SCIS 2007 The 2007 Symposium on Cryptography and Information Security
Sasebo, Japan, Jan. 23-26, 2007
The Institute of Electronics, Information and Communication Engineers

強偽造不可能性を満たす署名方式を作る一般的変換方法
General Conversion for Obtaining Strongly Existentially Unforgeable Signatures[1]

寺西勇*† 小山拓郎† 尾形わかは†
Isamu Teranishi Takuro Oyama Wakaha Ogata

あらまし 署名方式が強偽造不可能性を満たすとは，選択文書攻撃が可能ないかなる攻撃者も，(既知もしくは新たな) メッセージに対する新たな署名文を生成することができないことを指す．強偽造不可能性は，公開鍵暗号方式やグループ署名方式など多くの暗号プロトコルを作る際に有用である．本稿では，通常の安全性を満たす署名方式を強偽造不可能性を満たす署名方式に変換する一般的変換方法を 2 つ提案する．第一の変換方法はランダムオラクルを必要とするが，その代わり変換後の方式の署名長が第二の変換方法で変換された方式のそれよりも短い．それに対し第二の変換方法はランダムオラクルを必要としない．よってもし変換前の方式の安全性がスタンダードモデルで示せるなら，変換後の方式の強偽造不可能性もスタンダードモデルで示せることになる．両変換とも，変換後の方式の強偽造不可能性はベースとなっている安全性仮定に tight に帰着される．しかも第一もしくは第二の方法で変換された方式は on-line/off-line 性を満たす．すなわち署名者は，署名すべきメッセージを受け取る前に，署名計算のほとんどを事前計算できる．よって署名者は非常に効率的に署名文を計算できる．

キーワード 署名方式，強偽造不可能性，スタンダードモデル

1 はじめに

強偽造不可能性は，署名方式の通常の安全性概念である偽造不可能性の変種である．強偽造不可能性は通常の偽造不可能性と同じく，攻撃者が署名文を偽造できないことを要請するが、強偽造不可能性の方が攻撃者により強い制約を課す。通常の偽造不可能性は署名者が過去に署名したことのないメッセージに対する署名文が偽造されていない事が保証するが，署名者がすでに署名したことのあるメッセージに対して新しい署名文を偽造されないことは保証しない．すなわち攻撃者は，与えられたメッセージ・署名文ペア (M,σ) に対し，M に対する新たな署名文 $\sigma' \neq \sigma$ を偽造することができるかも知れないのである．それに対し強偽造不可能性はそのような偽造すらもできないことを要請している．

強偽造不可能性は，IND-CCA2 安全な暗号方式 [DDN00, CHK04] やグループ署名方式 [BBS04] をはじめ，様々な暗号プロトコルを作るのに有用である．こうした暗号プロトコルでは，署名文が何らかのデータの一部として使われている．強偽造不可能性は，そのデータに関する non malleability を保証するのに使われる．

成果: 偽造不可能性を満たす署名方式を強偽造不可能性を満たす署名方式に変換する一般的方法を 2 つ提案する．第一の変換方法はランダムオラクルに頼っているが，変換後の方式の署名長が第二の方法で変換された方式のそれよりも短い．それに対し第二の変換方法はランダムオラクルを必要としない．よってもし変換前の方式の安全性がスタンダードモデルで示せるなら，変換後の方式の強偽造不可能性もスタンダードモデルで示せることになる．両変換とも，離散対数仮定をベースにしており，変換後の方式の強偽造不可能性はもとの方式の偽造不可能性と離散対数仮定とに tight に帰着される．しかも第一もしくは第二の方法で変換された方式は on-line/off-line 性を満たす．すなわち署名者は，署名すべきメッセージを受け取る前に，署名計算のほとんどを事前計算できる．よって署名者は非常に効率的に署名文を計算できる．

関連研究: Boneh 等 [BSW06] も同様な変換を提案しているが，彼らの変換は，*partitioned*[BSW06] という性質を満たす署名方式に対してしか適応できなかった．それに対し我々の変換は任意の署名方式に適応できる．また我々の第二の変換とほぼ同じものを，Steinfeld 等が我々

* NEC 〒 211-8666 神奈川県川崎市中原区下沼部 1753 1753, Shimonumabe, Nakahara-Ku, Kawasaki, Kanagawa, 211-8666, Japan. teranisi@ah.jp.nec.com
† 東京工業大学〒 152-8552 東京都目黒区大岡山 2-12-1 Tokyo Institute of Technology. 2-12-1 Ookayama, Meguro-ku Tokyo, 152-8550, Japan. wakaha@mot.titech.ac.jp
[1] 本研究は Indocrypt 2006 で発表した内容 [TOO06] と同一である。

とは独立に提案している [SPW07].

2 準備

定義 2.1. (偽造不可能性 [GMR88], 強偽造不可能性 [ADR02])
κ をセキュリティ・パラメータとし，$\Sigma = (\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$ を署名方式とし，$\mathcal{A}$ を攻撃者とする．以下のゲームを考える：$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\kappa)$，$(M_0, \sigma_0) \leftarrow \mathcal{A}^{\mathsf{Sig}_{\mathsf{sk}}}(\mathsf{pk})$.

$\mathcal{A}$ の i 番目の署名オラクルクエリ・返答ペアを (M_i, σ_i) とする．任意の i に対して $M_0 \neq M_i$(resp. $(M_0, \sigma_0) \neq (M_i, \sigma_i)$) でかつ $\mathsf{Ver}_{\mathsf{pk}}(M_0, \sigma_0) = \mathsf{accept}$ となるとき，$\mathcal{A}$ はゲームに**弱い意味で** *(resp.* **強い意味で***)* **勝った**という．

$t = t(\kappa)$，$q_S = q_S(\kappa)$，$\varepsilon = \varepsilon(\kappa)$ を非負値関数とする．Σ が次を満たすとき，Σ は (t, q_S, ε)-**偽造不可能**(resp. (t, q_S, ε)-**強偽造不可能**) であるという：任意の攻撃者 $\mathcal{A}$ に対し，もし $\mathcal{A}$ が最大 t ステップしか動作せず，$\mathcal{A}$ が q_S 回以下しか署名オラクルにクエリしないなら，$\mathcal{A}$ はゲームに弱い意味で (resp. 強い意味で) 勝つ確率は ε 未満．

