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

2005－ＣＳＥＣ－30（54）
2005／7／22

素因数分解に基づく無衝突関数を利用した暗号方式に関する検討

和田　純平†　神崎　元†　廣瀬　勝一††　吉田　進†

† 京都大学大学院情報学研究科　〒606–8501 京都府京都市吉田本町
†† 福井大学工学部　〒910–8507 福井市文京 3–9–1
E-mail: †{wada,kanzaki,yoshida}@hanase.kuee.kyoto-u.ac.jp, ††hirose@fuee.fukui-u.ac.jp

あらまし　無衝突関数は同じ出力に対応する異なる二つの入力を見つけるのが困難な関数であり，暗号・署名・認証など，情報セキュリティの様々な分野で用いられている．本稿では素因数分解に基づく無衝突関数として Schmidt-Samoa の関数と Shamir と Tauman の関数に注目し，それらを利用した暗号方式についての検討を行った．はじめにそれらの関数に基づくコミットメント方式を構成し，それらの方式の安全性について検討した．また，離散対数に基づく無衝突関数を用いた場合との比較を行った．次に，Schmidt-Samoa の関数に基づく故障停止署名について，複数メッセージに対する署名を効率化する方式を構成し，その方式が安全であることを示した．

キーワード　無衝突関数，Schmidt-Samoa の関数，Shamir と Tauman の関数，コミットメント，故障停止署名

A note on cryptographic schemes using collision-resistant functions based on factoring

Jumpei WADA†, Hajime KANZAKI†, Shoichi HIROSE††, and Susumu YOSHIDA†

† Graduate School of Informatics, Kyoto University　Yoshida-hommachi, Sakyo-ku, Kyoto, 606–8501 Japan
†† Faculty of Engineering, The University of Fukui　Bunkyo 3–9–1, Fukui, 910–8507 Japan
E-mail: †{wada,kanzaki,yoshida}@hanase.kuee.kyoto-u.ac.jp, ††hirose@fuee.fukui-u.ac.jp

Abstract　A many-to-one function is called collision-resistant if it is infeasible to find two distinct inputs which correspond to the same output. Collision-resistant functions are used for a lot of cryptographic schemes such as encryption, digital signature and identification. In this paper, we consider a few cryptographic schemes using two collision-resistant functions based on factoring: The Schmidt-Samoa function and the Shamir-Tauman function. First, we consider commitment schemes using these functions and discuss the security of the schemes. We also compare them with the one using a collision-resistant function based on discrete logarithm. Then, we present a scheme to improve the efficiency of the fail-stop signature using the Schmidt-Samoa function for multiple messages. We also prove the security of this scheme.

Key words　collision-resistant function, Schmidt-Samoa function, Shamir-Tauman function, commitment scheme, fail-stop signature

1. まえがき

無衝突関数は同じ出力に対応づけられる相異なる入力を見つけるのが困難な関数であり，暗号・署名・認証などの様々な暗号方式に用いられている．無衝突関数には MD5 [1] や SHA-1 [2] のように特別に構成された関数をはじめとして，素因数分解に基づく関数 [3] や離散対数に基づく関数 [4] のように，数論に基づく関数も様々なものが提案されている．本稿では，素因数分解に基づく無衝突関数である Schmidt-Samoa の関数 [5] と Shamir と Tauman の関数 [6] に注目し，これらの関数を利用した暗号方式について検討した．

はじめに，それらの無衝突関数を用いたコミットメント方式 (commitment scheme) について検討を行った．コミットメント方式では離散対数に基づく無衝突関数を用いた安全な方式は提案されている [4]．そこで，素因数分解に基づく無衝突関数を利用したコミットメント方式を示し，その安全性について検討するとともに，離散対数に基づく無衝突関数を利用した場合との比較を行った．

次に，Schmidt-Samoa [5] による故障停止署名 (fail-stop signature) について，複数のメッセージに対する効率化について検

討した．離散対数に基づく無衝突関数を利用した方式では，複数のメッセージに対して秘密鍵の長さを通常の半分程度にできる効率化の方法が提案されている [7]．その方法を Schmidt-Samoa の故障停止署名に適用し，同様の効率化ができることを示し，その方式が安全であることを証明した．

