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

2004－ＣＳＥＣ－26　（４）
2004／7／20

並列型・直列型 Davies-Meyer に基づく安全な倍ブロック長ハッシュ関数

廣瀬　勝一†

† 京都大学情報学研究科　〒606–8501 京都市左京区吉田本町
E-mail: †hirose@i.kyoto-u.ac.jp

あらまし　ブロック暗号を利用した倍ブロック長ハッシュ関数については，出力長を ℓ とするとき，無衝突性に対する任意の攻撃の時間計算量が $\Omega(2^{\ell/2})$ であるような効率の良いハッシュ関数が存在するかどうかは未解決問題である．本稿では，ブラックボックスモデルで，この問題に対する部分的でありながら肯定的な解が与えられる．ここで部分的な解であるという理由は，これまでとは異なり，安全性の証明においてハッシュ関数が 2 種類のブロック暗号を利用することを仮定するということである．

キーワード　並列型 Davies-Meyer, 直列型 Davies-Meyer, 倍ブロック長ハッシュ関数, ブラックボックスモデル, ブロック暗号

Secure Double Block Length Hash Functions Based on Abreast/Tandem Davies-Meyer

Shoichi HIROSE†

† Graduate School of Informatics, Kyoto University, Kyoto 606–8501 JAPAN
E-mail: †hirose@i.kyoto-u.ac.jp

Abstract　It is an open question whether there exists an efficient double-block-length hash function such that time complexity of any collision-finding algorithm against it is $\Omega(2^{\ell/2})$, where ℓ is the length of the output. In this article, a partial but affirmative answer is given to this question in a black-box model. The answer is partial because it is assumed that two different block ciphers are used in the hash functions for the security proofs.

Key words　abreast Davies-Meyer, tandem Davies-Meyer, double-block-length hash function, black-box model, block cipher

1. まえがき

暗号用ハッシュ関数（cryptographic hash function）は，任意長の入力を固定長の出力に対応させる関数であり，暗号への応用のために，一方向性（preimage resistance），準無衝突性（second preimage resistance），無衝突性（collision resistance）を満たす．一方向性は与えられた出力に対応する入力を計算することが困難であるという性質である．準無衝突性は，与えられた入力と同じ出力に対応する別の入力を計算することが困難であるという性質である．無衝突性は，同じ出力に対応する相異なる二つの入力を計算することが困難であるという性質である．以下では簡単のため，暗号用ハッシュ関数を単にハッシュ関数と記す．

ハッシュ関数は通常，入出力が固定長の圧縮関数（compression function）の逐次的な反復適用によって計算されるが，この圧縮関数の構成法は二つに分類できる．一つはブロック暗号を利用する方法であり，もう一つはそのような暗号の基本要素を利用することなく一から構成する方法である．前者には安全なブロック暗号を利用することにより，設計の負担を軽減できるという利点があるが，処理速度の観点からは後者が有利である．但し，処理速度に関する前者の欠点は，AES などの高速なブロック暗号を利用することにより，ある程度補償することが可能である．

本稿ではブロック暗号を利用した圧縮関数からなるハッシュ関数を扱う．このようなハッシュ関数は，出力長に応じて，単ブロック長ハッシュ関数と倍ブロック長ハッシュ関数に分類される．これらはそれぞれ，その構成要素であるブロック暗号のブロック長と同じ長さ，あるいは 2 倍の長さの出力をもつハッシュ関数である．

ハッシュ関数の出力長を ℓ ビットとするとき，無衝突性に関

しては，バースデー攻撃により $O(2^{\ell/2})$ 時間で，同じ出力に対応する相異なる二つの入力が得られることが広く知られている．一方，AES をはじめとするブロック暗号のブロック長は 128 ビットあるいはそれ以下であり，これらを利用してハッシュ関数を構成することを考えると，単ブロック長ハッシュ関数は無衝突性に関して必ずしも十分に安全であるとは言えない．

倍ブロック長ハッシュ関数の構成および安全性に関しては，これまでにも，幾つかの研究が行われている [2]〜[5], [8]．しかし，無衝突性に関して真に安全な倍ブロック長ハッシュ関数，すなわち，同じ出力に対応する相異なる二つの入力の計算に要する時間が $\Omega(2^{\ell/2})$ であるような倍ブロック長ハッシュ関数の提案はなされていない．

本稿では，無衝突性に関して真に安全な倍ブロック長ハッシュ関数を示す．これらのハッシュ関数の圧縮関数は，鍵長がブロック長の 2 倍のブロック暗号を利用して，並列型あるいは直列型 Davies-Meyer 倍ブロック長ハッシュ関数 [5] と Preneel, Govaerts, Vandewalle の 12 個の安全な圧縮関数 [7] に基づいて構成される．

