ハッシュ関数とその応用

廣瀬勝一

福井大学

平成 23 年度 電気関係学会 北陸支部 連合大会
(2011/9/17-18, 福井大学)

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

任意長入力，固定長出力の関数

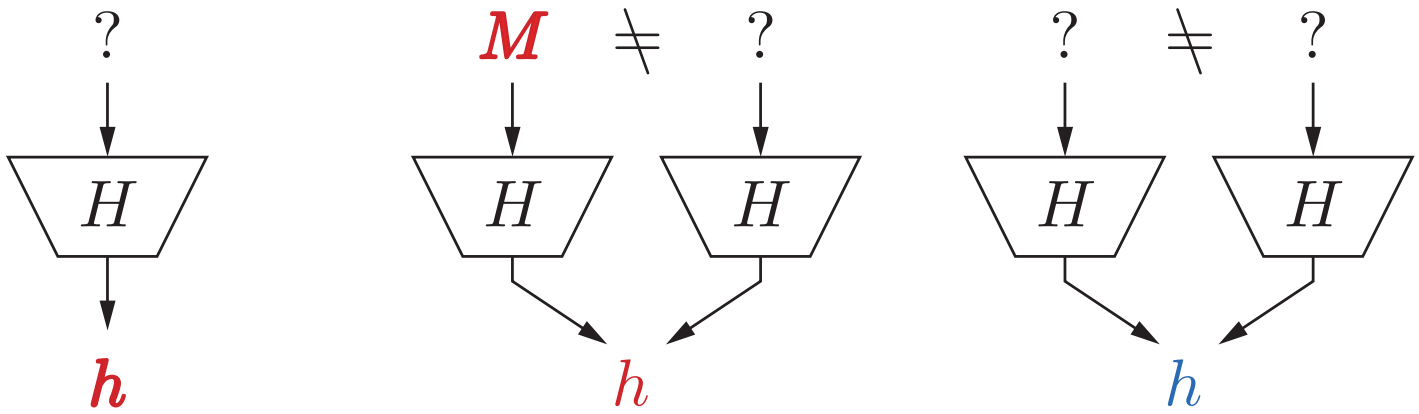
暗号プロトコルで最も良く用いられる構成要素

- ディジタル署名のためのメッセージダイジェスト
- 公開鍵暗号の平文の前処理（OAEP など）
- メッセージ認証
- ハッシュ木（ディジタル署名，時刻印サービス）
- 共通鍵暗号
- …

