Provable Security of Cryptographic Hash Functions

Mohammad Reza Reyhanitabar

Centre for Computer and Information Security Research
University of Wollongong
Australia

Outline

- **Introduction**
- **Security Properties of Hash Functions**
- **Hash Functions with a Security Proof**
  - Provable Security in Idealized Models
    - Block cipher/permutation-based constructions
  - Provable Security in the Standard Model
    - Constructions based on general complexity-theoretic assumptions
    - Constructions based on specific number-theoretic assumptions
  - Dual-Model Provable Security
    - Mix-Compress-Mix (MCM) [Ristenpart and Shrimpton, Asiacrypt 2007]
    - Multi-Property Combiners [Fischlin, Lehmann and Pietrzak, ICALP 2008]
    - Improved MCM [Lehmann and Tessaro, Asiacrypt 2009]
    - FIL MCM with invertible permutations [Reyhanitabar and Susilo, ePrint 2012]
- **Conclusion**

Introduction

Two Settings for Hash Functions

1. Keyless Setting: $H : \mathcal{M} \rightarrow \mathcal{C}$

   - Examples:
     - ★ SHA-1 : $\{0,1\}^{<2^{64}} \rightarrow \{0,1\}^{160}$
     - ★ Some SHA-3 finalists: JH, Keccak, Grøstl

2. Dedicated-key Setting (Family of Functions): $\mathcal{H} : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}$

   A member of the family is chosen by a key (index or salt) $K \in \mathcal{K}$ and is a function $H \triangleq \mathcal{H}_K : \mathcal{M} \rightarrow \mathcal{C}$

   - Examples:
     - ★ CRHF family (Damgård, CRYPTO 1987)
     - ★ UOWHF family (Naor and Yung, STOC 1989)
     - ★ VSH (Contini et al., EUROCRYPT 2006)
     - ★ Some SHA-3 finalists: Blake, Skein

Note: Keying a keyless hash function is not a trivial task unless the hash function or its components are assumed to be “ideal” (random function/permutation).

Two-step paradigm for constructing a hash function

1. Construct a compression function capable of hashing fixed-length messages

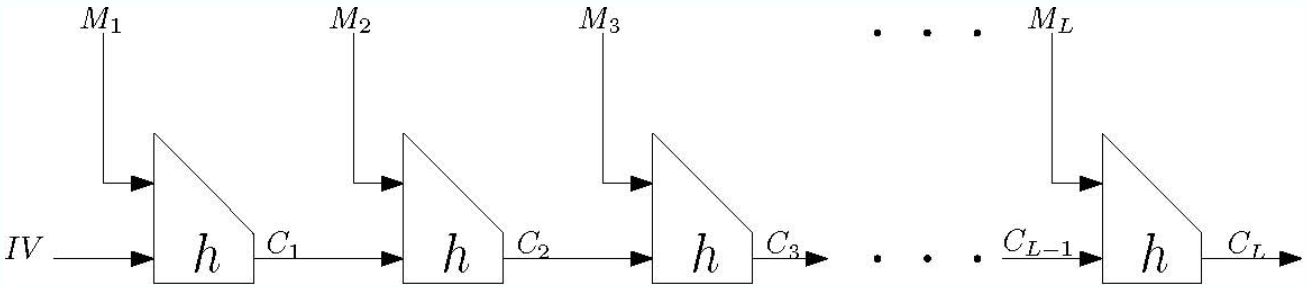
2. Apply a domain extension transform (a.k.a. mode of operation) to build the full-fledged hash function capable of hashing messages of variable length

- Hash Domain Extension: '**Padding**' + '**Iteration**'

Merkle-Damgård (MD) Construction

Merkle-Damgård Transforms:

- Padding:
  - Plain
  - MD Strengthening (length indicating or suffix-free)
  - Prefix-free (Coron et al., 2005)
  - Split (Yasuda, 2008)
  - HAIFA (Biham and Dunkelman, 2007)
- Iteration:



Security Properties of Hash Functions

Security Notions for keyless hash functions $H : \mathcal{M} \rightarrow \{0,1\}^n$

***Definitions of Conventional Properties*:**

- **Collision Resistance**

  Informal: Finding two distinct messages *M* and *M'* such that *H*(*M*)=*H*(*M'*) must be "hard" ("infeasible").

  Formal: ! "foundations-of-hashing dilemma".

  For any compressing function there always **exist** collisions, and hence, there **exists an efficient adversary** that can output a colliding pair; namely, the one that has a colliding pair hardwired in, but **nobody knows** the description of such an efficient algorithm for a good hash function! (Human Ignorance) [Rogaway, VIETCRYPT 2006]

- **Second-Preimage Resistance**

  Informal: Given a message *M*, finding a different message *M'* such that *H*(*M*)=*H*(*M'*) must be "hard".

  Formal: $\mathrm{Adv}_H^{SPR[\delta]}(A) = \Pr\left\{M \xleftarrow{\$} \{0,1\}^{\delta}\ ;\ M' \xleftarrow{\$} A(M) :\ M \neq M' \ \wedge\ H(M) = H(M')\right\}$

- **Preimage Resistance**

  Informal: Given a hash value C, finding a message M such that H(M)=C must be "hard".

  Formal (1): $\mathrm{Adv}_H^{PR[\delta]}(A) = \Pr\left\{M \xleftarrow{\$} \{0,1\}^{\delta}\ ;\ C \leftarrow H(M);\ M' \xleftarrow{\$} A(C) :\ H(M') = C\right\}$

  Formal (2): $\mathrm{Adv}_H^{PR^*}(A) = \Pr\left\{C \xleftarrow{\$} \{0,1\}^{n}\ ;\ M' \xleftarrow{\$} A(C) :\ H(M') = C\right\}$

  If the hash function is regular then these two **variants of the one-way property** are the same.

Security Notions for dedicated-key hash functions

Rogaway and Shrimpton (FSE 2004) showed that, for a dedicated-key hash function, formalization of the three basic security properties may yield to seven different security notions.