Σ がランダムオラクルモデルにおける署名方式である場合には，$(t, q_S, q_H, \varepsilon)$-**偽造不可能性**や $(t, q_S, q_H, \varepsilon)$-**強偽造不可能性**も同様に定義する．ただし q_H は $\mathcal{A}$ がランダムオラクルにクエリする回数の上限．

(t, ε)-**離散対数仮定**やハッシュ関数の (t, ε')-**衝突困難性**も同様に定義する．

3 ランダムオラクルを用いた変換

本章では偽造不可能性を満たす署名方式をランダムオラクルモデルのもと強偽造不可能性を満たす署名方式に変換する一般的方法を提案する．κ をセキュリティ・パラメータとし，$\mathcal{G}$ を位数 q の巡回群とする．さらに $\mathcal{H} : \{0,1\}^* \to \mathbb{Z}_q$ を (安全性証明ではランダム・オラクルに置き換える) ハッシュ関数とする．$\Sigma = (\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$ を署名方式とする．

提案する変換方法で Σ を変換した後の方式を図 1 に載せる．ここで我々はカメレオン・コミットメント $C = g^x h^r$[KR97, KR00] を部品として使っている．変換後の方式は on-line/off-line 性を満たす．すなわち署名者は，メッセージ M をもらう前に x^{-1}，C，σ を事前計算できる．これらの事前計算を行っておけば，署名者は $\mathcal{H}(M||\sigma)$ と $r = (t - m)x^{-1} \bmod q$ を計算するのみで署名が生成でき，非常に効率的である．

定理 3.1. Σ' の $(t', q_S, q_H, \varepsilon')$-強偽造不可能性を破ることができる攻撃者が存在するなら，Σ の (t, q_S, ε)-偽造不可能性もしくは $\mathcal{G}$ の (t, ε)-離散対数仮定を破ることができる攻撃者が存在する．ただし

$$\begin{cases} t = t' + q_S(S' + E) + (\text{lower terms}), \\ \varepsilon = \frac{\varepsilon'}{9} - \frac{(q_H + q_S)q_S}{3q} - (\text{lower terms}). \end{cases}$$

—$\mathsf{Gen}'(1^\kappa)$— $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\kappa)$, $g \leftarrow \mathcal{G}$, $x \leftarrow \mathbb{Z}_q$, $h \leftarrow g^x$. $\mathsf{pk}' \leftarrow (\mathsf{pk}, g, h)$, $\mathsf{sk}' \leftarrow (\mathsf{sk}, x)$. $(\mathsf{pk}', \mathsf{sk}')$ を出力.
—$\mathsf{Sig}'_{\mathsf{sk}'}(M)$— $t \leftarrow \mathbb{Z}_q$, $C \leftarrow g^t$, $\sigma \leftarrow \mathsf{Sig}_{\mathsf{sk}}(C)$, $m \leftarrow \mathcal{H}(M\|\sigma)$. $m + rx = t \bmod q$ を満たす $r \in \mathbb{Z}_q$ を選ぶ. $\sigma' \leftarrow (\sigma, r)$. σ' を出力.
—$\mathsf{Ver}'_{\mathsf{pk}'}(M, \sigma')$— σ' を (σ, r) にパースする. $m \leftarrow \mathcal{H}(M\|\sigma)$, $C \leftarrow g^m h^r$. $\mathsf{Ver}_{\mathsf{pk}}(C, \sigma) = \mathsf{accept}$ なら accept を出力. そうでなければ reject を出力.

図 1: ランダムオラクルモデル版の変換で変換された方式

ここで S' は Σ' の署名計算量であり，E は $\mathcal{G}$ における冪乗剰余の計算量である．

Proof. $\mathcal{A}$ を Σ' の強偽造不可能性に対する攻撃者とする．$\mathcal{A}$ はまず公開鍵 $\mathsf{pk}' = (\mathsf{pk}, g, h)$ を与えられ，署名オラクルに $M_1, \ldots, M_{q_S}$ を適応的にクエリし，返答として署名文 $\sigma'_1 = (\sigma_1, r_1)$, ..., $\sigma'_{q_S} = (\sigma_{q_S}, r_{q_S})$ を受け取り，最後にメッセージ M と署名文 $\sigma' = (\sigma, r)$ とを出力する．m_i，m，C_i，C でそれぞれ $\mathcal{H}(M_i||\sigma_i)$，$\mathcal{H}(M||\sigma)$，$g^{m_i} h^{r_i}$，$g^m h^r$ を表す．

ε_1，ε_2，ε_3 をそれぞれ，$\mathcal{A}$ が Σ' の強偽造不可能性のゲームに勝ち，しかも (1)，(2)，(3) が成立する確率とする：

(1) 任意の i に対し $C \neq C_i$ が成立.
(2) $C = C_i$ となる i が存在し，しかもある k があって署名オラクルが $\sigma_k = \mathsf{Sig}_{\mathsf{sk}}(C_k)$ を計算した段階ですでに $M_k||\sigma_k$ が (署名オラクルもしくは攻撃者によって) ランダムオラクルにクエリされている.
(3) $C = C_i$ となる i が存在するが，(2) で説明した k は存在しない.

なお，(2) の後半の条件は，次のいずれかが成立することと等価：$M_k||\sigma_k = M_j||\sigma_j$ となる $j < k$ が存在，もしくは署名オラクルが σ_k を計算する前に $\mathcal{A}$ が σ_k を予言し，$M_k||\sigma_k$ をランダムオラクルにクエリした．

ε_1，ε_2，ε_3 のいずれかは明らかに $\varepsilon'/3$ 以上である．以下の性質を満たす機械 $\mathcal{B}_1$，$\mathcal{B}_2$，$\mathcal{B}_3$ を後で作る：

1. $i \in \{1, 2\}$ に対し，もし $\varepsilon_i \geq \varepsilon'/3$ なら $\mathcal{B}_i$ は Σ の $(t, q_S, 3\varepsilon)$-偽造不可能性を破ることに成功する.
2. $\varepsilon_3 \geq \varepsilon'/3$ なら $\mathcal{B}_3$ は $\mathcal{G}$ の $(t, 3\varepsilon)$-離散対数仮定を破ることに成功する.