ハッシュ関数の性質

$H : \{0,1\}^* \to \{0,1\}^n$

原像計算困難性	第二原像計算困難性	衝突計算困難性
PR	2ndPR	CR



	PR	2ndPR	CR
攻撃計算量	$O(2^n)$	$O(2^n)$	$O(2^{n/2})$

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）

ハッシュ関数の構成

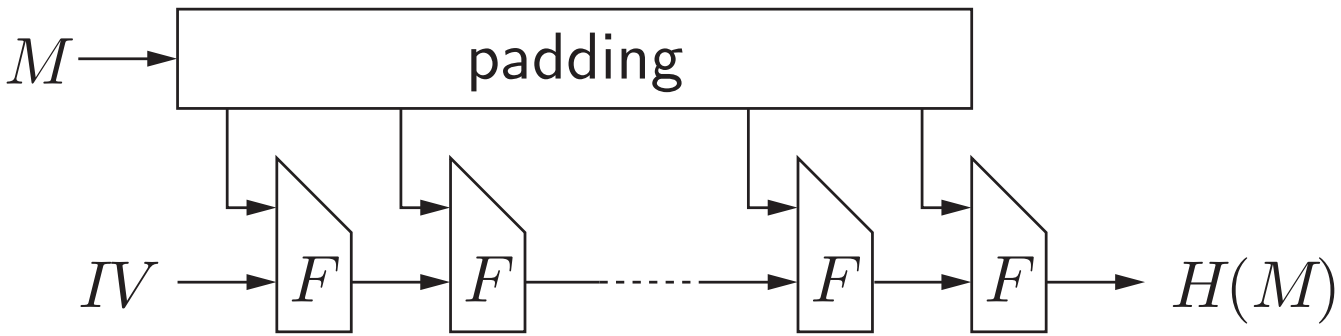
ハッシュ関数 = 圧縮関数 + 定義域拡大

圧縮関数 固定長入出力で，入力長 > 出力長

定義域拡大 圧縮関数による任意長入力の処理法

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

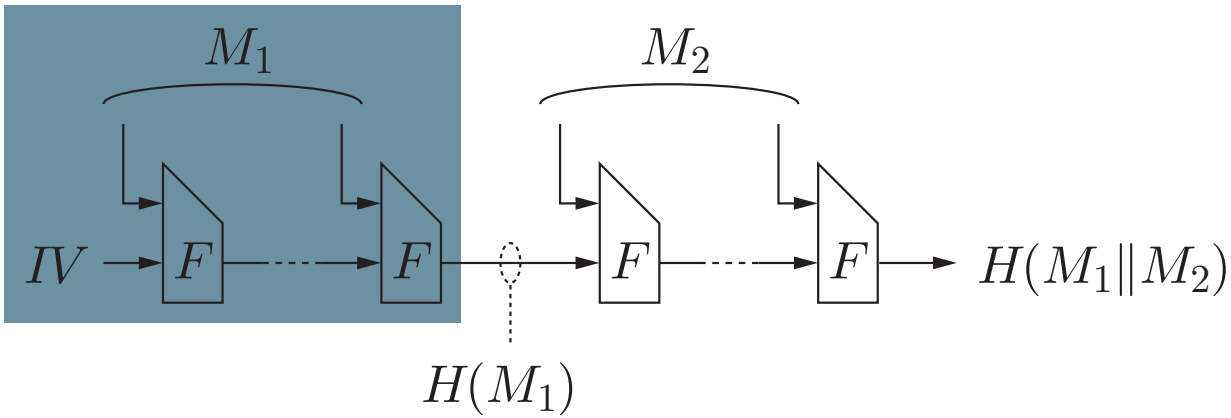


反復型ハッシュ関数

利点 圧縮関数 F が CR $\Rightarrow$ ハッシュ関数 H は CR [Damgård 89]

欠点 Length-Extension

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



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)

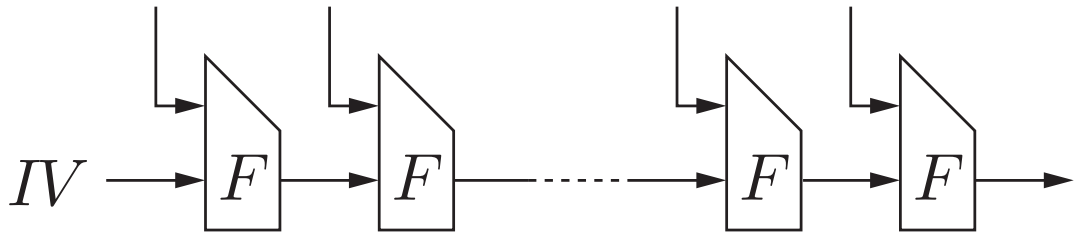
- SHA-1, SHA-224/256/384/512

Secure Hash Standard (SHS)

