ハッシュ関数の標準化と最新動向

廣瀬勝一

福井大学工学研究科電気・電子工学専攻

2008 年 12 月 19 日

暗号ハッシュ関数 (Cryptographic Hash Function)

$H : \{0,1\}^* \to \{0,1\}^n$　　任意長入力，固定長出力の関数

性質

原像計算困難性 (preimage resistance, PR)

与えられた出力 h について，$H(M) = h$ を満たす M を計算するのが困難

第二原像計算困難性 (second-preimage resistance, 2ndPR)

与えられた入力 M について，$H(M) = H(M')$ かつ $M \neq M'$ を満たす M' を計算するのが困難

衝突計算困難性 (collision resistance, CR)

$H(M) = H(M')$ を満たす相異なる M, M' を計算するのが困難

ハッシュ関数攻撃の計算量

所望の結果が得られるまで，入力を選択して出力の計算を繰返す場合

（ハッシュ関数の内部構造を一切利用しない場合）

原像計算	$O(2^n)$
第二原像計算	$O(2^n)$
衝突計算	$O(2^{n/2})$

n は出力長

誕生日のパラドクス

23 人集まれば，誕生日の同じ人が存在する確率はおよそ 1/2

どの二人の誕生日も異なる確率は

$$\frac{365-1}{365} \times \frac{365-2}{365} \times \cdots \times \frac{365-22}{365} \approx \frac{1}{2}$$

一般に

N 個の要素から無作為に 1 個を選択する試行を繰り返すと，
およそ $1.17\sqrt{N}$ 回で，

2 回以上選択される要素の存在する確率 $\approx 1/2$

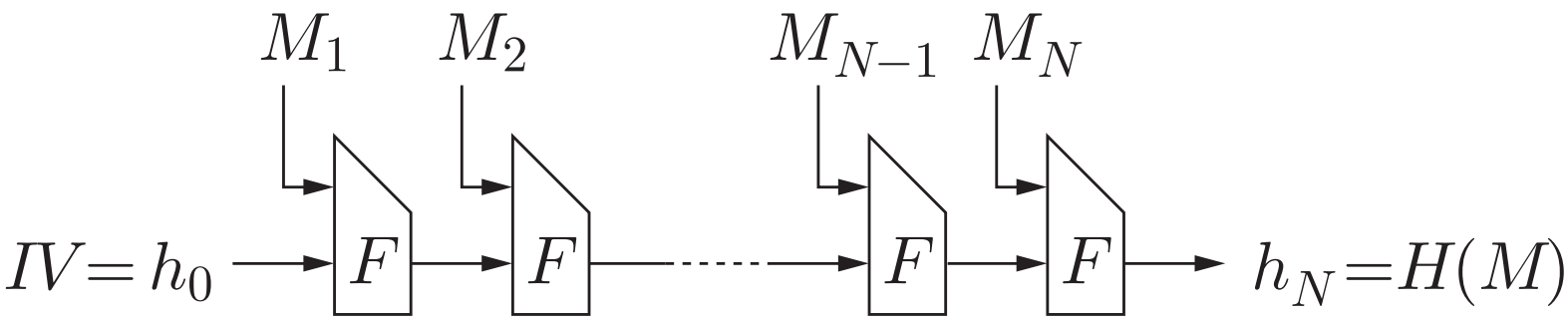
反復型ハッシュ関数

圧縮関数 $F : \{0,1\}^n \times \{0,1\}^b \to \{0,1\}^n$

初期値 $IV \in \{0,1\}^n$

パディング 入力を b の倍数の長さの系列に変換する処理

入力 M のパディング後の系列 $(M_1, M_2, \ldots, M_N)$ について



パディング

入力 $M = (M_1, M_2, \ldots, M_N)$

- $|M_i| = b$ $(i = 1, 2, \ldots, N-1)$
- $1 \leq |M_N| \leq b$

曖昧さのない簡易な方法

M_1	$\cdots$	M_{N-1}	$M_N 10 \cdots 0$

MD 強化法 (MD-strengthening, by Merkle & Damgård)

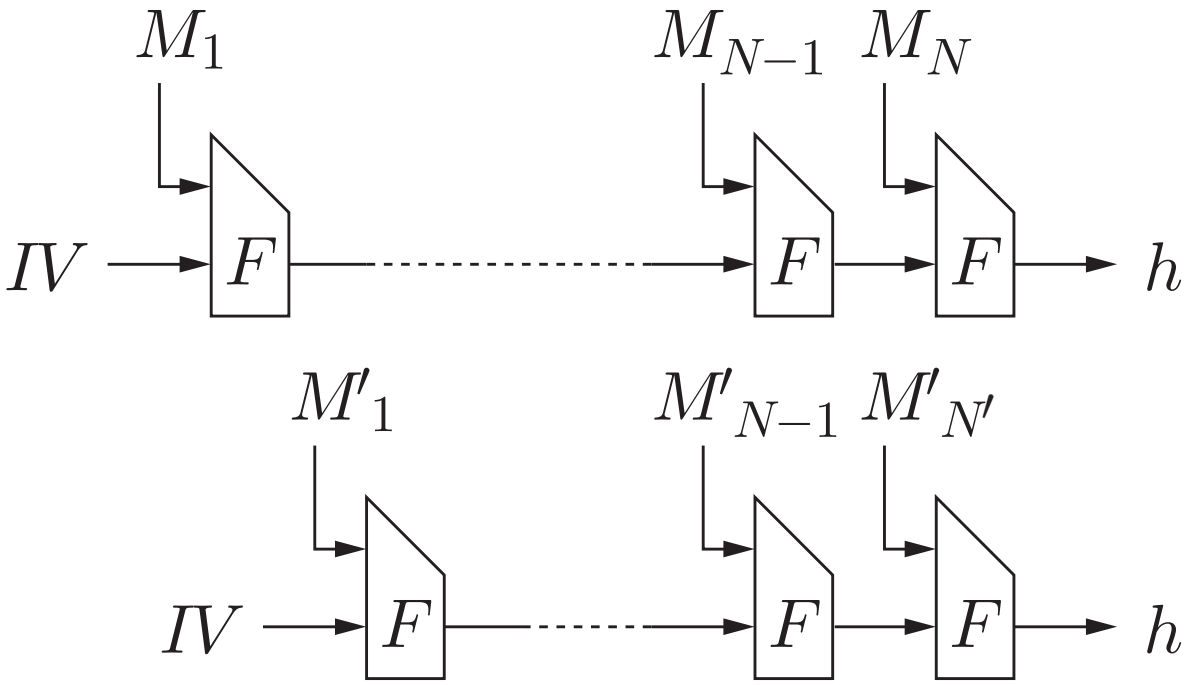
M_1	$\cdots$	M_{N-1}	$M_N 00 \cdots 0$	$\|M\|$

