsf{DM}}(k)$,	3. for $i = 1$ to $q_{\mathsf{DM}}(k)$,
(a) $M_i \leftarrow \mathcal{A}(\varrho, \boldsymbol{c}, \boldsymbol{r})$	(a) $\mathsf{cmt}_i \leftarrow \mathsf{S_{com}}(\varrho, \mathsf{td})$
(b) $r_i \in_{\mathrm{U}} \{0,1\}^{\mathrm{poly}(k)}$	(b) $M_i \leftarrow \mathcal{A}(\varrho, \boldsymbol{c}, \boldsymbol{r})$
(c) $\mathsf{cmt}_i \leftarrow \mathsf{Com}_\varrho(M_i; r_i)$	(c) $r_i \leftarrow \mathsf{S_{com}}(\varrho, \mathsf{td}, \mathsf{cmt}_i, M_i)$
(d) $\boldsymbol{c} := (\mathsf{cmt}_1, \mathsf{cmt}_2, \ldots, \mathsf{cmt}_i)$ and $\boldsymbol{r} := (r_1, r_2, \ldots, r_i)$.	(d) $\boldsymbol{c} := (\mathsf{cmt}_1, \mathsf{cmt}_2, \ldots, \mathsf{cmt}_i)$ and $\boldsymbol{r} := (r_1, r_2, \ldots, r_i)$.
4. output $\mathcal{A}(\varrho, \boldsymbol{c}, \boldsymbol{r})$.	4. output $\mathcal{A}(\varrho, \boldsymbol{c}, \boldsymbol{r})$.

図 3: $\mathbf{Exp}^{\mathsf{DM}}_{\mathsf{Com},\mathcal{A}}$ と $\mathbf{Exp}^{\mathsf{DM}}_{\mathsf{S_{com}},\mathcal{A}}$ の概要

と PPT アルゴリズム $\mathcal{A}$ について,

$$\begin{aligned}&\mathsf{Adv}^{\mathsf{DM}}_{\mathcal{A}}(k)\\ &:= \Big|\Pr\Big[\mathbf{Exp}^{\mathsf{DM}}_{\mathsf{Com},\mathcal{A}}(k) = 1\Big]\\ &\quad - \Pr\Big[\mathbf{Exp}^{\mathsf{DM}}_{\mathsf{S_{com}},\mathcal{A}}(k) = 1\Big]\Big| \le \epsilon_{\mathsf{DM}},\end{aligned}$$

が成り立つ. ここで, $\mathbf{Exp}^{\mathsf{DM}}_{\mathsf{Com},\mathcal{A}}$ と $\mathbf{Exp}^{\mathsf{DM}}_{\mathsf{S_{com}},\mathcal{A}}$ は図 3 に示すとおりである.

dual-mode コミットメントの具体的な構成は [17] で与えられている.

2.4 KWID スキームと KW 署名

KWID スキーム [14] は証明者 (prover) と検証者 (verifier) による 3-move のプロトコルであり, 詳細は図 4 に示すとおりである.

KW 署名は KWID スキームに FS 変換を適用して得られる署名方式であり, その詳細は図 5 に示すとおりである. KW 署名は DDH 仮定の下で ROM において EUF-CMA であることが知られている [14].

3 改良 KW 署名

本節では KW 署名の改良方式の提案を行い, その安全性の証明を行う. 改良には dual-mode コミットメント $\mathfrak{D} = (\mathsf{GenCRS}, \mathsf{Com}, \mathsf{S_{com}})$ を使用する. 改良方式の概要は以下のとおりである. 公開鍵 pk は KW 署名の公開鍵に加え, dual-mode コミットメント $\mathfrak{D}$ の $\mathrm{CRS}\,\varrho \leftarrow \mathsf{GenCRS}(1^k)$ から構成される. 署名アルゴリズムはコミットメント $\mathsf{cmt} := \mathsf{Com}_\varrho(A, B, m; r)(r \in_{\mathrm{U}} \{0,1\}^{\ell_{\mathsf{rand}}})$ を計算し, チャレンジ $\mathsf{cha} := H_{pk}(\mathsf{cmt}, m)$ を生成する. res は KW 署名と同様に計算され, 署名は $\sigma = (\mathsf{cha}, \mathsf{res}, r)$ である. 改良 KW 署名の詳細を図 6 に示す. 改良 KW 署名の安全性について, 次の定理が成り立つ.

定理 1 $\mathfrak{D} = (\mathsf{GenCRS}, \mathsf{Com}, \mathsf{S_{com}})$ を *dual-mode* コミットメントとする. $(\mathsf{Com}, \mathsf{S_{com}})$ の $(q_S, \epsilon_{\mathsf{DM}})$-*DM-indistinguishability,* および $(T_{\mathsf{DDH}}, \epsilon_{\mathsf{DDH}})$-*DDH* 仮定が成り立つと仮定する. このとき, 改良 *KW* 署名は *NPROM* において (T, ϵ, q_S, q_H)-*EUF-CMA* である. ただし,

$$\begin{aligned}T &\simeq T_{\mathsf{DDH}} - O(\mathrm{poly}(k)),\\ \epsilon &\le \epsilon_{\mathsf{DDH}} + \epsilon_{\mathsf{DM}} + \frac{1}{p} + \frac{q_H + 1}{p},\end{aligned}$$

である.