シミュレータはまず $i \in \{1, 2, 3\}$ をランダムに選び，$\mathcal{B}_i$ を使ってシミュレーションを行う．明らかにシミュレータは確率 $1/3$ で正しい $\mathcal{B}_i$ を選ぶので，定理が成立する．

$\mathcal{B}_1$ の構成 公開鍵 pk_* を Σ の偽造問題に対するインスタンスとする．Σ の (t, q_S, ε)-偽造不可能性を破る攻撃者 $\mathcal{B}_1$ を $\mathcal{A}$ を使って作る．$\mathcal{B}_1$ は以下の処理を行う．

セットアップ: $\mathcal{B}_1$ は Gen' とほぼ同じ動作をするが，pk を pk_* にセットする．すなわち $\mathcal{B}_1$ は $g \in \mathcal{G}$ と $x \in \mathbb{Z}_q$ をランダムに選び，$h = g^x$，$\mathsf{pk}' = (\mathsf{pk}_*, g, h)$ とする．そして pk' を $\mathcal{A}$ に入力する．

ランダムオラクルのシミュレート: X を $\mathcal{A}$ のクエリとする．$\mathcal{H}(X)$ がすでに決まっていたら $\mathcal{B}_1$ は $\mathcal{A}$ に $\mathcal{H}(X)$ を返す．そうでなければ $m \in \mathbb{Z}_q$ をランダムに選び，$\mathcal{H}(X)$ を m にセットし，$m = \mathcal{H}(X)$ を $\mathcal{A}$ に返す．

署名オラクルのシミュレート: M_i を $\mathcal{A}$ が i 番目にクエリしたメッセージとする．$\mathcal{B}_1$ は $t_i \in \mathbb{Z}_q$ をランダムに選び，$C_i = g^{t_i}$ とする．さらに C_i を $\mathcal{B}_1$ 用の署名オラクルにクエリし，C_i に対する署名文 σ_i をオラクルから受け取る．$\mathcal{B}_1$ はハッシュ値 $m_i = \mathcal{H}(M_i||\sigma_i)$ をランダムオラクル・シミュレーションのときと同様のルールで決める．

そして $\mathcal{B}_1$ は $m_i + r_i x = t_i \bmod q$ を満たす $r_i \in \mathbb{Z}_q$ を選び，$\sigma'_i = (\sigma_i, r_i)$ とする．($x = 0$ ならこのような r_i は選べないが，negligible な確率 $1/q$ でしか $x = 0$ にならない．) $\mathcal{B}_1$ は最後に σ'_i を $\mathcal{A}$ に送る．

抽出: $\mathcal{A}$ がメッセージ・署名ペア (M, σ') の偽造に成功したとする．強偽造不可能性の定義より，任意の i に対して $(M, \sigma') \neq (M_i, \sigma'_i)$ が成立する．$\mathcal{B}_1$ はランダムオラクル・シミュレーションの場合と同様に $m = \mathcal{H}(M||\sigma)$ を決め，そして $C = g^m h^r$ を計算する．$\sigma' = (\sigma, r)$ は M への valid な署名なので，σ は C への valid な署名である．

署名オラクルをシミュレートする為に $\mathcal{B}_1$ は署名クエリをしている．この署名クエリを $C_1, \ldots, C_{q_S}$ と表す．偽造不可能性のルールより，$\mathcal{B}_1$ は $C_1, \ldots, C_{q_S}$ を出力することはできない．任意の i に対し $C \neq C_i$ が成立すれば $\mathcal{B}_1$ は (C, σ) を出力する．そうでなければ，$\mathcal{B}_1$ のシミュレーションは失敗である．

$\mathcal{B}_1$ がシミュレーションに失敗するのは $C = C_i$ となる i が存在するときのみ．ε_1 の定義より，$\mathcal{A}$ が (M, σ') の偽造に成功してかつ任意の i に対し $C \neq C_i$ となる確率は ε_1．よって $\varepsilon_1 \geq \varepsilon'/3$ である場合、$\mathcal{B}_1$ の成功確率は $\varepsilon_1 \geq (\varepsilon'/3) - ((q_H + q_S)q_S/q)$ 以上．

$\mathcal{B}_1$ が停止するまでに用するステップ数は明らかに $t' + q_S E + 2E \leq t' + (S' + E)q_S + (\text{lower terms})$ 以下．

$\mathcal{B}_2$ の構成 公開鍵 pk_* を Σ の偽造問題に対するインスタンスとする．Σ の (t, q_S, ε)-偽造不可能性を破る攻撃者 $\mathcal{B}_2$ を $\mathcal{A}$ を使って作る．$\mathcal{B}_2$ は以下の処理を行う．

$\mathcal{B}_2$ は Gen' とほぼ同じ動作をするが，pk を pk_* にセットする．すなわち $\mathcal{B}_2$ は $g \in \mathcal{G}$ と $x \in \mathbb{Z}_q$ をランダムに選び，$h = g^x$，$\mathsf{pk}' = (\mathsf{pk}_*, g, h)$ とする．そして pk' を $\mathcal{A}$ に入力する．$\mathcal{B}_2$ は $\mathcal{B}_1$ と同様の方法でランダムオラクルをシミュレートする．ランダムオラクルへの入力と $\mathcal{B}_2$ が決めたハッシュ値との表を以後ハッシュテーブルと呼ぶ．

各 k に対し，$\mathcal{A}$ が k 番目の署名クエリ M_k を出したら $\mathcal{B}_2$ は署名オラクルの第一ステップをシミュレートする．すなわち，$\mathcal{B}_2$ は $t_k \in \mathbb{Z}_q$ をランダムに選び $C_k = g^{t_k}$ とする．(注：$\mathcal{B}_2$ は署名オラクルの第一ステップしかシミュレートしないので，$\mathcal{B}_2$ は C_k を署名オラクルにクエリしない.)

