A Hash Function Using an MMO-Type Double-Block Compression Function

Shoichi Hirose

University of Fukui

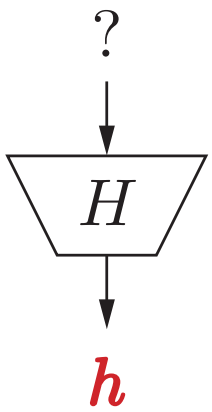
Hash Workshop
(2011/9/22, Ito Campus, Kyushu University)

Cryptographic Hash Function

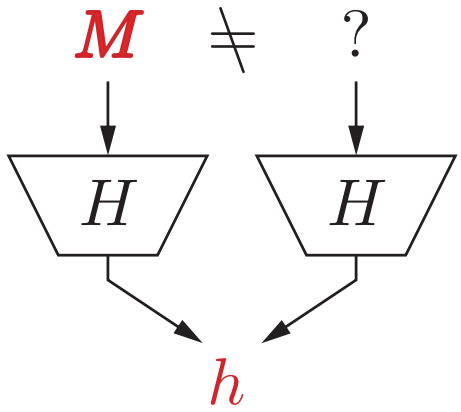
$H : \{0,1\}^* \rightarrow \{0,1\}^n$

Properties

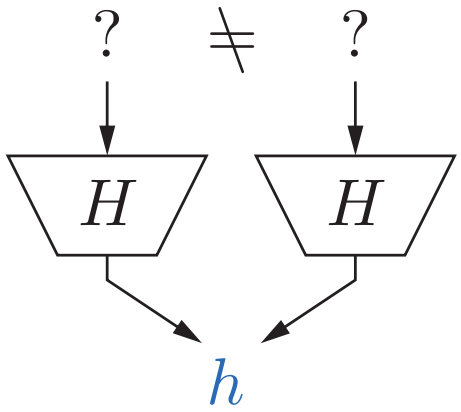
Preimage Resistance



Second PR



Collision Resistance

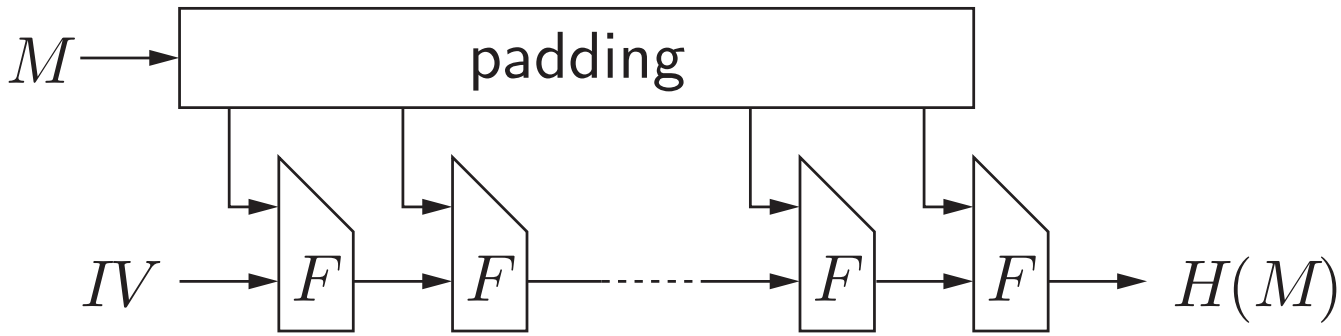


	PR	2ndPR	CR
Complexity	$O(2^n)$	$O(2^n)$	$O(2^{n/2})$

Iterated Hash Function (Merkle-Damgård)

- Compression function
  $F : \{0,1\}^n \times \{0,1\}^b \to \{0,1\}^n$
- Initial value $IV \in \{0,1\}^n$

