東京工業大学理財工学研究センター科研費シンポジウム (2006/11/16-17)

安全なハッシュ関数の構成法について

廣瀬勝一

福井大学工学研究科電気・電子工学専攻

2006 年 11 月 16 日

暗号ハッシュ関数の性質

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

原像計算困難性 (preimage resistance)

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

原像計算困難性 (second-preimage resistance)

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

衝突計算困難性 (collision resistance)

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

誕生日のパラドクス

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

およそ $1.17\sqrt{N}$ 回の試行で，2 回以上選択される要素の存在する確率は 1/2

例）23 人集まれば，誕生日の同じ人が存在する確率は 1/2

誕生日攻撃

ハッシュ関数の衝突を見つける自明な攻撃

ハッシュ関数の内部の構造は一切利用しない

入力を無作為に選択して出力を計算することを繰り返す

ハッシュ関数の出力長を ℓ ビットとすると

およそ $1.17 \times 2^{\ell/2}$ 回の計算で，衝突の生じる確率は $1/2$

定義　ハッシュ関数が衝突計算困難性 (CR) について最適

誕生日攻撃より本質的に効率の良い攻撃法が存在しない

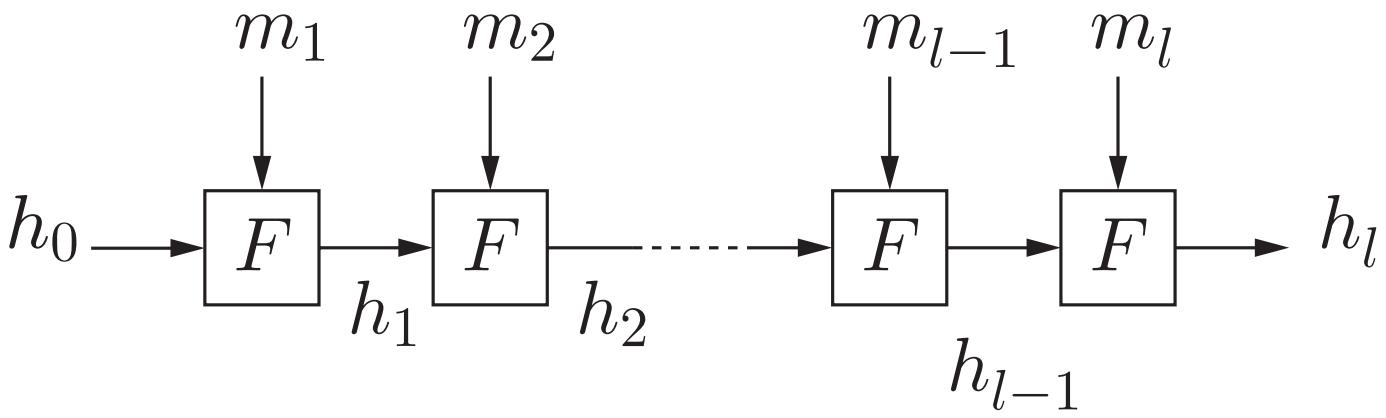
反復型ハッシュ関数

圧縮関数 $F : \{0,1\}^{\ell} \times \{0,1\}^{\ell'} \to \{0,1\}^{\ell}$

初期値 $h_0 \in \{0,1\}^{\ell}$

パディング 入力を ℓ' 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 $(m_1, m_2, \ldots, m_l)$ について

