ブロック暗号に基づくハッシュ関数の構成法

廣瀬勝一

福井大学

電子情報通信学会 2010 年ソサイエティ大会
(2010/9/14-17, 大阪府立大学)

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 が計算困難

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' が計算困難

衝突計算困難性 (collision resistance, CR)

$H(M) = H(M')$ を満たす相異なる M, M' が計算困難

背景

ハッシュ関数はほぼすべての暗号方式で用いられている.

- 多様な応用のための多様な安全性
  - 衝突計算困難性 (メッセージダイジェスト, ハッシュ木)
  - ランダムオラクルの代替 (RSA-OAEP など)
  - 擬似ランダム関数 (HMAC, 乱数生成, 鍵導出)
  - ...
- 多様なプラットフォームでの実装
  - ソフトウェア
  - ハードウェア

ハッシュ関数の現状と動向

MD5, SHA-1 の危殆化

- SHA-2 への移行
- NIST SHA-3 Competition
  - 14 個の第二ラウンド候補
  - 2012 年に勝者

SHA-3 第二ラウンド候補は以下を重視（？）

- ハイエンドプロセッサ上のソフトウェア処理速度
- セキュリティマージン (Double pipe)

本講演の内容

ブロック暗号に基づくハッシュ関数

- 汎用ハッシュ関数
- ハードウェア軽量実装可能なハッシュ関数

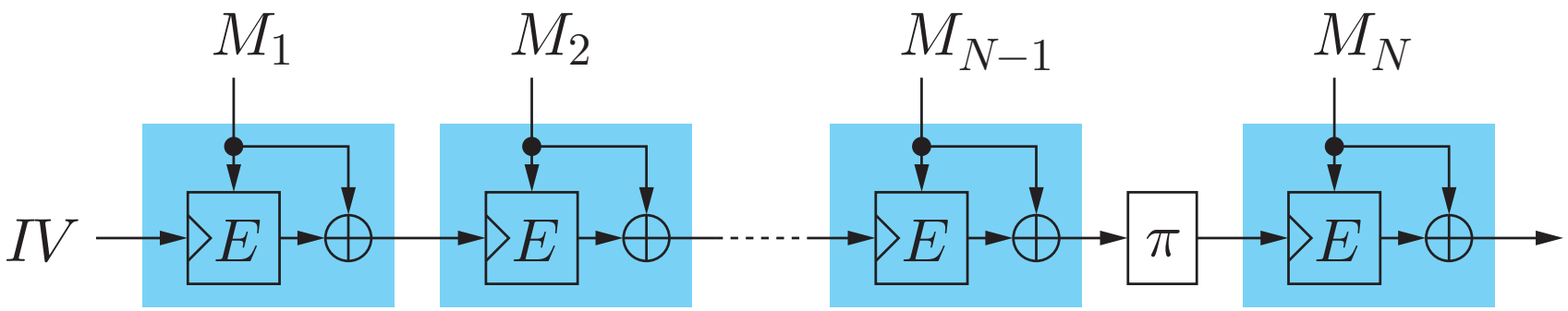
情報通信研究機構 (NICT)，高度通信・放送研究開発委託研究

「次世代ハッシュ関数の研究開発」(平成 19 年度から 21 年度)