そして $\mathcal{B}_2$ はハッシュテーブルから $\mathsf{Ver}_{\mathsf{pk}'}(C_k, \sigma) = \mathsf{accept}$ を満たす $M||\sigma$ を探す．

もしそのような σ があるとき，我々は現在の k を *good* な値と呼ぶ．k が good な値なら，$\mathcal{B}_2$ は $i = 1, \ldots, k-1$ に対し $C_k \neq C_i$ が成立するかどうかをチェックする．ここで C_i は $\mathcal{B}_2$ の i 番目の署名クエリ．$C_k = C_i$ となる i がなければ $\mathcal{B}_2$ は (C_k, σ) を出力して停止する．$C_k = C_i$ となる i があれば，$\mathcal{B}_2$ は過去に $C_k = C_i$ を署名オラクルにクエリしたことがあることになるので偽造不可能性のルールより $\mathcal{B}_2$ は (C_k, σ) を出力できない．よってシミュレーションは失敗で，$\mathcal{B}_2$ は fail_1 を出力して停止する．

k が good ではないときは，$\mathcal{B}_2$ は $\mathcal{B}_1$ と同様に (σ_k, r_k) を決め，シミュレーションを継続する．

$\mathcal{A}$ が停止するまで good な k が表れなければシミュレーションは失敗し，$\mathcal{B}_2$ は fail_2 を出力して停止する．

以上のようにして作った $\mathcal{B}_2$ は明らかに $t' + q_S E + 2E \leq t' + (S' + E)q_S + (\text{lower terms})$ ステップ以内に停止する．最後に $\varepsilon_2 \geq \varepsilon'/3$ という条件下、$\mathcal{B}_2$ が偽造に成功する確率を評価する．ε_2 の定義より，$\mathcal{B}_2$ が fail_2 を出力する確率は $1 - \varepsilon_2$ 以下．また，$C_k = g^{t_k}$ は $\mathcal{G}$ 上にランダムに分布するので，good な k に対して $C_k = C_i$ となる i が存在する確率は $(k-1)/q \leq q_S/q$ 以下．よって $\mathcal{B}_2$ が (C_k, σ) の偽造に成功する確率は $\varepsilon_2 - (q_S/q) \geq (\varepsilon'/3) - ((q_H + q_S)q_S/q)$ 以上．

$\mathcal{B}_3$ の構成 $\mathcal{G}$ の (t, ε)-離散対数仮定を解く攻撃者 $\mathcal{B}_3$ を $\mathcal{A}$ を用いて作る．$(h_*, g_*) \in \mathcal{G}^2$ を $\mathcal{G}$ 上の離散対数仮定に対するゲームのインスタンスとする．$\mathcal{B}_3$ の目標は $g_* = h_*^{z_*}$ を満たす $z_* \in \mathbb{Z}_q$ を見付けること．$\mathcal{B}_3$ は以下の処理を行う．

セットアップ: $\mathcal{B}_3$ は Gen' とほぼ同じ動作をするが，(g, h) を (g_*, h_*) にセットする．すなわち $\mathcal{B}_3$ は $\mathsf{Gen}(1^\kappa)$ を実行して Gen の出力 $(\mathsf{pk}, \mathsf{sk})$ を得，$(g, h) = (g_*, h_*)$ とし，$\mathsf{pk}' = (\mathsf{pk}, g, h)$ とする．そして $\mathcal{B}_3$ は $\mathcal{A}$ に pk' を入力する．

ランダムオラクル・シミュレーション: X を $\mathcal{A}$ のクエリとする．$\mathcal{H}(X)$ が既に定義されていたら $\mathcal{B}_3$ は $\mathcal{H}(X)$ を $\mathcal{A}$ に返す．そうでなければ $m \in \mathbb{Z}_q$ をランダムに選び，$\mathcal{H}(X)$ を m にセットし，$m = \mathcal{H}(X)$ を $\mathcal{A}$ に返す．

署名オラクルのシミュレーション: M_i を $\mathcal{A}$ の i 番目のオラクルクエリとする．$\mathcal{B}_3$ は $m_i, r_i \in \mathbb{Z}_q$ をランダムに選び，$C_i = g^{m_i} h^{r_i}$ とする．そして秘密鍵 sk を使い $\sigma_i = \mathsf{Sig}_{\mathsf{sk}}(C_i)$ を計算する．$M_i||\sigma_i$ に対応するハッシュ

値がすでに定義されていたらシミュレーションは失敗で，$\mathcal{B}_3$ は fail_1 を出力して停止する．そうでなければ $\mathcal{B}_3$ はハッシュ値 $\mathcal{H}(M_i||\sigma_i)$ を m_i にセットする．最後に $\mathcal{B}_3$ は $\mathcal{A}$ に σ_i' を送信する．

抽出: $\mathcal{A}$ がメッセージ M と M への署名文 $\sigma' = (\sigma, r)$ とを出力したとする．強偽造不可能性のルールより，任意の i に対して $(M, \sigma') \neq (M_i, \sigma_i')$ が成立するとしてよい．$C = C_i$ を満たす i が存在しなければシミュレーションは失敗で，$\mathcal{B}_3$ は fail_2 を出力して停止する．

$C = C_i$ となる i が存在する場合を考える．m，m_i をそれぞれ $\mathcal{H}(M||\sigma)$，$\mathcal{H}(M_i||\sigma_i)$ とする．$C = g^m h^r = {g_*}^m {h_*}^r$ は $C_i = g^{m_i} h^{r_i} = {g_*}^{m_i} {h_*}^{r_i}$ に等しいので，${h_*}^{r-r_i} = {g_*}^{m_i - m}$ が成立する．$r - r_i \neq 0$ なら $\mathcal{B}_3$ は h_* を底とした g_* の離散対数 $z_* = (m_i - m)/(r - r_i) \bmod q$ を計算できる．そうでなければシミューレションは失敗で，$\mathcal{B}_3$ は fail_3 を出力して停止する．

Σ の署名計算量を S とすると $S' = S + E$ で、$\mathcal{B}_3$ が停止するまでに用するステップ数は明らかに $t' + 2E + (S + 2E)q_S = t' + (S' + E)q_S + (\text{lower terms})$ 以下．