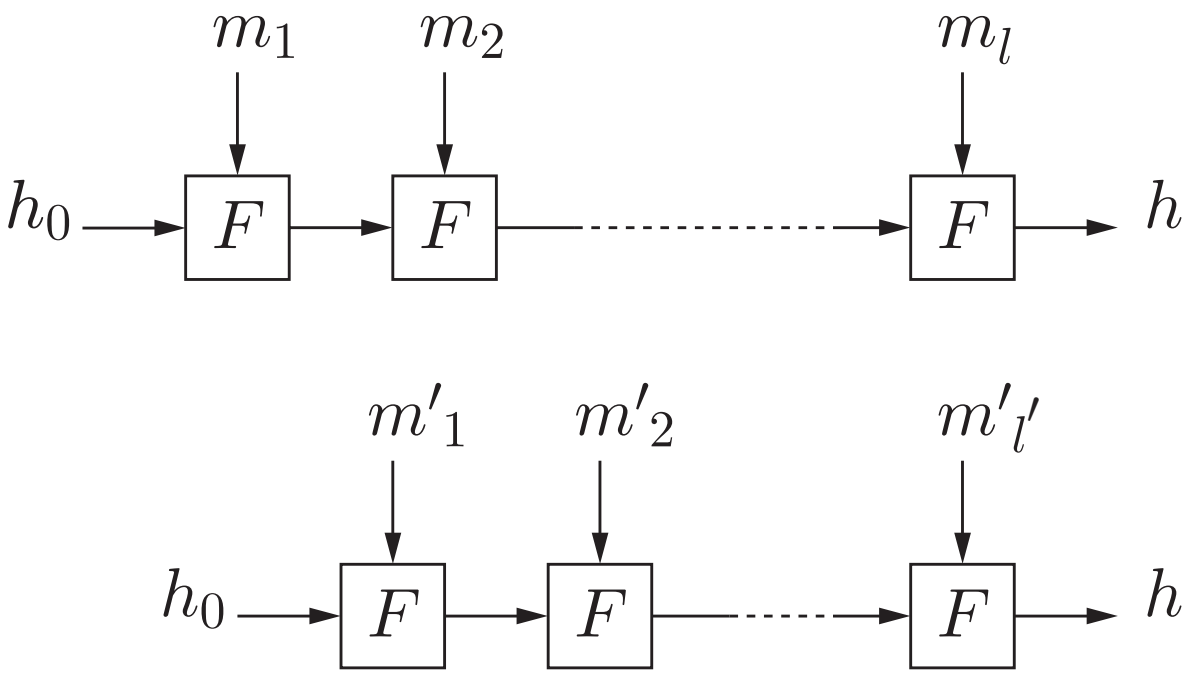


$h_l = H(M)$

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 H に衝突が見つかれば，圧縮関数 F にも衝突が見つかる

圧縮関数の構成法

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

ブロック暗号を用いたハッシュ関数を考える動機

- 極小規模のハードウェアで有効
- AES を用いた場合，MDx 族より Wang らの差分攻撃に強い (？)

倍ブロック長ハッシュ関数を考える動機

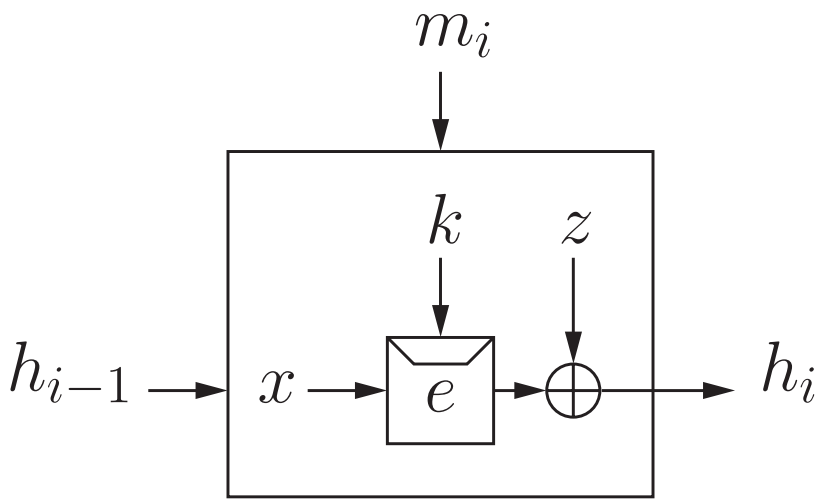
- AES で構成される単ブロック長ハッシュ関数は安全でない
  - 出力長は 128 ビット
  - 誕生日攻撃の計算量 $\approx 2^{64}$