Input $M \in \{0,1\}^*$



Compression Function Construction

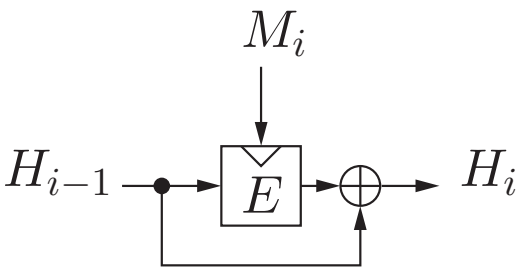
Customized (1990–)

- MDx family
  MD4, MD5; RIPEMD-160; SHA-1, SHA-224/256/384/512
- Whirlpool
- SHA-3 candidates

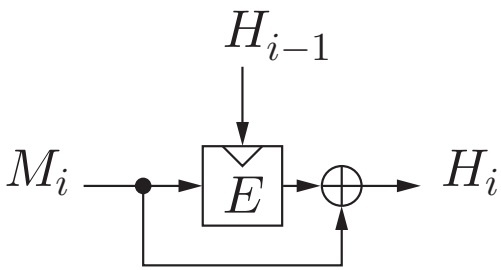
Using a block cipher

- Single block length (SBL): output-length = block-length
- Double block length (DBL): output-length = $2 \times$ block-length

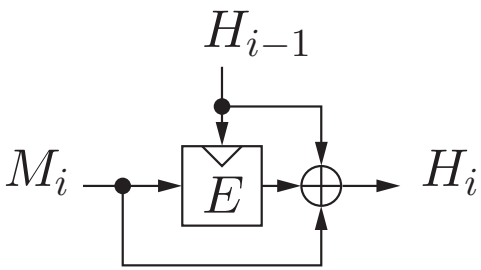
SHA-1/2	DM mode using a dedicated block cipher SHACAL-1/2
Whirlpool	MP mode using a dedicated block cipher W



Davies-Meyer



Matyas-Meyer-Oseas



Miyaguchi-Preneel

Related Work

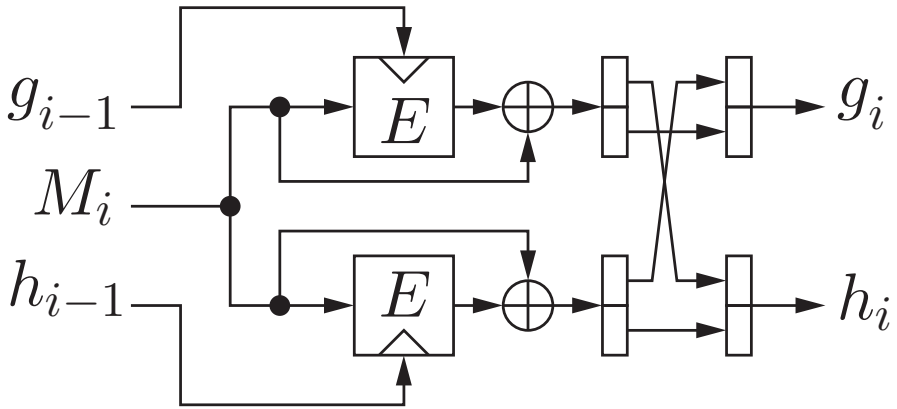
- Single-block-length constructions
  - PGV model [Preneel, Govaerts, Vandewalle 93]
  - Provable security of PGV modes [Black, Rogaway, Shrimpton 02]
  - Stam model [Stam 09]
- Double-block-length constructions
- Permutation-based constructions
  - Impossibility result [Black, Cochran, Shrimpton 05]
  - Security/efficiency tradeoff [Rogaway, Steinberger 08]
  - Sponge [Bertoni, Daemen, Peeters, van Assche 07]
- Multi-property preserving domain extension [Bellare, Ristenpart 06]
  - EMD (Enveloped Merkle-Damgård)
  - ...