Experiments used for defining the properties:

- Collision Resistance (**Coll**)

$$\{\mathbf{K} \xleftarrow{\$} \mathcal{K};\ (\mathbf{M}, \mathbf{M}') \xleftarrow{\$} \mathbf{A}(\mathbf{K}) :\ \mathbf{M} \neq \mathbf{M}' \ \wedge\ \mathcal{H}_{\mathbf{K}}(\mathbf{M}) = \mathcal{H}_{\mathbf{K}}(\mathbf{M}')\}$$

- Second-Preimage Resistance
  - **Sec**

$$\{\mathbf{K} \xleftarrow{\$} \mathcal{K};\ \mathbf{M} \xleftarrow{\$} \{\mathbf{0},\mathbf{1}\}^{\delta};\ \mathbf{M}' \xleftarrow{\$} \mathbf{A}(\mathbf{K}, \mathbf{M}) :\ \mathbf{M} \neq \mathbf{M}' \ \wedge\ \mathcal{H}_{\mathbf{K}}(\mathbf{M}) = \mathcal{H}_{\mathbf{K}}(\mathbf{M}')\}$$

  - **aSec**

$$\{(\mathbf{K}, \mathbf{State}) \xleftarrow{\$} \mathbf{A_1}();\ \mathbf{M} \xleftarrow{\$} \{\mathbf{0},\mathbf{1}\}^{\delta};\ \mathbf{M}' \xleftarrow{\$} \mathbf{A_2}(\mathbf{M}, \mathbf{State}) :\ \mathbf{M} \neq \mathbf{M}' \ \wedge\ \mathcal{H}_{\mathbf{K}}(\mathbf{M}) = \mathcal{H}_{\mathbf{K}}(\mathbf{M}')\}$$

  - **eSec**

$$\{(\mathbf{M}, \mathbf{State}) \xleftarrow{\$} \mathbf{A_1}();\ \mathbf{K} \xleftarrow{\$} \mathcal{K};\ \mathbf{M}' \xleftarrow{\$} \mathbf{A_2}(\mathbf{K}, \mathbf{State}) :\ \mathbf{M} \neq \mathbf{M}' \ \wedge\ \mathcal{H}_{\mathbf{K}}(\mathbf{M}) = \mathcal{H}_{\mathbf{K}}(\mathbf{M}')\}$$

- Preimage Resistance
  - **Pre**

$$\{\mathbf{K} \xleftarrow{\$} \mathcal{K}; \mathbf{M} \xleftarrow{\$} \{\mathbf{0},\mathbf{1}\}^{\delta}; \mathbf{Y} \leftarrow \mathcal{H}_{\mathbf{K}}(\mathbf{M});\ \mathbf{M}' \xleftarrow{\$} \mathbf{A}(\mathbf{K}, \mathbf{Y}) :\ \mathcal{H}_{\mathbf{K}}(\mathbf{M}') = \mathbf{Y}\}$$

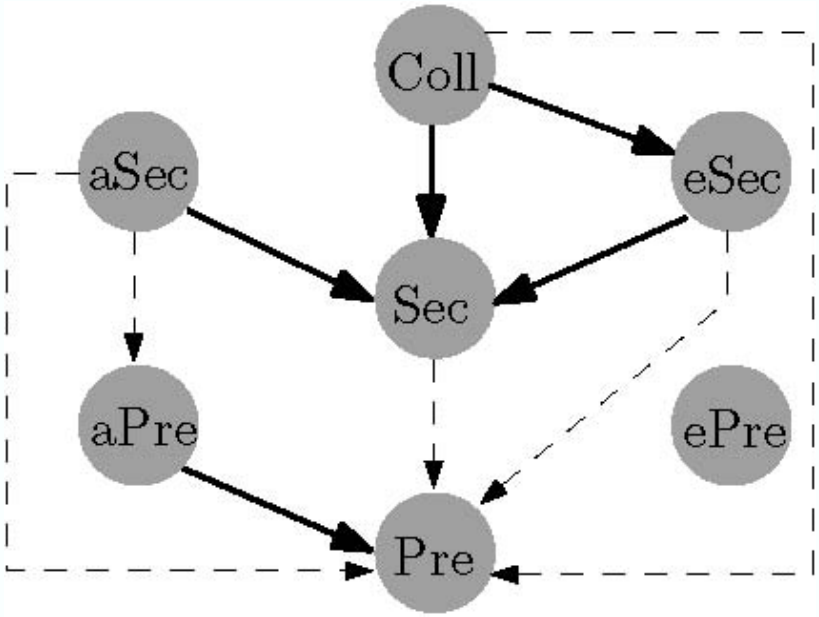
  - **aPre**

$$\{(\mathbf{K}, \mathbf{State}) \xleftarrow{\$} \mathbf{A_1}();\ \mathbf{M} \xleftarrow{\$} \{\mathbf{0},\mathbf{1}\}^{\delta};\ \mathbf{Y} \leftarrow \mathcal{H}_{\mathbf{K}}(\mathbf{M});\ \mathbf{M}' \xleftarrow{\$} \mathbf{A_2}(\mathbf{Y}, \mathbf{State}) : \mathcal{H}_{\mathbf{K}}(\mathbf{M}') = \mathbf{Y}\}$$

  - **ePre**

$$\{(\mathbf{Y}, \mathbf{State}) \xleftarrow{\$} \mathbf{A_1}();\ \mathbf{K} \xleftarrow{\$} \mathcal{K};\ \mathbf{M}' \xleftarrow{\$} \mathbf{A_2}(\mathbf{K}, \mathbf{State}) : \mathcal{H}_{\mathbf{K}}(\mathbf{M}') = \mathbf{Y}\}$$

Relations among the seven security notions



[Rogaway and Shrimpton, FSE 2004]

(This figure is the revised version from ePrint 2004/035)

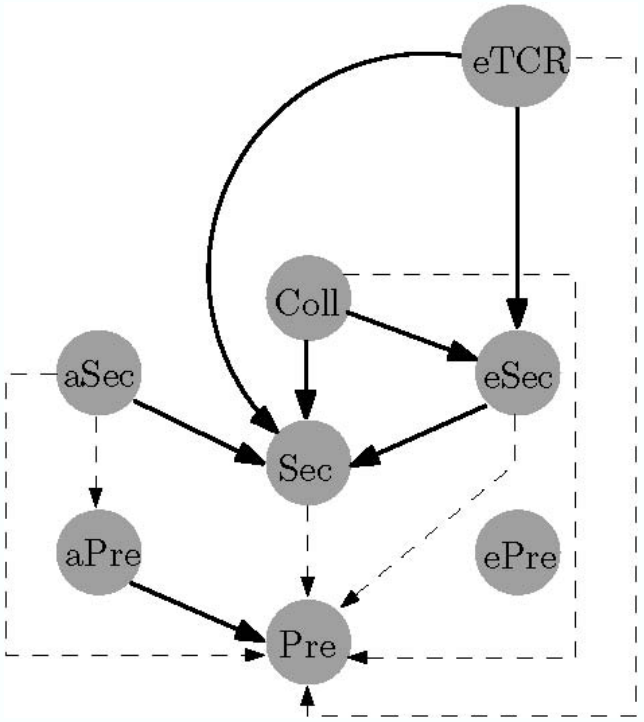
Enhanced Target Collision Resistance (eTCR)