本稿で提案されるハッシュ関数には，鍵長がブロック長の 2 倍のブロック暗号が利用されるが，例えば AES では鍵長が 256 ビットの場合の仕様も定められている．また，圧縮関数のレートは 1/2 であり，圧縮関数の計算では，ブロック暗号による暗号化が 2 回行われる．

従来の倍ブロック長ハッシュ関数と異なり，本稿で提案されるハッシュ関数で新たに導入される仮定は，安全性を保証するために，2 個の相異なるブロック暗号を圧縮関数に利用するということである．なお，2 個の相異なるブロック暗号は，例えば，tweakable ブロック暗号 [6] であれば，相異なる tweak を利用することにより，実際上は 1 種類の tweakable ブロック暗号で実現できると考えられる．また，例えば，[2] で扱われているレート 1 の倍ブロック長ハッシュ関数では，仮に相異なる 2 個のブロック暗号を用いても，安全性が増すことはない．

ハッシュ関数の安全性の解析は，真にランダムなブロック暗号を仮定して行われる．これまでに提案されているブロック暗号を利用したハッシュ関数に対する攻撃法の殆どは，ブロック暗号の内部構造を利用しておらず，これまでにも，同じ仮定の下で安全性の解析が行われている [1], [9]．なお，本稿で提案されるハッシュ関数の安全性の解析では，2 種類のブロック暗号が互いに独立で真にランダムであるということが仮定される．

本稿の構成は以下の通りである．2 章は後の議論のための準備である．3 章では，真に安全な倍ブロック長ハッシュ関数の構成を示すと共に，無衝突性に関する安全性の証明を与える．4 章は 3 章の結果に関する考察である．5 章はむすびであり，今後の課題についても触れる．

2. 準　　備

2.1 暗号用ハッシュ関数

暗号用ハッシュ関数 H は，任意長の入力を固定長の出力に対応させる関数である．H が満たすべき性質は以下の三つである．

一方向性　出力 y が与えられたときに，$y = H(x)$ なる入力 x を見つけることが困難である．

準無衝突性　入力 x が与えられたときに，$H(x) = H(x')$ かつ $x \neq x'$ を満たす入力 x を見つけることが困難である．

無衝突性　$H(x) = H(x')$ かつ $x \neq x'$ を満たす入力 x，x' を見つけることが困難である．

以下では簡単のため，暗号用ハッシュ関数を単にハッシュ関数と記す．

ハッシュ関数 $H : \{0,1\}^* \to \{0,1\}^\ell$ は通常，入出力が固定長の圧縮関数 $f : \{0,1\}^{\ell'} \to \{0,1\}^\ell$ の逐次的な反復適用によって計算される．ここで，$\ell' > \ell$ である．入力 m は長さ $\ell' - \ell$ の l 個のブロック $m_1, m_2, \ldots, m_l$ に分割され，$1 \leq i \leq l$ について，

$$h_i = f(h_{i-1}, m_i)$$

が計算される．$h_l = H(m)$ である．なお，h_0 はあらかじめ与えられる初期値である．m の長さが $\ell' - \ell$ の倍数でない場合は，適当なパディングが行われるが，これについては本稿では立ち入らない．

圧縮関数の構成法は二つに分類できる．一つはブロック暗号を利用する方法であり，もう一つはそのような暗号の基本要素を利用することなく一から構成する方法である．本稿では，ブロック暗号を利用する構成法について考察する．

2.2 ブロック暗号とブラックボックスモデル

ブロック長 n，鍵長 κ のブロック暗号 $e : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$ を (n,κ) ブロック暗号と呼ぶ．以下では，(n,κ) ブロック暗号すべての集合を $B(n,\kappa)$ と表記する．

ブロック暗号を利用したハッシュ関数に対してこれまでに知られている殆んどすべての攻撃法は，ブロック暗号の内部構造を利用しない．このことから，ブロック暗号に基づくハッシュ関数の安全性の解析は，しばしば，各鍵 k について，$e(k,\cdot)$ が真にランダムでありかつ可逆な置換であると仮定して行われる．ブロック暗号に対するこのような仮定はブラックボックスモデルと呼ばれる．

ブラックボックスモデルでは，ブロック暗号による暗号化 e および復号 e^{-1} は以下のようなオラクルへの問合わせにより行われる．暗号化オラクル e は鍵と平文の組である問合わせ (k,x) に対して，暗号文 y を返す．復号オラクル e^{-1} は鍵と暗号文の組である問合わせ (k,y) に対して，平文 x を返す．なお，e, e^{-1} は，それまでの問合わせと返答からなる鍵，平文，暗号文の組 (k_i, x_i, y_i) の一覧を共有し，新しい問合わせ (k,x) あるいは (k,y) に対して，$e(k,\cdot)$ が置換であるという制約の下に，暗号文 y または平文 x を無作為に選んで返答する．同時に (k,x,y) を一覧に追加する．