次に $\varepsilon_3 \geq \varepsilon'/3$ という仮定のもと、$\mathcal{B}_3$ が離散対数 z_* を得ることができる確率 ε を評価する．$\mathcal{A}$ が署名偽造に成功し，$C = C_i$ となる i が存在し，署名オラクルが $\sigma_k = \mathsf{Sig}_{\mathsf{sk}}(C_k)$ を計算した時点で $M_k||\sigma_k$ がすでにハッシュテーブルに書き込まれているような k は存在しなとき、$\mathcal{B}_3$ は fail_1 も fail_2 も出力しない．また仮定より，これらが全て起こる確率は $\varepsilon_3 \geq \varepsilon'/3$ 以上．したがって $\varepsilon = (\varepsilon'/3) - \Pr[\mathcal{B}_3 \text{ が } \mathsf{fail}_3 \text{ を出力}]$．

最後に $\mathcal{B}_3$ が fail_3 を出力する確率を評価する．$\mathcal{A}$ は q_H 回，署名オラクルは q_S 回しかランダムオラクルにクエリせず、しかもハッシュ値は $\mathbb{Z}_q$ からランダムに選ばれたものであった．よって事象 $\mathcal{X}$ を

$$^{\exists}\ell, {}^{\exists}X \in (\text{hash table}) : X \neq M_\ell||\sigma_\ell \wedge \mathcal{H}(X) = \mathcal{H}(M_\ell||\sigma_\ell)$$

とすると $\mathcal{X}$ が起こる確率は $(q_H + q_S)q_S/q$ 以下．

事象 $\mathcal{X}$ が起らなければ $\mathcal{B}_3$ が fail_3 を出力しないことを証明する．$\mathcal{B}_3$ が fail_3 を出力したと仮定すると，$r = r_i \bmod q$ となる i が存在する．$C = C_i$ が成立していたので，$g^m h^r = C = C_i = g^{m_i} h^{r_i} = g^{m_i} h^r$ となり，よって $g^m = g^{m_i}$ となる．従って $m = m_i \bmod q$ が成立し，よって $\mathcal{H}(M||\sigma) = m = m_i = \mathcal{H}(M_i||\sigma_i)$ が成立．$X \neq M_i||\sigma_i$ と $\mathcal{H}(X) = \mathcal{H}(M_i||\sigma_i)$ をともに満たす X が存在しないのだから，よって $(M, \sigma) = (M_i, \sigma_i)$ が成立する．強偽造不可能性の定義より $(M, \sigma') = (M, (\sigma, r))$ は $(M_i, \sigma_i') = (M_i, (\sigma_i, r_i))$ に等しくない．よって $r \neq r_i \bmod q$ とならねばならず，矛盾．従って，事象 $\mathcal{X}$ が起らないという仮定のもとでは $\mathcal{B}_3$ は fail_3 を出力しない．

以上の議論より $\mathcal{B}_3$ が離散対数を出力する確率は $(\varepsilon'/3) - (q_H + q_S)q_S/q$ 以上． □

最後に変換後の方式の安全性をより直観的に評価する．この為に離散対数問題の**困難さ**という概念を導入する．$\mathcal{G}$ の (t, ε)-離散対数仮定に対する攻撃者 $\mathcal{A}$ に対し，$\mathcal{A}$ が離散対数問題を解くまで $\mathcal{A}$ を繰り返し実行する機械を $\mathcal{A}^*$ とする．明らかに $\mathcal{A}^*$ は平均 t/ε ステップで離散対数問題を確率 1 で解く．これはすなわち，離散対数問題の困難さを計る指標として t/ε を用いることができることを意味する．より厳密には以下の通り．

定義 3.2. $t/\varepsilon < T$ を満たす任意の (t, ε) に対して (t, ε)-離散対数仮定が成り立つとき，離散対数問題の**困難さ**は T 以上であるという。

署名方式の偽造不可能問題や強偽造不可能問題の**困難さ**も同様に定義する．

系 3.3. Σ' の署名計算量を S' とし，$\mathcal{G}$ における冪乗剰余の計算量を E とし，$C_0 = 20(1 + E/S)$ とする．Σ の偽造不可能問題と $\mathcal{G}$ 上の離散対数問題の困難さが T_1，T_2 以上であるとする．このとき，Σ' の強偽造不可能問題の困難さ T' は

$$T' \geq \min\{T_1, T_2\}/C_0 + (\text{lower terms})$$

を満たす．

Proof. Σ' の強偽造不可能性を $2^{\kappa/2} + (\text{lower terms})$ ステップ以内に確率 1 で解く攻撃者 $\mathcal{A}_0$ が存在することを後で証明する．よって $t'/\varepsilon' \leq 2^{\kappa/2} + (\text{lower terms})$ が成立する．

q_S と q_H の定義より，$Sq_S \leq t'$ と $q_H \leq t'$ が成立．$S' = S + E + (\text{lower terms})$ なので，$t \leq t' + q_S(S' + E) \leq (1 + (S' + E)/S)t' = (1 + (S + 2E)/S)t' = (2 + 2E/S)t'$ と $(q_H + q_S)q_S/(3q\varepsilon') \leq (t' + t'/S)(t'/S)/(3q\varepsilon') \simeq t'^2/(3qS\varepsilon') \leq (t'/\varepsilon')^2/(3qS) \leq (2^{\kappa/2})^2/(32^{\kappa-1}S) = 2/3S$, と $\varepsilon = \varepsilon'/9 - (q_H + q_S)q_S/(3q) = \varepsilon' \cdot (1/9 - (q_H + q_S)q_S/(3q\varepsilon')) \geq \varepsilon' \cdot (1/9 - 2/3S) \geq \varepsilon'/10$ とが成立する．(式変形中で $\kappa >> 0$ なら $S >> 0$ となることを使った)．よって $\min\{T_1, T_2\} \leq t/\varepsilon \leq (2 + 2E/S)t'/(\varepsilon'/10) = 20(1 + E/S) \cdot (t'/\varepsilon') = C_0 \cdot (t'/\varepsilon')$ となり，従って $\min\{T_1, T_2\} \leq C_0 \cdot T'$ となる．よって $T' \leq \min\{T_1, T_2\}/C_0$ が成立する．