DBL Compression Functions: MDC-2 & MDC-4

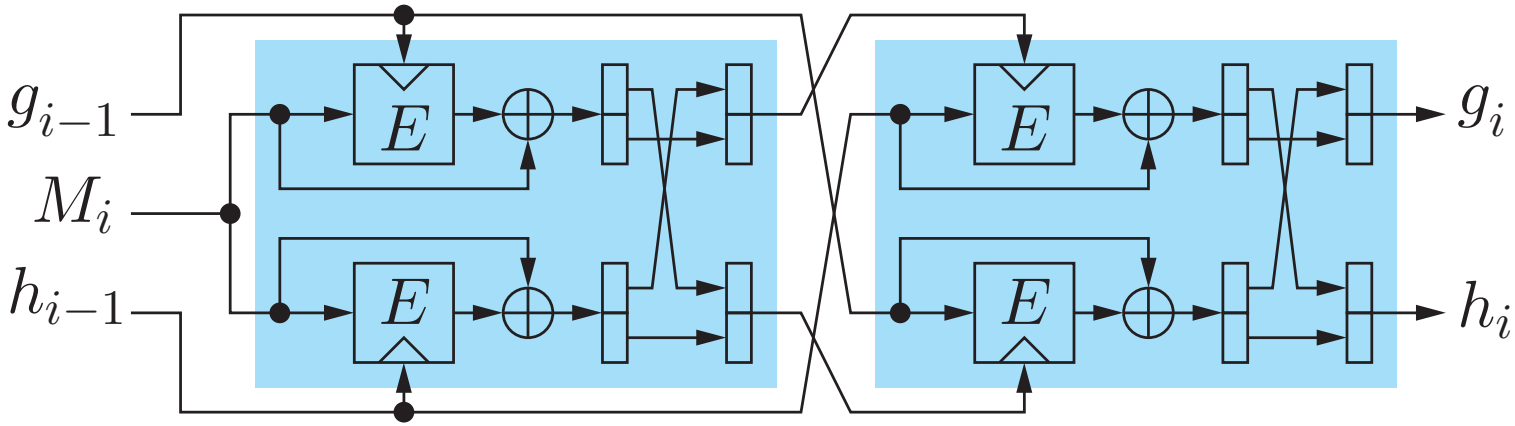
[Brachtl, Coppersmith, et.al. 88]