参考文献

[1] M. Abdalla, J.H. An, M. Bellare, and C. Namprempre, "From Identification to

(1) 証明者は $\mathsf{st} \in_{\mathrm{U}} \mathbb{Z}_p$ を選び $A := g^{\mathsf{st}}$, $B := h^{\mathsf{st}}$ を検証者に送る.

(2) 検証者はチャレンジ $\mathsf{cha} \in_{\mathrm{U}} \mathbb{Z}_p$ を証明者に送る.

(3) 証明者はレスポンス $\mathsf{res} := \mathsf{st} + sk \cdot \mathsf{cha} \bmod p$ を検証者に送る.

(4) 検証者は $A = g^{\mathsf{res}} y_1^{-\mathsf{cha}}$ と $B = h^{\mathsf{res}} y_2^{-\mathsf{cha}}$ が成り立つとき受理する.

図 4: KWID スキーム

$\mathsf{KGen}(1^k)$ 公開鍵と秘密鍵のペア $(pk, sk) := ((\mathbb{G}, p, g, h, y_1, y_2), x) \leftarrow \mathsf{Samp}_{\mathsf{DDH}}(1^k)$ を生成する.

$\mathsf{Sign}(pk, sk, m)$ 以下のように署名 $\sigma = (\mathsf{cha}, \mathsf{res})$ を作成する:

(1) $\mathsf{st} \in_{\mathrm{U}} \mathbb{Z}_p$;

(2) $A := g^{\mathsf{st}}$, $B := h^{\mathsf{st}}$;

(3) $\mathsf{cha} := H_{pk}(A, B, m)$; and

(4) $\mathsf{res} := \mathsf{st} + sk \cdot \mathsf{cha} \bmod p$.

$\mathsf{Ver}(pk, m, (\mathsf{cha}, \mathsf{res}))$ $a := g^{\mathsf{res}} y_1^{-\mathsf{cha}}$, $b := h^{\mathsf{res}} y_2^{-\mathsf{cha}}$ とし, $\mathsf{cha} = H_{pk}(a, b, m)$ ならば 1 を出力する.

図 5: KW 署名

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. (Conference Ver.: Proc. EUROCRYPT 2002, LNCS, vol. 2332, pp. 418–433, 2002).

[2] M. Abe, J. Groth, and M. Ohkubo, "Separating Short Structure-Preserving Signatures from Non-interactive Assumptions," Proc. ASIACRYPT 2011, LNCS, vol.7073, pp.628–646, 2011.

[3] M. Abe, K. Haralambiev, and M. Ohkubo, "Group to Group Commitments Do Not Shrink," Proc. EUROCRYPT 2012, LNCS, vol.7237, pp.301–317, 2012.

[4] M. Bellare, C. Namprempre, D. Pointcheval, and M. Semanko, "The One-More-RSA-Inversion Problems and the Security of Chaum's Blind Signature Scheme," J. Cryptology, vol.16, no.3, pp.185–215, 2003. (Conference Ver.: Proc. Financial Cryptography 2001, LNCS, vol. 2339, 2002).

[5] M. Bellare and S. Shoup, "Two-Tier Signatures, Strongly Unforgeable Signatures, and Fiat-Shamir Without Random Oracles," Proc. PKC 2007, LNCS, vol.4450, pp.201–216, 2007.

[6] D. Boneh, "The Decision Diffie-Hellman problem," Proc. Algorithmic Number Theory, LNCS, vol.1423, pp.48–63, 1998.

[7] D. Catalano and I. Visconti, "Hybrid commitments and their applications to zero-knowledge proof systems," Theoretical Computer Science, vol.374, no.1–3, pp.229–260, 2007.

[8] A. Fiat and A. Shamir, "How to Prove Yourself: Practical Solutions to Identification and Signature Problems," Proc.

$\mathsf{KGen}(1^k)$ 公開鍵と秘密鍵のペア (pk, sk) を以下のように生成する:

(1) $\varrho \leftarrow \mathsf{GenCRS}(1^k)$;

(2) $((\mathbb{G}, p, g, h, y_1, y_2), x) \leftarrow \mathsf{Samp}_{\mathsf{DDH}}(1^k)$; and

(3) set $pk := (\varrho, \mathbb{G}, p, g, h, y_1, y_2)$ and $sk := x$.

