社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2003－ＣＳＥＣ－22　(22)
2003／7／18

メッセージに依存するベキ指数を用いたRSA署名の証明可能安全性

古江　岳大†　清藤　武暢†　四方　順司†　松本　勉†

† 横浜国立大学大学院　環境情報研究院　〒240–8501 横浜市保土ヶ谷区常盤台 79–7
E-mail: †{furue,seito,shikata,tsutomu}@mlab.jks.ynu.ac.jp

あらまし　本稿では，de Jonge と Chaum が提案した，メッセージに依存するベキ指数を用いた RSA 署名方式に注目する．de Jonge と Chaum の論文では 3 種類の方式が提案されており，本稿ではそれらを JC1，JC2，JC3 とよぶことにする．まず，本稿では，Michels，Stadler，Sun らによる JC3 署名に対する選択文書攻撃アルゴリズムを再考し，署名オラクルへの問い合わせ回数を減らした条件下でもその攻撃アルゴリズムが有効であることを示す．また，JC1 および JC3 署名をもとにして，それぞれ証明可能安全性を持つ署名方式を提案する．

キーワード　電子署名，証明可能安全性，RSA 署名，強 RSA 問題，FDH，Division-intractable hash

Provable security of RSA signature schemes with message-dependant exponents

Takahiro FURUE†, Takenobu SEITO†, Junji SHIKATA†, and Tsutomu MATSUMOTO†

† Graduate School of Environment and Information Sciences, Yokohama National University
79–7 Tokiwadai, Hodogaya-ku, Yokohama, 240–8501 Japan
E-mail: †{furue,seito,shikata,tsutomu}@mlab.jks.ynu.ac.jp

Abstract　In this paper, we address the RSA signature schemes with message-dependant exponents proposed by de Jonge and Chaum. In de Jonge and Chaum's paper, three signature schemes were proposed, and we call them JC1 signature scheme, JC2 signature scheme and JC3 signature scheme, respectively, in this paper. In this paper, we reconsider the chosen message attack for JC3 signature scheme proposed by Michels, Stadler and Sun, and show that a chosen message attack for JC3 signature scheme is still valid even if the number of queries by an adversary is reduced. Also, in this paper we propose provable secure signature schemes based on JC1 and JC3 signatures.

Key words　digital signature, provable security, RSA signature, strong RSA problem, FDH, Division-intractable hash

1. まえがき

公開鍵署名方式では，署名生成／検証時にメッセージに対してベキ乗計算処理を行うものが多い．ベキ乗計算の底の部分がメッセージに依存する例として RSA 署名 [13]，ESIGN 署名 [8] が挙げられ，ベキ指数の部分がメッセージに依存する例として ElGamal 署名 [7] および DSA 署名 [14] が挙げられる．

RSA 署名に用いられる RSA 関数では，メッセージ M_1 と M_2 の積 $M_1 \cdot M_2$ の署名が M_1 の署名と M_2 の署名の積になるという性質を持つ．この性質を RSA 関数の乗法性という．この乗法性を利用し，RSA 関数の逆関数を計算することなく署名を偽造する攻撃法を multiplicative attack という．通常 RSA 関数を利用した署名においては，Padding やハッシュ関数を付加することで証明可能安全性を持つ方式である RSA-FDH [2] [3] [4] や RSA-PSS [3] [5] が注目されており，これらの方式では乗法性は除かれている．

1986 年に de Jonge と Chaum は RSA 署名の変形方式を提案した [11]．彼らは RSA 署名のベキ乗構造に注目し，底とベキ指数の両方をメッセージ M に依存する形に変更することで，RSA 署名から乗法性を取り除き，multiplicative attack に対する耐性を持つ署名方式の構成を試みている．しかし彼らの署名方式には multiplicative attack が存在することが 1998 年に Michels，Stadler および Sun によって示されている [12]．

本稿では，de Jonge と Chaum が提案した，メッセージに依存するベキ指数を用いた RSA 署名方式に注目する．de Jonge と Chaum の論文では 3 種類の方式が提案されており，本稿ではそれらを JC1，JC2，JC3 とよぶことにする．まず，本稿では，Michels，Stadler，Sun らによる JC3 署名に対する選択文

書攻撃アルゴリズムを再考し，署名オラクルへの問い合わせ回数を減らした条件下でもその攻撃アルゴリズムが有効であることを示す．また，JC1 および JC3 署名をもとにして，それぞれ証明可能安全性を持つ署名方式を提案する．

2. 準　　備

2.1 電子署名のモデル

［定義 1］ 電子署名は以下の要素から構成される [10].