Use a block cipher with key-size = block-size

MDC-2



MDC-4

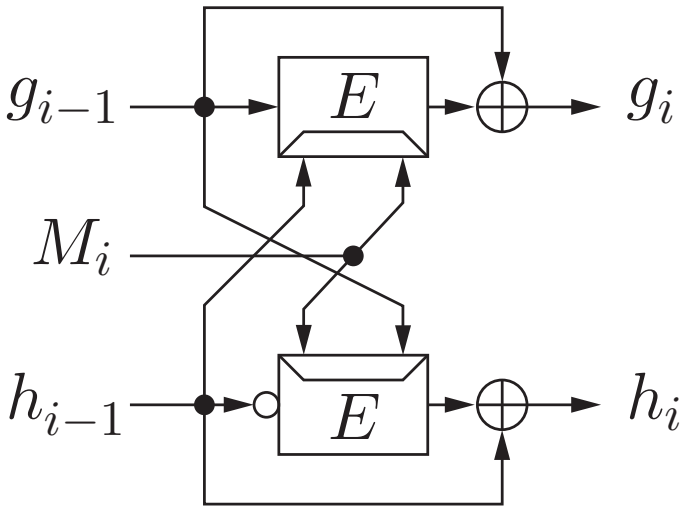


message-block-size = n

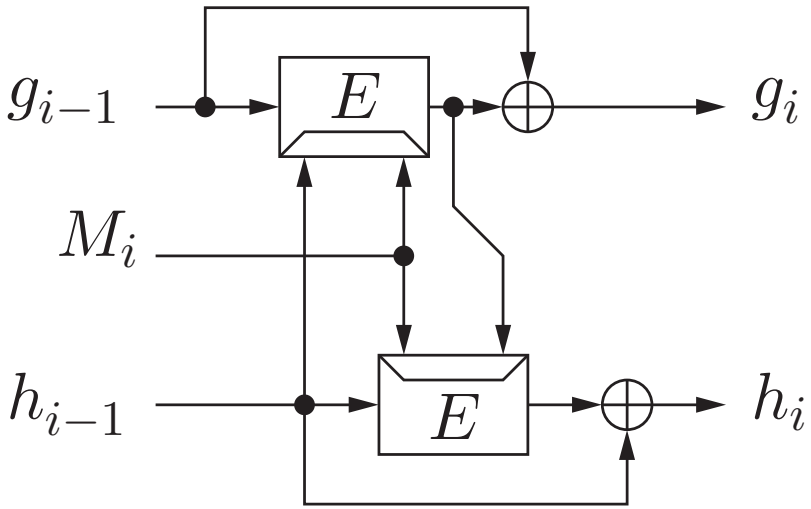
DBL Compression Functions: Abreast-/Tandem-DM

[Lai, Massey 92]

Use a block cipher with key-size (k) > block-size (n)



abreast Davies-Meyer

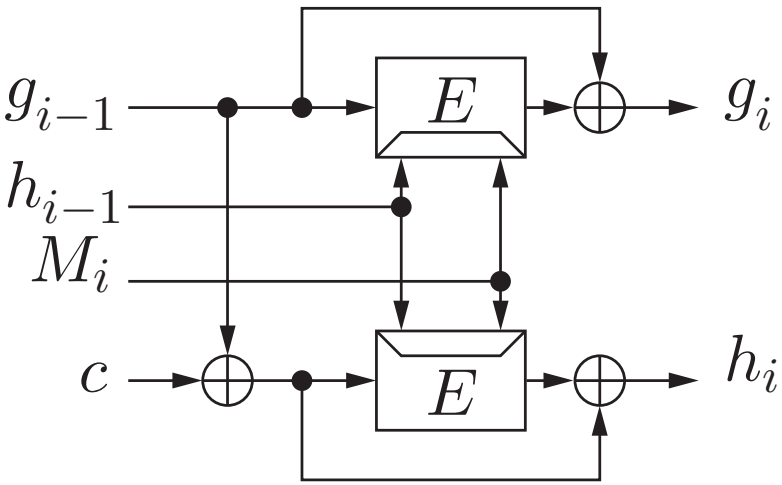


tandem Davies-Meyer

message-block-size $= k - n$

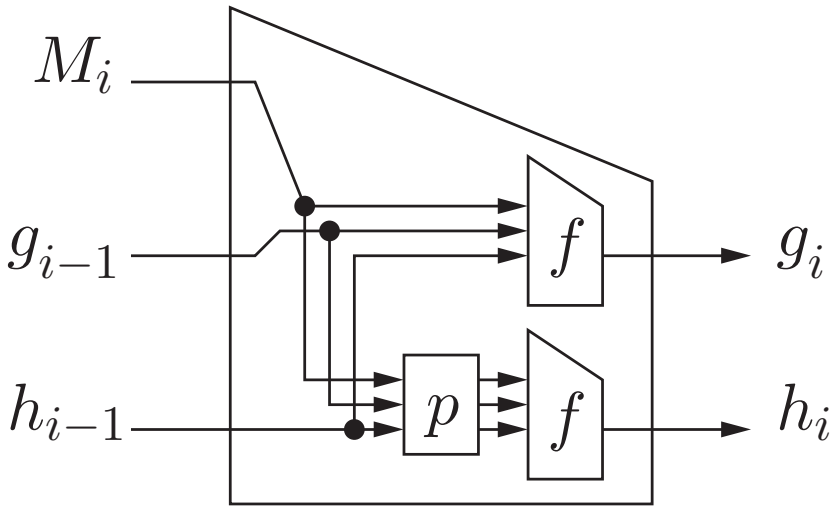
DBL Compression Functions: Hirose 06

Uses a block cipher with key-size (k) > block-size (n)