単ブロック長圧縮関数のモデル

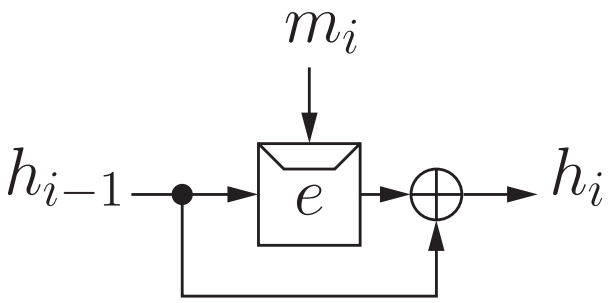
Preneel, Govaerts, Vandewalle 93

$x, k, z \in \{h_{i-1}, m_i, h_{i-1} \oplus m_i, 0\}$

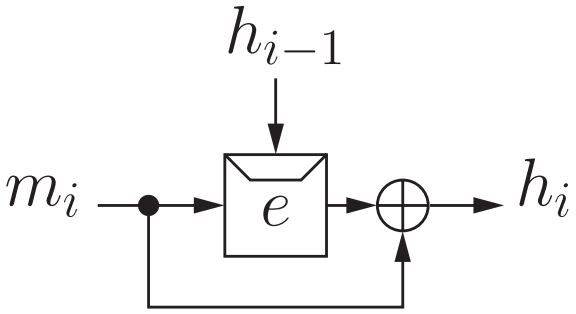
$4^3 = 64$ 通りの構成



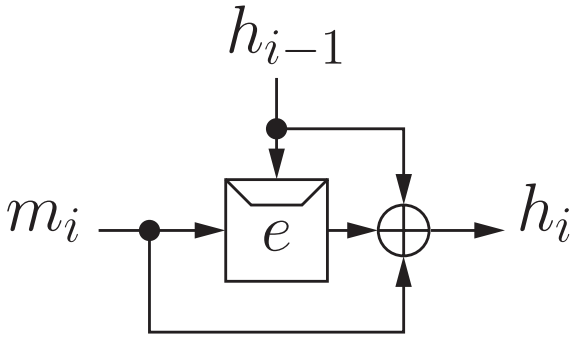
例）



Davies-Meyer



Matyas-Meyer-Oseas



Miyaguchi-Preneel

理想的暗号モデル

各鍵について，ブロック暗号の暗号化関数は**可逆のランダム置換**

暗号化，復号はそれぞれ**オラクルへの質問**によって計算される．

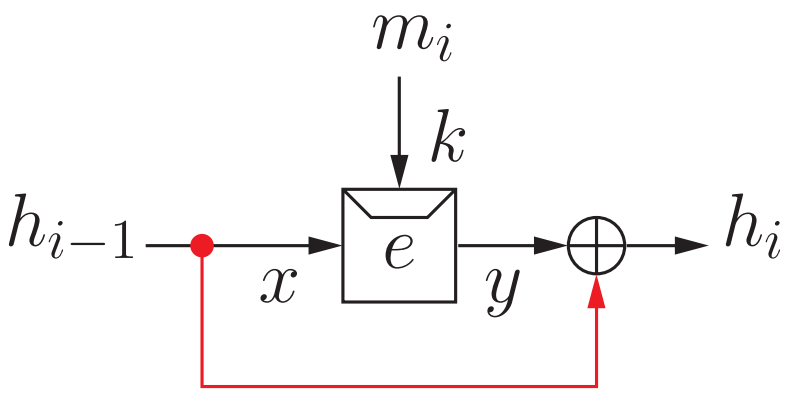
オラクル	質問	返答
暗号化 e	(鍵, 平文)	暗号文
復号 e^{-1}	(鍵, 暗号文)	平文

- 各鍵について，e, e^{-1} は 1 対 1 関数
- e, e^{-1} に不一致のないように

攻撃の計算量はオラクルへの**質問回数**

単ブロック長ハッシュ関数の安全な構成法

定理 **(Merkle 89)** 理想的暗号モデルで，
圧縮関数 $h_i = e_{m_i}(h_{i-1}) \oplus h_{i-1}$ は CR について最適