（1） [鍵生成アルゴリズム **Gen**] セキュリティパラメータ k をとり，公開鍵と秘密鍵の組 $\mathrm{Gen}(1^k) = (PK, SK)$ を返す確率的アルゴリズム．

（2） [署名生成アルゴリズム **Sign**] メッセージ M と秘密鍵 SK をとり，署名 $\mathrm{Sign}_{SK}(M) = \sigma$ を返す確率的アルゴリズム．

（3） [署名検証アルゴリズム **Verify**] メッセージ M，署名 σ，公開鍵 PK をとり，σ が M と PK について正当な署名ならば $\mathrm{Verify}(M, \sigma, PK) = 1$ を，そうでなければ $\mathrm{Verify}(M, \sigma, PK) = 0$ を返す確定的アルゴリズム．

以下に RSA 署名方式の構成を示す．

RSA 署名

[鍵生成] 入力 1^k に対して，$k/2$ bit の素数 p, q をランダムに選ぶ．$N = pq$ とする．$ed \equiv 1 \bmod \phi(N)$ を満たす (e, d) の組をランダムに選び，$PK = (N, e), SK = (\phi(N), d)$ を返す．ただし ϕ はオイラー関数である．

[署名生成] メッセージ M に対して $\sigma = M^d \bmod N$ を計算し，σ を M の署名として返す．

[署名検証] 署名付き文書 (M, σ) に対して $\sigma^e \equiv M \bmod N$ が成り立てば 1 を，そうでなければ 0 を返す．

2.2 安全性の定義

［定義 2］ 攻撃者 F が A の署名を（確率 ϵ で）偽造するとは，F が A の秘密鍵 SK_A を知らずに，公開鍵 PK_A とメッセージ M について正当な署名 σ を（確率 ϵ で）生成することである．署名偽造の攻撃モデルを以下に示す [10].

（1） **KOA(Key Only Attack)**　公開情報のみから署名の偽造を行う．受動的攻撃ともよばれる．

（2） **KMA(Known Message Attack)**　いくつかのメッセージとその署名が存在するとき，その情報をもとにして署名の偽造を行う．

（3） **GCMA(Generic Chosen Message Attack)**　攻撃者はあらかじめ任意に選択したメッセージに対する署名を取得でき，その情報をもとにして署名の偽造を行う．

（4） **ACMA(Adaptive Chosen Message Attack)**　攻撃者は任意に選択したメッセージに対する署名を取得でき，その情報をもとにして署名の偽造を行う．攻撃者は署名を要求するメッセージをそれまでに取得したメッセージとその署名をもとに選択することができる．

また，署名を偽造可能なメッセージの範囲により分類した安全性のモデルを以下に示す [10].

［定義 3］

（1） **UUF（Universally UnForgeable）**　署名の偽造ができないメッセージが存在する．

（2） **SUF（Selectively UnForgeable）**　特定のメッセージについてのみ署名を偽造できる．

（3） **EUF（Existentially UnForgeble）**　全てのメッセージについて署名の偽造はできない．

署名方式が ACMA に対して EUF であるとき EUF-ACMA であるという．これは現在考えられる最も強い安全性の概念である．

［定義 4］ 確率的チューリングマシン A が $(t, \epsilon, q_{sig}, q_H)$ で署名方式を破るとは，A が署名オラクルに q_{sig} 回，ハッシュオラクルに q_H 回の問い合わせを適応的に行い，計算時間 t および成功確率 ϵ で署名を存在的に偽造するということである．$(t, \epsilon, q_{sig}, q_H)$ で署名方式を破る確率的チューリングマシンが存在しないとき，署名方式は $(t, \epsilon, q_{sig}, q_H)$-安全であるという．

［定義 5］ 確率的チューリングマシン A が関数 f の一方向性を (t, ϵ) で破るとは，A が計算時間 t で，関数 f の一方向性を成功確率 $Succ(A) = Pr[A(f(w)) = y, \text{ただし } f(y) = f(w)] = \epsilon$ で破るということである．そのような A が存在しないとき，f は (t, ϵ)-one-way であるという．

3. JC 署 名

本章では，de Jonge と Chaum が [11] で提案した RSA 署名の変形方式について述べる．

3.1 概　　要

de Jonge と Chaum は RSA 署名のベキ乗構造に注目し，以下のような一般化された形式を考え，GES（Generalized Exponentiation Signature）と定義した．

$$S(M) = F_1(M, N)^{F_2(M,N)} \bmod N \tag{1}$$

ただし M はメッセージ，N は公開鍵，$S(M)$ は M の署名である．RSA 署名は式（1）において $F_1(M, N) = M$, $F_2(M, N) = e^{-1} \bmod \phi(N)$ の場合にあたる．de Jonge と Chaum は F_1，F_2 の構成を変えることにより段階的に 3 種類の署名方式を提案した．以下，それらの方式を提案された順に JC1，JC2，JC3 署名とよぶことにする．また，それらをまとめて JC 署名とよぶことにする．