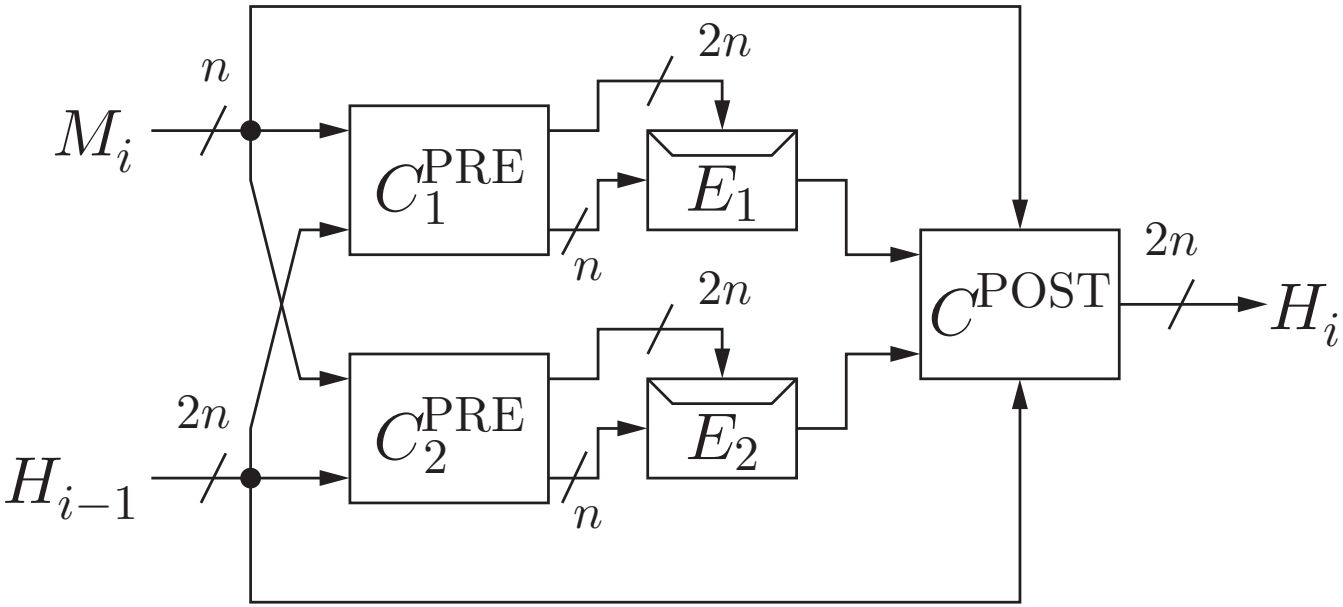


- c is a non-zero constant
- message-block-size $= k - n$
- **single key expansion**

Note) Based on [Nandi 05]. p is involution $(p = p^{-1})$



Özen-Stam Model (2010)



Security (Number of Oracle Queries)

Output length: $2n$

Attack	MDC-2	ab-DM	ta-DM	Hir
Collision	$\Omega(2^{0.6\,n})^{(1)}$	$\Theta(2^n)^{(2)}$	$\Omega(2^n/n)^{(3)}$	$\Theta(2^n)^{(4)}$
Preimage	$O(2^n)^{(5)}$	$\Theta(2^{2n})^{(6)}$	$\Theta(2^{2n})^{(6,7)}$	$\Theta(2^{2n})^{(6)}$

1. [Steinberger 06]
2. [Fleischmann, Gorski, Lucks 09], [Lee, Kwon 09]
3. [Lee, Stam, Steinberger 10]
4. [Hirose 06]
5. Requires $O(2^n)$ memory [Knudsen, Mendel, Rechberger, Thomsen 09]
6. [Lee, Stam, Steinberger 11]
7. $O(2^n)$ if digest $= 0^{2n}$.

Ideal Cipher Model

Let E be a block cipher.

For each key K, $E_K(\cdot)$ is an **invertible random permutation**.