本稿の構成は以下の通りである．2 節では準備として本稿で用いる記法や定義を述べる．3 節では Schmidt-Samoa の関数と Shamir と Tauman の関数に基づくコミットメント方式の構成を示し，安全性について検討する．さらに，離散対数に基づく関数を利用した方式との比較を行う．4 節では素因数分解に基づく故障停止署名の複数メッセージに対する効率化の方法を示し，その安全性を証明する．5 節は本稿のまとめである．

2. 準　　備

2.1 表 記 法

本稿では以下の表記法を用いる．

$\{0,1\}^b$　長さ b の 2 値系列の集合．
$|x|_2$　非負整数 x を二進数表現で表したときのビット数．
$\lfloor y \rfloor$　実数 y 以下の最大の整数．
$u \circ v$　2 値系列 u，v の連結 (concatenation)．
$|A|$　集合 A の要素数．

2.2 定　　義

本節では，本稿で用いる関数や概念についての定義を行う．

無衝突関数　関数 f がいかなる確率多項式時間アルゴリズムを用いても $f(x)=f(y)$ かつ $x \neq y$ を満たすような (x,y) を求めることが困難であるとき，f を無衝突関数と呼ぶ．

束ね準同型写像　$(G,+)$ と $(H,\cdot)$ を可換群とする．写像 $h: G \to H$ が以下の条件を満たすとき，h を束ね準同型写像 (bundling homomorphism) と呼ぶ．

（1）　準同型写像である．すなわち，任意の $x,y \in G$ について $h(x+y)=h(x)\cdot h(y)$ を満たす．

（2）　任意の出力 $\mu \in h(G)$ に対して，以下が成り立つ．

$$|\{x|\mu = h(x)\}| \geq 2^{\tau} \tag{1}$$

ここで，2^{τ} は束ね次数 (bundling degree) と呼ばれる．

（3）　無衝突関数である．

カーマイケル関数　n が $n = {p_1}^{e_1} \cdots {p_s}^{e_s}$ と素因数分解されるとする．すなわち，$p_1,\ldots,p_s$ はすべて異なる素数であり，$e_1,\ldots,e_s$ は 1 以上の整数とする．このとき，カーマイケル関数 (Carmichael function) $\lambda(n)$ は以下の式で定義される．

$$\lambda(n) = \mathrm{lcm}({p_1}^{e_1-1}(p_1-1),\ldots,{p_s}^{e_s-1}(p_s-1)) \tag{2}$$

カーマイケル関数は乗法群 $\mathbb{Z}_n^*$ の元の最大の位数を表す．

メッセージ空間　コミットメント方式ではコミットすることができるメッセージ，署名方式では署名することができるメッセージ全体の集合をメッセージ空間 (message space) と呼び，$\mathcal{M}$ で表す．

インデックス空間　コミットメント方式において，メッセージをコミットする際に，ランダム化するために用いる要素全体からなる集合をインデックス空間 (indexing space) と呼び，$\mathcal{R}$ で表す．

2.3 Schmidt-Samoa の関数

2 つの異なる素数 p,q による積を $n = p^2q$ とするとき，Schmidt-Samoa の関数は以下の式で表される．

$$f(x) = x^n \bmod n \tag{3}$$

Schmidt-Samoa の関数は束ね準同型写像である [5]．すなわち，以下の性質がある．

（1）　乗法群 $\mathbb{Z}_n^*$ から $\mathbb{Z}_n^*$ への準同型写像である．

（2）　各出力について p 個の原像が存在する．

（3）　$n = p^2q$ の素因数分解の困難性を仮定すると，無衝突関数である．

さらに，出力に対する入力の分布について，以下の補題が成り立つ．

[補題 1]　任意の出力 $c \in f(\mathbb{Z}_n^*)$ に対して $f(x)=c$ を満たす p 個の解を $\{x_0,x_1,\ldots,x_{p-1}\}$ とする．このとき，x_i $(i \geq 1)$ は x_0 を用いて以下の式で表される．

$$x_i = x_0 + ipq \quad (i \geq 1) \tag{4}$$

2.4 Shamir と Tauman の関数

p,q を安全な素数 (safe prime)，すなわち $p' = (p-1)/2$，$q' = (q-1)/2$ も素数である十分大きな素数とし，$n = pq$ とする．g を位数 $\lambda(n) = 2p'q'$ の元とするとき，Shamir と Tauman の関数は以下の式で表される．

$$f(m,r) = g^{m \circ r} \bmod n \tag{5}$$

n の素因数分解の困難性を仮定すると，f は無衝突関数である [6]．

3. コミットメント

3.1 定義と安全性

コミットメントは送信者と受信者による交信プロトコルで，以下の 2 つのフェーズから構成されるプロトコルである．

コミット　送信者はコミットするメッセージ $m \in \mathcal{M}$ について乱数 $r \in \mathcal{R}$ を選び，受信者に $c = f(m,r)$ を送信する．