圧縮関数を計算するためには，e か e^{-1} かを計算しなければならない

$$h_i = e_k(x) \oplus x \quad \text{または} \quad h_i = y \oplus {e^{-1}}_k(y)$$

理想的暗号モデルでは，圧縮関数の出力はランダムに決まる

いかなる攻撃の成功確率も，誕生日攻撃の成功確率と同等

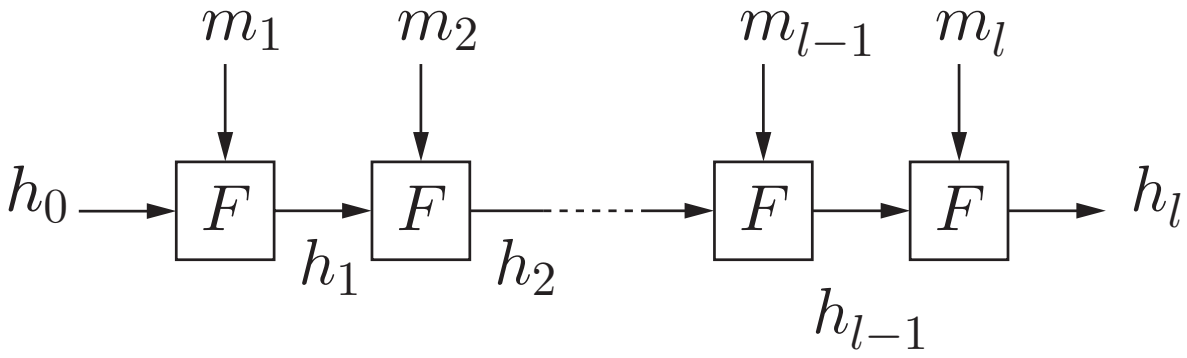
単ブロック長ハッシュ関数の安全な構成法

定理 (Black, Rogaway, Shrimpton 02)
Preneel らのモデルに属する圧縮関数について，理想的暗号モデルで

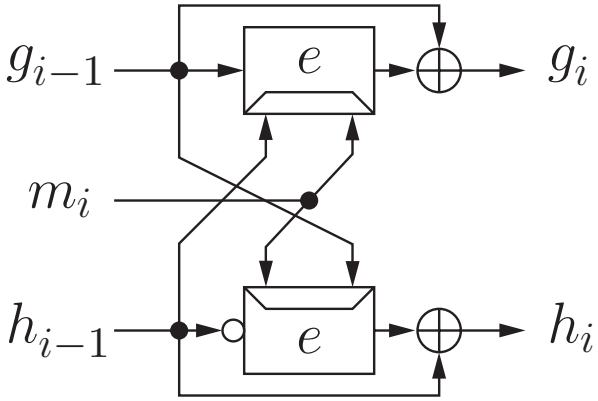
1. CR について最適な圧縮関数が 12 個存在する
2. 上記以外の 8 個の圧縮関数を用いて，CR について最適な反復型ハッシュ関数が構成できる