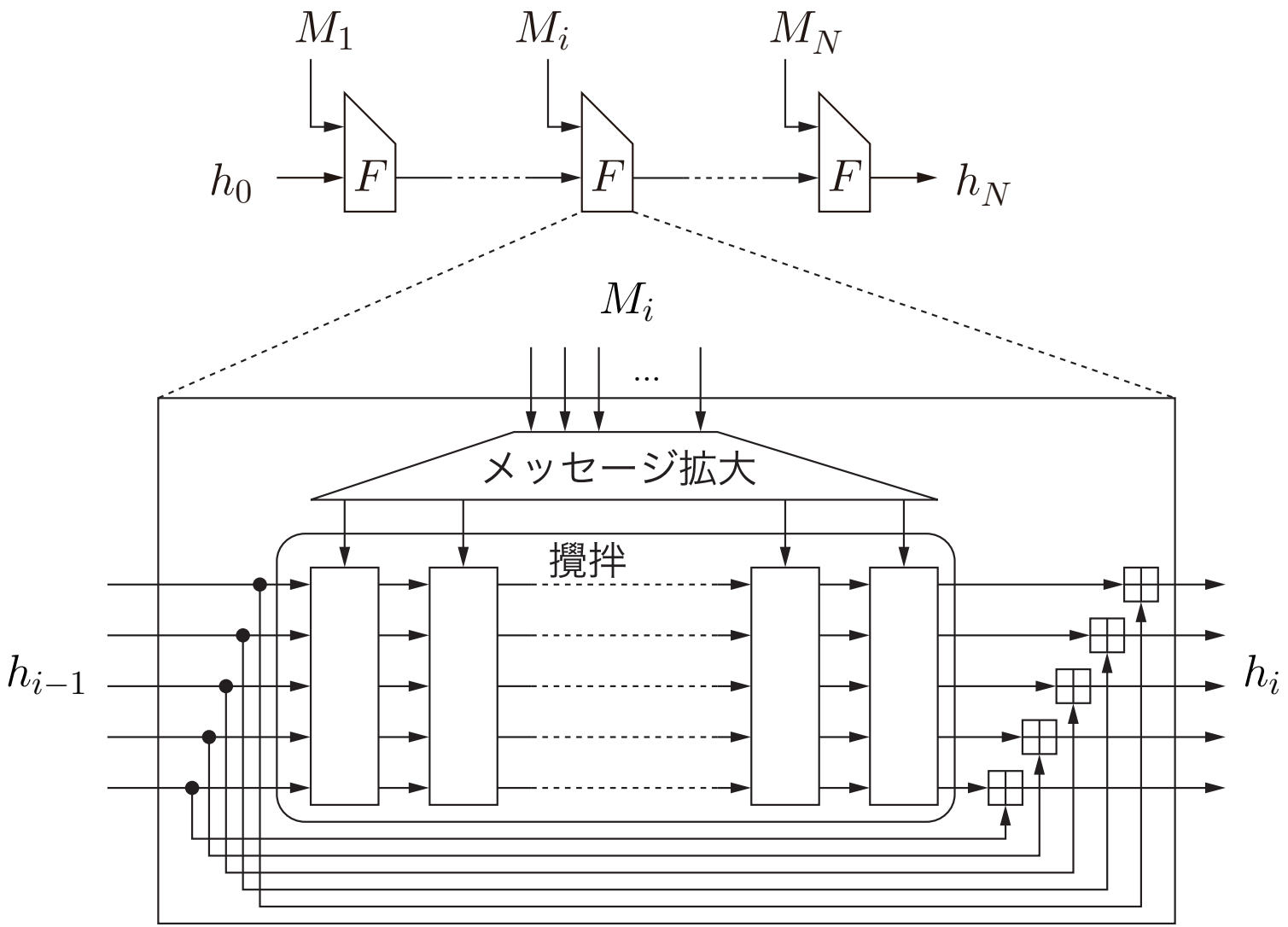
アルゴリズム	入力長	ブロック長	ワード長	出力長
SHA-1	$< 2^{64}$	512	32	160
SHA-224	$< 2^{64}$	512	32	224
SHA-256	$< 2^{64}$	512	32	256
SHA-384	$< 2^{128}$	1024	64	384
SHA-512	$< 2^{128}$	1024	64	512

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.