開示　送信者は m,r を開示する．受信者は $c = f(m,r)$ であればメッセージ m を受理する．そうでなければ拒否する．

コミットメントの安全性としては以下の条件が要求される．

（1）　コミットフェーズにおいて，いかなる受信者もメッセージ m を特定することはできない．

（2）　開示フェーズにおいて，いかなる送信者も，コミットしたメッセージ m と異なるメッセージ m' に対する，受信者に受理されるような (m',r') の組を開示することは困難である．

本稿では受信者の計算能力は無制限で，送信者の計算能力は確率多項式時間限定である unbounded-bounded モデルを考える．2 つの条件を満たすためにはコミットメントに用いる関数 f が無衝突関数であれば十分である．

3.2 Schmidt-Samoa の関数を利用した方式

本節では式 (3) で表される Schmidt-Samoa の関数を利用したコミットメントの構成を示し，その安全性を検討する．

式 (3) は 1 入力関数なので，入力をメッセージ部分と乱数部分に分け，$x = r \circ m$ としてコミットメントに利用することを考える．つまり，コミットメントに用いる関数 f は

$$f(m,r) = (r \circ m)^n \bmod n \tag{6}$$

である．この関数を利用したコミットメント方式は以下のようになる．

コミット　送信者はメッセージ $m \in \mathcal{M}$ について乱数 $r \in \mathcal{R}$ を選び，$c = (r \circ m)^n \bmod n$ を送信する．

開示　送信者は m, r を開示する．受信者は $r \circ m \in \mathbb{Z}_n^*$ であることを確認し，$f(m,r) = c$ であればメッセージを受理する．そうでなければ拒否する．

ここで，$|p|_2 = |q|_2 = k$ とした場合のメッセージ空間ならびにインデックス空間について検討する．

与えられた $c \in f(\mathbb{Z}_n^*)$ について，$c = x^n \bmod n$ の解の個数は p である．したがって $|\mathcal{M}| > p$ の場合には，いくつかの m について c は m のコミットメントとなり得ないことになる．したがって c が $\mathcal{M}$ のすべてのメッセージのコミットメントになるためには $|\mathcal{M}| \leqq p$ が必要である．今，$|p|_2 = k$ なので，$|m|_2 = k-1$ とすると，$\mathcal{M} = \{0,1\}^{k-1}$ であり，$|\mathcal{M}| \leqq p$ を満たす．次にインデックス空間 $\mathcal{R}$ について検討を行う．インデックス空間をある a に対して $\mathcal{R} = \{0,1,\ldots,a\}$ とする．ここで，r は任意のメッセージについて $r \circ m < n$ を満たす必要があるので，以下では a を上記のように $\mathcal{M}$ を定めた場合の最大値とする．すなわち，

$$a = \left\lfloor \frac{n}{2^{k-1}} - 1 \right\rfloor \tag{7}$$

である．

次の補題はインデックス空間 $\mathcal{R}$ の大きさが $pq-1 \leqq |\mathcal{R}| < 2pq$ であることを示している．証明は付録におく．

[補題 2]　$|p|_2 = |q|_2 = k$ とするとき，式 (7) で定義される a について，以下の式が成り立つ．

$$pq - 1 \leqq a \leqq 2pq - 2 \tag{8}$$

上記のコミットメント方式の安全性に関して以下の定理が成り立つ．

[定理 1]　Schmidt-Samoa の関数を利用したコミットメントにおいて，メッセージ空間 $\mathcal{M}$，インデックス空間 $\mathcal{R}$ を上記のように定める．任意の出力 $c \in f(\mathbb{Z}_n^*)$ が与えられたとき，任意のメッセージ $m \in \mathcal{M}$ に対して $c = f(m,r)$ を満たす $r \in \mathcal{R}$ が 1 つまたは 2 つ存在する．