なお，一般性を失うことなく，オラクル e, e^{-1} を利用する任意の攻撃アルゴリズムは，問合わせとそれに対する返答により得られた鍵，平文，暗号文に対しては，再び問合わせを行うことはないと仮定することができる．例えば i 回目の問い合わせにより (k_i, x_i, y_i) が得られた場合，それ以降，(k_i, x_i)，(k_i, y_i) のどちらも問合わせることがない．

2.3 関 連 研 究

ブロック暗号を利用したハッシュ関数は，出力長がブロック暗号のブロック長と等しいとき，単ブロック長ハッシュ関数と呼ばれる．また，出力長がブロック長の 2 倍のとき，倍ブロック長ハッシュ関数と呼ばれる．倍ブロック長ハッシュ関数の処

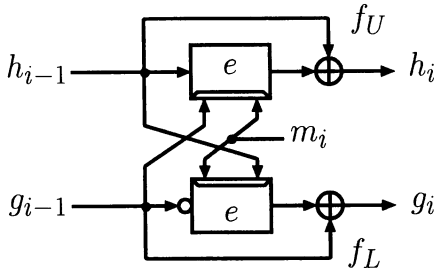

図 1　並列型 DM 倍ブロック長ハッシュ関数

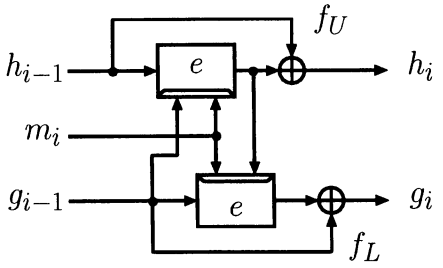

図 2　直列型 DM 倍ブロック長ハッシュ関数

理効率の尺度としてレートが次のように定義される．圧縮関数 $f(h_{i-1}, m_i)$ で，(n, κ) ブロック暗号が σ 回使われるとき，レートは $|m_i|/(n\sigma)$ である．

Preneel, Govaerts, Vandewalle [7] は，$h_i = e(k, x) \oplus z$ なる圧縮関数からなるすべての単ブロック長ハッシュ関数について，幾つかの攻撃法に対する安全性を考察している．なお，e は (n, n) ブロック暗号であり，$k, x, z \in \{h_{i-1}, m_i, h_{i-1} \oplus m_i, v\}$ で v は定数である．彼らは，表 1 の 12 種類の圧縮関数をもつ単ブロック長ハッシュ関数が安全であるとした．

Black, Rogaway, Shrimpton [1] は，ブラックボックスモデルを仮定して，Preneel, Govaerts, Vandewalle と同じ単ブロック長ハッシュ関数の安全性を解析した．特に，上の 12 個を含む 20 個の単ブロック長ハッシュ関数について，無衝突性に対する任意の攻撃の時間計算量が $\Omega(2^{\ell/2})$ であることを示した．ここで，ℓ はハッシュ関数の出力長で $\ell = n$ である．

倍ブロック長ハッシュ関数については，Knudsen, Lai, Preneel [4] が，(n, n) ブロック暗号を利用したレート 1 のハッシュ関数の安全性について議論している．また，Hohl, Lai, Meier, Waldvogel [3] は，レート 1/2 のハッシュ関数の圧縮関数の安全性について議論している．一方，Satoh, Haga, Kurosawa [8] や Hattori, Hirose, Yoshida [2] は，$(n, 2n)$ ブロック暗号を用いたレート 1 のハッシュ関数の安全性について議論している．これらの研究にもかかわらず，無衝突性に関して真に安全な倍ブロック長ハッシュ関数，即ち，無衝突性に対する任意の攻撃の時間計算量が $\Omega(2^{\ell/2}) = \Omega(2^n)$ である倍ブロック長ハッシュ関数が存在するかどうかは未解決問題である．

並列型・直列型 DM 倍ブロック長ハッシュ関数は，$(n, 2n)$ ブロック暗号を利用して構成されるレート 1/2 の倍ブロック長ハッシュ関数である [5]．並列型 DM 倍ブロック長ハッシュ関数の構成は図 1 の通りである．直列型 DM 倍ブロック長ハッシュ関数の構成は図 2 の通りである．これらのハッシュ関数については十分な安全性の解析がなされていない．

2.4　本稿で扱う倍ブロック長ハッシュ関数

本稿では $(n, 2n)$ ブロック暗号を利用したレート 1/2 の倍ブロック長ハッシュ関数を扱う．倍ブロック長ハッシュ関数の圧縮関数 f は，

$$(h_i, g_i) = f(h_{i-1}, g_{i-1}, m_i)$$

のように表記できる．ここで，$h_i, g_i, m_i \in \{0,1\}^n$ である．m_i は入力のブロックである．h_i, g_i はさらに，以下のように表記できる．

$$\begin{cases} h_i = f_U(h_{i-1}, g_{i-1}, m_i) \\ g_i = f_L(h_{i-1}, g_{i-1}, m_i, h_i) \end{cases}$$