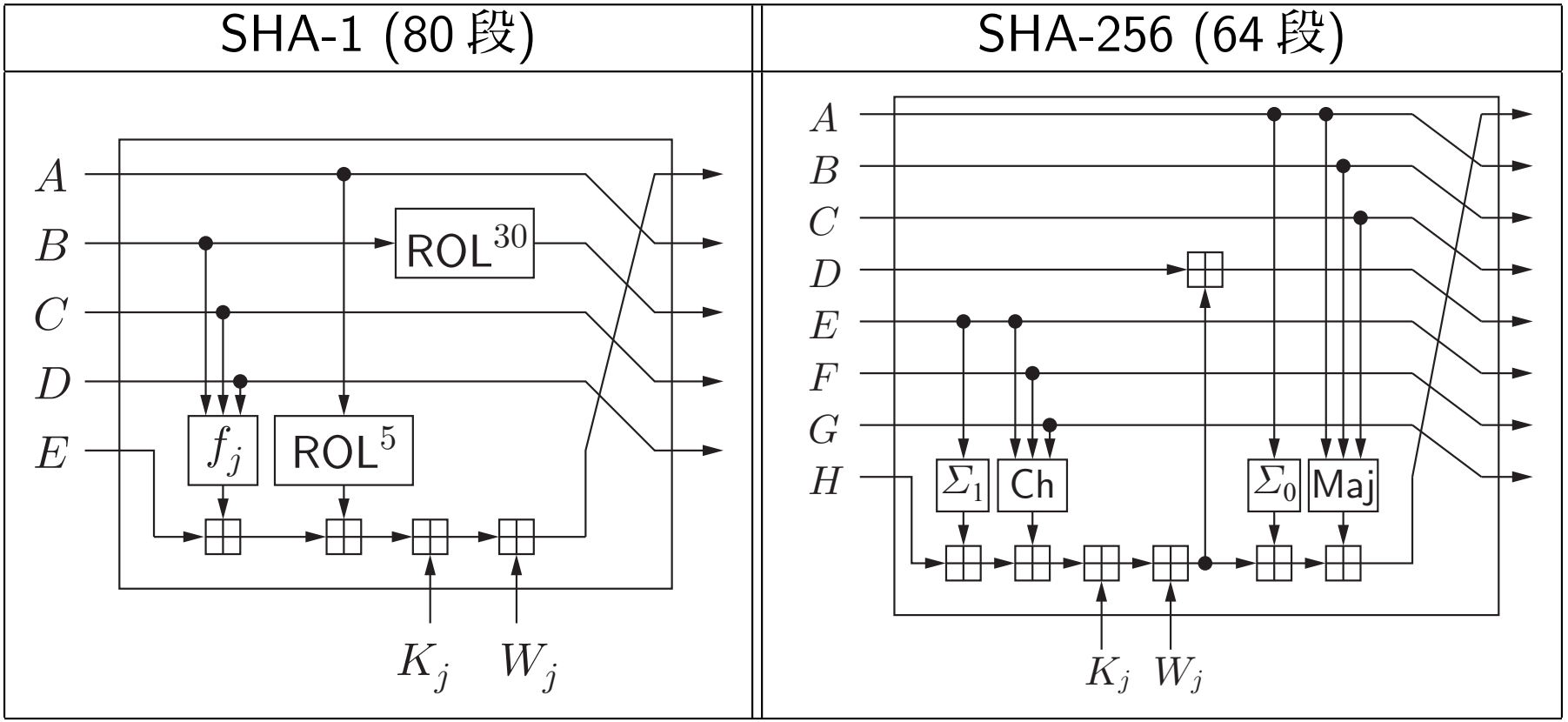
- SHA-256 と SHA-224 の相違は，初期値と出力の切り捨てのみ.
- SHA-512 と SHA-384 の相違も同様.



SHS の圧縮関数の概略



圧縮関数の攪拌部



K_j は定数

f_j は 20 段ごとに，Ch, Parity, Maj, Parity

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

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

SHA-1 圧縮関数の攪拌部

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

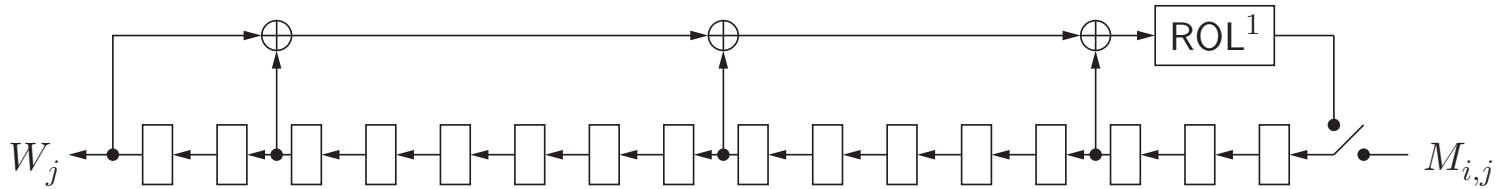
f_j はビットごとの演算

圧縮関数のメッセージ拡大

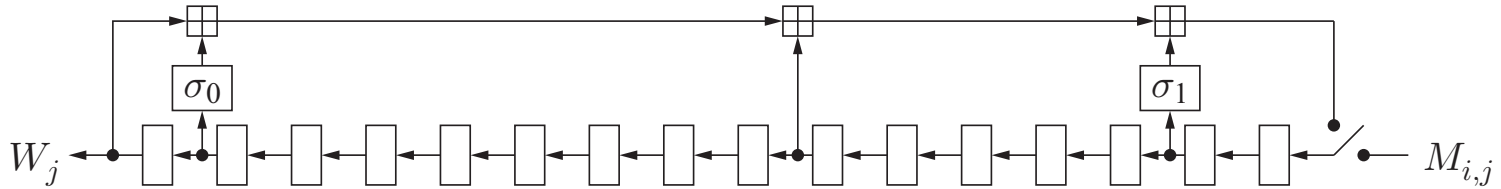
入力 $M_i = (M_{i,0}, M_{i,1}, \ldots, M_{i,15})$, $M_{i,j} \in \{0,1\}^{32}$