(証明) 各 $c \in f(\mathbb{Z}_n^*)$ について，$f(x) = c$ の解は p 個であり，式 (4) のように表される．ここで，$0 \leqq x_0 < pq$ としても一般性は失われない．$r \circ m = 2^{k-1}r + m$ と表すことができるので，任意のメッセージ m について $f(m,r) = c$ を満たす r が存在するかどうかは

$$2^{k-1}r + m = x_0 + ipq \quad (i = 0,1,\ldots,p-1) \tag{9}$$

を満たす r が存在するかどうかを考えればよい．ここで，$x_0 < pq$ かつ pq の最下位ビットは 1 であるので，m が $k-1$ ビットであることを考えると，式 (9) の i は最上位ビットを除いて一意に定まる．i の最上位ビットが 1 で $i \leqq p-1$ であれば最上位ビットを 0 にした場合も 1 にした場合も式 (9) の右辺は有効な値であり，そうでなければ最上位ビットが 0 のときのみ有効な値である．したがって，式 (9) を満たす r は 1 つまたは 2 つ存在する．　□

3.3 Shamir と Tauman の関数を利用した方式

本節では式 (5) で表される Shamir と Tauman の関数を利用したコミットメントの構成を示し，その安全性を検討する．

Shamir と Tauman の関数は 2 入力なので，そのままコミットメントに利用することを考える．この場合の構成は以下のようになる．

コミット　送信者はメッセージ $m \in \mathcal{M}$ について乱数 $r \in \mathcal{R}$ を選び，$c = g^{m \circ r} \bmod n$ を送信する．

開示　送信者は m, r を開示する．受信者は $f(m,r) = c$ であればメッセージ m を受理する．そうでなければ拒否する．

ここで，$|p|_2 = |q|_2 = k$ とした場合のメッセージ空間ならびにインデックス空間について検討する．はじめに，インデックス空間について検討する．$|r|_2 = l$ とすると，$m \circ r = 2^l m + r$ と表すことができるので，式 (5) は以下のように表すことができる．

$$\begin{aligned} f(m,r) &= g^{2^l m + r} \bmod n \\ &= g^{2^l m} \cdot g^r \bmod n \end{aligned} \tag{10}$$

ここで，g の位数は $\lambda(n) = 2p'q'$ であるので，関数 f の出力の取り得る値は，集合

$$\{g, g^2, \ldots, g^{2p'q'}\} \tag{11}$$

である．したがって，$|\mathcal{R}| > 2p'q'$ を満たす場合には g^r はすべての出力値を取りうる．$|r|_2 = 2k-1$ とすると，$\mathcal{R} = \{0,1\}^{2k-1}$ であり，$|\mathcal{R}| = 2^{2k-1} > 2p'q'$ を満たす．次にメッセージ空間について検討する．ある整数 a について

$$m' \circ r' = m \circ r + a \cdot 2p'q' \tag{12}$$

となるように m', r' を定めれば，送信者は受信者を容易にだますことができる．しかし，$2p'q'$ は $n = pq$ から求めることは困難であり，仮に $2p'q'$ の倍数を求めることができた場合には n の素因数分解が多項式時間で求められることが示されている [8]．したがって，メッセージ空間は任意の長さの系列の集合

$\mathcal{M}=\{0,1\}^*$ とすることができる.

上記のコミットメント方式の安全性に関して以下の定理が成り立つ.

[定理 2] Shamir と Tauman の関数を利用したコミットメントにおいて, メッセージ空間 $\mathcal{M}$, インデックス空間 $\mathcal{R}$ を上記のように定める. 任意の出力 $c\in\{g,g^2,\ldots,g^{2p'q'}\}$ が与えられたとき, 任意のメッセージ $m\in\mathcal{M}$ に対して $c=f(m,r)$ を満たす $r\in\mathcal{R}$ が 1 つまたは 2 つ存在する.