Definition [Halevi and Krawczyk, Crypto 2006]

$$\mathrm{Adv}_{\mathcal{H}}^{eTCR}(A) = \Pr\left\{ \begin{array}{ll} (M, State) \xleftarrow{\$} A_1(); & \\ K \xleftarrow{\$} \mathcal{K}; & : (K, M) \neq (K', M') \ \wedge \ \mathcal{H}_K(M) = \mathcal{H}_{K'}(M') \\ (K', M') \xleftarrow{\$} A_2(K, State); & \end{array} \right\}$$

New relations

[Reyhanitabar, Susilo and Mu, FSE 2009 and ePrint 2009/506)]



Enhanced Collision Resistance (eColl)

Definition [Yasuda, Asiacrypt 2008]

$$\mathrm{Adv}_{\mathcal{H}}^{eColl}(A) = \Pr\left\{K \xleftarrow{\$} \mathcal{K}; (K', M', M) \xleftarrow{\$} A_2(K, State) : (K, M) \neq (K', M') \ \wedge \ \mathcal{H}_K(M) = \mathcal{H}_{K'}(M')\right\}$$

Some of the relations (in the complexity-theoretic sense) between eColl and other properties were considered by Yasuda [Asiacrypt 2008].

Enhanced (Strengthened) variants of the other properties

1. Strengthened "Coll": s-Coll (= "eColl")
2. Strengthened "Sec": s-Sec
3. Strengthened "aSec": s-aSec
4. Strengthened "eSec": s-eSec (= "eTCR")
5. Strengthened "Pre": s-Pre
6. Strengthened "aPre": s-aPre
7. Strengthened "ePre"? 

Definitions

The s-XXX property, for $\mathrm{XXX} \in \{\mathbf{Coll}, \mathbf{Sec}, \mathbf{aSec}, \mathbf{eSec}, \mathbf{Pre}, \mathbf{aPre}\}$ is defined by modifying the game that defines the XXX property, s.t. the adversary gets to choose a second key, possibly different from the first key, and the success event is defined accordingly.

$$\mathrm{Adv}_H^{\text{s-Sec}[\delta]}(A) = \Pr\left[\begin{array}{l} K \xleftarrow{\$} \mathcal{K}; M \xleftarrow{\$} \{0,1\}^\delta; \\ K', M' \xleftarrow{\$} A(K, M) \quad : \ (K, M) \neq (K', M') \ \wedge \ H_K(M) = H_{K'}(M') \end{array}\right]$$

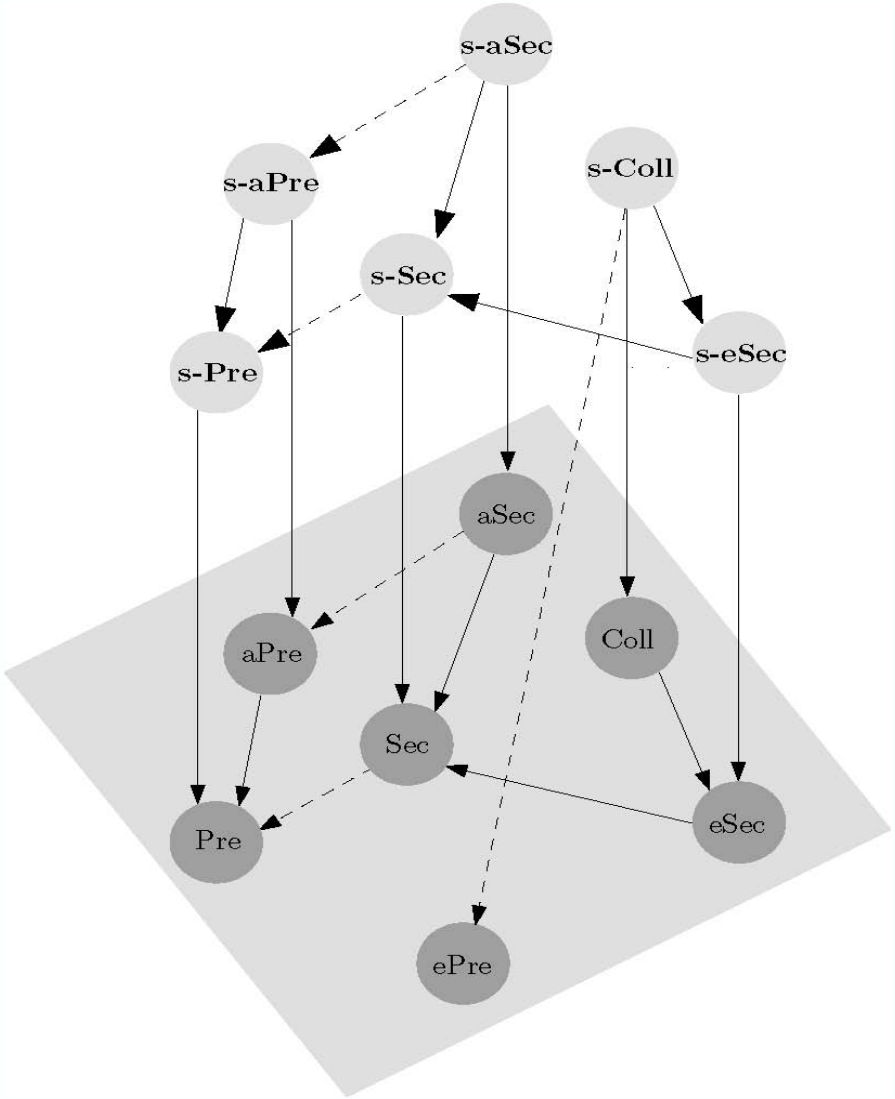
$$\mathrm{Adv}_H^{\text{s-aSec}[\delta]}(A) = \Pr\left[\begin{array}{l} (K, State) \xleftarrow{\$} A_1(); \\ M \xleftarrow{\$} \{0,1\}^\delta; \\ K', M' \xleftarrow{\$} A_2(M, State) \quad : \ (K, M) \neq (K', M') \ \wedge \ H_K(M) = H_{K'}(M') \end{array}\right]$$

$$\mathrm{Adv}_H^{\text{s-Pre}[\delta]}(A) = \Pr\left[\begin{array}{l} K \xleftarrow{\$} \mathcal{K}; M \xleftarrow{\$} \{0,1\}^\delta; Y \leftarrow H_K(M); \\ K', M' \xleftarrow{\$} A(K, Y) \quad : \quad H_{K'}(M') = Y \end{array}\right]$$

$$\mathrm{Adv}_H^{\text{s-aPre}[\delta]}(A) = \Pr\left[\begin{array}{l} (K, State) \xleftarrow{\$} A_1(); \\ M \xleftarrow{\$} \{0,1\}^\delta; Y \leftarrow H_K(M); \\ K', M' \xleftarrow{\$} A_2(Y, State) \quad : \quad H_{K'}(M') = Y \end{array}\right]$$