1 の証明は Merkle の定理と同様

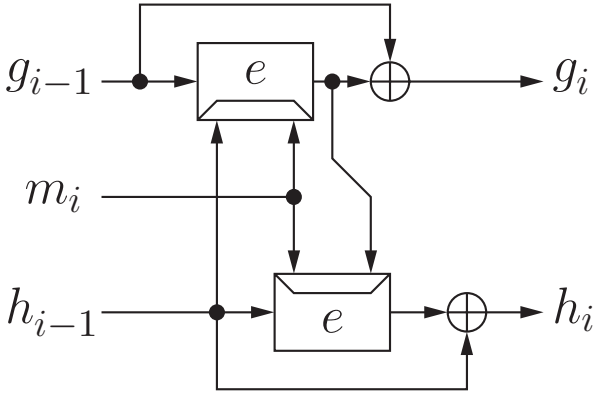
2 の証明は反復型の構造を利用して行われる



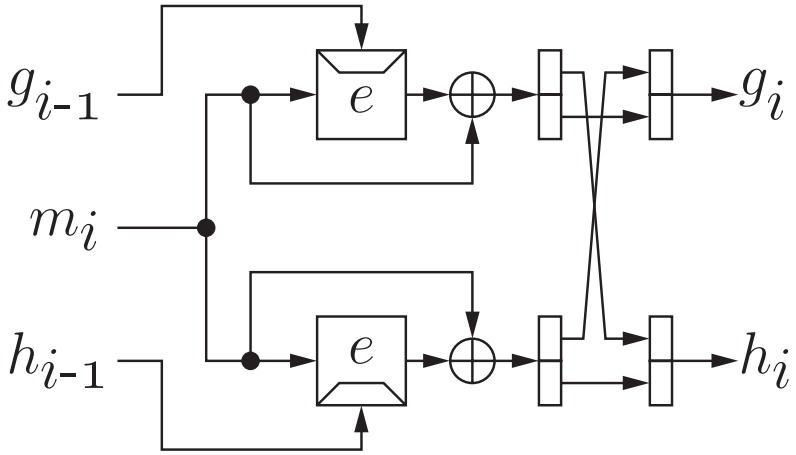
倍ブロック長ハッシュ関数の既存の主な構成法



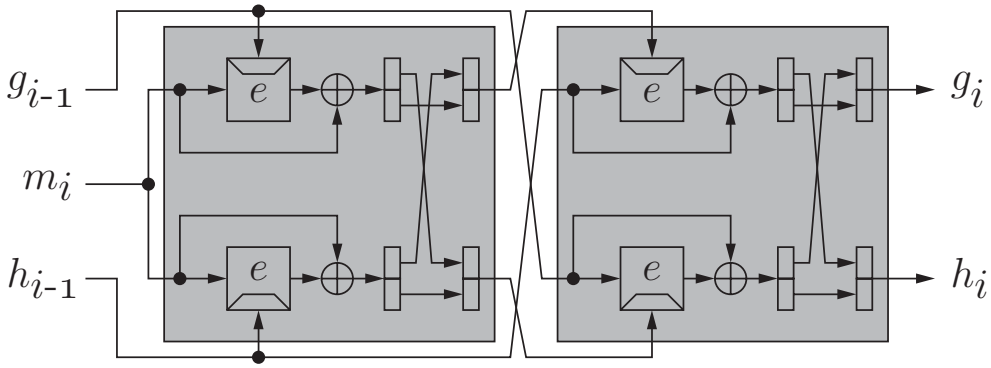
abreast Davies-Meyer



tandem Davies-Meyer