JC 署名は RSA 署名と異なり公開鍵 N に対して $S(M+N) \neq S(M)$ という性質を持つ．そのため，RSA 署名と比較して，ハッシュ関数や圧縮処理を用いることなく M のサイズを N より大きくとれるという利点がある．

de Jonge と Chaum は JC3 署名に multiplicative attack が存在しないと主張したが，その後 Michels，Stadler および Sun によって JC3 署名に対する multiplicative attack が指摘された [12].

3.2 JC1 署名方式

JC1 署名は式（1）において

$$F_1(M, N) = M$$
$$F_2(M, N) = Md$$

としたものである．JC1 署名の構成を以下に示す．

JC1 署名

[鍵生成] RSA 署名と同じ.

[署名生成] メッセージ M に対して $\sigma = M^{Md \bmod \phi(N)} \bmod N$ を計算し，σ を M の署名として返す.

[署名検証] (M, σ) に対して $\sigma^e \equiv M^M \bmod N$ が成り立てば 1 を，そうでなければ 0 を返す.

JC1 署名方式には multiplicative attack による KMA が存在することが [11] で示されている．また，以下の 2 種類の KOA が存在する.

（1） M，e を Z の元と考えて，$e|M$ であるとき，$M' = M/e \in Z$ とおくと，M の署名 σ は $\sigma = M^{M'} \bmod N$ により公開鍵のみから求められる．実際

$$M^{M'} \equiv M^{M'ed} \equiv M^{Md} \pmod N$$

である.

（2） 同様に，$M, M', e \in Z$ が $M = M'^e$ の関係を満たすとき，M の署名 σ は $\sigma = M'^M \bmod N$ により公開鍵のみから求められる．実際

$$M'^M \equiv M'^{Med} \equiv M^{Md} \pmod N$$

である.

3.3 JC2 署名方式と GHR 署名方式

JC2 署名は式（1）において

$$F_1(M, N) = C \quad (C \in Z_N^*: \text{定数})$$
$$F_2(M, N) = (2M+1)^{-1} \bmod \phi(N)$$

としたものである．JC2 署名の構成を以下に示す.

JC2 署名

[鍵生成] 入力 1^k に対して，$k/2$ bit の素数 p, q で，素数 p', q' を用いて $p = 2p' + 1, q = 2q' + 1$ と表せるものをランダムに選ぶ．$N = pq$ とする．$C \in Z_N^*$ をランダムに選び，$PK = (N, C), SK = \phi(N)$ を返す.

[署名生成] メッセージ M に対して $\sigma = C^{(2M+1)^{-1} \bmod \phi(N)} \bmod N$ を計算し，σ を M の署名として返す.

[署名検証] (M, σ) に対して $\sigma^{2M+1} \equiv C \bmod N$ が成り立てば 1 を，そうでなければ 0 を返す.

ここで JC2 署名方式には multiplicative attack による KMA が存在することが示されていることに注意する [11].

ランダムオラクルモデルよりも現実的なモデルのもとで証明可能安全性を持つ署名方式を構成するという観点から，Gennaro らにより GHR 署名方式が提案されている [9]．GHR 署名は JC2 署名にハッシュ関数を 1 個付加した形式になっている．GHR 署名の概要を以下に示す.

GHR 署名

[鍵生成] 入力 1^k に対して，$k/2$ bit の素数 p, q で，素数 p', q' を用いて $p = 2p' + 1, q = 2q' + 1$ と表せるものをランダムに選ぶ．$N = pq$ とする．$C \in Z_N^*$ をランダムに選び，$PK = (N, C), SK = \phi(N)$ を返す.

[署名生成] メッセージ M に対して $\sigma = C^{H(M)^{-1} \bmod \phi(N)} \bmod N$ を計算し，σ を M の署名として返す．ただし $H: \{0,1\}^* \to Z_N^*$ は出力長が N と同じサイズであるハッシュ関数（Full Domain Hash，FDH）[2] である.

[署名検証] (M, σ) に対して $\sigma^{H(M)} \equiv C \bmod N$ が成り立てば 1 を，そうでなければ 0 を返す.