Extended relations among the thirteen security notions

(Reyhanitabar, Susilo and Mu, FSE 2010)



Hash functions with a "security" proof

Provable Security in Idealized Models

Block Cipher-based Compression Functions

$E : \{0,1\}^k \times \{0,1\}^m \rightarrow \{0,1\}^m$

$H^E : \{0,1\}^{n_i} \rightarrow \{0,1\}^n$; where $n < n_i$

Rate (measure of efficiency): $r = \dfrac{n_i - n}{(\#\ \text{calls to}\ E\ \text{in}\ H^E) \times m}$

Single-Block-Length (SBL) Constructions: $n=m$

Double-Block-Length (DBL) Constructions: $n=2m$

Provable security (collision resistance and preimage resistance) of block cipher-based hash functions from PGV

[Preneel, Govaerts and Vandewalle, Crypto'93] provided an attack-based analysis of 64 block cipher-based compression functions.

[Black, Rogaway and Shrimpton, Crypto'02] proved collision resistance and preimage resistance bounds in the **ideal cipher model**. Among the 64 PGV constructions:

- 12 compression functions are optimally CR and PR*
- 8 compression functions yield to provably CR and PR* (only up to the birthday limit) MD iterated hash functions, despite the compression functions themselves being invertible and hence not CR.

[Stam, FSE'09] revisited the constructions and provided generalized classification and refined proofs.

[Black, Rogaway, Shrimpton and Stam, Journal of Cryptology, Vol 23, No. 4, 2010] put the previous results together and provided refined proofs.

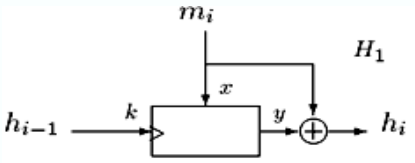
12 provably secure SBL compression functions from PGV

[Black et al., *Journal of Cryptology*, Vol. 23, No. 4, 2010]

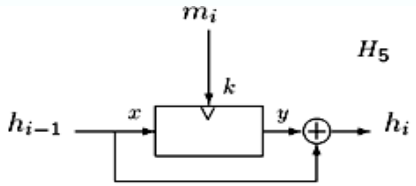
Bounds:

CR : $\Theta(\frac{q^2}{2^n})$

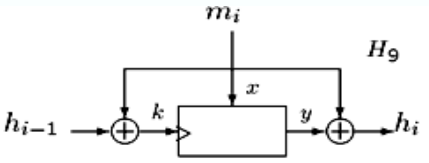
PR* : $\Theta(\frac{q}{2^n})$

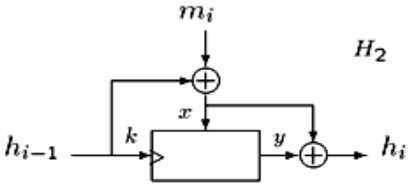


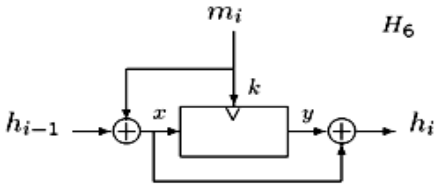
Matyas-Meyer-Oseas

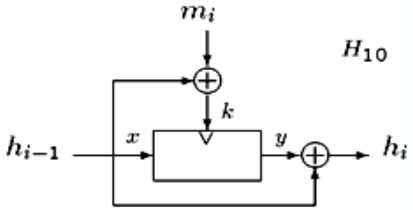


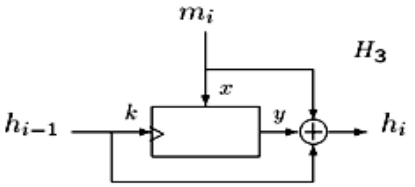
Davies-Meyer



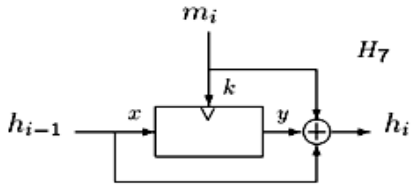


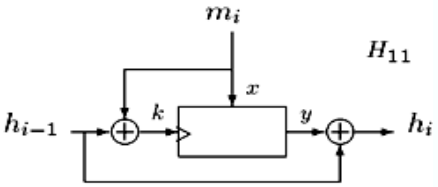


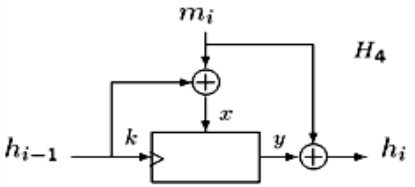


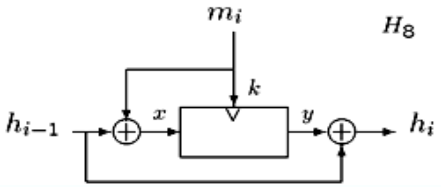


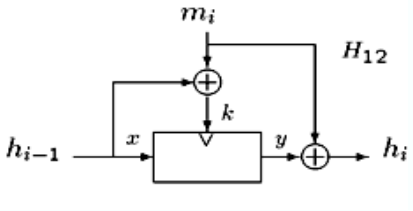
Miyaguchi-Preneel





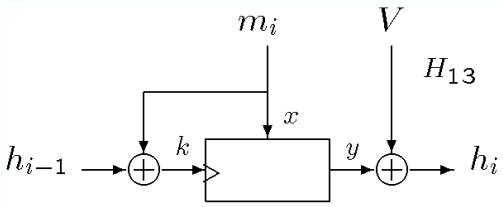


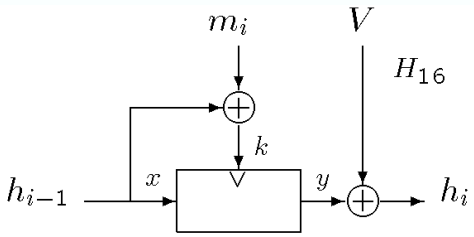


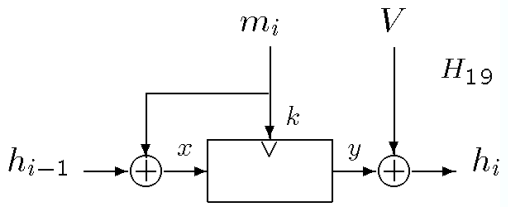


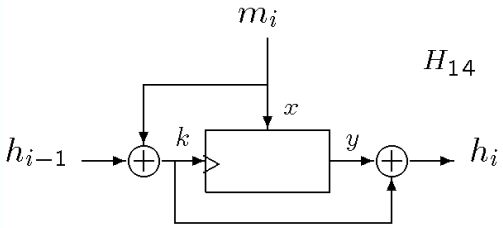
8 compression functions that are not collision resistant (CR) but become CR when MD iterated