このように，g_i が h_i に依存するハッシュ関数は直列型，h_i には依存せず，h_i と同様，h_{i-1}, g_{i-1}, m_i のみで決まるハッシュ関数は並列型と呼ばれる．

f_U, f_L はそれぞれ，以下のように，ブロック暗号を 1 回利用して計算される．

$$\begin{cases} h_i = e_U((k_{U1}, k_{U2}), x_U) \oplus z_U \\ g_i = e_L((k_{L1}, k_{L2}), x_L) \oplus z_L \end{cases}$$

さらに，本稿では，k_{U1}, k_{U2}, x_U, z_U が h_{i-1}, g_{i-1}, m_i の線形結合，k_{L1}, k_{L2}, x_L, z_L が $h_{i-1}, g_{i-1}, m_i(, h_i)$ の線形結合で表されるような倍ブロック長ハッシュ関数のみを対象とする．

なお通常一般に，e_U と e_L とは同一のブロック暗号であるが，本稿では，安全性の解析の際に，それらは相異なる二つのブロック暗号であると仮定される．

2.5　安全性に関する定義

本章で既に述べたように，本稿では，ブラックボックスモデルにより倍ブロック長ハッシュ関数の安全性を評価する．本稿では，Black, Rogaway, Shrimpton [1] による安全性の定義及び表記法に従う．

[定義 1]（ハッシュ関数の無衝突性）　2 種類のブロック暗号を用いた倍ブロック長ハッシュ関数 H に対する敵 $\mathcal{A}$ の無衝突性に関する有利度は以下のように定義される．

$$\mathbf{Adv}_H^{\mathrm{coll}}(\mathcal{A}) = \Pr[m \neq m' \wedge H(m) = H(m') \mid e_U \leftarrow_{\mathrm{R}} B(n,2n) \wedge e_L \leftarrow_{\mathrm{R}} B(n,2n) \wedge (m, m') \leftarrow_{\mathrm{R}} \mathcal{A}^{e_U^{\pm 1}, e_L^{\pm 1}}]$$

なお，$e_U^{\pm 1}$ はオラクル e_U, e_U^{-1} の組を表す．e_L についても同様である．また，$\leftarrow_{\mathrm{R}}$ は，右辺が集合のとき，要素の無作為な抽出を表し，右辺がアルゴリズムのとき，その入力の分布とコイン投げに基づく出力を表す．　◇

$q \geq 1$ について，

$$\mathbf{Adv}_H^{\mathrm{coll}}(q) = \max_{\mathcal{A}} \left\{ \mathbf{Adv}_H^{\mathrm{coll}}(\mathcal{A}) \right\}$$

と定義する．但し，$\mathcal{A}$ は $e_U^{\pm 1}$ と $e_L^{\pm 1}$ のそれぞれに対して高々 q 回の問合わせをする．

[定義 2]（圧縮関数の無衝突性） 2種類のブロック暗号を用いた圧縮関数 f に対する敵 $\mathcal{A}$ の無衝突性に関する有利度は以下のように定義される．

$$\mathbf{Adv}_f^{\mathrm{comp}}(\mathcal{A}) = \Pr[(h,m) \neq (h',m') \wedge f(h,m) = f(h',m') \vee f(h,m) = h_0 \mid e_U \leftarrow_{\mathrm{R}} B(n,2n) \wedge e_L \leftarrow_{\mathrm{R}} B(n,2n) \wedge ((h,m),(h',m')) \leftarrow_{\mathrm{R}} \mathcal{A}^{e_U^{\pm 1}, e_L^{\pm 1}}]$$

h_0 はあらかじめ与えられたハッシュ関数の初期値である． ◊

$q \geq 1$ について，

$$\mathbf{Adv}_f^{\mathrm{comp}}(q) = \max_{\mathcal{A}} \left\{ \mathbf{Adv}_f^{\mathrm{comp}}(\mathcal{A}) \right\}$$

と定義する．但し，$\mathcal{A}$ は $e_U^{\pm 1}$ と $e_L^{\pm 1}$ のそれぞれに対して高々 q 回の問合わせをする．

3. 安全な倍ブロック長ハッシュ関数

本章では，無衝突性に関して安全な圧縮関数から安全なハッシュ関数が構成されることを表す以下の事実を利用して，ハッシュ関数の無衝突性に関する安全性を示す．

[補題 1] [1] H を圧縮関数 f からなるハッシュ関数とするとき，$q \geq 1$ について，$\mathbf{Adv}_H^{\mathrm{coll}}(q) \leq \mathbf{Adv}_f^{\mathrm{comp}}(q)$． ◊