日立製作所　井手口恒太, 大和田徹, 吉田博隆
神戸大学　桑門秀典
福井大学　廣瀬勝一

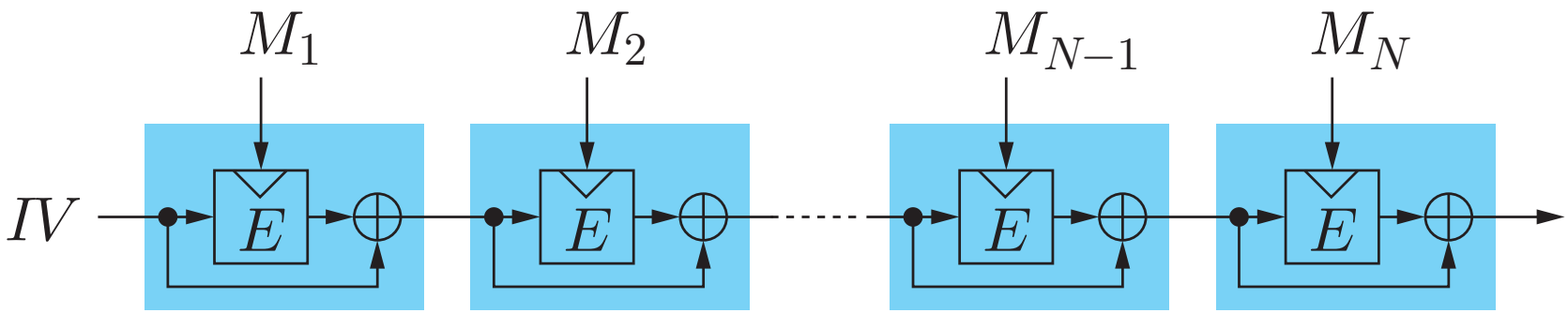
ブロック暗号を用いた汎用ハッシュ関数の構成法

MMO-MDP

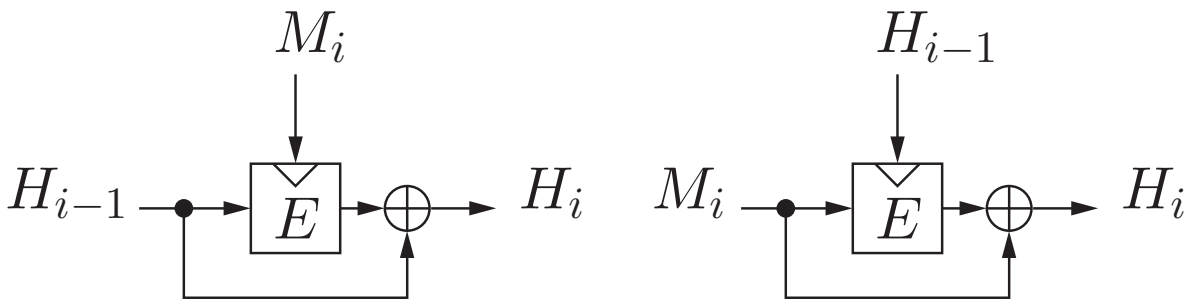


- ブロック暗号 E を用いた MMO 圧縮関数
- π は不動点を（ほとんど）持たない置換

Cf.) DM-MD (現在広く利用されているハッシュ関数の構成)



ブロック暗号を用いた圧縮関数の構成



- DM は高速処理に有利
  - $|M_i| > |H_i|$ とできる.
- 安全性の観点からは MMO が有利
  - ブロック暗号 E の鍵に相当する入力が，直接には制御できない.

Multi-Property Preservation [Bellare, Ristenpart 06]

ハッシュ関数 = 圧縮関数 + 定義域拡大

問題　圧縮関数の以下のような性質を保存する定義域拡大の設計

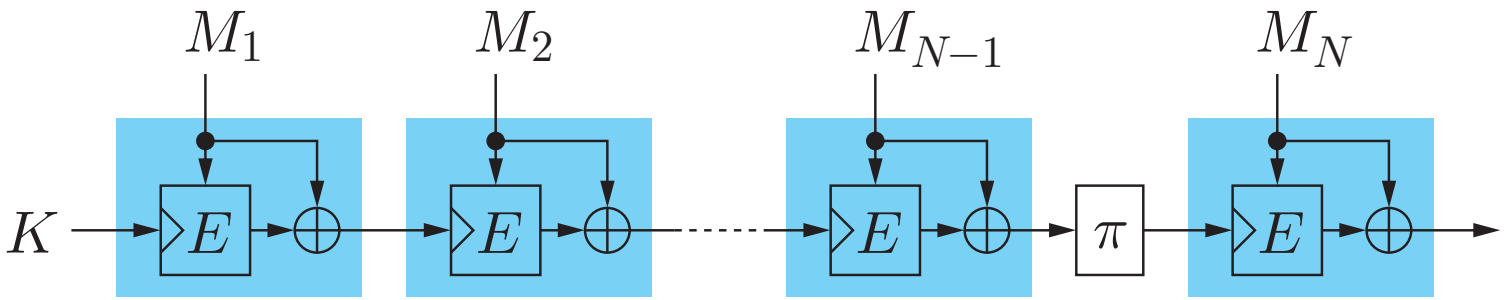
- 衝突計算困難性
- 疑似ランダム関数
- メッセージ認証 (MAC) 関数
- 強識別不能性
- ...