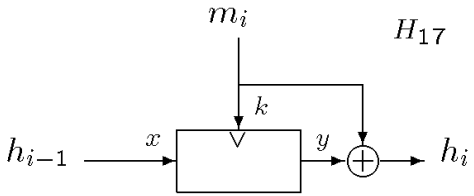
[Black et al., *Journal of Cryptology*, Vol. 23, No. 4, 2010]

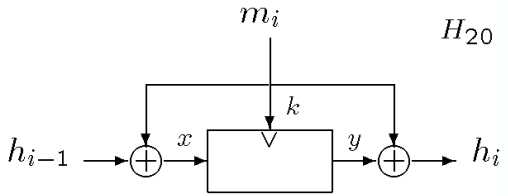


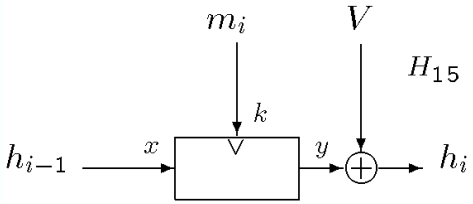




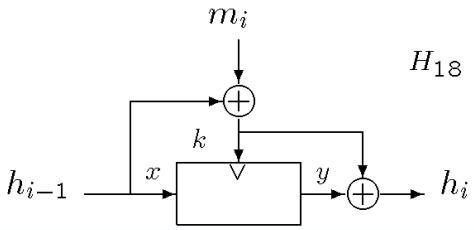








Rabin, 1978



Bounds for MD itetaed hash functions:

$$\mathrm{CR} : \Theta\left(\frac{q^2}{2^n}\right)$$

$$\mathrm{PR}^* : \Theta\left(\frac{q^2}{2^n}\right)$$

PGV hash functions are **SBL**, i.e. the hash length, n, is equal to the block length, m.

If the key and block lengths of the block cipher are the same then these are **rate 1** constructions.

Two issues with SBL constructions:

I. The CR bound for the 8 **optimally secure** SBL constructions from PGV are proved up to the birthday limit ($q^2/2^n$).

Is this an issue? Well, if one insists on using a standard block cipher with relatively small block length (e.g. AES with m=128) then he/she would not get a satisfactory security level against highly resourced adversaries.

This has been a motivation for constructing DBL hash functions where $n=2m$.

II. **Rekeying the block cipher**: secure PGV constructions requires rekeying the block cipher in each iteration. Key scheduling in a block cipher can be quite expensive.

This has been a motivation for designing fixed-key block cipher (random permutation)-based constructions.

Security Analysis of DBL Constructions:

Some key results (the list is not exhaustive)

[Hirose, ICISC'04] provided a rate-1/2 DBL construction with optimal CR bound.

[Fleischmann et al., FSE'09] analysed collision resistance of Abreast-DM and Tandem-DM constructions.

[Özen and Stam, IMA Int. Conf. 2009] studied a large class of DBL constructions.

[Stam, FSE 2009] provided a rate-1 compression function with optimal CR up to a logarithmic factor.

[Lee et al., Crypto 2011] reconsidered Tandem-DM and showed that the analysis of [Fleischmann et al., FSE'09] was incorrect and provided a new analysis for the collision security of Tandem-DM

[Armknecht et al., Asiacrypt 2011] presented new techniques for deriving preimage resistance bounds for DBL constructions and improved bounds for Abreast-DM, Tandem-DM, and Hirose's construction.

Constructions from non-compressing primitives:

Some key results (the list is not exhaustive)

[Black et al. Eurocrypt'05, JoC 2009]: impossibility of "highly-efficient" (rate-1 and fixed-key) block-cipher based hash functions

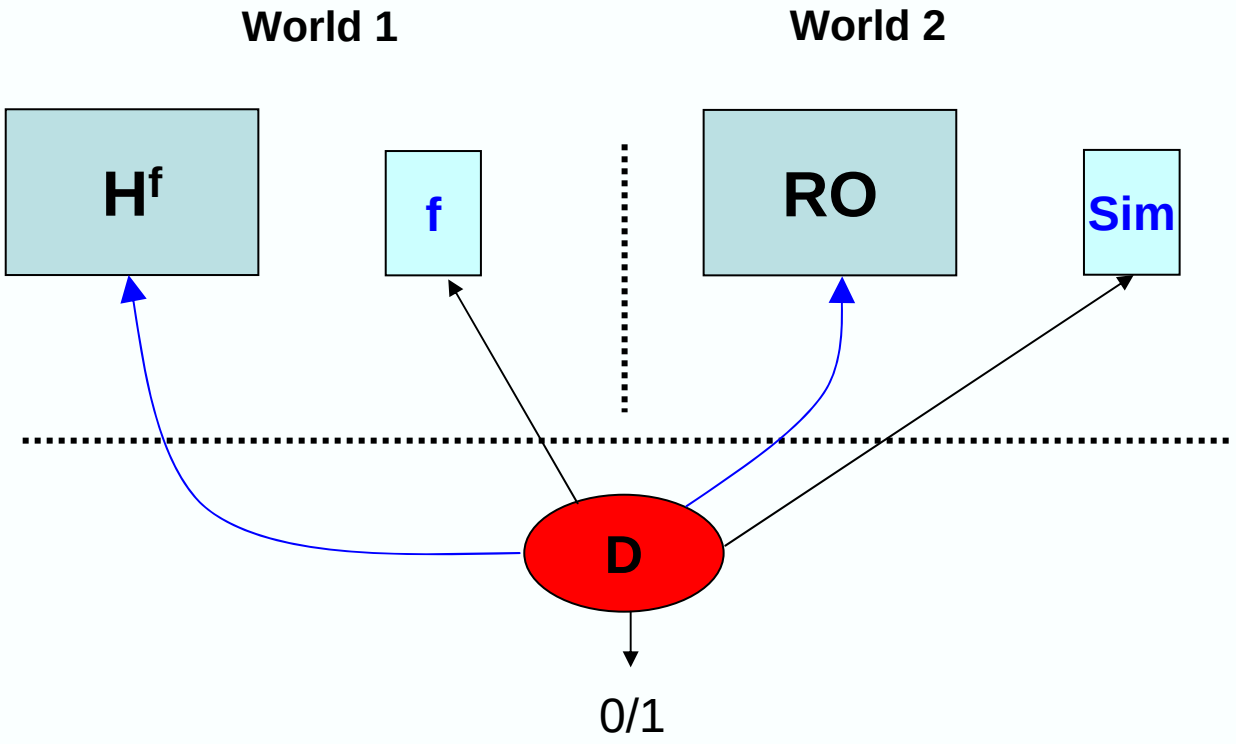
[Rogaway and Steinberger, Crypto'08], [Shrimpton and Stam, ICALP'08], [Stam, Crypto 2008]: possibility of constructing secure (lower rate) compression functions from non-compressing primitives.