[定義 6] k bit 出力のハッシュ関数 H が Division-intractable であるとは，$H(Y) | \prod_{i=1}^{n} H(X_i)$ を満たす入力の組 $(X_1, \ldots, X_n, Y)$ を k に関して無視できない確率で計算する確率的多項式アルゴリズムが存在しないことである.

ハッシュ関数が Division-intractable であるという仮定は，ランダムオラクルモデルよりも弱い仮定であると考えられていた [9] が，これに関して否定的な結果が報告されている [6].

[定義 7] 強 RSA 問題とは，$N = pq$（p, q は秘密の素数），$s \in Z_N^*$ が与えられたとき，$r^e = s \bmod N$ を満たす (r, e)（ただし $e > 1$）を見つける問題である．N が大きいとき，(r, e) から s を求めるのは容易だが，その逆は難しいと考えられている．つまり強 RSA 問題を解くとは $f: (r, e) \mapsto y = r^e \bmod N$ の一方向性を破ることである.

ハッシュ関数 H が Division-intractable [1] であると仮定すると，強 RSA 問題 [1] を解くアルゴリズムを GHR 署名を破るアルゴリズムに帰着させることができる [9] [5].

3.4 JC3 署名方式

JC3 署名は式（1）において

$$F_1(M, N) = M$$
$$F_2(M, N) = (2M+1)^{-1} \bmod \phi(N)$$

としたものである.

JC3 署名

[鍵生成] 入力 1^k に対して，$k/2$ bit の素数 p, q で，素数 p', q' を用いて $p = 2p' + 1, q = 2q' + 1$ と表せるものをランダムに選ぶ．$N = pq$ とし，$PK = N, SK = \phi(N)$ を返す.

[署名生成] メッセージ M に対して $\sigma = M^{(2M+1)^{-1} \bmod \phi(N)} \bmod N$ を計算し，σ を M の署名として返す.

[署名検証] (M, σ) に対して $\sigma^{2M+1} \equiv M \bmod N$ が成り立てば 1 を，そうでなければ 0 を返す.

JC3 署名方式には multiplicative attack が存在しないであろうと考えられていたが，後に [12] で multiplicative attack による GCMA が示された．以下，[12] の攻撃法を MSS 攻撃とよぶことにする．具体的なアルゴリズムについては次章に譲る.

4. MSS 攻撃

本章では，MSS 攻撃のアルゴリズムを説明するとともに，MSS 攻撃における攻撃者の署名オラクルへの問い合わせ回数について考察する.

4.1 MSS 攻撃アルゴリズム

MSS 攻撃のアルゴリズムについて述べる．攻撃者は 2 個のメッセージ M_1，M_2 に対する署名 σ_1，σ_2 を入手することで署名を偽造できる.

MSS 攻撃： Forger F が署名を偽造したいメッセージを

M とする．

（1） F は任意の整数 $u>0$ を選び，

$$M_1=\frac{(2M+1)(2u+1)-1}{2}$$

を計算する．

（2） $2MM_1+2kN+1=j(2M+1)$ を満たす k，j を計算する．$\gcd(N,2M+1)=1$ ならば，

$$k\equiv\frac{-2MM_1-1}{2N}\equiv\frac{M_1-1}{2N}\pmod{2M+1}$$

で k および j が求まる．

（3） F は $M_2=MM_1+kN$ を計算する．

（4） F は署名オラクルに M_1，M_2 を問い合わせ，署名 σ_1，σ_2 を入手する．

（5） F は M の署名 σ を以下の式で計算できる．

$$\sigma=\frac{\sigma_2^j}{\sigma_1^{(2u+1)}}$$

σ が署名検証に合格することは以下の計算で確かめられる．

$$\sigma^{2M+1}=\frac{\sigma_2^{j(2M+1)}}{\sigma_1^{2M_1+1}}=\frac{\sigma_2^{(2MM_1+2kN+1)}}{M_1}$$
$$=\frac{\sigma_2^{2M_2+1}}{M_1}\equiv\frac{M_2}{M_1}\equiv\frac{MM_1+kN}{M_1}\equiv M\pmod N$$

MSS 攻撃は，ハッシュ値のパディングなどでメッセージに冗長性を付加する，あるいは署名方式で用いるメッセージの大きさを一定以下に制限する，という方法により防ぐことが出来る [12].