最後に $\mathcal{A}_0$ を作る．$\mathcal{A}_0(\mathsf{pk}')$ はまず Baby Step and Giant Step (BSGS) アルゴリズム [BSS99] を用いて (g, h) の離散対数 x を計算し，メッセージ M を任意に選んで M を署名オラクルにクエリし，署名文 $\sigma' = (\sigma, r)$ を返答として受け取り，$m = \mathcal{H}(M||\sigma)$ と $C = g^m h^r$ を計算する．すると $\mathsf{Ver}_{\mathsf{pk}}(C, \sigma) = \mathsf{accept}$ が成立．$\mathcal{A}_0$ はメッセージ $M_0 \neq M$ を任意に選び，$m_0 = \mathcal{H}(M_0||\sigma)$ を計算し，$m_0 + r_0 x = m + rx \bmod q$ を満たす $r_0 \in \mathbb{Z}_q$ を選び，$\sigma_0 = (\sigma, r_0)$ とし，(M_0, σ_0) を出力する．σ_0 が $M_0 \neq M$ への valid な証明であることを簡単に示すことができる．BSGS アルゴリズムは $2^{\kappa/2} + (\text{lower terms})$ ステップを要

—$\mathsf{Gen}'(1^\kappa)$— $(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{Gen}(1^\kappa)$, $g \leftarrow \mathcal{G}$, $x, y \leftarrow \mathbb{Z}_q$, $(h_1, h_2) \leftarrow (g^x, g^y)$. $\mathsf{pk}' \leftarrow (\mathsf{pk}, g, h_1, h_2)$, $\mathsf{sk}' \leftarrow (\mathsf{sk}, x, y)$. $(\mathsf{pk}', \mathsf{sk}')$ を出力.
—$\mathsf{Sig}'_{\mathsf{sk}'}(M)$— $t \leftarrow \mathbb{Z}_q$, $C \leftarrow g^t$, $\sigma \leftarrow \mathsf{Sig}_{\mathsf{sk}}(C)$, $m \leftarrow H(M\|\sigma)$. $m + rx + sy = t \bmod q$ を満たす $r, s \in \mathbb{Z}_q$ をランダムに選ぶ. $\sigma' \leftarrow (\sigma, r, s)$. σ' を出力.
—$\mathsf{Ver}'_{\mathsf{pk}'}(M, \sigma')$— σ' を (σ, r, s) にパースする. $m \leftarrow H(M\|\sigma)$, $C \leftarrow g^m {h_1}^r {h_2}^s$. $\mathsf{Ver}_{\mathsf{pk}}(C, \sigma) = \mathsf{accept}$ なら accept を出力. そうでなければ reject を出力.

図 2: スタンダードモデル版の変換で変換された方式

するので，$\mathcal{A}_0$ の用するステップ数も $2^{\kappa/2}$+(lower terms) である．□

4 スタンダードモデルにおける変換

この章ではランダムオラクルを用いない変換方法を提案する．κ，$\mathcal{G}$，q，$\Sigma = (\mathsf{Gen}, \mathsf{Sig}, \mathsf{Ver})$ を前章と同様に取る．$\{H_\kappa\}$ を衝突困難なハッシュ関数 $H = H_\kappa : \{0,1\}^* \to \mathbb{Z}_q$ の族とする．提案する変換方法で Σ を変換した後の方式を図 2 に載せる．前章の方式と同じく，変換後の方式は on-line/off-line 性を満たし，署名者はメッセージ M をもらう前に x^{-1}，C，σ を事前計算できる．

定理 4.1. Σ' の署名計算量を S' とする．Σ' の $(t', q_S, q_H, \varepsilon')$-強偽造不可能性を破ることができる攻撃者が存在したとする．このとき，次の性質を満たす攻撃者が存在する：Σ の (t, q_S, ε)-偽造不可能性，$\mathcal{G}$ の (t, ε)-離散対数仮定，もしくは H の (t, ε)-衝突困難性を破ることができる．ただしここで

$$t = t' + q_S S' + (\text{lower terms}),$$
$$\varepsilon = \frac{\varepsilon'}{4} - (\text{lower terms}).$$

Proof. $\mathcal{A}$ を Σ' の (t', q_S, ε')-強偽造不可能性を破ることができる攻撃者とする．$\mathcal{A}$ は公開鍵 $\mathsf{pk}' = (\mathsf{pk}, g, h_1, h_2)$ を与えられ，署名オラクルにメッセージ $M_1, \ldots, M_{q_S}$ を適応的にクエリし，署名オラクルから対応する署名文 $\sigma'_1 = (\sigma_1, r_1, s_1)$, …, $\sigma'_{q_S} = (\sigma_{q_S}, r_{q_S}, s_{q_S})$ を受け取り，最後にメッセージ M と署名文 $\sigma' = (\sigma, r, s)$ を出力する．m_i，m，C_i，C をそれぞれ $H(M_i\|\sigma_i)$，$H(M\|\sigma)$，$g^{m_i} {h_1}^{r_i} {h_2}^{s_i}$，$g^m {h_1}^r {h_2}^s$ とする．

$\mathcal{A}$ の偽造方法を以下の 4 種類に場合分けする．

タイプ 1: $C = C_i$ となる i が存在しない．
タイプ 2: $(C, r, s) = (C_i, r_i, s_i)$ となる i が存在する．
タイプ 3A: $C = C_i$ と $r \neq r_i$ が成立する i が存在する．
タイプ 3B: $C = C_i$ と $s \neq s_i$ が成立する i が存在する．

後で 4 つの機械 $\mathcal{B}_1$，$\mathcal{B}_2$，$\mathcal{B}_{3A}$，$\mathcal{B}_{3B}$ を作り以下を示す：$\mathcal{A}$ がタイプ 1，2，3A，3B ならそれぞれ，$\mathcal{B}_1$，$\mathcal{B}_2$，$\mathcal{B}_{3A}$，$\mathcal{B}_{3B}$ がそれぞれ Σ の (t, q_S, ε')-偽造不可能性，H の (t, ε')-衝突困難性，$\mathcal{G}$ の (t, ε')-離散対数仮定，$\mathcal{G}$ の (t, ε')-離散対数仮定を破る．