通常，MD 強化法に基づく方法が利用されている．

反復型ハッシュ関数の衝突計算困難性

定理 (Merkle, Damgård 89)

圧縮関数 F が CR $\Rightarrow$ ハッシュ関数 H が CR



ハッシュ関数に衝突が見つかれば，圧縮関数にも衝突が見つかる．

圧縮関数の構成法

- ブロック暗号を用いた構成法 (1990 年半ば以前)
  - 単ブロック長 (出力長＝ブロック長)
    Davies-Meyer, Matyas-Meyer-Oseas, Miyaguchi-Preneel
  - 倍ブロック長 (出力長＝ 2 ×ブロック長)
    MDC-2, MDC-4, abreast/tandem Davies-Meyer
- 専用構成法 (1990 年以降)
  - MDx 族
    MD4, MD5, RIPEMD-160, HAVAL,
    SHA-1, SHA-224/256/384/512
  - Whirlpool
  - ···

Secure Hash Standard (SHS) の変遷

FIPS 180 (Federal Information Processing Standards) (1993 年 5 月)

- SHA (Secure Hash Algorithm, SHA-0 とも呼ばれる)

FIPS 180-1 (1995 年 4 月)

- SHA-1 (メッセージ拡大に 1 ビット左巡回シフトを付加)

FIPS 180-2 (2002 年 8 月)

- SHA-1, SHA-256/384/512

FIPS 180-2, Change Notice (2004 年 2 月)

- SHA-224

FIPS 180-3 (2008 年 10 月)

- SHA-1, SHA-224/256/384/512

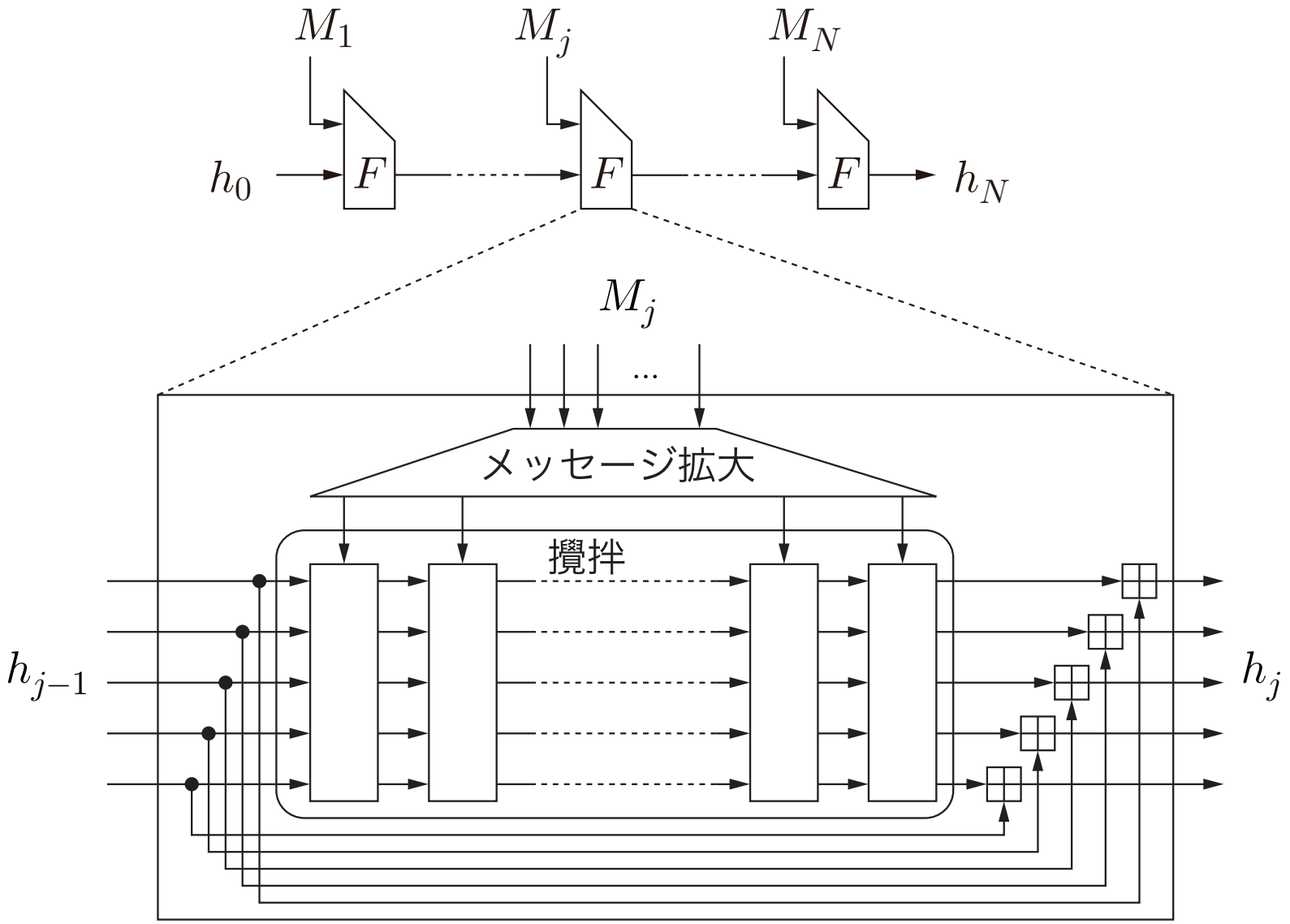
Secure Hash Standard (SHS)