(証明) 各出力 c が与えられたとき, $c=g^{c'}$ とすると,

$$c'\equiv 2^l m+r \pmod{2p'q'} \tag{13}$$

となる. 今, $|\mathcal{R}|>2p'q'$ より, 任意のメッセージ m に対して式 (13) を満たす r が存在する. ここで,

$$|\mathcal{R}|=2^{2k-1}<2\cdot 2p'q'=4p'q' \tag{14}$$

が成り立つので, 式 (13) を満たす r の個数はたかだか 2 つである. □

3.4 離散対数に基づく無衝突関数を利用した方式との比較

本節では Pedersen [4] による離散対数に基づく無衝突関数を利用した方式を説明し, Schmidt-Samoa の関数を利用した方式, Shamir と Tauman の関数を用いた方式と比較する.

p,q を q が $p-1$ を割り切るような十分大きな素数とする. このとき, 位数が q である部分群 G_q がただひとつ存在する. ランダムに $g,h\in G_q$ を選択し, 関数 $f:\mathbb{Z}_q\times\mathbb{Z}_q\to G_q$ を以下の式により定義する.

$$f(m,r)=g^m h^r \bmod p \tag{15}$$

この関数は離散対数問題の困難性を仮定すると, 無衝突関数である.

この関数を利用したコミットメント方式の安全性に関して以下の定理が成り立つ. この方式ではメッセージ空間 $\mathcal{M}=\mathbb{Z}_q$, インデックス空間 $\mathcal{R}=\mathbb{Z}_q$ である.

[定理 3] 上記の関数 f を用いたコミットメントにおいて, 任意の出力 $c\in f(\mathbb{Z}_q,\mathbb{Z}_q)$ が与えられたとき, 任意のメッセージ $m\in\mathcal{M}$ に対して $c=f(m,r)$ を満たす $r\in\mathcal{R}$ がただ 1 つ存在する.

(証明) 式 (15) より, 関数 f はメッセージ m を固定した場合, $f:\mathcal{R}\to G_q$ という 1 対 1 関数になる [4]. したがって, 任意の出力 $c\in G_q$ に対する $r\in\mathbb{Z}_q^*$ はただ 1 つ存在する. □

離散対数に基づく方式では, 上記のように任意の出力 c が与えられたときに, 任意のメッセージ m に対する r は 1 つであり, 出力の分布が一様であることが言える. 一方, Schmidt-Samoa の関数に基づく方式と Shamir と Tauman の関数に基づく方式ではともに任意のメッセージ m に対する r は 1 つまたは 2 つであり, 出力の分布は完全に一様ではない. したがって, 離散対数に基づく方式の方が, より安全な方式であるといえる.

ただし, 離散対数に基づく方式もメッセージ空間は有限である. したがって, Shamir と Tauman の関数に基づく方式の, 任意長の系列をメッセージにできるという特長は注目すべき性質であるといえる.

4. 故障停止署名の効率化

4.1 故障停止署名

故障停止署名とは, 正しく検証されるような署名が, 無限あるいは非常に計算能力の高い攻撃者によって偽造された場合でも, 署名者がほとんど 1 に近い確率でそれが偽造された署名であることを証明できる署名方式である.

故障停止署名のアルゴリズムは通常の署名と同様の鍵生成アルゴリズム G, 署名アルゴリズム S, 検証アルゴリズム T の他に, 偽造証明アルゴリズム P と偽造証明の検証アルゴリズム V からなる. 偽造証明アルゴリズムは正しく検証された署名が偽造されたものかどうかを証明するアルゴリズムで, 偽造証明 (proof of forgery) を計算する. 偽造証明の検証アルゴリズムはその偽造証明を検証する.

故障停止署名方式では, 各公開鍵に対して正しくはたらく秘密鍵が多数存在し, 署名者はそのうちの 1 つだけを知っている. 仮に, 無限あるいは非常に計算能力の高い攻撃者が公開鍵に対応するすべての秘密鍵を計算できたとしても, 署名者がどの秘密鍵を使用したのかは不明である. 攻撃者は署名を偽造する際に, これらの秘密鍵の中から 1 つを選んで署名の偽造を行うことになるが, その鍵が署名者の秘密鍵と一致する確率は非常に小さい. すなわち, これらの鍵によって生成される署名は非常に高い確率で異なる. それによって偽造されたことを判定することができる. 以上が故障停止署名の原理である.

4.2 Schmidt-Samoa の故障停止署名

本節では束ね準同型写像である Schmidt-Samoa の関数を利用した故障停止署名 [5] を説明する. この方式は $n=p^2q$ の素因数分解の困難性を仮定すると, 安全性が保証される.