シミュレータは $i \in \{1, 2, 3A, 3B\}$ をランダムに選び，i の値に応じて $\mathcal{B}_1$，$\mathcal{B}_2$，$\mathcal{B}_{3A}$，$\mathcal{B}_{3B}$ を実行する．シミュレータが正しい $\mathcal{B}_i$ を選ぶ確率は $1/4$ なので，定理が成立する．

$\mathcal{B}_1$ の構成 Σ の (t, q_S, ε')-偽造不可能性を破る機械 $\mathcal{B}_1$ を $\mathcal{A}$ を使って作る．公開鍵 pk_* を Σ の偽造不可能性のゲームのインスタンスとする．$\mathcal{B}_1$ は以下の処理を行う．

セットアップ: $\mathcal{B}_1$ は Gen' とほぼ同じ動作をするが，pk を pk_* にセットする．すなわち，$\mathcal{B}_1$ は $g \in \mathcal{G}$，$x, y \in \mathbb{Z}_q$ をランダムに選び，$(h_1, h_2) = (g^x, g^y)$，$\mathsf{pk} = \mathsf{pk}_*$，$\mathsf{pk}' = (\mathsf{pk}, g, h_1, h_2)$ とする．そして $\mathcal{B}_1$ は $\mathcal{A}$ に pk' を入力する．

署名オラクルのシミュレーション: $\mathcal{A}$ の i 番目のクエリを M_i とする．$\mathcal{B}_1$ は署名オラクルとほぼ同じ動きをするが，$\mathsf{Sig}_{\mathsf{sk}}$ を実行する代わりに $\mathcal{B}_1$ の署名オラクルにクエリする．すなわち，$\mathcal{B}_1$ は以下の手順を行う：$t_i \in \mathbb{Z}_q$ をランダムに選び，$C_i = g^{t_i}$ とし，C_i を $\mathcal{B}_1$ の署名オラクルにクエリし，その返答として署名文 σ_i を受け取り，$m_i = H(M_i\|\sigma_i)$ を計算し，$m_i + r_i x + s_i y = t_i \bmod q$ を満たす $r_i, s_i \in \mathbb{Z}_q$ をランダムに選び，$\sigma'_i = (\sigma_i, r_i, s_i)$ とし，σ'_i を $\mathcal{A}$ に送信する．

抽出: $\mathcal{A}$ がメッセージ M と M への署名 $\sigma' = (\sigma, r, s)$ を出力したとする．$\mathcal{B}_1$ は (σ, C) を出力する．$\sigma' = (\sigma, r, s)$ が M に対する valid な署名であれば，σ は C に対する valid な署名である．$\mathcal{B}_1$ が署名オラクルにクエリしたのは $C_1, \ldots, C_{q_S}$ のみである．$\mathcal{A}$ はタイプ 1 なら任意の i に対し $C \neq C_i$ であり，これはすなわち $\mathcal{B}_1$ が C に対する valid な署名文 σ を偽造することに成功したことを意味する．

$(2q_S + 2)E \simeq 2q_S E + (\text{lower terms}) \leq q_S S' + (\text{lower terms})$ が成立することを使えば，$\mathcal{B}_1$ が Σ の (t, q_S, ε')-偽造問題を解けることを簡単に証明できる．

$\mathcal{B}_2$ の構成 H の (t, ε)-衝突困難性を破ることができる攻撃者 $\mathcal{B}_2$ を，$\mathcal{A}$ を使って作る．$\mathcal{B}_2$ は以下の処理を行う．

セットアップ: $\mathcal{B}_2$ は $\mathsf{Gen}'(1^\kappa)$ を実行し，Gen' の出力 $\mathsf{pk}' = (\mathsf{pk}, g, h_1, h_2)$，$\mathsf{sk}' = (\mathsf{sk}, x, y)$ を得，pk' を $\mathcal{A}$ に入力する．

署名オラクルのシミュレーション: 秘密鍵 sk' を使うことでシミュレートできる．

抽出: $\mathcal{A}$ がメッセージ M と M への署名文 $\sigma' = (\sigma, r, s)$ を出力したとする．$\mathcal{A}$ がタイプ 2 であれば、$(C, r, s) = (C_i, r_i, s_i)$ となる i が存在する．$C = g^{H(M\|\sigma)} {h_1}^r {h_2}^s$

と $C_i = g^{H(M_i||\sigma_i)} {h_1}^{r_i} {h_2}^{s_i} = g^{H(M_i||\sigma_i)} {h_1}^{r} {h_2}^{s}$ は等しいので，ハッシュ値 $H(M||\sigma)$ と $H(M_i||\sigma_i)$ は等しい．$(M, \sigma') \neq (M_i, \sigma_i')$ だったので，これは $(M||\sigma, M_i||\sigma_i)$ が H の衝突であることを意味する．よって $\mathcal{B}_2$ は $(M||\sigma, M_i||\sigma_i)$ を出力して停止する．

$\mathcal{B}_2$ のステップ数が t 以下で、成功確率が ε' より大きい事を簡単に証明できる．

$\mathcal{B}_{3A}$ の構成 $\mathcal{G}$ の (t, ε)-離散対数仮定を破ることができる攻撃者 $\mathcal{B}_{3A}$ を，$\mathcal{A}$ を使って作る．$(h_*, g_*) \in \mathcal{G}^2$ を $\mathcal{G}$ 上の離散対数仮定に対するゲームのインタンスとする．$\mathcal{B}_3$ の目標は $g_* = {h_*}^{z_*}$ を満たす離散対数 $z_* \in \mathbb{Z}_q$ を求めることである．$\mathcal{B}_{3A}$ は以下の処理を行う．