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

SHA-1



SHA-256



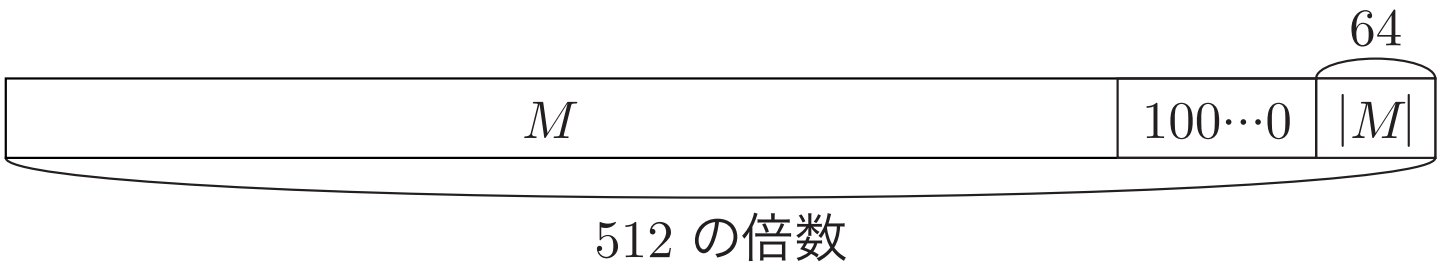
$$\sigma_0(x) = \mathsf{ROR}^7(x) \oplus \mathsf{ROR}^{18}(x) \oplus \mathsf{SHR}^3(x)$$
$$\sigma_1(x) = \mathsf{ROR}^{17}(x) \oplus \mathsf{ROR}^{19}(x) \oplus \mathsf{SHR}^{10}(x)$$

パディング

例）SHA-1, SHA-224/256

入力 M のパディング

1. $z = M\|10^d$ とする.
   d は $|M| + 1 + d + 64$ 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 $|\alpha| = 64$.



SHA-0/1 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

Wang, et. al. (1997, 1998, 2004–)

衝突攻撃の計算量 (単位は圧縮関数の計算回数)

SHA-0	$\lesssim 2^{33}$	
SHA-1	$\lesssim 2^{63}$	← 衝突はまだ得られていない.

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

SHS の現状

NIST's Policy on Hash Functions (3/15/2006)

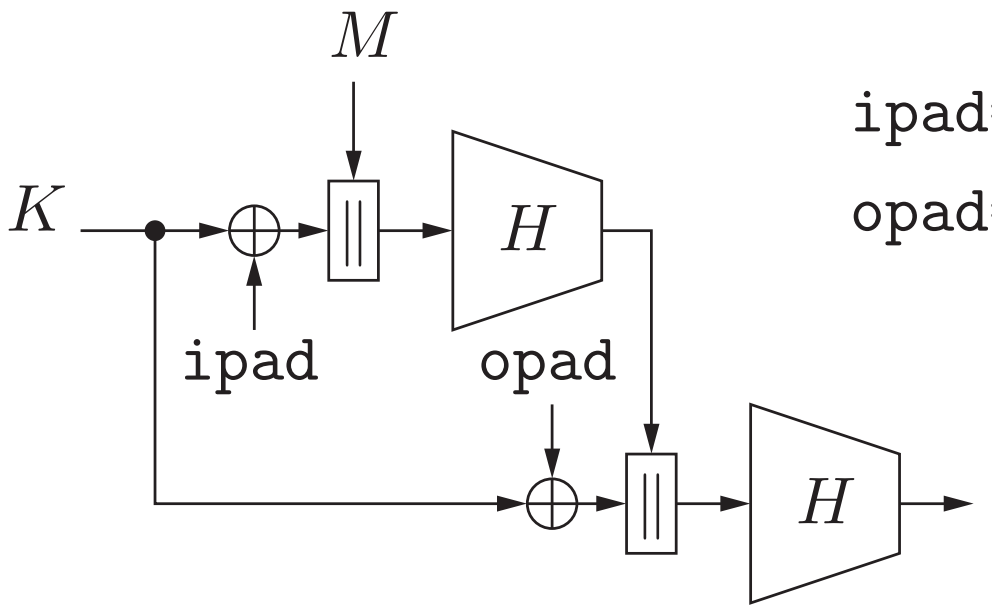
http://csrc.nist.gov/groups/ST/hash/policy.html