3.1 並列型 DM に基づく安全な倍ブロック長ハッシュ関数

本節では，図 3 のような型の圧縮関数をもつ倍ブロック長ハッシュ関数について考察する．より正確には，

$$\begin{cases} h_i = e_U((k_{U1}, k_{U2}), x_U) \oplus z_U \\ g_i = e_L((k_{L1}, k_{L2}), x_L) \oplus z_L, \end{cases}$$

ここで

$$k_{U1} = g_{i-1},\ \begin{pmatrix} k_{U2} \\ x_U \\ z_U \end{pmatrix} = U \begin{pmatrix} h_{i-1} \\ m_i \end{pmatrix}$$

$$k_{L1} = h_{i-1},\ \begin{pmatrix} k_{L2} \\ x_L \\ z_L \end{pmatrix} = L \begin{pmatrix} g_{i-1} \\ m_i \end{pmatrix}$$

であり，U と L とはともに 3×2 の $\{0,1\}$ 行列である．以下では，このような圧縮関数をもつハッシュ関数を並列型 DM に基づく倍ブロック長ハッシュ関数と呼ぶ．

[補題 2] 並列型 DM に基づく任意の倍ブロック長ハッシュ関数について，U_{12} と L_{12} とはそれぞれ，U と L とから第 3 行を除いた 2×2 部分行列を表すものとする．U_{12} と L_{12} とがともに正則ならば，(k_{U1}, k_{U2}, x_U) と (k_{L1}, k_{L2}, x_L) との対応は 1 対 1 である． ◊

証明）U_{12} が正則だから，$k_{U1} = g_{i-1}$ と

$$\begin{pmatrix} k_{U2} \\ x_U \end{pmatrix} = U_{12} \begin{pmatrix} h_{i-1} \\ m_i \end{pmatrix}$$

より，(k_{U1}, k_{U2}, x_U) と (h_{i-1}, g_{i-1}, m_i) との対応は 1 対 1 である．同様に，(k_{L1}, k_{L2}, x_L) と (h_{i-1}, g_{i-1}, m_i) との対応は 1 対 1 である．したがって，(k_{U1}, k_{U2}, x_U) と (k_{L1}, k_{L2}, x_L) との対応は 1 対 1 である． □

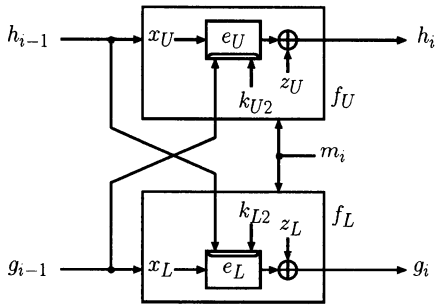

図 3 並列型 DM に基づく倍ブロック長ハッシュ関数

[補題 3] 並列型 DM に基づく倍ブロック長ハッシュ関数の圧縮関数を f とする．f の U と L とがともに表 1 の Preneel, Govaerts, Vandewalle モデルにおける安全な圧縮関数の行列であるならば，任意の $1 \leq q \leq 2^{n-1}$ について，

$$\mathbf{Adv}_f^{\mathrm{comp}}(q) \leq q(q+1)/2^{2n-1}$$

である． ◊

証明）$\mathcal{A}$ を $e_U^{\pm 1}$ と $e_L^{\pm 1}$ とをオラクルとする f の無衝突性に関する攻撃アルゴリズムとする．また，$e_U^{\pm 1}$，$e_L^{\pm 1}$ それぞれへの $\mathcal{A}$ の問合わせ回数を q とする．

U と L とがともに Preneel, Govaerts, Vandewalle モデルにおける安全な圧縮関数の行列であるなら，表 1 より，U，L それぞれについて，第 3 行を除いて得られる 2×2 行列は正則であるから，補題 2 より，(k_{U1}, k_{U2}, x_U) と (k_{L1}, k_{L2}, x_L) との対応が 1 対 1 であることがわかる．したがって，$\mathcal{A}$ がまず e_U または e_U^{-1} どちらか一方のオラクルへの問合わせを決めて，それに対する返答により，e_U の入出力 $(k_{U1}, k_{U2}, x_U, y_U)$ が定まると，それに対応して (k_{L1}, k_{L2}, x_L) が一意に定まる．まず e_L または e_L^{-1} どちらか一方のオラクルへの問合わせを決めた場合も同様である．

f の入出力を定めるためには，$e_U^{\pm 1}$ と $e_L^{\pm 1}$ に対して，それぞれ 1 回ずつの問合わせが必要であるが，上の事実より，これらの問合わせと返答の組は 1 対 1 に対応することが分かる．