セットアップ: $\mathcal{B}_{3A}$ は Gen' とほぼ同様の手順を行うが (g, h_1) を (g_*, h_*) にセットする．すなわち，$\mathcal{B}_{3A}$ は $\mathsf{Gen}(1^\kappa)$ を実行して Gen の出力 $(\mathsf{pk}, \mathsf{sk})$ を得，$y \in \mathbb{Z}_q$ をランダムに選び，$(g, h_1) = (g_*, h_*)$，$h_2 = g^y$，$\mathsf{pk}' = (\mathsf{pk}, g, h_1, h_2)$ とする．そして $\mathcal{B}_{3A}$ は $\mathcal{A}$ に pk' を入力する．

署名オラクルのシミュレーション: $\mathcal{A}$ の i 回目の署名クエリを M_i とする．$\mathcal{B}_{3A}$ は $t_i', r_i \in \mathbb{Z}_q$ をランダムに選び，$C_i = g^{t_i'} {h_1}^{r_i}$ とする．そして秘密鍵 sk を使って $\sigma_i = \mathsf{Sig}_{\mathsf{sk}}(C_i)$ を計算する．そして $m_i = H(M_i||\sigma_i)$ を計算し，$m_i + s_i y = t_i' \bmod q$ を満たす $s_i \in \mathbb{Z}_q$ を選び，$\sigma_i' = (\sigma_i, r_i, s_i)$ とし，σ_i' を $\mathcal{A}$ に返答する．

抽出: $\mathcal{A}$ がメッセージ M と M への署名 $\sigma' = (\sigma, r, s)$ を出力したと仮定する．$\mathcal{A}$ はタイプ 3A の攻撃者なので，$C = C_i$ と $r \neq r_i$ を満たす i が存在する．m，m_i をそれぞれ $H(M||\sigma)$，$H(M_i||\sigma_i)$ とする．$C = g^m {h_1}^r {h_2}^s = {g_*}^{m+sy} {h_*}^r$ は $C_i = g^m {h_1}^{r_i} {h_2}^{s_i} = {g_*}^{m_i + s_i y} {h_*}^{r_i}$ に等しいので，${h_*}^{r-r_i} = {g_*}^{m_i + s_i y - m - sy}$ が成立する．$r \neq r_i$ だったので，$z_* = (m_i + s_i y - m - sy)/(r - r_i) \bmod q$ は h_* を底にした g_* の離散対数．よって $\mathcal{B}_{3A}$ は z_* を出力して停止する．

$\mathcal{B}_{3A}$ のステップ数が t 以下で、成功確率が ε' より大きい事を簡単に証明できる．

$\mathcal{B}_{3B}$ の構成 (g_*, h_*) を (g, h_1) でなく (g, h_2) に埋め込むことをのぞけば，$\mathcal{B}_{3B}$ の構成は $\mathcal{B}_{3A}$ の構成とほぼ同様である． □

以下の系を簡単に示すことができる．

系 4.2. Σ の偽造不可能性，$\mathcal{G}$ の離散対数問題，H の衝突困難問題の困難性がそれぞれ T_1，T_2，T_3 以上であるとする．このとき Σ' の強偽造不可能性 T' は

$$T' \geq (2 + 2(E/S)) \min\{T_1, T_2, T_3\} + (\text{lower terms}).$$

を満たす．

参考文献

[ADR02] Jee Hea An, Yevgeniy Dodis, Tal Rabin. On the Security of Joint Signature and Encryption. In Eurocrypt 2002, pp.83-107.

[BR93] Mihir Bellare, Phillip Rogaway. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. ACM Conference on Computer and Communications Security 1993. pp.62-73

[BSS99] Ian F. Blake, Gadiel Seroussi, Nigel P. Smart. Elliptic Curve in Cryptography. Cambridge University Press, 1999.

[BBS04] Dan Boneh, Xavier Boyen, Hovav Shacham. Short Group Signatures. In Crypto 2004, pp. 41-55.

[BSW06] Dan Boneh, Emily Shen, and Brent Waters. Strongly Unforgeable Signatures Based on Computational Diffie-Hellman. In PKC 2006, pp. 229-240.

[CHK04] Ran Canetti, Shai Halevi, and Jonathan Katz. Chosen-Ciphertext Security from Identity-Based Encryption In Eurocrypt 2004, pp. 229-235.

[CG04] Jan Camenisch, Jens Groth. Group Signatures: Better Efficiency and New Theoretical Aspects. In SCN 2004, pp. 120-133.

[CLS06] Scott Contini, Arjen K. Lenstra, Ron Steinfeld. VSH, an Efficient and Provable Collision-Resistant Hash Function. Eurocrypt 2006, pp. 165-182.

[DDN00] Danny Dolev, Cynthia Dwork, Moni Naor. Nonmalleable Cryptography. SIAM J. of Computing, 30(2), pp.391-437, 2000.

[GMR88] Shafi Goldwasser, Silvio Micali, Ronald L. Rivest. A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks. SIAM J. Comput. 17(2), pp. 281-308 (1988)

[KR97] Hugo Krawczyk, Tal Rabin. Chameleon Hashing and Signatures. 1997.
http://ibm.com/security/chameleon.ps,
http://iacr.org/1998/010.ps.gz

[KR00] Hugo Krawczyk, Tal Rabin. Chameleon Signatures. In NDSS 2000, pp. 143–154.

[MOV96] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. HANDBOOK of APPLIED CRYPTOGRAPHY, CRC Press, 1996.

[ST01] Adi Shamir, Yael Tauman. Improved Online/Offline Signature Schemes. Crypto 2001. pp.355-367

[S97] Victor Shoup. Lower Bound for Discrete Logarithms and Related Problems. In Eurocrypt'97. pp.256-266.

[SPW07] Ron Steinfeld, Josef Pieprzyk, and Huaxiong Wang. How to Strengthen any Weakly Unforgeable Signature into a Strongly Unforgeable Signature. CT-RSA 2007.

[TOO06] Isamu Teranishi, Takuro Oyama, and Wakaha Ogata. General Conversion for Obtaining Strongly Existentially Unforgeable Signatures. Indocrypt 2006. pp.191-205. (本論文の英語版)

[W05] Brent Waters. Efficient identity-based encryption without random oracles. In Eurocrypt 2005, pp. 114-127.