ブロック暗号に基づく構成では，さらに，

ハッシュ関数の安全性をブロック暗号の安全性に帰着したい

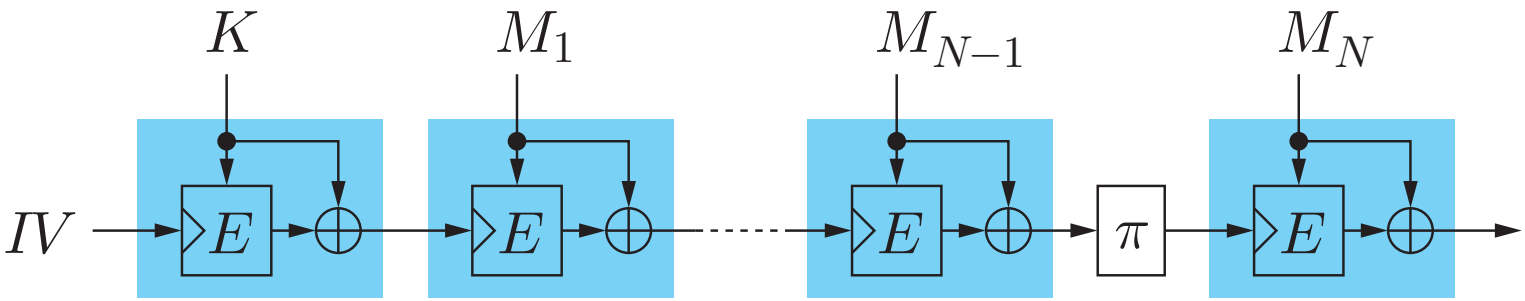
鍵付ハッシュモード

- **鍵初期値 (KIV) モード**



E が π に関する関連鍵攻撃に対して PRP $\Rightarrow$ KIV モードは PRF

- **鍵前置 (KP) モード**



KIV モードが PRF $\wedge$ $E_{IV}(K) \oplus K$ が PRG $\Rightarrow$ KP モードは PRF

π に関する関連鍵攻撃に対して PRP

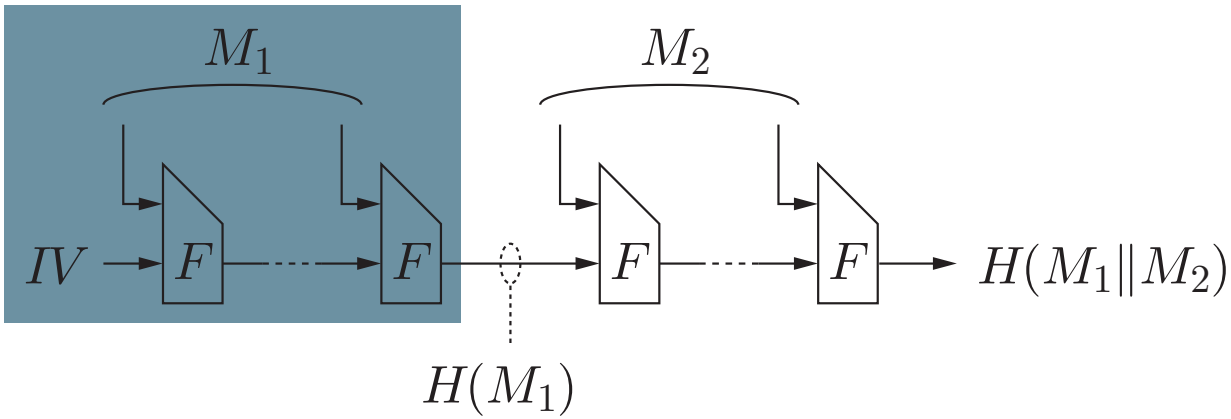
入出力を観察しても以下の二つを識別できない

- E_K と $E_{\pi(K)}$（K は秘密鍵）
- 独立かつ一様な二つのランダム置換

入力は攻撃者が選択できる

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．

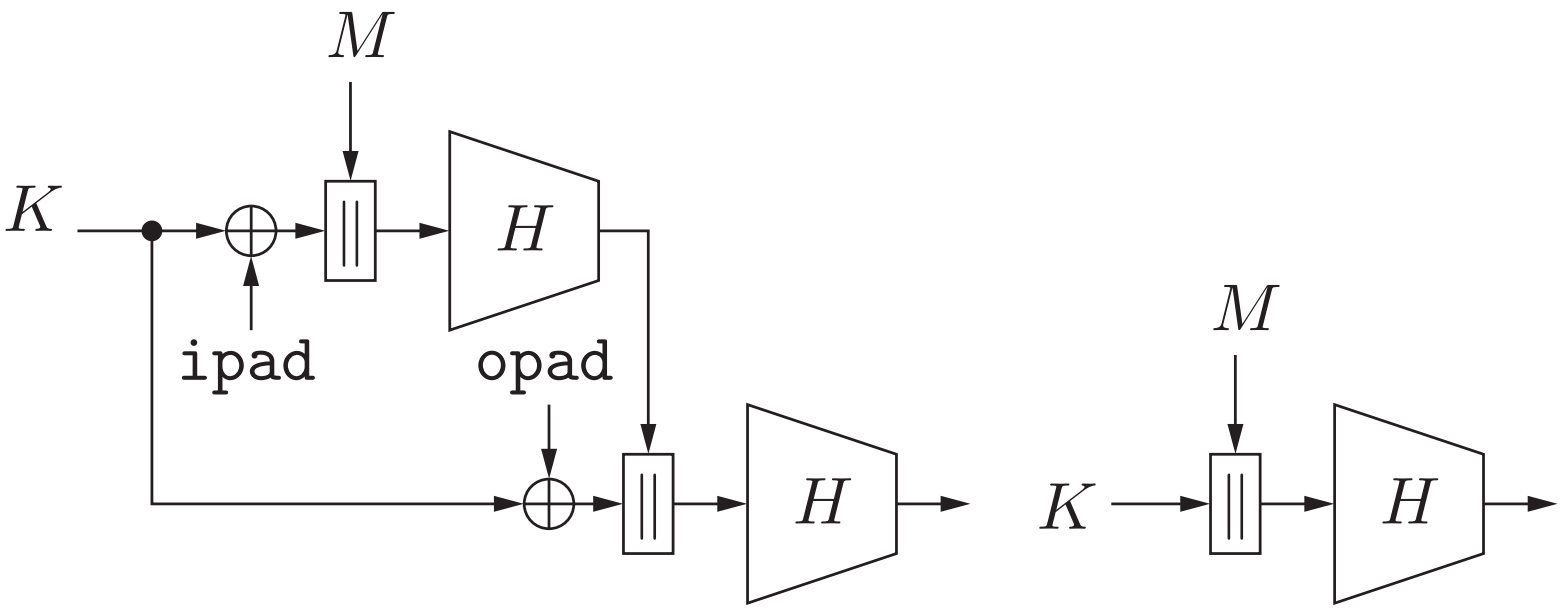


欠点：$H_K(M) = H(K \| M)$ が擬似ランダム関数とならない．

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

π により length-extension 攻撃が回避できる．

HMAC vs. KP モード



HMAC　　KP モード

ipad = 0x3636 · · · 36

opad = 0x5c5c · · · 5c

まとめ

安全性	MMO-MDP	DM-MD
衝突計算困難性	○ 理想暗号モデル	○ 理想暗号モデル
原像計算困難性	○ 理想暗号モデル	○ 理想暗号モデル
擬似ランダム関数 (KIV モード)	○ 擬似ランダム置換	×
強識別不能性	○ 理想暗号モデル	×

既存の HW 軽量実装可能な方式

ブロック暗号

- mCrypton [Lim, Korkishko, 2005]
- HIGHT [Hong, et al. 2006]
- DESL [Poschmann, et al. 2007]
- PRESENT [Bogdanov, et al. 2007]
- KATAN, KTANTAN [Cannière, et al. 2009]