4.2 MSS 攻撃アルゴリズムの再考

本節では，MSS 攻撃のアルゴリズムに対して，署名偽造に必要な署名オラクルへの問い合わせ回数を減らすことを考える．その結果，攻撃者は 2 個のメッセージ $M1$，$M2$ と 1 個の署名 σ_2 から署名を偽造できることを示す．実際，以下にそのアルゴリズムを示すが，基本的なアイデアは，k，j のとり方を変更し，M_2 として，MM_1+kN のかわりに $MM_1^{2M_1+1}+kN$ を用いていることにある．

（1） Forger F が署名を偽造したいメッセージを M とする．F は任意の整数 $u>0$ を選び，

$$M_1=\frac{(2M+1)(2u+1)-1}{2}$$

を計算する．

（2） $2MM_1^{2M_1+1}+2kN+1=j(2M+1)$ を満たす k，j を計算する．$\gcd(N,2M+1)=1$ ならば，

$$k\equiv\frac{-2MM_1^{2M_1+1}-1}{2N}$$
$$\equiv\frac{MM_1^{2M_1}-1}{2N}\pmod{2M+1}$$

で k および j が求まる．

（3） F は $M_2=MM_1^{2M_1+1}+kN$ を計算する．

（4） F は署名オラクルに M_2 を問い合わせ，署名 σ_2 を入手する．

（5） F は M の署名 σ を以下の式で計算できる．

$$\sigma=\frac{\sigma_2^j}{M_1^{(2u+1)}}$$

σ が署名検証に合格することは以下の計算で確かめられる．

$$\sigma^{2M+1}=\frac{\sigma_2^{j(2M+1)}}{M_1^{2M_1+1}}=\frac{\sigma_2^{(2MM_1^{2M_1+1}+2kN+1)}}{M_1^{2M_1+1}}$$
$$=\frac{\sigma_2^{2M_2+1}}{M_1^{2M_1+1}}\equiv\frac{M_2}{M_1^{2M_1+1}}\equiv M\pmod N$$

ただし，この攻撃法は，元の MSS 攻撃と同様に，ハッシュ値のパディングなどでメッセージに冗長性を付加する，あるいは署名方式で用いるメッセージの大きさを一定以下に制限する，という方法により防ぐことができる．

5. 証明可能安全性を持つ署名方式の提案

GHR 署名は JC2 署名をもとに証明可能安全性を与えた方式と考えることが出来る．本章では JC1 および JC3 署名をもとに，証明可能安全性を持つ署名方式を提案する．

5.1 JC1-FDH

本節では，JC1 署名にハッシュ関数を 2 個付加することで，証明可能安全性を持つ署名方式 JC1-FDH を構成する．

JC1-FDH 署名

[鍵生成] 入力 1^k に対して，$k/2$ bit の素数 p,q で，素数 p',q' を用いて $p=2p'+1, q=2q'+1$ と表せるものをランダムに選ぶ．$N=pq$ とする．$e\in\mathbf{Z}^*_{\phi(N)}$ をランダムに選び，$d=e^{-1}\bmod\phi(N)$ を計算する．$PK=(N,e)$，$SK=(\phi(N),d)$ を返す．また，G を $G:\{0,1\}^*\to Z_N^*$ の Full Domain Hash 関数，H を $H:\{0,1\}^*\to Z_N^*$ のハッシュ関数とし，H_e を

$$H_e(x)=\begin{cases}H(x)+1 & e|H(x)\text{ のとき}\\ H(x) & \text{それ以外のとき}\end{cases}$$

とする．H_e は出力が e の倍数にならないハッシュ関数である．

[署名生成] メッセージ M に対して $\sigma=G(M)^{H_e(M)d\bmod\phi(N)}\bmod N$ を計算し，σ を M の署名として返す．

[署名検証] (M,σ) に対して $\sigma^e\equiv G(M)^{H_e(M)}\bmod N$ が成り立てば 1 を，そうでなければ 0 を返す．

JC1-FDH 署名の安全性は，RSA 関数の一方向性を破る確率的アルゴリズムを，署名を破る確率的アルゴリズムに帰着させることで以下のように証明できる．

[定理 1] ランダムオラクルモデルのもとで，RSA 関数が (t_I,ϵ_I)-one-way であるとき，JC1-FDH 署名方式は (t_F,ϵ_F)-安全である．ただし

$$\epsilon_F=\epsilon_I\cdot q_{sig}\cdot\frac{1}{(1-\frac{1}{1+q_{sig}})^{1+q_{sig}}}\approx\epsilon_I\cdot q_{sig}\cdot\exp(1)$$

$$t_F=t_I-(q_{sig}+q_G+q_H+1)\cdot O(k^3)$$

（証明）以下の補題 1 よりただちに導かれる． □

［補題 1］ G, H をランダム関数と仮定すると，JC1-FDH 署名を (t_F, ϵ_F) で破る Forger F が存在するとき，F を用いて RSA 関数の一方向性を $(t_I, \epsilon_I, q_{sig}, q_G, q_H)$ で破る Inverter I を構成できる．ただし