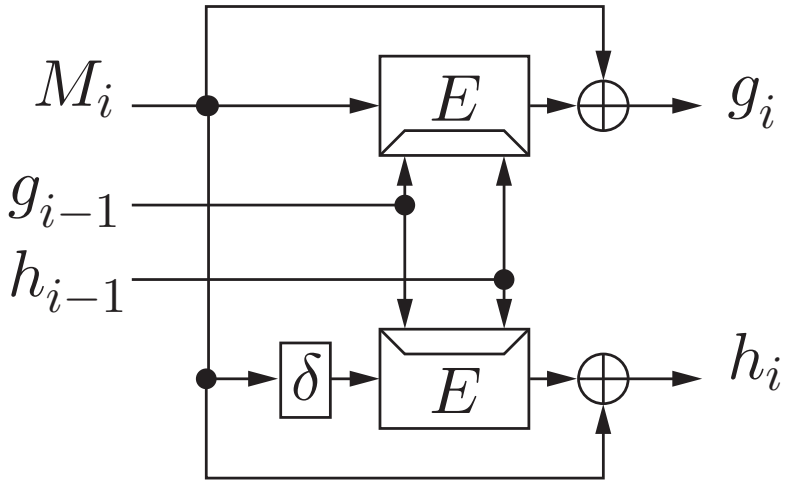
E is evaluated by two kinds of **oracle queries**:

oracle	query	answer
E	(key, plaintext)	ciphertext
E^{-1}	(key, ciphertext)	plaintext

Provable security in the ideal cipher model

covers cryptanalysis not using intenal structure of E

Jonsson & Robshaw 05

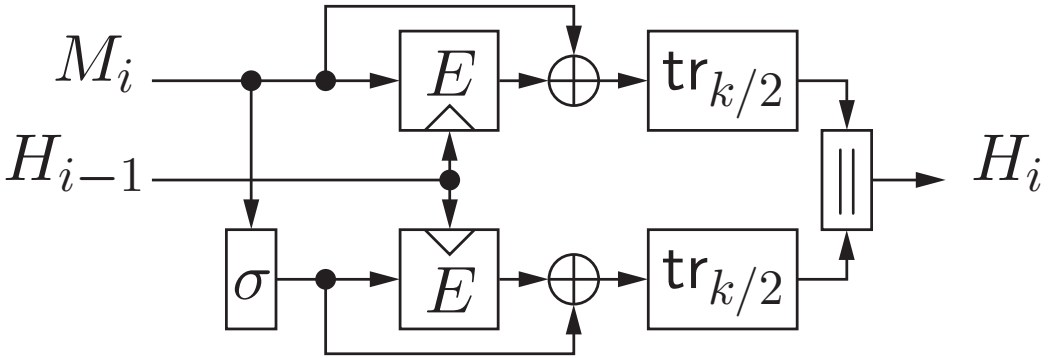


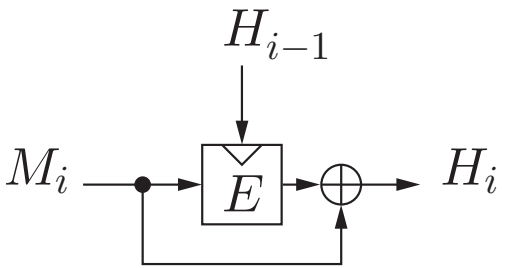
- E is a block cipher with key-size $= 2 \times$ block-size
- $\delta(r) = \delta((a)_2 \| r') = (a + 1 \bmod 4)_2 \| r'$

r	$00\|\|r'$	$01\|\|r'$	$10\|\|r'$	$11\|\|r'$
$\delta(r)$	$01\|\|r'$	$10\|\|r'$	$11\|\|r'$	$00\|\|r'$

Proposed Mode: Modified Jonsson-Robshaw

mJR (or abreast-MMO)





- E is a block cipher with key-size (k) > block-size (n)
- σ is an involution with no fixed points ($\sigma \circ \sigma$ is an identity)
- $\mathrm{tr}_{k/2}$ outputs $k/2$ least significant bits of inputs.