アルゴリズム	入力長	ブロック長	ワード長	出力長
SHA-1	$< 2^{64}$	512	32	160
SHA-224	$< 2^{64}$	512	32	224
SHA-256	$< 2^{64}$	512	32	256
SHA-384	$< 2^{128}$	1024	64	384
SHA-512	$< 2^{128}$	1024	64	512

長さの単位はビット．ブロック長は圧縮関数のメッセージブロック長.

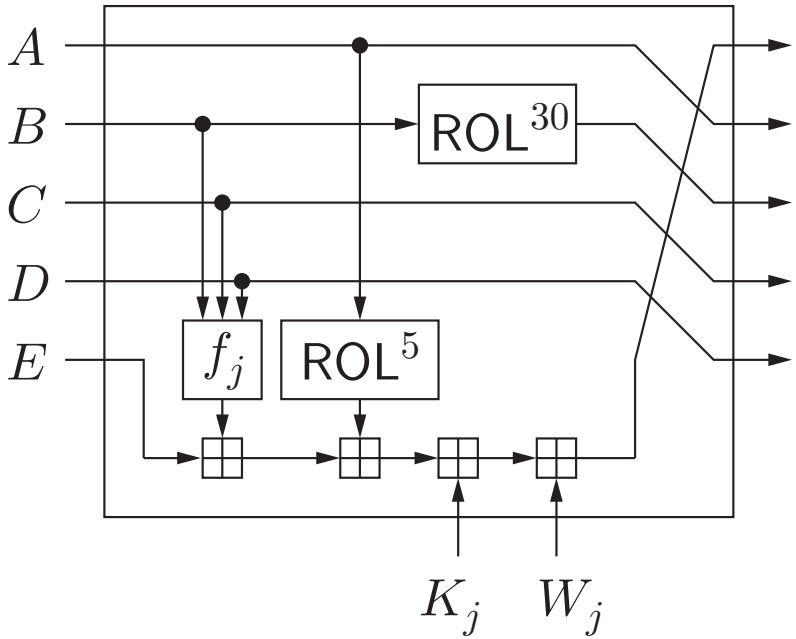
- SHA-256 と SHA-224 の相違は，初期値と出力の切り捨てのみ.
- SHA-512 と SHA-384 の相違も同様.

MDx 族の圧縮関数の概略

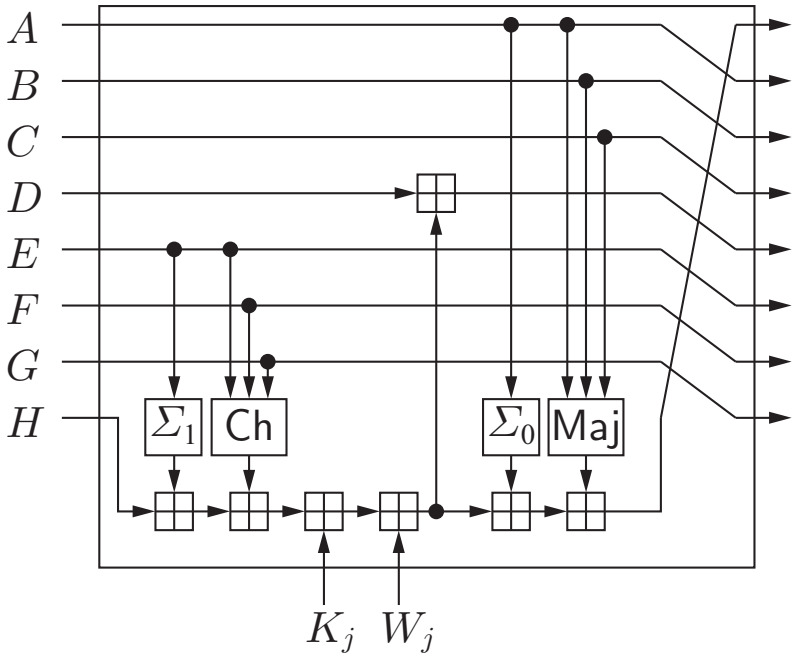


圧縮関数の攪拌部

SHA-1 (80 段)



SHA-256 (64 段)



K_j は定数

f_j は 20 段ごとに，Ch, Parity, Maj, Parity

$$\Sigma_0(x) = \mathsf{ROR}^2(x) \oplus \mathsf{ROR}^{13}(x) \oplus \mathsf{ROR}^{22}(x)$$

$$\Sigma_1(x) = \mathsf{ROR}^6(x) \oplus \mathsf{ROR}^{11}(x) \oplus \mathsf{ROR}^{25}(x)$$

SHA-1 圧縮関数の攪拌部

$$f_j(u,v,w) = \begin{cases} \mathsf{Ch}(u,v,w) = u\,v \vee \overline{u}\,w & (0 \le j \le 19) \\ \mathsf{Parity}(u,v,w) = u \oplus v \oplus w & (20 \le j \le 39) \\ \mathsf{Maj}(u,v,w) = u\,v \vee u\,w \vee v\,w & (40 \le j \le 59) \\ \mathsf{Parity}(u,v,w) & (60 \le j \le 79) \end{cases}$$