鍵生成 セキュリティパラメータ (σ,k) を入力とし, 信頼されたセンターは $|p|_2=|q|_2=\tau=\max(\sigma,k/3)$ となる相異なる素数 p, q を選び, $n=p^2q$ とする. 署名者は秘密鍵 $sk_i\in\mathbb{Z}_n^*$ $(i=1,2)$ を選び, 公開鍵 pk_1, pk_2 を以下のように計算する.

$$\begin{aligned} pk_1 &= {sk_1}^n \bmod n \\ pk_2 &= {sk_2}^n \bmod n \end{aligned} \tag{16}$$

署名 メッセージ $m\in\mathbb{Z}_p$ に対する署名 s を

$$s=sk_1{sk_2}^m \bmod n \tag{17}$$

とする. なお, 署名者は p を知らないので, 実際には $m\in\mathbb{Z}_{2^\tau}$ とする.

検証 検証者は m に対する署名 s について, $m\in\mathbb{Z}_{2^\tau}$, $s\in\mathbb{Z}_n^*$ であることを確認する. さらに, m,s が検証式

$$pk_1{pk_2}^m\equiv s^n \pmod n \tag{18}$$

を満たすならば, s は m の正しい署名であるとする.

偽造証明 $\hat{s}$ を検証式 (18) を満たす署名とする. 署名者はこ

の $\hat{s}$ と同じメッセージに対する署名 s を生成する．このとき，$s=\hat{s}$ ならば署名 $\hat{s}$ は偽造ではないと判定される．そうでなければこの $(s,\hat{s})$ を偽造証明とする．

偽造証明の検証　$(x,\hat{x})\in\mathbb{Z}_n^*\times\mathbb{Z}_n^*$ に対して $x\neq\hat{x}$ かつ $x^n\equiv\hat{x}^n \pmod n$ が成立するとき，偽造が行われたと判定する．偽造証明 $(x,\hat{x})$ を用いることで n が容易に素因数分解される．

ただし，この署名方式では1つの秘密鍵につき，1つのメッセージにしか署名を行うことができない．仮に，秘密鍵 (sk_1,sk_2) による複数のメッセージ m_1,m_2 に対する署名 s_1,s_2 が得られた場合，$\gcd(m_1-m_2,n)=1$ より

$$\alpha(m_1-m_2)+\beta n=1 \tag{19}$$

なる α,β が存在する．これを用いることで sk_2 を以下のように計算することができる．

$$(s_1/s_2)^{\alpha}\,pk_2{}^{\beta} \bmod n = sk_2{}^{\alpha(m_1-m_2)}sk_2{}^{\beta n}=sk_2 \tag{20}$$

sk_2 が求まれば，sk_1 も求められることは自明である．

4.3 複数のメッセージに対する効率化

前節の理由により，N 個のメッセージに対して署名を行う場合，単純な方法では $2N$ 個の公開鍵，秘密鍵が必要になる．本節では Pedersen ら [7] による N 個のメッセージに対して秘密鍵を $(N+1)$ 個しか用いない方法を，前節の Schmidt-Samoa の故障停止署名方式に適用した場合についても，同様に効率化できることを示し，その安全性を証明する．

鍵生成　セキュリティパラメータ (σ,k) を入力とし，信頼されたセンターは $|p|_2=|q|_2=\tau=\max(\sigma,k/3)$ となるような素数 p,q を選び，$n=p^2q$ とする．署名者は $i=1,2,\ldots,N+1$ について $x_i\in\mathbb{Z}_n^*$ をランダムに選び，秘密鍵を

$$sk=(x_1,x_2,\ldots,x_{N+1}) \tag{21}$$

とする．これに対する公開鍵は

$$pk=(pk_1,pk_2,\ldots,pk_{N+1}) \tag{22}$$

であり，各 i $(i=1,2,\ldots,N+1)$ について

$$pk_i={x_i}^n \bmod n \tag{23}$$

である．

署名　j 番目のメッセージ m_j に対する署名 s_j を

$$s_j=(j,x_jx_{j+1}{}^{m_j} \bmod n) \tag{24}$$

とする．ただし，$m_j\neq 0$ とする．

検証　検証者は m_j に対する署名 $s_j=(j,y_j)$ について，$m_j\in\mathbb{Z}_n^*$，$0\leq j\leq N$，$y_j\in\mathbb{Z}_n^*$ であることを確認する．さらに，検証式

$$pk_jpk_{j+1}{}^{m_j}\equiv {y_j}^n \pmod n \tag{25}$$

を満たすならば，s_j は m_j の正しい署名であるとする．

偽造証明　$\hat{s}$ を検証式 (25) を満たす署名とする．署名者はこの $\hat{s}$ と同じメッセージに対する署名 s を生成する．このとき，$s=\hat{s}$ ならば署名 $\hat{s}$ は偽造ではないと判定される．そうでなければこの $(s,\hat{s})$ を偽造証明とする．