以上のことから，$\mathcal{A}$ は，一方のオラクルへの問合わせに対して返答が得られると直ちに，もう一方のオラクルに，それと対応する問合わせを行うものと仮定する．

以下では，

$$U = L = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}$$

の場合について証明する．その他の場合についても同様に証明できる．任意の $1 \leq i \leq q$ について，C_i を以下の事象とする．

$$(x_{Ui} \oplus y_{Ui} = h_0 \wedge x_{Li} \oplus y_{Li} = g_0) \vee \exists j < i\,(x_{Ui} \oplus y_{Ui} = x_{Uj} \oplus y_{Uj} \wedge x_{Li} \oplus y_{Li} = x_{Lj} \oplus y_{Lj})$$

このとき，

$$\Pr[\mathsf{C}_i] \leq \frac{i}{(2^n - (i-1))^2}$$

したがって，$q \leqq 2^{n-1}$ のとき，

$$\begin{aligned}\mathbf{Adv}_f^{\mathrm{comp}}(\mathcal{A}) &\leqq \Pr[\mathsf{C}_1 \vee \cdots \vee \mathsf{C}_q] \\ &\leqq \sum_{i=1}^{q} \Pr[\mathsf{C}_i] \\ &\leqq \sum_{i=1}^{q} \frac{i}{(2^n-(i-1))^2} \\ &\leqq \sum_{i=1}^{q} \frac{i}{(2^n-2^{n-1})^2} = \frac{q(q+1)}{2^{2n-1}}\end{aligned}$$

以上より，

$$\mathbf{Adv}_f^{\mathrm{comp}}(q) \leqq q(q+1)/2^{2n-1}$$

である． □

補題 1，3 より，直ちに以下の定理が成立することが分かる．

［定理 1］ 並列型 DM に基づく倍ブロック長ハッシュ関数を H とする．H の圧縮関数 f の U と L とがともに Preneel, Govaerts, Vandewalle モデルにおける安全な圧縮関数の行列であるならば，任意の $1 \leqq q \leqq 2^{n-1}$ について，

$$\mathbf{Adv}_H^{\mathrm{coll}}(q) \leqq q(q+1)/2^{2n-1}$$

である． ◊

この定理より，成功確率が定数であるためには，$q = \Omega(2^n)$ となることが導かれる．

3.2 直列型 DM に基づく安全な倍ブロック長ハッシュ関数

本節では，図 4 のような型の圧縮関数をもつ倍ブロック長ハッシュ関数を考える．より正確には，

$$\begin{cases} h_i = e_U((k_{U1}, k_{U2}), x_U) \oplus z_U \\ g_i = e_L((k_{L1}, k_{L2}), x_L) \oplus z_L \end{cases}$$

ここで

$$k_{U1} = g_{i-1}, \quad \begin{pmatrix} k_{U2} \\ x_U \\ z_U \end{pmatrix} = U \begin{pmatrix} h_{i-1} \\ m_i \end{pmatrix}$$

$$k_{L1} = e_U(k_{U1}, k_{U2}, x_U), \quad \begin{pmatrix} k_{L2} \\ x_L \\ z_L \end{pmatrix} = L \begin{pmatrix} g_{i-1} \\ m_i \end{pmatrix}$$

U と L とはともに 3×2 の $\{0,1\}$ 行列である．本稿ではこのような圧縮関数をもつハッシュ関数を直列型 DM に基づく倍ブロック長ハッシュ関数と呼ぶ．

［補題 4］ 直列型 DM に基づく任意の倍ブロック長ハッシュ関数について，U_{12} と L_{12} とはそれぞれ，U と L とから第 3 行を除いた 2×2 部分行列を表すものとする．U_{12} と L_{12} とがともに正則であり，かつ，U_{12}^{-1} の第 2 行第 2 列が 0 であれば，(k_{U1}, k_{U2}, x_U) と (k_{L1}, k_{L2}, x_L) との対応は 1 対 1 である． ◊

証明）

$$U_{12}{}^{-1} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \quad L_{12} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

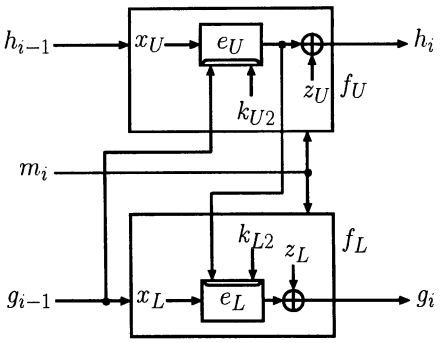

図 4 直列型 DM に基づく倍ブロック長ハッシュ関数

と記すと，

$$\begin{pmatrix} k_{L2} \\ x_L \end{pmatrix} = L_{12} \begin{pmatrix} k_{U1} \\ \gamma k_{U2} \oplus \delta x_U \end{pmatrix} = \begin{pmatrix} a & b\gamma & b\delta \\ c & d\gamma & d\delta \end{pmatrix} \begin{pmatrix} k_{U1} \\ k_{U2} \\ x_U \end{pmatrix}$$