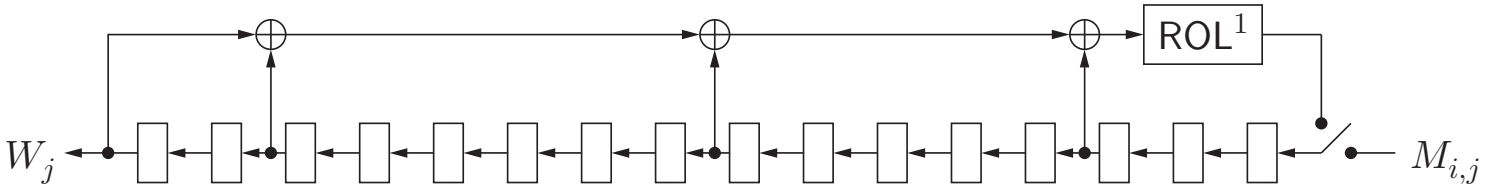
f_j はビットごとの演算

圧縮関数のメッセージ拡大

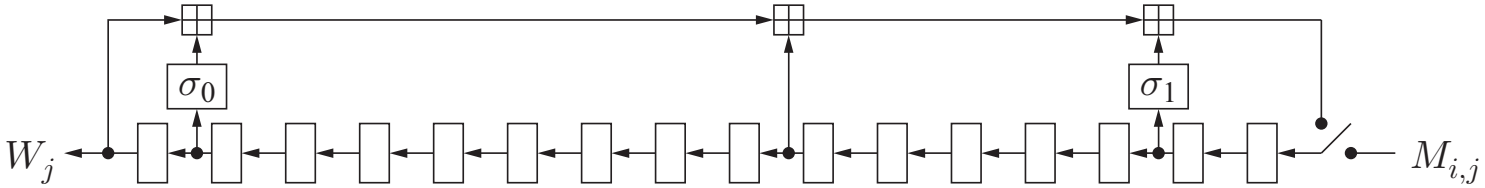
入力 $M_i = (M_{i,0}, M_{i,1}, \ldots, M_{i,15})$, $M_{i,j} \in \{0,1\}^{32}$

$$(W_0, W_1, \ldots, W_r) \leftarrow (M_{i,0}, M_{i,1}, \ldots, M_{i,15}) \quad W_j \in \{0,1\}^{32}$$

SHA-1



SHA-256



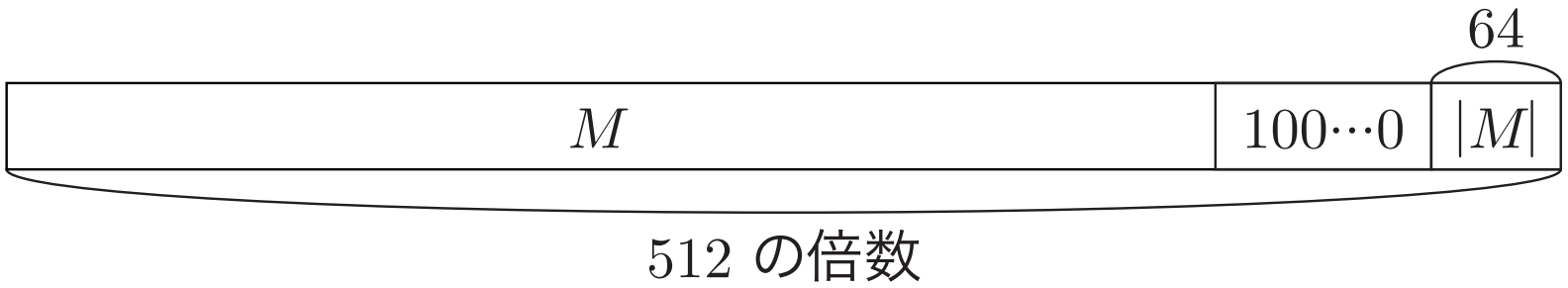
$$\sigma_0(x) = \mathsf{ROR}^7(x) \oplus \mathsf{ROR}^{18}(x) \oplus \mathsf{SHR}^3(x)$$

$$\sigma_1(x) = \mathsf{ROR}^{17}(x) \oplus \mathsf{ROR}^{19}(x) \oplus \mathsf{SHR}^{10}(x)$$

パディング

入力 M のパディング

1. $z = M \| 10^r$ とする.
   r は $|M| + 1 + r + 64$ が 512 の倍数となる最小の非負整数.
2. $z = z \| \alpha$ とする.
   α は $|M|$ の 2 進数表現で $|\alpha| = 64$.



MDx 族ハッシュ関数に対する強力な衝突攻撃

ハッシュ関数 H に対する衝突攻撃

$H(M) = H(M')$ を満たす相異なる M, M' を得ようとする攻撃

- Dobbertin (1996)

  MD4, MD5

- Chabaud & Joux (1998)

  SHA-0

- Wang, et. al. (1997, 1998, 2004–)