偽造証明の検証　$(x,\hat{x})\in\mathbb{Z}_n^*\times\mathbb{Z}_n^*$ に対して $x\neq\hat{x}$ かつ $x^n\equiv\hat{x}^n \pmod n$ が成立するとき，偽造が行われたと判定する．偽造証明 $(x,\hat{x})$ を用いることで n が容易に素因数分解される．

この故障停止署名方式の構成の安全性に関して以下の定理が成り立つ．

[定理 4]　$n=p^2q$ の素因数分解が困難であれば，上記の構成は安全な故障停止署名である．

(証明) 署名者の N 個のメッセージ $m_1,m_2,\ldots,m_N$ に対する署名 $(1,s_1),(2,s_2),\ldots,(N,s_N)$ を考える．ここで，

$${s_1}^n=(x_1x_2^{m_1})^n=pk_1pk_2{}^{m_1} \bmod n \tag{26}$$

$$pk_1={x_1}^n \bmod n \tag{27}$$

$$pk_2={x_2}^n \bmod n \tag{28}$$

より，$pk_1\equiv s_1pk_2{}^{-m_1} \pmod n$ なので，式 (27) は冗長である．同様に，$pk_i={x_i}^n \bmod n$ $(i=1,2,\ldots,N)$ は冗長であるので，結局

$$s_j=x_jx_{j+1}{}^{m_j} \bmod n \ (j=1,2,\ldots,N) \tag{29}$$

$$pk_{N+1}={x_{N+1}}^n \bmod n \tag{30}$$

を考えればいいことになる．ここで，式 (30) において x_{N+1} をひとつ決めると，式 (29) から，すべての x_j $(j=1,2,\ldots,N+1)$ が一意に定まる．式 (30) の解は p 個なので，式 (29) の解も p 個である．なお，$m_j=0$ であれば，式 (29) より x_{j+1} に関わらず x_j が一意に定まる．それにより $x_1,x_2,\ldots,x_j$ がすべて一意に定まるため，ここでは $m_j\neq 0$ としている．

今，ある i について，$m_i\neq m_i^*$ なるメッセージに対して偽造が行われたと仮定する．すなわち，式 (29)(30) に加えて，

$$s_i^*=x_ix_{i+1}{}^{m_i^*} \bmod n \tag{31}$$

を考える．このとき，

$$s_i^*/s_i\equiv {x_{i+1}}^{m_i^*-m_i} \pmod n \tag{32}$$

である．この式の解の1つを v とする．v は

$$\begin{aligned} &{x_{i+1}}^n\equiv v^n \pmod n \\ &(x_{i+1}/v)^{m_i^*-m_i}\equiv 1 \pmod n \end{aligned} \tag{33}$$

を満たすので，$x_{i+1}/v=d$，$m_i^*-m_i=\hat{m}$ とすると，式 (32) の可能な解の個数は $T=\{d\in\mathbb{Z}_n^*|d^n\equiv 1 \pmod n \wedge d^{\hat{m}}\equiv 1 \pmod n\}$ という T の要素である．$d^n\equiv 1 \pmod n$ より，$d=1$ または d の位数が p であるが，$\hat{m}\in\mathbb{Z}_p^*$ かつ $d^{\hat{m}}\equiv 1 \pmod n$ なので，d の位数は p ではない．したがって $d=1$ であり，$|T|=1$ である．

以上より，署名者の公開鍵 $pk=\{pk_1,pk_2,\ldots,pk_{N+1}\}$ に対応する，検証式(25)を満たす秘密鍵 $sk=\{sk_1,sk_2,\ldots,sk_{N+1}\}$ は p 組あり，それらが互いに相異なることがいえた．つまり，署名者と同じ署名を生成することができる秘密鍵は p 組のうちひとつだけである．すなわち，偽造証明 (s_i,s_i^*) が偽造ではないと判定される秘密鍵はそれら p 組のうちひとつだけであり，これはいかなる攻撃者に対しても $1/p$ の確率でしか偽造に成功しないことを示している． □