ハッシュ関数

- MAME [Yoshida, et al. 2007]
- ブロック暗号を利用した構成 [Bogdanov, et al. 2008]
- Quark [Aumasson, et al. 2010]

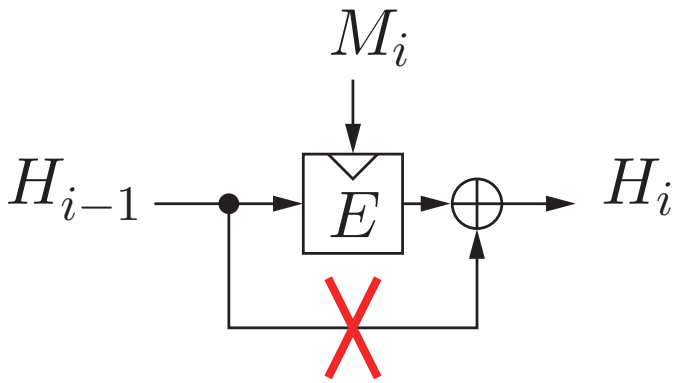
軽量ハッシュ関数の設計指針

安全性　ブロック暗号の利用

- 鍵付きハッシュモード

軽量実装　内部状態のサイズを小さくする

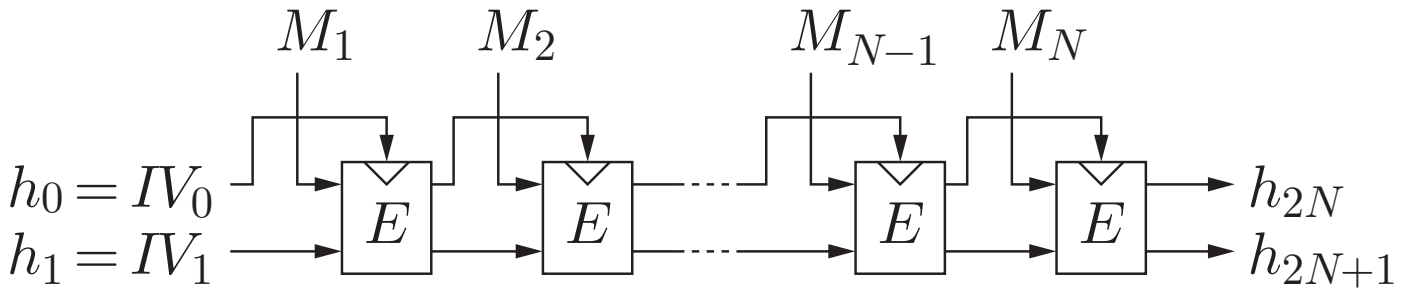
- 鍵長を小さくする
  - 衝突困難性のため，出力長は小さくできない
- フィードフォワードを使わない