SHA-3 candidates: Keccak, JH, Grøstl

Indifferentiability

[Maurer et al., TCC'04]

[Coron et al., Crypto'05]



Simulator, Sim, tries to make World 2 indistinguishable from World 1 from the viewpoint of D by simulating the answers to f-queries in World 1.

Pseudorandom Oracle (PRO): if $\exists$ Sim s.t. $\forall$ D the distinguishing advantage is negligible then H^f is called a PRO.

Composition Theorem [Maurer et al., TCC'04]:

Iff **H** is indifferentiable from **R** then in **any cryptosystem C** that is **secure** when using **R** as a component, one can securely replace R with H (i.e. the system C using H will be as secure as the system C using R).

[Ristenpart et al., Eurocrypt'11]:

"**Careful with composition**"! Maurer et al.'s composition theorem does not apply to "any cryptosystem" with an arbitrary "security" notion! It is only correct if one considers a cryptosystem C whose security is defined via a single-stage adversarial game.

Reset Indifferentiability: an extension to the indifferentiabilty notion to make the composition theorem work for cryptosystems whose security is defined via multi-stage games. (The simulator must function even under resets by the adversary during a multi-stage game.)

This requires revisiting the notion of PRO!

Open Problem:

How to construct a PRO (even an "inefficient" one) in the sense of reset-indifferentiability?

Provable "security" in the **standard model**

Constructions based on "**general**" complexity-theoretic assumptions:

[Damgard, Eurocrypto'87 and Crypto'89] proved that given a family of **claw-free permutations**, one can *construct* a family of **collision resistant** (CR) hash functions.

– Concrete candidates for claw-free permutations can be built with a security reduction from **factorization** or **discrete logarithm** problems.

[Naor and Yung, STOC'89] introduced **UOWHF** (a security notion weaker than CR) and proved that given a **one-way permutation**, one can construct a UOWHF family.

[Rompel, STOC'90]: **One-way function** ⟺ **UOWHF**

– *Corollary*: One-way function ⟺ Digital Signatures

• **These general constructions are quite inefficient for practical applications.**

Constructions based on "**specific**" (number-theoretic) assumptions:

[Pointcheval, PKC'00], [Shamir and Tauman Crypto'01]: **factorization based CR function**

$$H(m) = x^m \bmod n$$

Inefficient: requires on average 1.5 multiplications modulo *n* per message bit.

More efficient constructions:

VSH: [Contini et al., Eurocrypt'06] introduced a new number-theoretic hardness assumption, "**VSSR**", and provided an MD iterated hash function that is provably CR based on the VSSR assumption.

VSSR assumption: finding a nontrivial modular **square root of very smooth number** modulo *n* is hard.

SWIFFT [Lyubashevsky et al., FSE'08]: a provably CR function based on the assumption that finding short vectors in cyclic/ideal lattices is hard.

SWIFFTX: a hash function, using SWIFFT as its core, proposed for SHA-3 competition but was not selected for the second round.

Sigma-Hash: [Bellare and Ristov, Asiacrypt'08] showed that any "suitable" Sigma protocol can be converted to a provably CR (chameleon) hash function.

VSH*: a sigma hash function that improves the performance of VSH on short messages.

Although these specific constructions (VSH, SWIFFT, Sigma-Hash) are more efficient than the general constructions, they still suffer from several issues when considered for **general-purpose** hashing in practice:

- **cannot provide the ideal security levels of $O(2^{n/2})$ and $O(2^n)$ for the CR and PR properties, respectively, as expected from an *n*-bit practical hash function; hence, they have longer hash length compared to practical hash functions,**
- **less efficient than most of practical hash functions,**
- **VSH and Sigma-Hash type functions are chameleon (trapdoor) hash functions,**
- **The compression function of VSH is not CR, and iterated VSH hash function is easily invertible for short and some sparse messages,**
- **SWIFFT is a linear function.**

Suggestion:

These functions should be called provably collision-resistant functions, rather than "provably secure hash functions"!

Dual-model provable security

- **Hash functions with proven security bounds in an idealized model** (e.g. in the ideal cipher model or the random function/permutation models) do not provide any "provable" security guarantee against arbitrary adversaries who do not consider the primitives as black-boxes in the real world (i.e., outside the "ideal" model for the primitives in which a proof is given, the security becomes unclear).

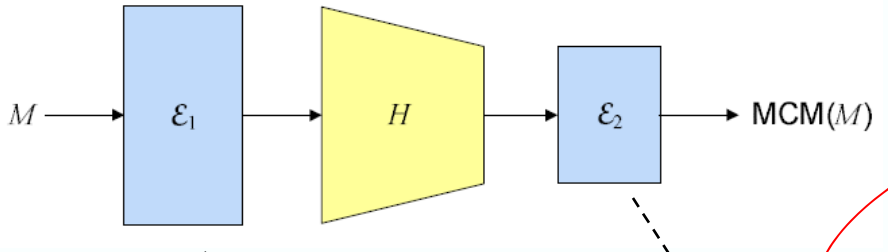
- **Hash functions with a security reduction in the standard model** are usually highly structured, only guarantee specific properties (e.g. CR), and deviate from "random behaviour"; hence, inappropriate for general-purpose hashing in practice, particularly, for instantiation of random oracles.

- **Problem**:

  How to design a Dual-Model Secure (DMS) hash function; that is, a hash function which is simultaneously provable secure (particularly CR) in the standard model and provably PRO (indifferentiable from a random oracle) in an idealized model?