5. むすび

本稿では，はじめに，素因数分解に基づく無衝突関数であるSchmidt-Samoaの関数とShamirとTaumanの関数を利用したコミットメント方式を構成し，それらの方式では無限の計算能力を持つ受信者もメッセージを特定することはできないという安全性を証明した．さらに，離散対数に基づく無衝突関数を利用した方式との比較を行った．次に，Schmidt-Samoaの故障停止署名方式について，秘密鍵の長さを通常の半分程度にできる複数のメッセージに対する効率化の方法を適用し，その方式が無限の計算能力をもつ攻撃者に対しても安全な方式であることを証明した．

文　献

[1] R. Rivest, "The MD5 message digest algorithm," Request for Comments (RFC), 1321, 1992.

[2] National Institute of Standards and Technology, "Secure hash standard," FIPS Publication, no. 180–1, 1995.

[3] S. Goldwasser, S. Micali, and R. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," *SIAM Journal of Computing*, vol. 17, pp. 281–308, 1988.

[4] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," In *CRYPTO'91*, Lecture Note in Computer Science, vol. 576, pp. 129–140, 1992.

[5] K. Schmidt-Samoa, "Factorization-based fail-stop signatures revisited," *ICICS 2004*, Lecture Note in Computer Science, vol. 3269, pp. 118–131, 2004.

[6] A. Shamir, and Y. Tauman, "Improved online/offline signature schemes," In *CRYPTO 2001*, Lecture Note in Computer Science, vol. 2139, pp. 355–367, 2001.

[7] T. P. Pedersen, and B. Pfitzmann, "Fail-stop signatures," *SIAM Journal on Computing*, vol. 26, no.2, pp. 291–330, 1997.

[8] G. Miller, "Riemann's hypothesis and tests for primality," *Journal of Computer and System sciences*, vol. 13, pp. 300–317, 1976.

[9] S. Halevi, and S. Micali, "Practical and provably-secure commitment scheme from collision-free hashing," In *CRYPTO'96*, Lecture Notes in Computer Science, vol. 1109, pp. 201–215, 1996.

付　録

[補題1の証明]

すべての i $(i=1,2,\ldots,p-1)$ について ${x_i}^n={x_0}^n$ が成り立つことを示す．$(x_0+ipq)^n$ を二項展開すると，以下のようになる．

$$\begin{aligned}(x_0+ipq)^n&=\sum_{j=0}^{n}\binom{n}{j}{x_0}^{n-j}(ipq)^j\\&=\binom{n}{0}{x_0}^n+\binom{n}{1}{x_0}^{n-1}ipq\\&\quad+\binom{n}{2}{x_0}^{n-2}(ipq)^2+\cdots\end{aligned}\tag{A·1}$$

ここで，両辺の $\bmod p^2q$ を考える．第二項は $n=p^2q$，第三項以降は $(pq)^2$ を約数としてもつため余りは0となり，結局第一項のみが残る．すなわち，すべての i $(i=1,2,\ldots,p-1)$ について

$$(x_0+ipq)^n \bmod n={x_0}^n \bmod n.\tag{A·2}$$

である． □

[補題2の証明]

まず，$pq-1\leqq a$ を証明する．今，$|p|_2=k$ なので，$p>2^{k-1}$ である．$n=p^2q$ であるので，式(7)の $\lfloor\ \rfloor$ 内は以下のように評価できる．

$$\begin{aligned}\frac{p^2q}{2^{k-1}}-1&>\frac{2^{k-1}\cdot pq}{2^{k-1}}-1\\&=pq-1\end{aligned}\tag{A·3}$$

したがって，$pq-1\leqq a$ である．

次に，$a\leqq 2pq-2$ を証明する．$|p|_2=k$ より，$p<2^k$ であることを考えると，上記と同様に，式(7)の $\lfloor\ \rfloor$ 内は以下のように評価できる．

$$\begin{aligned}\frac{p^2q}{2^{k-1}}-1&<\frac{2^kpq}{2^{k-1}}-1\\&=2pq-1\end{aligned}\tag{A·4}$$

したがって，$a\leqq 2pq-2$ である．

以上で補題は証明された． □