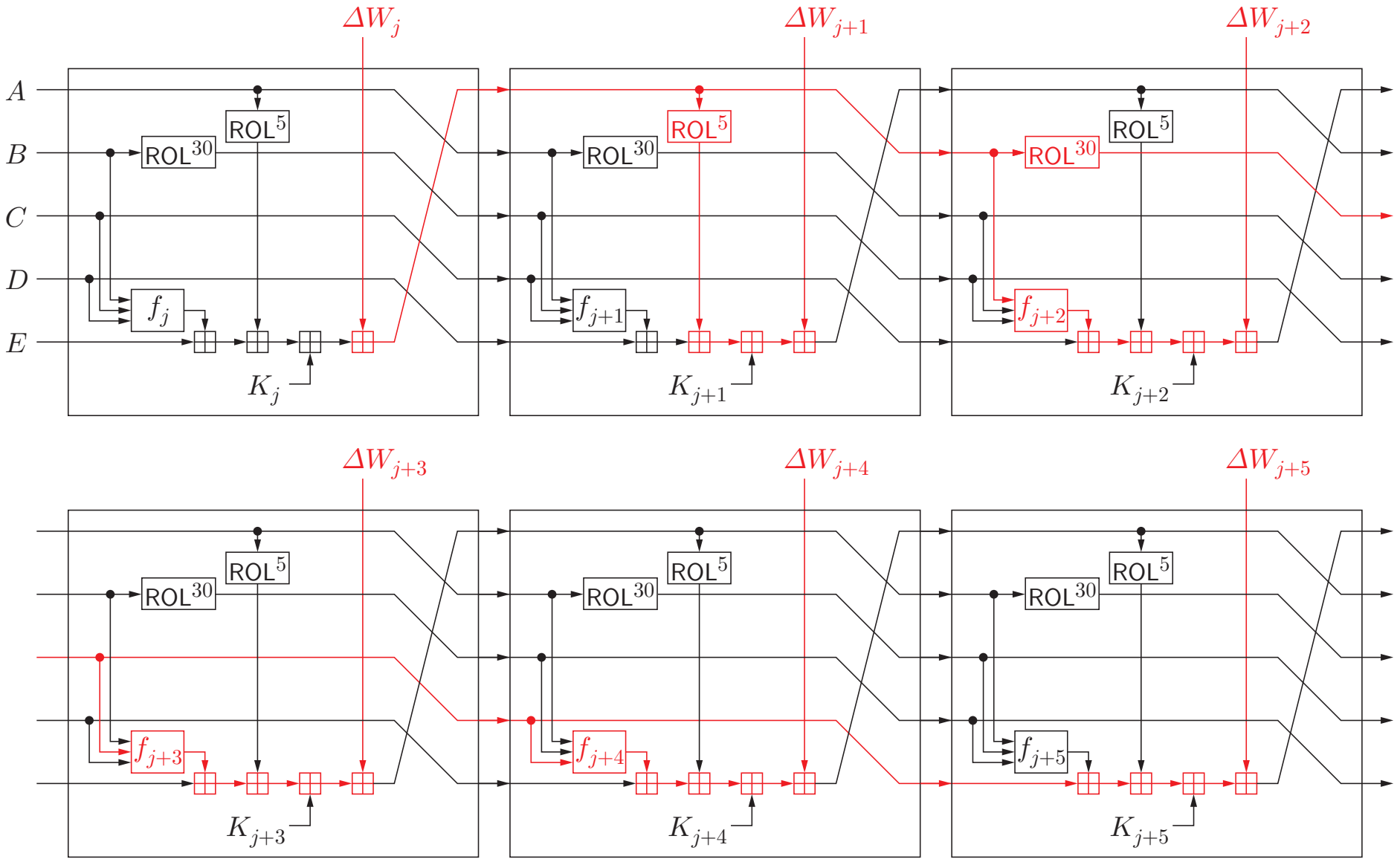
  MD4, MD5, HAVAL, SHA-0, SHA-1 など

衝突攻撃の計算量 (単位は圧縮関数の計算回数)

MD4	手計算でも可能
MD5	$\lesssim 2^{30}$
SHA-0	$\lesssim 2^{33}$
SHA-1	$\lesssim 2^{63}$ ← 衝突はまだ得られていない.

RIPEMD-160, SHA-224/256/384/512 に対して有効な攻撃法は発見されていない.

SHA-0/1 の局所衝突


ΔW_j
ΔW_{j+1}
ΔW_{j+2}
A
B
C
D
E
ROL^{30}
ROL^{5}
f_j
f_{j+1}
f_{j+2}
K_j
K_{j+1}
K_{j+2}
ΔW_{j+3}
ΔW_{j+4}
ΔW_{j+5}
f_{j+3}
f_{j+4}
f_{j+5}
K_{j+3}
K_{j+4}
K_{j+5}

SHA-0/1 の局所衝突を利用した衝突攻撃

j 段目の差分の影響は後続の 5 段で解消できる．ただし，

- 各 W_j に独立かつ任意に差分を設定することは不可能
  - メッセージ拡大による依存関係が存在.
- いつも同じパタンで解消できるとは限らない.
  - f_j の非線形性．f_j が 20 段ごとに変わる.
  - 加算の桁上げ

Wang の着想

- 初めの方の差分の影響は，メッセージをうまく選んで確実に解消
  - 80 段のうち 16 段の入力は自由に選択できる.
- 残りの差分の影響は，メッセージの残りの自由度で確率的に解消

SHS の現状

NIST のコメント

衝突計算困難性を要求する応用に関して

- SHA-2 (SHA-224/256/384/512) への早急な移行を推奨.
- 米国政府機関に対し，2010 年末までの SHA-1 の使用停止を勧告.

SHA-2 の問題点

- どのような基準に基づいて設計されたか明らかにされていない.

NIST Cryptographic Hash Algorithm Competition

- 公募要項案に対するコメントの募集 (2007 年 1 月 23 日)
- 公募開始 (2007 年 11 月 2 日)
- 締切 (2008 年 10 月 31 日)
- 応募総数 64 件.
- 51 件が Round 1 候補として公開された. (2008 年 12 月 10 日)

The SHA-3 Zoo

- 応募アルゴリズムに関する ECRYPT の web ページ
- 2008 年 12 月 12 日現在
  - 64 件中 55 件が公開されている.
  - 9 件が破られたとの報告 (内 6 件が Round 1 候補)

NIST Hash Competition: 最小必須要件

- 特許権，知的財産権等の制約なく利用可能であること．
- 多様なハードウェア・ソフトウェアで実装可能であること．
- 入出力長について以下の要件を満たすこと．
  - 出力長：224, 256, 384, 512 ビットのサポート
  - 最小入力長 $\geq 2^{64} - 1$