Mix-Compress-Mix

[Ristenpart and Shrimpton, Asiacrypt 2007]



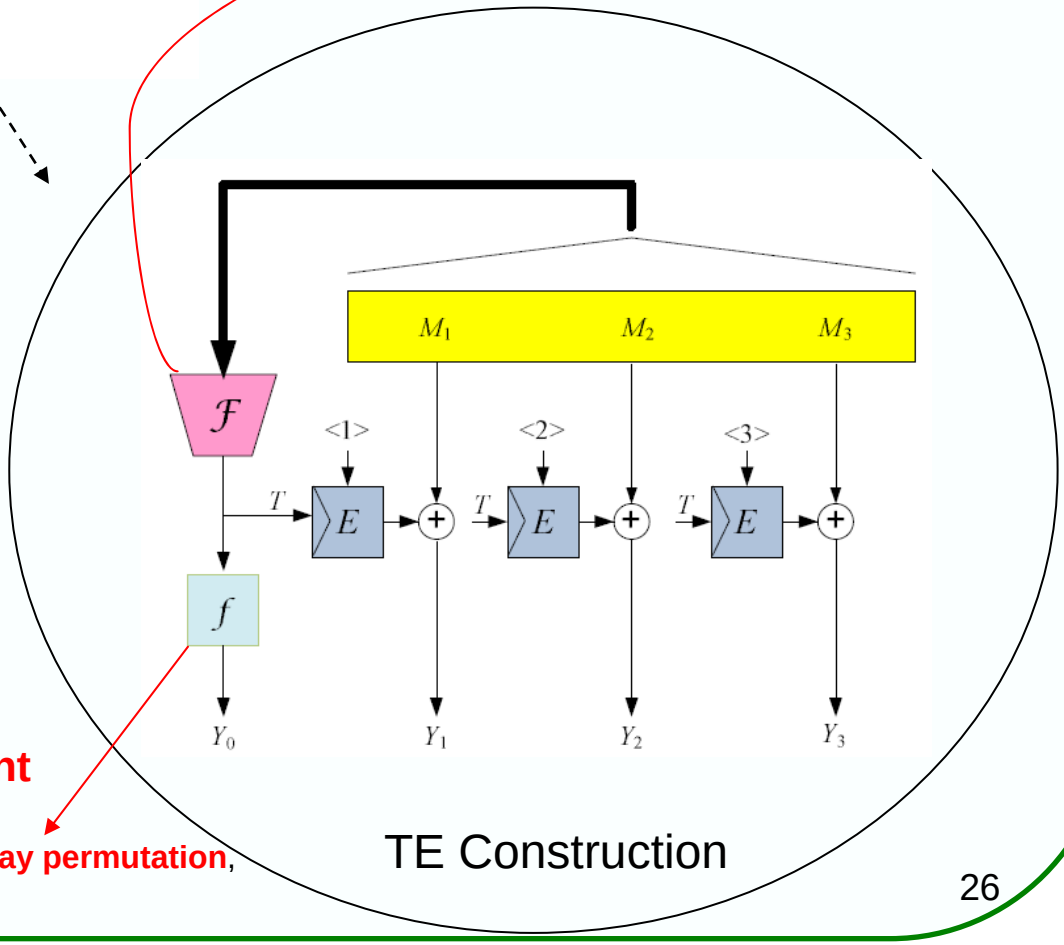
random oracle

***H*:** a full-fledged (iterated) hash function that is provably CR in the standard model

ε_1 and ε_2:
non-invertible random injection oracles

How to instantiate "non-invertible" random injection oracles?

TE: proof-of-concept, but quite **inefficient**



TE Construction

trapdoor one-way permutation, (e.g. RSA)

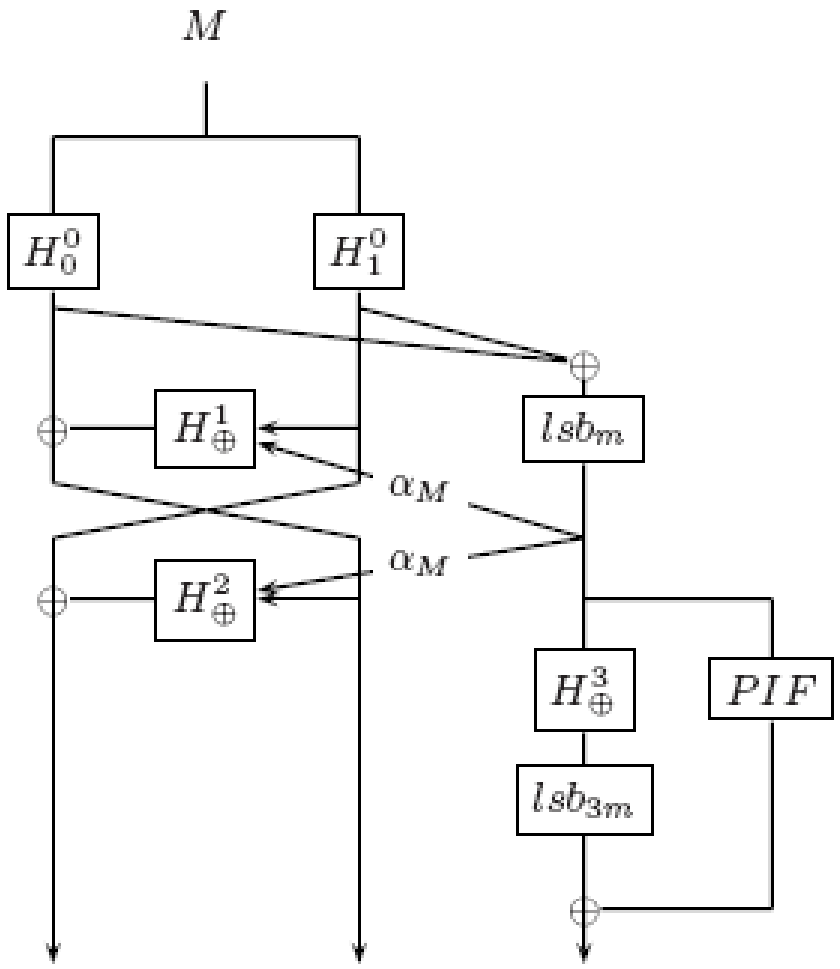
DMS hash using a multi-property combiner for hash functions

[Fischlin, Lehmann and Pietrzak, ICALP 2008]

H_0 and H_1 are two n-bit hash functions.

$H_b^i(.) = H_b(\langle i \rangle_2 \,||.)$

$H_\oplus^i(.) = H_0^i(.) \oplus H_1^i(.)$



Inefficient DMS:

requires 8 calls to its underlying two hash functions.