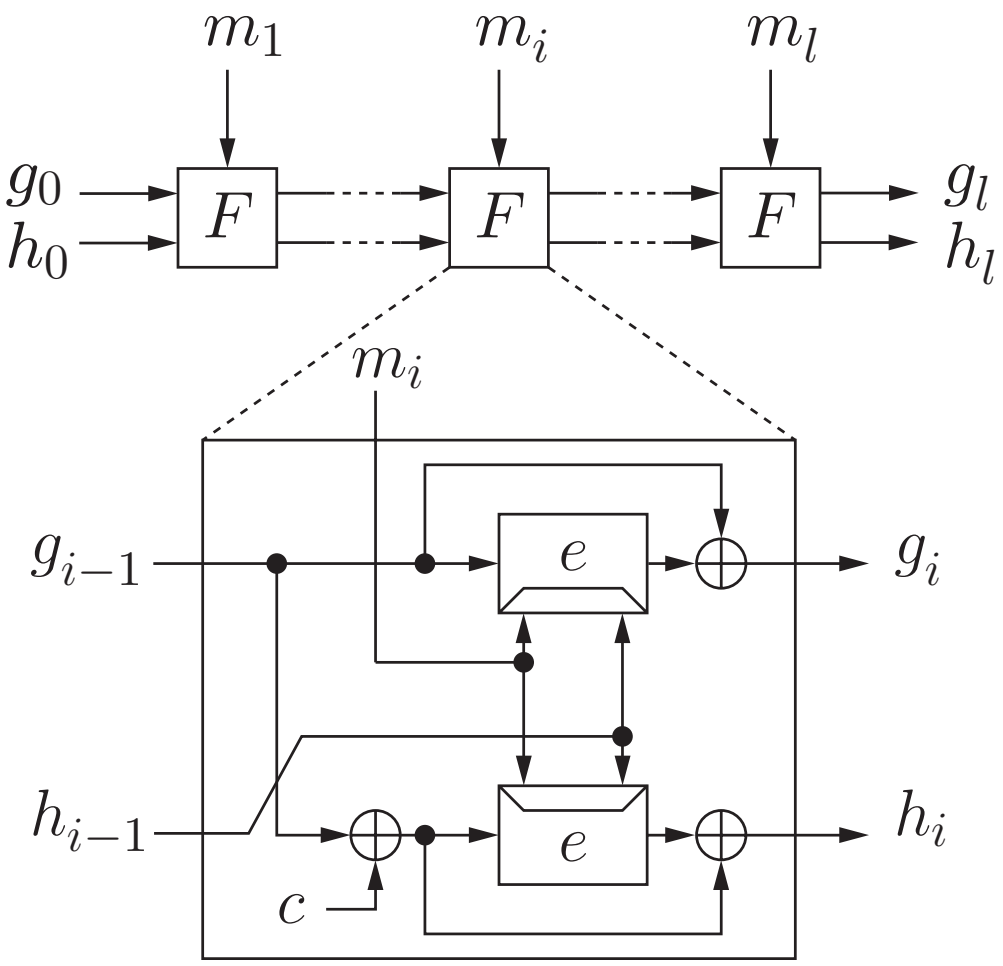


MDC-2



MDC-4

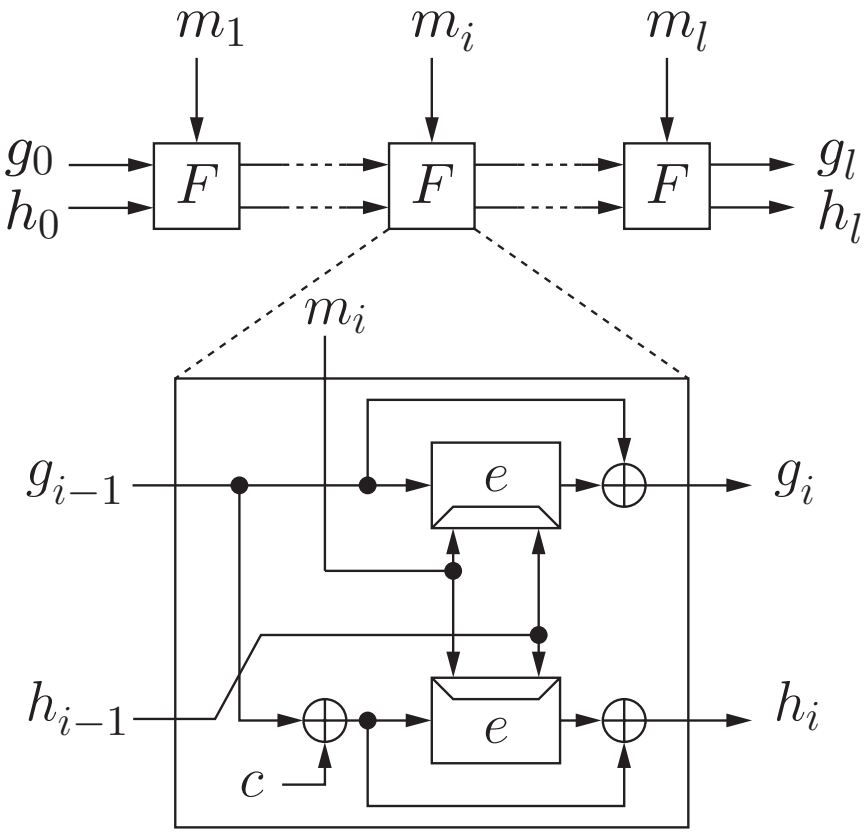
倍ブロック長ハッシュ関数の安全な構成法



- c は非零の定数
- 二つの暗号化関数の鍵に対応する入力が同一
  - 鍵拡大が 1 度で済む
- AES を利用する場合
  - 出力長は 256 ビット
  - 鍵長 192/256 ビットで利用