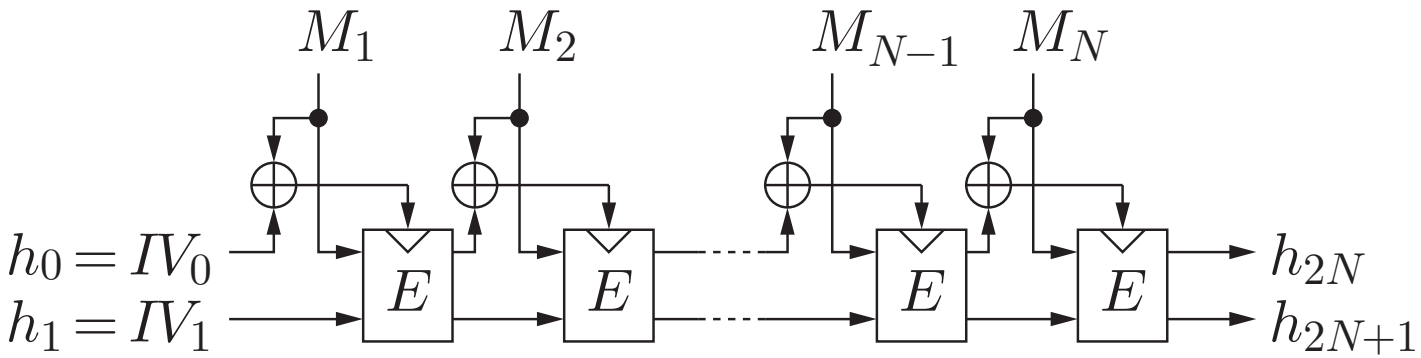
二つの提案方式

E はブロック暗号．鍵長はブロック長の半分．

LW-1



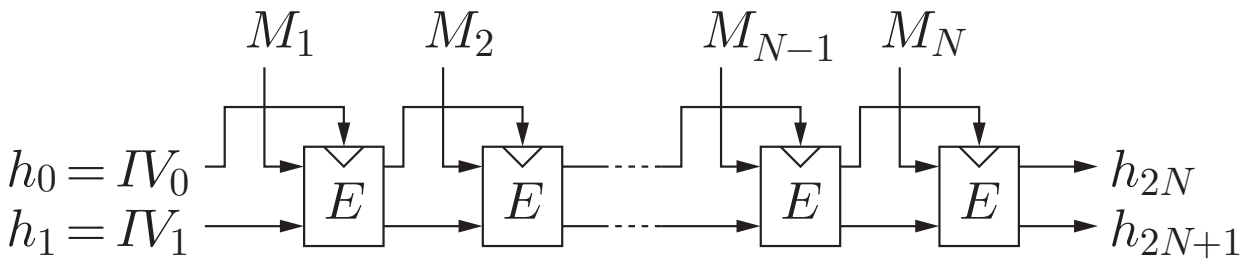
LW-2



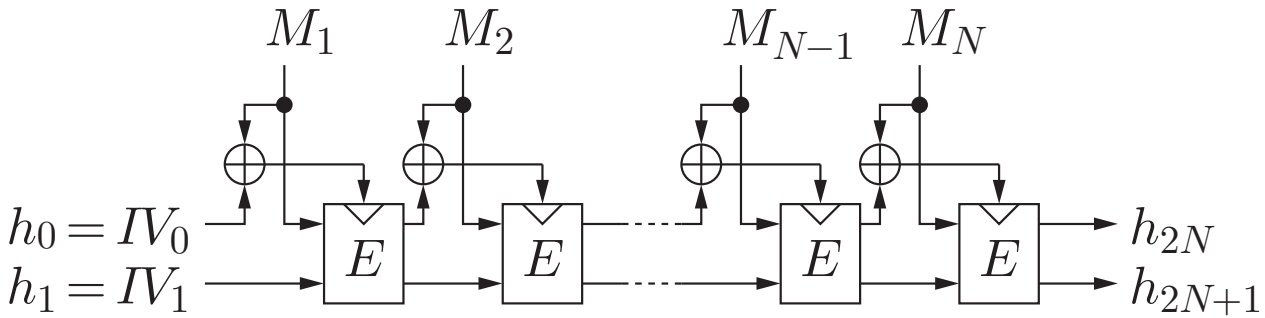
LW-1 は Lesamnta-LW の構成

衝突計算困難性，原像計算困難性

LW-1



LW-2



出力長を $2n$ とする．理想暗号モデルを仮定．

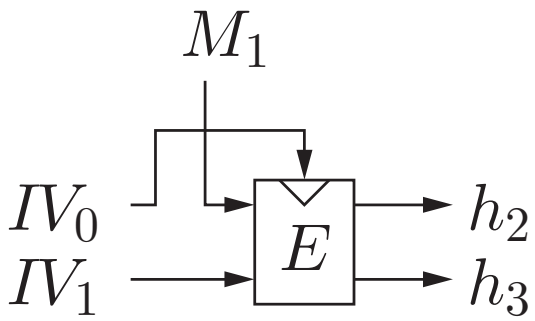
衝突・原像攻撃の計算量

LW-1: $\Omega(2^n(\log n)/n)$　　LW-2: $\Omega(2^n)$

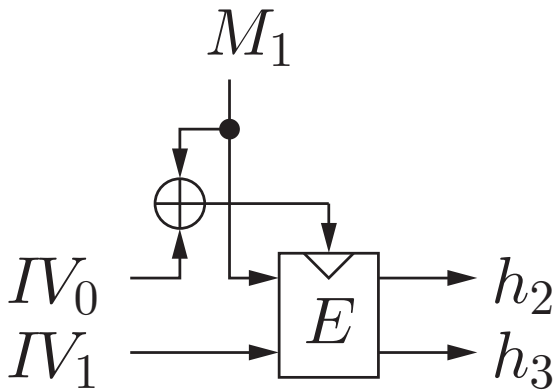
LW-1 の原像計算困難性

LW-1 には，メッセージ長が 2 ブロック以上となるパディングが必要.