$$\epsilon_I = \frac{\epsilon_F}{q_{sig}} \cdot (1 - \frac{1}{1+q_{sig}})^{1+q_{sig}} \approx \frac{\epsilon_F}{q_{sig} \cdot \exp(1)}$$

$$t_I = t_F + (q_{sig} + q_G + q_H + 1) \cdot O(k^3)$$

（証明）入力として，任意の (N, e, x)（ただし $e, x \in Z_N^*$）および q_G, q_H, q_{sig}（ただし q_G, q_H, q_{sig} はそれぞれ G オラクル，H_e オラクル，署名オラクルへのアクセス回数）を受け取り，$x^d = x^{e^{-1}} \bmod N$ を出力する Inverter I を以下に構成する．

I の構成

1. $i \leftarrow 0$ とする．
2. F に N を入力．
3. G オラクルシミュレーションにおいて，F が M を問い合わせてきたとき：
   $i \leftarrow i+1$, $M_i \leftarrow M$ とする．Bias γ のコイン c_i を投げ，確率 γ で $c_i \leftarrow 0$，確率 $1-\gamma$ で $c_i \leftarrow 1$ として，
   - $c_i = 0$ なら $K_i \in Z_N^*$ をランダムに選び，$G(M_i) \leftarrow k_i^{e_i}$ を返す．
   - $c_i = 1$ なら $K_i \in Z_N^*$ をランダムに選び，$G(M_i) \leftarrow k_i^{e_i x}$ を返す．
4. H_e オラクルシミュレーションにおいて，F が $G(M_i)$ を問い合わせてきたとき：
   - $c_i = 0$ なら $r_i \in Z_N^*$ を e の倍数以外からランダムに選び，$H_e(G(M_i)) \leftarrow r_i$ を返す．
   - $c_i = 1$ なら $r_i \in Z_N^*$ をランダムに選び，$H_e(G(M_i)) \leftarrow 1 + r_i^{e_i}$ を返す．
5. 署名オラクルシミュレーションにおいて，F が M_i の署名 σ_i を問い合わせてきたとき：
   - $c_i = 0$ なら $\sigma_i \leftarrow k_i^{r_i} \bmod N$ を返す．
   - $c_i = 1$ なら停止する．
6. F が (M_i, σ) を出力したとき：
   - $c_i = 0$ なら停止する．
   - $c_i = 1$ なら

$$\sigma = (k_i^e x)^{(1+r_i e)d} \equiv k_i^{(1+r_i e)} x^{d+r_i} \pmod N$$

だから

$$\frac{\sigma}{k_i^{1+r_i e} x^{r_i}} \equiv x^d \pmod N$$

を計算すれば x^d が求まる．

I の成功確率 ϵ_I は

$$\epsilon_I = \gamma^{q_{sig}} \cdot (1-\gamma) \cdot \epsilon_F$$

ϵ_I が最大値をとるのは $\gamma = 1 - \frac{1}{1+q_{sig}}$ のときで，その値は

$$\epsilon_I = (1 - \frac{1}{1+q_{sig}})^{1+q_{sig}} \cdot \frac{1}{q_{sig}} \cdot \epsilon_F \approx \frac{\epsilon_F}{\exp(1) \cdot q_{sig}}$$

実行時間 t_I は

$$t_I = t_F + (q_G + q_H + q_{sig} - 1 + 2) \cdot O(k^3)$$
$$= t_F + (q_G + q_H + q_{sig} + 1) \cdot O(k^3)$$

である． □

5.2 JC3-FDH

本節では，JC3 署名にハッシュ関数を 2 個付加することで，証明可能安全性を持つ署名方式 JC3-FDH を構成する．

JC3-FDH 署名

[鍵生成] 入力 1^k に対して，$k/2$ bit の素数 p, q で，素数 p', q' を用いて $p = 2p'+1, q = 2q'+1$ と表せるものをランダムに選ぶ．$N = pq$ とし，$PK = N$, $SK = \phi(N)$ を返す．また，G を $G : \{0,1\}^* \rightarrow Z_N^*$ の Full Domain Hash 関数，H を $H : \{0,1\}^* \rightarrow Z_N^*$ のハッシュ関数とする．

[署名生成] メッセージ M に対して $\sigma = G(M)^{H(M)^{-1} \bmod \phi(N)} \bmod N$ を計算し，σ を M の署名として返す．