NIST Hash Competition: 安全性要件

必須

- 応用の安全性の保証

  ディジタル署名 (FIPS 186-2), 鍵導出 (NIST SP 800-56A), HMAC (FIPS 198), DRBG (NIST SP 800-90), ...
- ランダム化ハッシュモードの安全性
- 衝突計算困難性，(第二) 原像計算困難性
- Length-extension 攻撃に対する安全性

オプション

- HMAC 以外の擬似ランダム関数モードの提供
- Joux 多衝突攻撃，Kelsey-Schneier 第二原像攻撃への対策

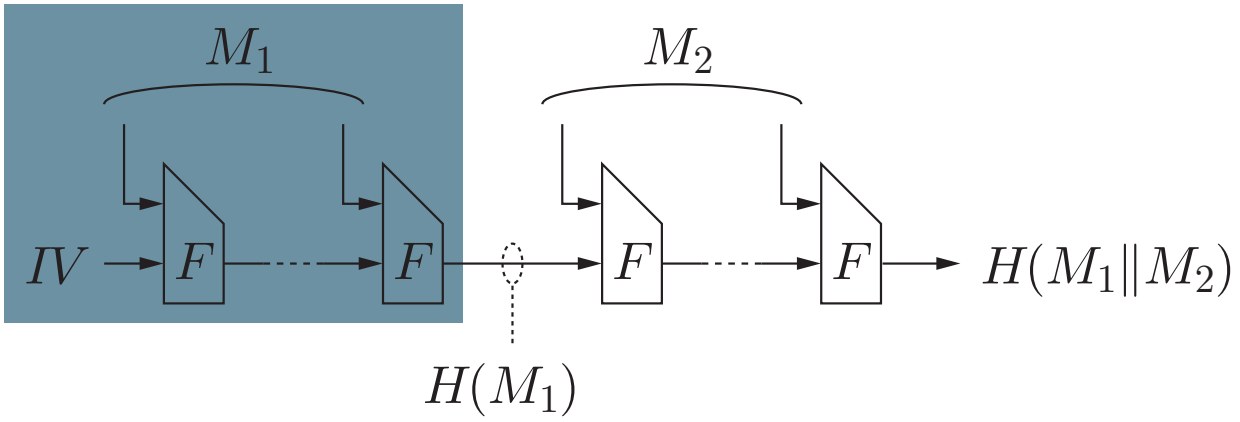
NIST Hash Competition: 安全性の定量的要件

要件	度合い
HMAC	$n/2$
ランダム化ハッシュ	$n-k$
衝突計算困難性	$n/2$
原像計算困難性	n
第二原像計算困難性	$n-k$

- 度合い s は，攻撃計算量 $\ll 2^s$ とならないことを表す.
- k は，与えられるメッセージ長が 2^k ビットであることを表す.

Length-Extension 攻撃

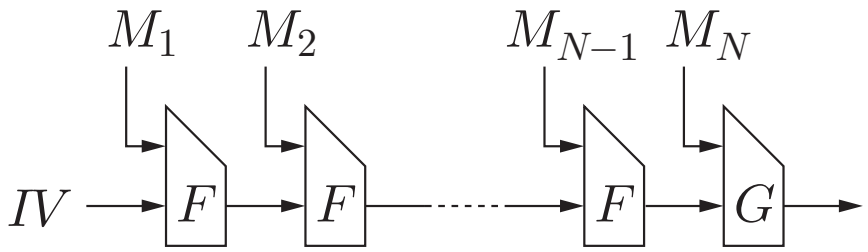
$H(M_1 \| M_2)$ は $H(M_1)$ と M_2 から計算できる．M_1 は不要．