Strong points

- message-block-size $= n$ (irelevant to the key-size)
- Requires a single key expansion
- Message blocks are not fed into the key of E

CR of a Hash Function Using the mJR Mode

Ideal cipher model

For $1 \leq q < 2^{n-1}$, if the number of queries $\leq q$, then

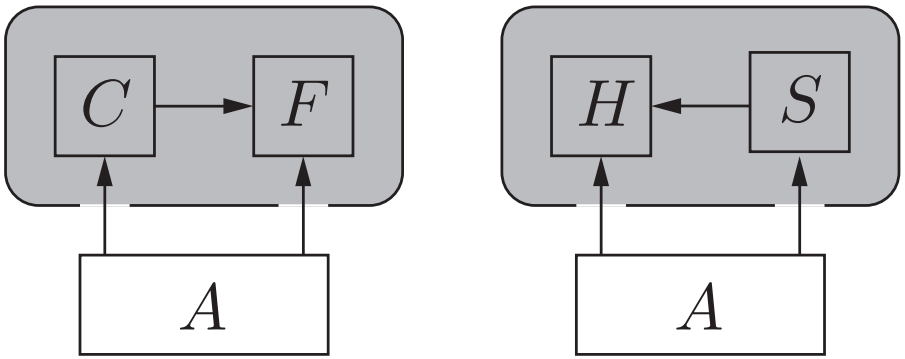
$$\Pr[\text{Finding a collision}] \leq \frac{q}{2^{k/2}(1 - q/2^{n-1})} + \frac{q^2 + 2q}{2^k(1 - q/2^{n-1})^2}$$

The value of q when the right side $= 1/2$:

$$\log_2 q = \begin{cases} 125.7 & \text{if } (n,k) = (128, 256) \\ 94.5 & \text{if } (n,k) = (128, 192) \end{cases}$$

Indifferentiability from RO (IRO)

[Maurer, Renner, Holenstein 04], [Coron, Dodis, Malinaud, Puniya 05]



- H is VIL RO
- F is FIL ideal primitive
  - Ideal block cipher
  - Random oracle

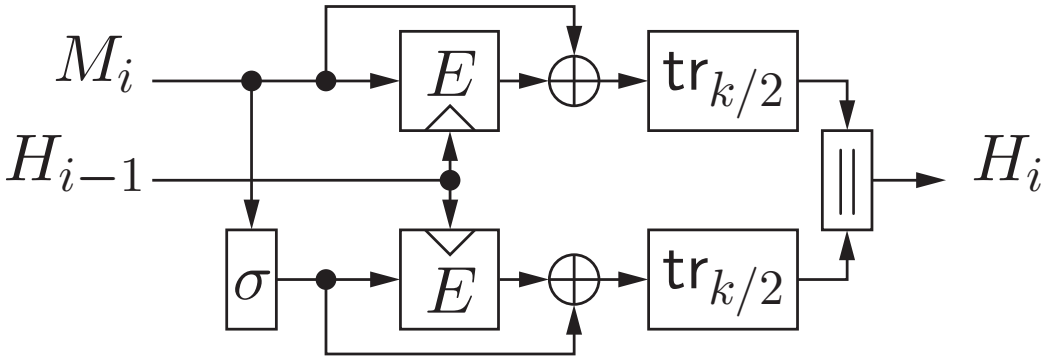
- C is hash function construction using F
- Simulator S tries to mimic F with access to oracle H

Definition

C^F is **indiff. from VIL RO (IRO)** if no efficient adver A can tell apart

$$(\boldsymbol{C^F}, \boldsymbol{F}) \quad \text{and} \quad (\boldsymbol{H}, \boldsymbol{S^H})$$

IRO of a Hash Function Using the mJR Mode



A weak point:

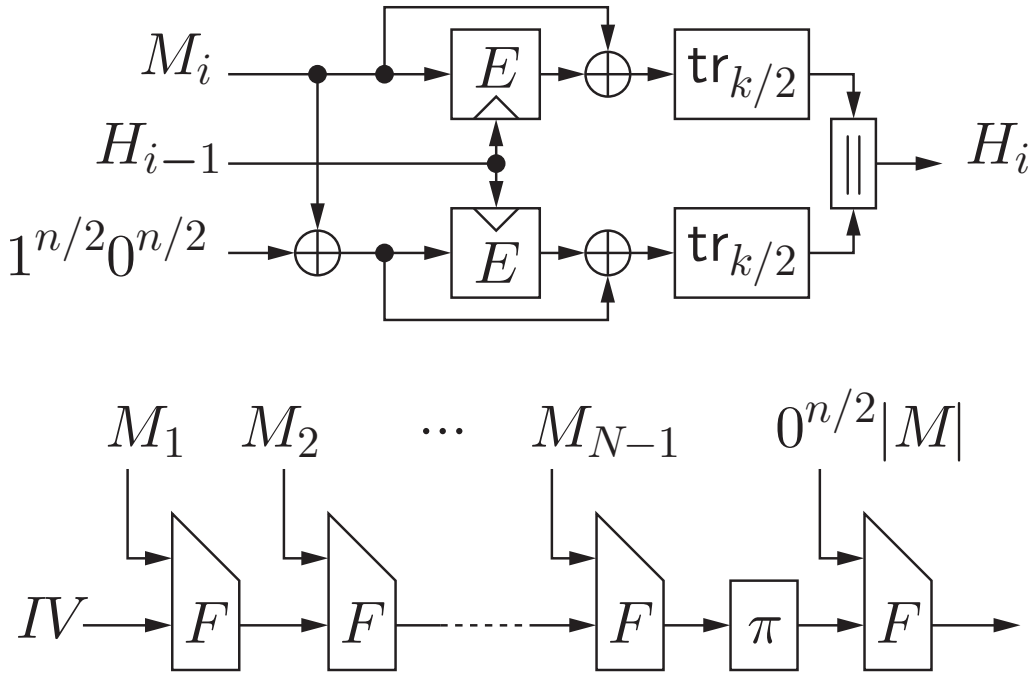
$$F(h_{i-1}, M_i) = h_{i,0} \| h_{i,1} \Rightarrow F(h_{i-1}, \sigma(M_i)) = h_{i,1} \| h_{i,0}$$

Avoidable by proper choices of σ and padding

Domain extension free from length-extension

IRO of a Hash Function Using the mJR Mode

Ideal cipher model



π is a permutation with no (or at most few) fixed points

For $1 \leq q < 2^{n-1}$, if the number of queries $\leq q$, then

$$\Pr[\text{Differentiation}] \leq \frac{1}{2} + O\left(\frac{q}{2^{k/2}}\right)$$

PRF of a Hash Function Using the mJR Mode

keyed-via-IV (KIV) mode

Rel $= \{\phi, \pi, \pi \circ \phi\}$, $\phi(x_{\mathrm{L}} \| x_{\mathrm{R}}) = x_{\mathrm{R}} \| x_{\mathrm{L}}$.

Let A be a prf-adversary against the KIV mode.

- runs in time at most t,
- makes at most q queries ($q \leq \alpha 2^n/\mathrm{e}$ for some const $0 < \alpha < 1$),
- each query has at most ℓ message blocks.

Then, there exists a prp-rka-adversary B against E such that

$$\mathrm{Adv}^{\mathrm{prf}}_{F^{\circ}_{\pi}}(A) \leq \ell q \cdot \mathrm{Adv}^{\text{prp-rka}}_{\mathsf{Rel},E}(B) + \frac{\ell\, 2^{k/2}}{1-\alpha}\left(\frac{\mathrm{e}\, q}{2^n}\right)^{2^{n-k/2}+1} .$$

B makes at most q queries restricted by Rel and runs in time at most $t + O(\ell q T_E)$.

Conclsion

- mJR: MMO-type double-block compression function
- Security of a hash function using mJR and MDP
  - Collision resistance
  - Indifferentiability from a random oracle
  - PRF