$(k_{U1}, k_{U2}, x_U) \neq (k'_{U1}, k'_{U2}, x'_U)$ とし，それぞれに $(k_{L1}, k_{L2}, x_L), (k'_{L1}, k'_{L2}, x'_L)$ が対応するものとする．

(i) $b = 0$ のとき，$a = d = 1$ より，

$$\begin{pmatrix} k_{L2} \\ x_L \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ c & \gamma & \delta \end{pmatrix} \begin{pmatrix} k_{U1} \\ k_{U2} \\ x_U \end{pmatrix}.$$

したがって，$k_{U1} \neq k'_{U1}$ のとき，$k_{L2} \neq k'_{L2}$．$k_{U1} = k'_{U1}$ かつ $k_{U2} \neq k'_{U2}$ のとき，$\delta = 0$ ならば，$x_L \neq x'_L$．$k_{U1} = k'_{U1}$ かつ $k_{U2} = k'_{U2}$ かつ $x_U \neq x'_U$ のとき，$k_{L1} \neq k'_{L1}$．

以上より，$\delta = 0$ ならば，$(k_{L1}, k_{L2}, x_L) \neq (k'_{L1}, k'_{L2}, x'_L)$ が成立する．

(ii) $d = 0$ のとき，$b = c = 1$ より，

$$\begin{pmatrix} k_{L2} \\ x_L \end{pmatrix} = \begin{pmatrix} a & \gamma & \delta \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} k_{U1} \\ k_{U2} \\ x_U \end{pmatrix}.$$

この場合も，$\delta = 0$ ならば，$(k_{L1}, k_{L2}, x_L) \neq (k'_{L1}, k'_{L2}, x'_L)$ が成立する．

(iii) $b = d = 1$ のとき，

$$\begin{pmatrix} k_{L2} \\ x_L \end{pmatrix} = \begin{pmatrix} a & \gamma & \delta \\ c & \gamma & \delta \end{pmatrix} \begin{pmatrix} k_{U1} \\ k_{U2} \\ x_U \end{pmatrix}$$

で，a, c の一方が 1，他方が 0 である．この場合も，$\delta = 0$ ならば，$(k_{L1}, k_{L2}, x_L) \neq (k'_{L1}, k'_{L2}, x'_L)$ が成立する． □

補題 4 より，前節と同様にして，以下の定理が証明できる．

［定理 2］ 直列型 DM に基づく倍ブロック長ハッシュ関数を H とする．H の圧縮関数 f の U と L とがともに Preneel, Govaerts, Vandewalle モデルにおける安全な圧縮関数の行列であり，かつ，U_{12}^{-1} の第 2 行第 2 列が 0 ならば，任意の $1 \leqq q \leqq 2^{n-1}$ について，

$$\mathbf{Adv}_H^{\mathrm{coll}}(q) \leqq q(q+1)/2^{2n-1}$$

である． ◊

表 1　Preneel, Govaerts, Vandewalle のモデルにおける安全な圧縮関数

圧縮関数	行列	圧縮関数	行列	圧縮関数	行列
$e(h_{i-1},m_i)\oplus m_i$	$\begin{pmatrix}1&0\\0&1\\0&1\end{pmatrix}$	$e(m_i,h_{i-1})\oplus h_i$	$\begin{pmatrix}0&1\\1&0\\1&0\end{pmatrix}$	$e(w_i,m_i)\oplus m_i$	$\begin{pmatrix}1&1\\0&1\\0&1\end{pmatrix}$
$e(h_{i-1},w_i)\oplus w_i$	$\begin{pmatrix}1&0\\1&1\\1&1\end{pmatrix}$	$e(m_i,w_i)\oplus w_i$	$\begin{pmatrix}0&1\\1&1\\1&1\end{pmatrix}$	$e(w_i,h_{i-1})\oplus h_{i-1}$	$\begin{pmatrix}1&1\\1&0\\1&0\end{pmatrix}$
$e(h_{i-1},m_i)\oplus w_i$	$\begin{pmatrix}1&0\\0&1\\1&1\end{pmatrix}$	$e(m_i,h_i)\oplus w_i$	$\begin{pmatrix}0&1\\1&0\\1&1\end{pmatrix}$	$e(w_i,m_i)\oplus h_{i-1}$	$\begin{pmatrix}1&1\\0&1\\1&0\end{pmatrix}$
$e(h_{i-1},w_i)\oplus m_i$	$\begin{pmatrix}1&0\\1&1\\0&1\end{pmatrix}$	$e(m_i,w_i)\oplus h_{i-1}$	$\begin{pmatrix}0&1\\1&1\\1&0\end{pmatrix}$	$e(w_i,h_{i-1})\oplus m_i$	$\begin{pmatrix}1&1\\1&0\\0&1\end{pmatrix}$