米国政府機関に対し

- SHA-2 (SHA-224/256/384/512) への早急な移行を推奨.
- 衝突計算困難性を要求する応用に関して，2010 年末までの SHA-1 の使用停止を勧告.
  - ディジタル署名，タイムスタンプなど
- 以下に限り，SHA-1 の使用継続を容認
  - メッセージ認証，鍵導出，擬似乱数生成

HMAC

ハッシュ関数によるメッセージ認証 (MAC) 関数



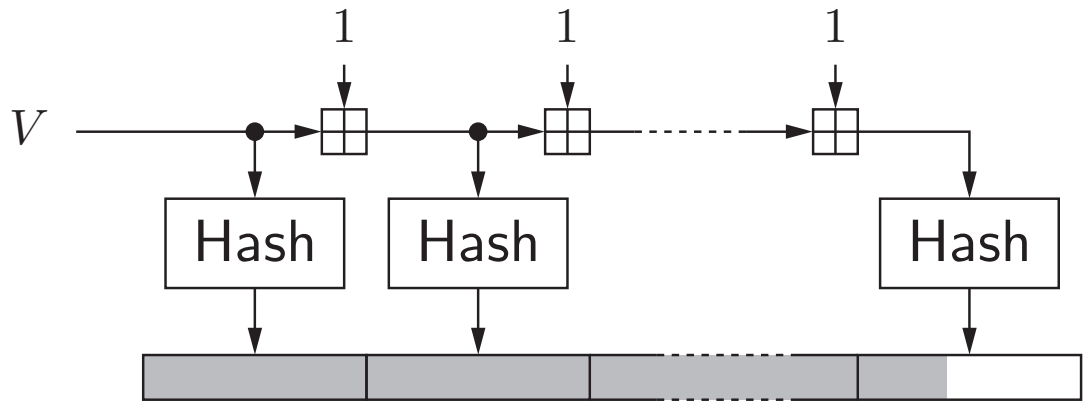

```
ipad=0x363636...
opad=0x5c5c5c...
```

- 短いメッセージに対して効率が悪い.

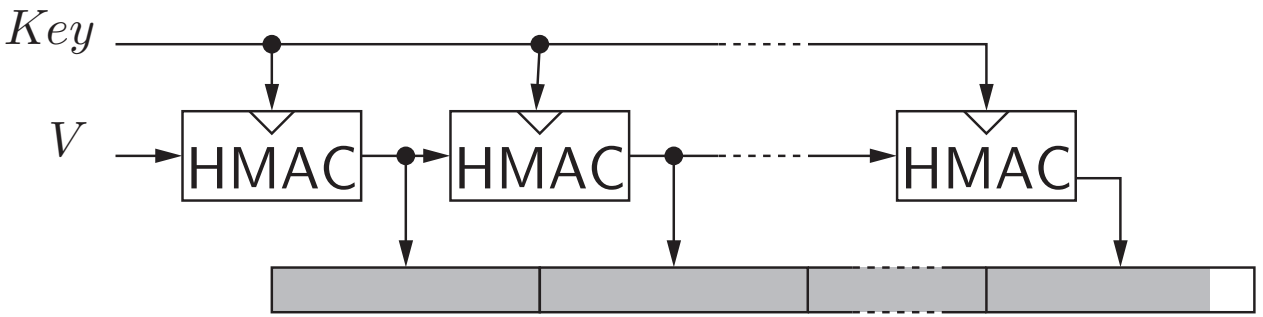
ハッシュ関数を用いた擬似乱数生成器

NIST SP 800-90

Hash_DRBG



HMAC_DRBG



Key, V は秘密鍵

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)

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.

NIST Hash Competition: 推移と予定

- 応募総数 64 件 (2008/10/31)
- ラウンド 1 候補 (51 件) の公開 (2008/12/10)
- The 1st SHA-3 Candidate Conference (2009/2/25-28)
- ラウンド 2 候補 (14 件) を選出 (2009/7/24)
- The 2nd SHA-3 Candidate Conference (2010/8/23-24)
- ラウンド 3 候補 (5 件) を選出 (2010/12/9)
- The 3rd SHA-3 Candidate Conference (2012/3/22-23)
- winner を選出 (2012 年第二四半期)

ラウンド 3 候補（ファイナリスト）

- BLAKE (CHE)
- Grøstl (DNK)
- JH (SGP)
- Keccak (CHE)
- Skein (USA)

むすび

- ハッシュ関数の性質と構成
- SHS (Secure Hash Standard)
- ハッシュ関数の応用
  - HMAC
  - 擬似乱数生成
- NIST Cryptographic Hash Algorithm Competition