倍ブロック長ハッシュ関数の安全な構成法

定理 (Hirose 06)



$F : \{0,1\}^{2n+b} \to \{0,1\}^{2n}$

このとき，理想的暗号モデルで，
$1 \le q \le 2^{n-2}$ に対して

$$\mathbf{Adv}_H^{\mathrm{coll}}(q) \le 12\left(\frac{q}{2^n}\right)^2$$

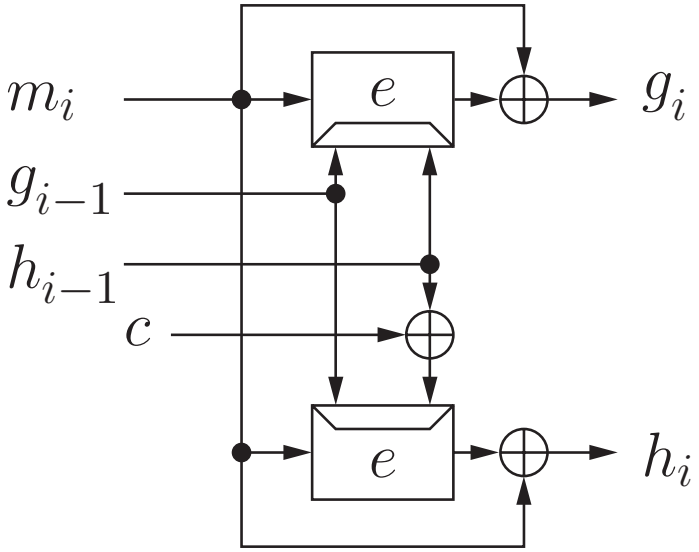
(CR について最適)

ここで

$\mathbf{Adv}_H^{\mathrm{coll}}(q) \stackrel{\mathrm{def}}{=} (e, e^{-1})$ への q 組の質問による攻撃成功確率の最大値

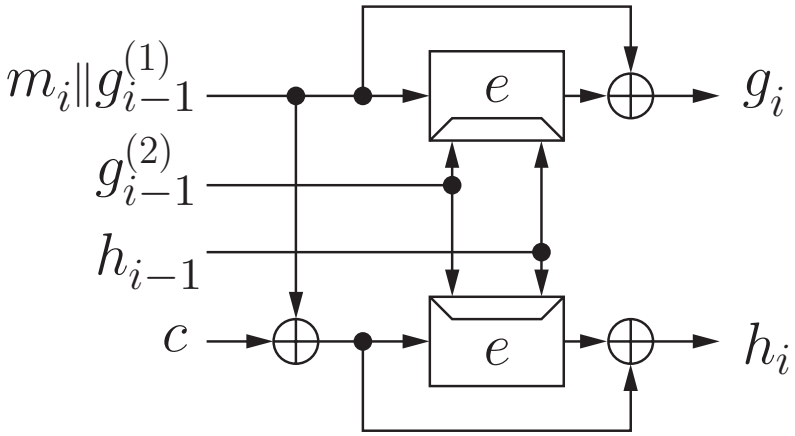
倍ブロック長ハッシュ関数の他の例

以下の圧縮関数によるハッシュ関数も CR について最適



256 ビット鍵 AES で実現可

鍵拡大は 2 回



192 ビット鍵 AES で実現可

鍵拡大は 1 回

MDC-2 vs. 筆者らの構成

効率

- 筆者らの構成では「鍵長 $>$ ブロック長」のブロック暗号が必要
  圧縮関数へのメッセージ入力長は「鍵長 $-$ ブロック長」
- MDC-2 は「鍵長 $=$ ブロック長」のブロック暗号で実現可
  圧縮関数へのメッセージ入力長は「ブロック長」

安全性

- 筆者らの構成は CR について最適
- MDC-2 が CR について最適かどうかは未解決問題
  理想的暗号モデルでの CR の証明 (Steinberger 06)

まとめ

ブロック暗号を用いたハッシュ関数の構成法について

- 単ブロック長と倍ブロック長
- 理想的暗号モデルを仮定した安全性証明

今後の課題

- 専用構成法によるハッシュ関数の安全性証明