[署名検証] (M, σ) に対して $\sigma^{H(M)} \equiv G(M) \bmod N$ が成り立てば 1 を，そうでなければ 0 を返す．

JC3-FDH 署名の安全性は，強 RSA 問題を解く確率的アルゴリズムを，署名を破る確率的アルゴリズムに帰着させることで以下のように証明できる．

［定理 2］ G をランダム関数，H を Division-intractable なハッシュ関数と仮定すると，強 RSA 問題が (t_I, ϵ_I)-one-way であるとき，JC3-FDH 署名方式は $(t_F, \epsilon_F,)$-安全である．ただし

$$\epsilon_F = \epsilon_I \cdot q_{sig} \cdot \frac{1}{(1 - \frac{1}{1+q_{sig}})^{1+q_{sig}}} \approx \epsilon_I \cdot q_{sig} \cdot \exp(1)$$

$$t_F = t_I - (q_G + q_H) \cdot t_f(k) - (q_G + 1) \cdot O(k^3)$$

ここで $t_f(k)$ は k bit の素数を生成するのに必要な実行時間とする．

（証明）以下の補題 2 よりただちに導かれる． □

［補題 2］ G をランダム関数，H を Division-intractable なハッシュ関数と仮定すると，JC1-FDH 署名を (t_F, ϵ_F) で破る Forger F が存在するとき，F を用いて強 RSA 問題を $(t_I, \epsilon_I, q_{sig}, q_G, q_H)$ で解く Inverter I を構成できる．ただし

$$\epsilon_I = \frac{\epsilon_F}{q_{sig}} \cdot (1 - \frac{1}{1+q_{sig}})^{1+q_{sig}} \approx \frac{\epsilon_F}{q_{sig} \cdot \exp(1)}$$

$$t_I = t_F + (q_G + q_H) \cdot t_f(k) + (q_G + 1) \cdot O(k^3)$$

ここで $t_f(k)$ は k bit の素数を生成するのに必要な実行時間とする．

（証明）入力として任意の (N, s)（ただし $s \in Z_N^*$）および q_G, q_H, q_{sig}（ただし q_G, q_H, q_{sig} はそれぞれ G オラクル，H オラクル，署名オラクルへのアクセス回数）を受け取り，$x^e = s \bmod N$ を満たす (r, e) を出力する Inverter I を以下に構成する．以下では強 RSA 問題を解く I を構成するという点は GHR 署名の安全性証明と同様だが，$q_G + q_H$ 個の素数を用いることで証明を行っている．

I の構成

1. $i \leftarrow 0$, $E \leftarrow 1$ とする．

2. q_G+q_H 個の k bit の素数 $e_1,\cdots,e_{q_G},f_1,\cdots,f_{q_H}$ を生成する.
3. Bias γ のコイン c_j $(j=1,\cdots,q_G)$ を投げ，確率 γ で $c_j\leftarrow 0$, $E\leftarrow E\cdot e_j$，確率 $1-\gamma$ で $c_j\leftarrow 1$ とする.
4. F に (N,y) を入力する.
5. G オラクルシミュレーションにおいて，F が M を問い合わせてきたとき：
   $i\leftarrow i+1$，$M_i\leftarrow M$ として，
   - $c_i=0$ なら $w_i\in Z_N^*$ をランダムに選び，$G(M_i)\leftarrow w_i^{e_i} \bmod N$ を返す.
   - $c_i=1$ なら $G(M_i)\leftarrow s^{Ef_i} \bmod N$ を返す.
6. H オラクルシミュレーションにおいて，F が $G(M_i)$ を問い合わせてきたとき，$H(G(M_i))\leftarrow e_i$ を返す.
7. 署名オラクルシミュレーションにおいて，F が M_i の署名 σ_i を問い合わせてきたとき：
   - $c_i=0$ なら $\sigma_i\leftarrow w_i$ を返す.
   - $c_i=1$ なら停止する.
8. F が (M_i,σ) を出力したとき：
   - $c_i=0$ なら停止する.
   - $c_i=1$ なら $a\cdot e_i+b\cdot f_i=1$ を満たす a,b を Euclid の互除法を用いて計算し，$r\leftarrow \sigma^b s^a \bmod N, e\leftarrow e_i$ として (r,e) を出力する.

このとき

$$r^e=(\sigma^b s^a)^{e_i}=\sigma^{e_i b}s^{ae_i}$$
$$\equiv y^b s^{ae_i}\equiv s^{bE+ae_i}\equiv s \pmod N$$

となり (r,e) は強 RSA 問題の解である.