欠点：$H_K(M) = H(K \| M)$ が擬似ランダム関数とならない．

- $H_K(M_1 \| M_2)$ が $H_K(M_1)$ と M_2 から計算できる．

対策：出力関数 $G(\neq F)$ を利用する．



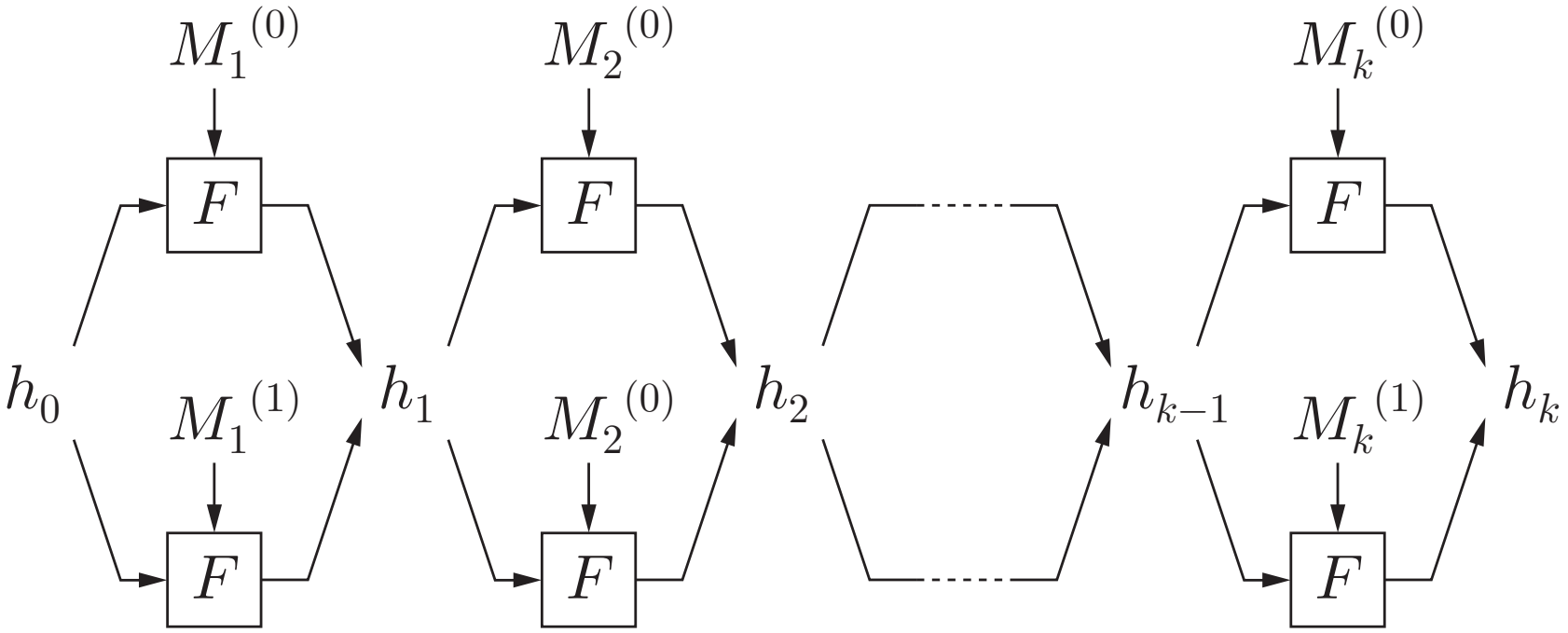
反復型ハッシュ関数の構造を利用した攻撃

- Joux の多衝突攻撃 (multi-collision attack) (2004)
- Kelsey と Schneier の第二原像攻撃 (2005)

Q 衝突攻撃 (Q-collision attack)

- 出力の等しい Q 個の相異なる入力を計算する攻撃
- 反復型構造を利用しない攻撃の計算量 $= O\left((Q!)^{\frac{1}{Q}} 2^{\frac{Q-1}{Q}n}\right)$
- Joux の攻撃の計算量 $= O\left((\log Q) 2^{\frac{n}{2}}\right)$

反復型ハッシュ関数に対する Joux の多衝突攻撃



2^k 衝突：$M_1^{(b_1)} \| M_2^{(b_2)} \| \cdots \| M_k^{(b_k)}$ に対応する出力はすべて等しい．

計算量は $\boldsymbol{O(k\, 2^{n/2})}$，$n$ はハッシュ値の長さ

Joux の多衝突攻撃の応用

H は反復型ハッシュ関数で出力長は n_1
G は任意のハッシュ関数で出力長は n_2

$H(M)||G(M)$ への衝突攻撃

1. H の $2^{n_2/2}$ 衝突を計算する．計算量は $\boldsymbol{O(n_2\, 2^{n_1/2})}$.
   H の $2^{n_2/2}$ 衝突を $C_H = \{M_1, M_2, \ldots, M_{2^{n_2/2}}\}$ とする．
2. C_H の中で G の 2 衝突を探す．計算量は $\boldsymbol{O(2^{n_2/2})}$.

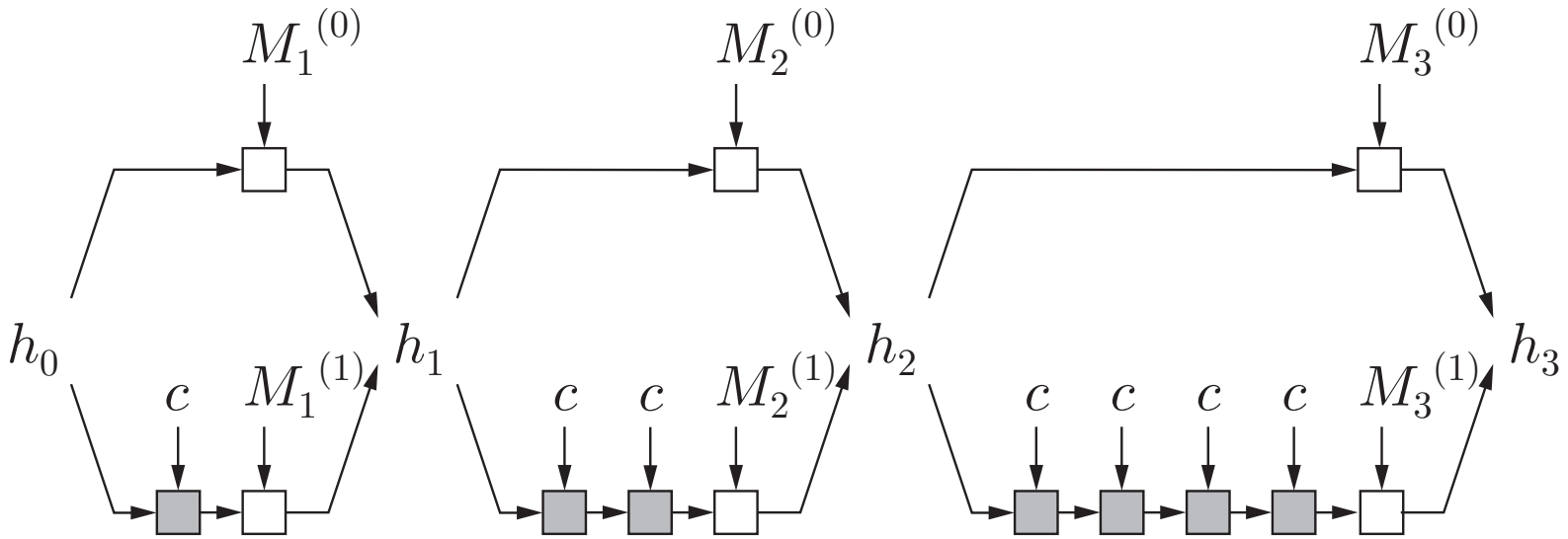
この攻撃の計算量は $\boldsymbol{O(n_2\, 2^{n_1/2} + 2^{n_2/2})}$.