$\mathsf{Sign}(pk, sk, m)$ 署名 $\sigma = (\mathsf{cha}, \mathsf{res}, r)$ を以下のように作成する:

(1) $\mathsf{st} \in_{\mathrm{U}} \mathbb{Z}_p$;

(2) $A := g^{\mathsf{st}}$, $B := h^{\mathsf{st}}$;

(3) $r \in_{\mathrm{U}} \{0,1\}^{\ell_{\mathsf{rand}}}$;

(4) $\mathsf{cmt} := \mathsf{Com}_{\varrho}(A, B, m; r)$;

(5) $\mathsf{cha} := H_{pk}(\mathsf{cmt}, m)$; and

(6) $\mathsf{res} := \mathsf{st} + sk \cdot \mathsf{cha} \bmod p$.

$\mathsf{Ver}(pk, m, (\mathsf{cha}, \mathsf{res}, r))$ $a := g^{\mathsf{res}} y_1^{-\mathsf{cha}}$, $b := h^{\mathsf{res}} y_2^{-\mathsf{cha}}$ とし, $c := \mathsf{Com}_{\varrho}(a, b, m; r)$ とする. $\mathsf{cha} = H_{pk}(c, m)$ ならば 1 を出力する.

図 6: 改良 KW 署名

CRYPTO'86, LNCS, vol.263, pp.186–194, 1987.

[9] M. Fischlin and N. Fleischhacker, "Limitations of the Meta-reduction Technique: The Case of Schnorr Signatures," Proc. EUROCRYPT 2013, LNCS, vol.7881, pp.444–460, 2013. (Full Ver.: Cryptology ePrint Archive, Report 2013/140).

[10] M. Fischlin, A. Lehmann, T. Ristenpart, T. Shrimpton, M. Stam, and S. Tessaro, "Random Oracles with(out) Programmability," Proc. ASIACRYPT 2010, LNCS, vol.6477, pp.303–320, 2010.

[11] M. Fukumitsu, S. Hasegawa, S. Isobe, E. Koizumi, and H. Shizuya, "Toward Separating the Strong Adaptive Pseudo-freeness from the Strong RSA Assumption," Proc. ACISP 2013, LNCS, vol.7959, pp.72–87, 2013.

[12] M. Fukumitsu, S. Hasegawa, S. Isobe, and H. Shizuya, "On the Impossibility of Proving Security of Strong-RSA Signatures via the RSA Assumption," Proc. ACISP 2014, LNCS, vol.8544, pp.290–305, 2014.

[13] S. Garg, R. Bhaskar, and S. Lokam, "Improved Bounds on Security Reductions for Discrete Log Based Signatures," Proc. CRYPTO 2008, LNCS, vol.5157, pp.93–107, 2008.

[14] E.J. Goh, S. Jarecki, J. Katz, and N. Wang, "Efficient Signature Schemes with Tight Reductions to the Diffie-Hellman Problems," J. Cryptology, vol.20, no.4, pp.493–514, 2007. (Conference Ver.: Proc. ACM CCS 2003, pp. 155–164, 2003).

[15] S. Goldwasser, S. Micali, and R.L. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," SIAM Journal on Computing, vol.17, no.2, pp.281–308, 1988.

[16] L.C. Guillou and J.J. Quisquater, "A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Transmission and Memory," Proc. Eurocrypt'88, LNCS, vol.330, pp.123–128, 1988.

[17] Y. Lindell, "An Efficient Transform from Sigma Protocols to NIZK with a CRS and Non-programmable Random Oracle," Proc. TCC 2015, LNCS, vol.9014, pp.93–109, 2015. (Full Ver.: Cryptology ePrint Archive, Report 2014/710).

[18] S. Micali and L. Reyzin, "Improving the exact security of digital signature schemes," J. Cryptology, vol.15, no.1, pp.1–18, 2002.

[19] D. Micciancio and S. Goldwasser, Complexity of Lattice Problems: A Cryptographic Perspective, Kluwer Academic Publishers, 2002.

[20] J. Nielsen, "Separating Random Oracle Proofs from Complexity Theoretic Proofs: The Non-committing Encryption Case," Proc. CRYPTO 2002, LNCS, vol.2442, pp.111–126, 2002.

[21] P. Paillier and D. Vergnaud, "Discrete-Log-Based Signatures May Not Be Equivalent to Discrete Log," Proc. ASIACRYPT 2005, LNCS, vol.3788, pp.1–20, 2005.

[22] D. Pointcheval and J. Stern, "Security Arguments for Digital Signatures and Blind Signatures," J. Cryptology, vol.13, no.3, pp.361–396, 2000.

[23] C. Schnorr, "Efficient Signature Generation by Smart Cards," J. Cryptology, vol.4, no.3, pp.161–174, 1991.

[24] Y. Seurin, "On the Exact Security of Schnorr-Type Signatures in the Random Oracle Model," Proc. EUROCRYPT 2012, LNCS, vol.7237, pp.554–571, 2012.

[25] J. Villar, "Optimal Reductions of Some Decisional Problems to the Rank Problem," Proc. ASIACRYPT 2012, LNCS, vol.7658, pp.80–97, 2012.