I の成功確率 ϵ_I は JC1-FDH の場合と同様に

$$\epsilon_I=\gamma^{q_{sig}}\cdot(1-\gamma)\cdot\epsilon_F$$

ϵ_I が最大値をとるのは $\gamma=1-\frac{1}{1+q_{sig}}$ のときで，その値は

$$\epsilon_I=(1-\frac{1}{1+q_{sig}})^{1+q_{sig}}\cdot\frac{1}{q_{sig}}\cdot\epsilon_F\approx\frac{\epsilon_F}{q_{sig}\cdot\exp(1)}$$

実行時間 t_I は

$$t_I=t_F+(q_G+q_H)\cdot t_f(k)+(q_G+1)\cdot O(k^3)$$

である．ただし $t_f(k)$ は k bit の素数を生成するのに必要な実行時間である. □

ランダム関数は Division-intractable であることから以下の系が導かれる.

[系] ランダムオラクルモデルのもとで，強 RSA 問題が (t_I,ϵ_I)-one-way であるとき，JC3-FDH 署名方式は $(t_F,\epsilon_F,)$-安全である．ただし

$$\epsilon_F=\epsilon_I\cdot q_{sig}\cdot\frac{1}{(1-\frac{1}{1+q_{sig}})^{1+q_{sig}}}\approx\epsilon_I\cdot q_{sig}\cdot\exp(1)$$

$$t_F=t_I-(q_G+q_H)\cdot t_f(k)-(q_G+1)\cdot O(k^3)$$

ここで $t_f(k)$ は k bit の素数を生成するのに必要な実行時間とする.

6. まとめ

本稿では，de Jonge と Chaum が提案したメッセージに依存するベキ指数を用いた RSA 署名方式に注目した．まず，JC3 署名に対する MSS 攻撃のアルゴリズムを再考し，署名オラクルへの問い合わせ回数が減らせることを示した．そして，JC1 および JC3 署名をもとにして，それぞれ証明可能安全性を持つ署名方式を提案した.

文献

[1] N. Baric, B. Pfitzmann, "Collision-Free Accumulators and Fail-Stop Signature Schemes Without Trees," Proc. Eurocrypt'97, LNCS vol.1233, pp.480-494, Springer-Verlag, 1997.

[2] M. Bellare, P. Rogaway, "Random Oracles are Practical: A Paradigm for Designing Efficient Protocols," Proc. 1st Annual Conf. on Computer and Communication Security, ACM, 1995.

[3] M. Bellare, P. Rogaway, "The exact security of digital signatures - How to sign with RSA and Rabin," Proc. Eurocryot'96, LNCS vol.1070, pp.399-416, Springer-Verlag, 1996.

[4] J. S. Coron, "On the exact security of Full Domain Hash," Proc. Crypto'2000, LNCS vol.1880, pp.229-235, Springer-Verlag, 2000.

[5] J. S. Coron, "Optimal security proofs for PSS and other signature scheme," Proc. Eurocrypt'02, LNCS vol.2332, pp.272-287, Springer-Verlag, 2002.

[6] J. S. Coron, D. Naccache, "Security analysis of the Gennaro-Halevi-Rabin signature scheme," Proc. Eurocrypt'00, LNCS vol.1807, pp.91-101, Springer-Verlag, 2000.

[7] T. ElGamal, "A Public key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Trans. on Information Theory, IT-31, 4, pp.469-472, 1985.

[8] A. Fujioka, T. Okamoto, S. Miyaguchi, "ESIGN: An Efficient Digital Signature Implementation on Smart Card," Proc. Eurocrypt'91, LNCS vol.547, pp.446-457, Springer-Verlag, 1991.

[9] R. Gennaro, S. Halevi, T. Rabin, "Secure Hash-and-Sign Signatures without the Random Oracle," Proc. Eurocrypt'99, LNCS vol.1592, pp.123-139, Springer-Verlag, 1999.

[10] S. Goldwasser, S. Micali, R. Rivest, "A Digital Signature Scheme Secure Against Adaptive Chosen-Message attacks," SIAM J.Computing, 17, 2, pp.281-308, 1988.

[11] W. de Jonge, D. Chaum, "Some Variations on RSA Signatures & their Security," Proc. Crypto'86, LNCS vol.263, pp.404-408, Springer-Verlag, 1987.

[12] M. Michels, M. Stadler, H. M. Sun, "On the Security of some Variants of the RSA Signature Scheme," Proc. ESORICS'98, LNCS vol.1485, pp.85-96, Springer-Verlag, 1998.

[13] R. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Crypotsystems," Communications of the ACM, vol.21, No.2, pp.120-126, 1978.

[14] "Proposed Federal Information Processing Standard for Digital Signature Standard (DSS)," Federal Register, v.56, n.169, 30, pp.42980-42982, 1991.