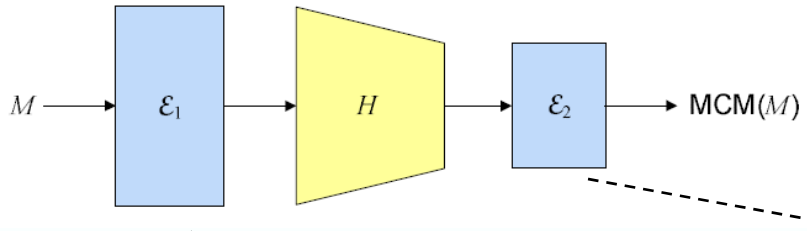
$2n \leq$ hash length $\leq 3n$

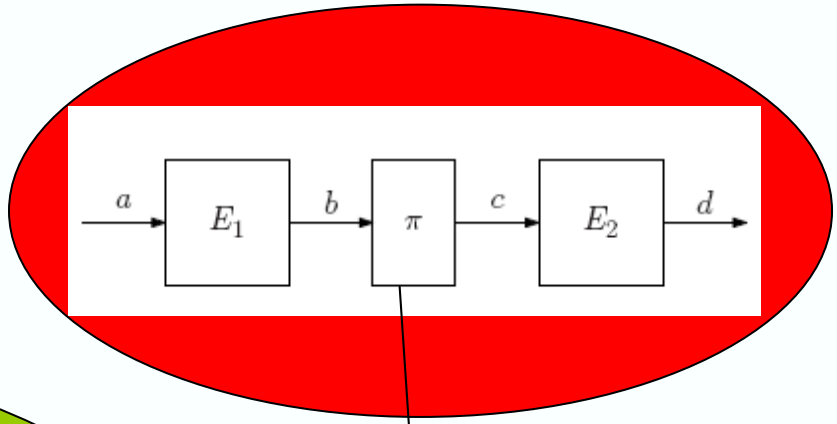
PRO bound: $\frac{3q^2}{2^m}$ where $m \leq n/3$

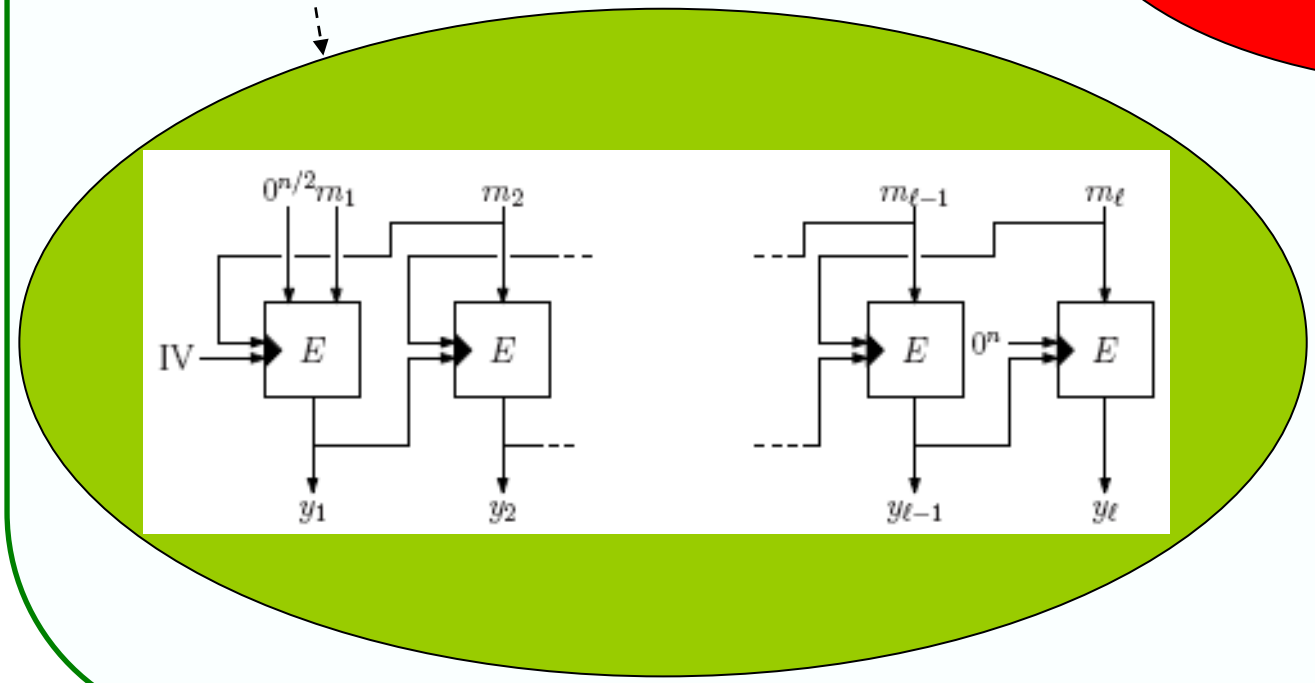
$C_{4P\&IRO}$

Improved MCM

[Lehmann and Tessaro, Asiacrypt 2009]







one-way permutation!
causing implementation issues

[Lehmann-Tessaro, Asiacrypt 2009]

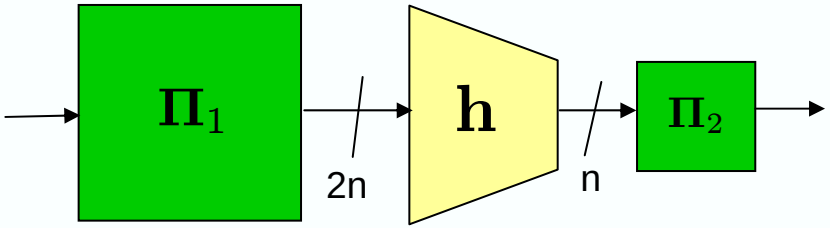
MCM with random "invertible" permutations

[Reyhanitabar and Susilo, ePrint 2012/479]

Classical two-step design paradigm:

Step 1: Build an efficient DMS compression function, i.e. a "fixed-input-length" (**FIL**) DMS hash function.

FIL MCM using invertible random permutations Π_1 and Π_2 for the mixing stages:



Step 2: Use an efficient multi-property-preserving (MPP) domain extender to build a full-fledged (variable-input-length) DMS hash function; e.g. use HAIFA or any other off-the-shelf MPP transform.

Conclusion

"If it's provably secure, it's probably not." – Lars Knudsen

- **A great deal of effort spent on proving bounds for the collision resistance and preimage resistance properties of block cipher/permutation based hash constructions in the idealized models (ideal cipher/random permutation models).**
  - **idealized world: Adversaries cannot look into the structural properties of the underlying primitives and if they could, they should promise not to use any of those properties for attacking the construction!**

- **Provably CR functions (VSH, SWIFFT, Sigma-Hash, ...) with a security reduction to hard problems are highly structured and inappropriate for practical multi-purpose hashing.** ☹

- **Can DMS hashing be made practical?**

  Maybe, but still needs further research. Also, it will only guarantee indifferentiability from a random oracle not reset-indifferentiability from a random oracle!

Thank You!

Acknowledgement:
Mohammad Reza Reyhaniatbar is supported by the NSFC Research Fund for International Young Scientists under Grant 61150110483.