$w_i = h_{i-1}\oplus m_i$ であり，各行列 C は，$e(k,x)\oplus z$ なる k,x,z について，以下を満たすように定められている．

$$\begin{pmatrix}k\\x\\z\end{pmatrix} = C\begin{pmatrix}h_{i-1}\\m_i\end{pmatrix}$$

4. 考　　察

前章では，並列型あるいは直列型 DM に基づく真に安全な倍ブロック長ハッシュ関数の構成を示した．なお，処理効率の観点からは，並列型 DM に基づく倍ブロック長ハッシュ関数の方がすぐれている．

前章で示した倍ブロック長ハッシュ関数は，2 種類のブロック暗号を用いる点で，従来と大きく異なる．

Hattori, Hirose, Yoshida [2] の定理 1 では，$(n,2n)$ ブロック暗号を利用したレート 1 の倍ブロック長ハッシュ関数の圧縮関数について，無衝突性に対する攻撃の時間計算量が高々$O(2^{n/2})$であることが示されている．なお，この証明から，その定理の対象である圧縮関数については，仮に本稿のハッシュ関数と同様に 2 種類のブロック暗号を利用しても，無衝突性に対する攻撃の時間計算量は同じく $O(2^{n/2})$ であることが分かる．なお，この定理の対象である圧縮関数は以下の通りである．この圧縮関数は並列型であるが，直列型についても同様に上記のことが言える．

$$\begin{cases} h_i = f_U(h_{i-1},g_{i-1},m_i^1,m_i^2)\\ g_i = f_L(h_{i-1},g_{i-1},m_i^1,m_i^2)\end{cases}$$

について，

$$\begin{cases} h_i = e((k_{U1},k_{U2}),x_U)\oplus z_U\\ g_i = e((k_{L1},k_{L2}),x_L)\oplus z_L\end{cases}$$

であり，$k_{U1},k_{U2},x_U,z_U,k_{L1},k_{L2},x_L,z_L$ はすべて，$h_{i-1},g_{i-1},m_i^1,m_i^2\in\{0,1\}^n$ の線形結合で表される．

5. む　す　び

本稿では，並列型・直列型 DM に基づく倍ブロック長ハッシュ関数の構成を提案した．さらに，真にランダムなブロック暗号を仮定して，その無衝突性に関する安全性を証明した．今後は一方向性に関する安全性の解析を行い，その結果を含めて論文をまとめる予定である．

本研究に関する未解決問題は，1 種類のみのブロック暗号を利用したレート 1 あるいは 1/2 の安全な倍ブロック長ハッシュ関数が存在するか否かである．

文　　献

[1] J. Black, P. Rogaway, and T. Shrimpton. Black-box analysis of the block-cipher-based hash-function constructions from PGV. In *CRYPTO 2002 Proceedings*, pages 320–335, 2002. Lecture Notes in Computer Science 2442.

[2] M. Hattori, S. Hirose, and S. Yoshida. Analysis of double block length hash functions. In *9th IMA International Conference on Cryptography and Coding*, pages 290–302, 2003. Lecture Notes in Computer Science 2898.

[3] W. Hohl, X. Lai, T. Meier, and C. Waldvogel. Security of iterated hash functions based on block ciphers. In *CRYPTO'93 Proceedings*, pages 379–390, 1994. Lecture Notes in Computer Science 773.

[4] L. R. Knudsen, X. Lai, and B. Preneel. Attacks on fast double block length hash functions. *Journal of Cryptology*, 11(1):59–72, 1998.

[5] X. Lai and J. L. Massey. Hash function based on block ciphers. In *EUROCRYPT'92*, pages 55–70, 1993. Lecture Notes in Computer Science 658.

[6] M. Liskov, R. L. Rivest, and D. Wagner. Tweakable block ciphers. In *CRYPT 2002 Proceedings*, pages 31–46, 2002. Lecture Notes in Computer Science 2442.

[7] B. Preneel, R. Govaerts, and J. Vandewalle. Hash functions based on block ciphers: A synthetic approach. In *CRYPTO'93 Proceedings*, pages 368–378, 1994. Lecture Notes in Computer Science 773.

[8] T. Satoh, M. Haga, and K. Kurosawa. Towards secure and fast hash functions. *IEICE Transactions on Fundamentals*, E82-A(1):55–62, 1999.

[9] R. S. Winternitz. A secure one-way hash function built from DES. In *IEEE Symposium on Security and Privacy*, pages 88–90, 1984.