メッセージ長が 1 ブロックの場合，容易に原像が得られる.

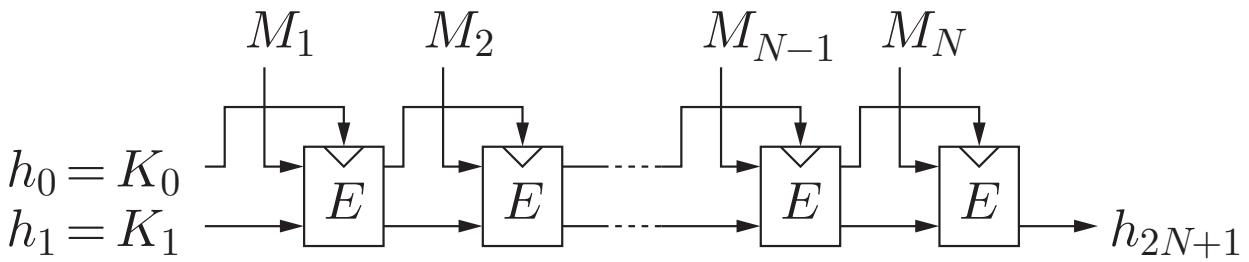


LW-2 については，メッセージ長が 1 ブロックでも原像計算は困難.

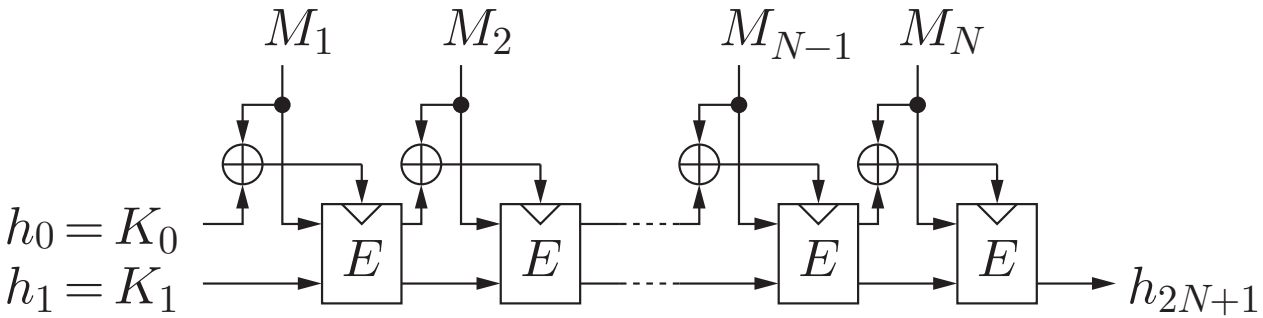


鍵初期値モード

LW-1



LW-2



出力の前半を切り捨て．← length extension 攻撃を回避するため

LW-1 : E が PRP ⇒ 鍵初期値モードは PRF

LW-2 : E が関連鍵攻撃に対して PRP ⇒ 鍵初期値モードは PRF

まとめと今後の課題

ブロック暗号を利用した HW 軽量ハッシュ関数の二つの構成法

安全性	ブロック暗号の仮定
衝突計算困難性	理想暗号モデル
原像計算困難性	理想暗号モデル
擬似ランダム関数（鍵付き）	擬似ランダム置換

今後の課題

- 強識別不能性の検討
- 構成法の一般化と安全性の検討