（参考）$H(x)||G(x)$ への誕生日攻撃の計算量は $O(2^{(n_1+n_2)/2})$

Kelsey と Schneier の第二原像攻撃

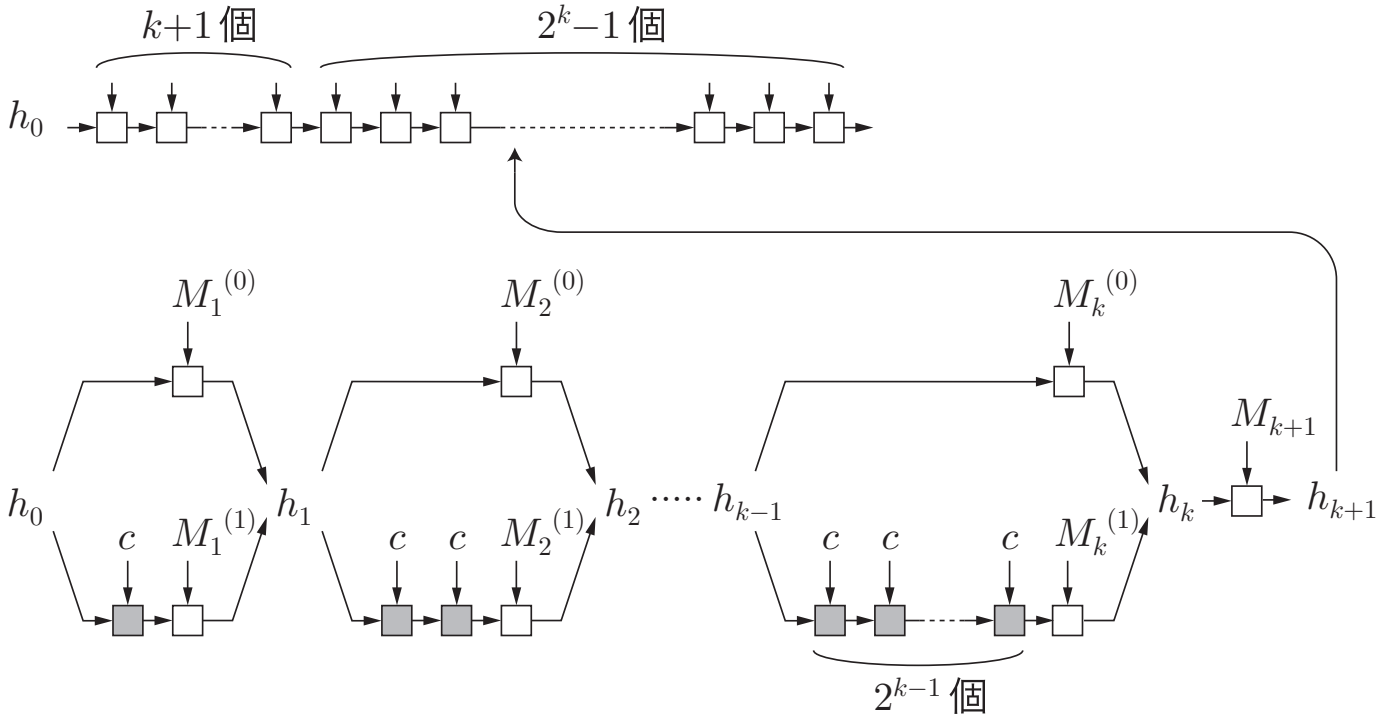
Joux の多衝突攻撃の応用

例)



- 長さが 3 から 10 $(= 3 + 2^0 + 2^1 + 2^2)$ ブロックの入力
- どの出力も h_3 で等しい

Kelsey と Schneier の第二原像攻撃



長さ $(2^k + k)$ ブロックのメッセージに対して

1. Joux の攻撃を用いて $h_1, \ldots, h_k$ を得る．計算量 $O(2^k + k\,2^{n/2})$.
2. M_{k+1} を乱択し，h_{k+1} を $2^k - 1$ 個のいずれかに一致させる．
   計算量 $O(2^{n-k})$.

反復型ハッシュ関数の構造を利用した攻撃の効果

Joux の多衝突攻撃

- 衝突攻撃が困難である限りは無効

Kelsey と Schneier の第二原像攻撃

- 計算量 $O(2^k + k\,2^{n/2} + 2^{n-k})$ で,

  $2^k \leq$ 最大メッセージブロック数

- SHS に対して

$$2^{n-k} \gtrsim \begin{cases} 2^{105} & \text{SHA-1} \\ 2^{201} & \text{SHA-224/256} \\ 2^{394} & \text{SHA-384/512} \end{cases}$$

NIST Hash Competition: 今後の予定

- The First SHA-3 Candidate Conference
  場所：K.U. Leuven, Belgium
  期間：2009 年 2 月 25 日〜28 日 (FSE 2009 の直後)
- Round 2 候補 (約 15 件) を選出 (2009 年夏)
- The Second SHA-3 Candidate Conference (2010 年 8 月)
- Round 3 候補 (finalist 約 5 件) を選出
- The Third SHA-3 Candidate Conference (2012 年第一四半期)
- winner を選出 (2012 年第二四半期)

NIST Hash Competition: 日本からの Round 1 候補

アルゴリズムと開発者 (アルファベット順)

AURORA

T. Akishita, T. Iwata, S. Moriai, K. Shibutani, T. Shirai

Lesamnta

S. Hirose, K. Ideguchi, H. Kuwakado, T. Owada, H. Yoshida

Luffa

C.D. Cannière, H. Sato, D. Watanabe

むすび

- MDx 族ハッシュ関数
  - SHS (Secure Hash Standard)
- NIST Cryptographic Hash Algorithm Competition

今回取り上げなかった話題

- NIST 以外の標準化
- ブロック暗号を利用した構成法