Provable Security of BLAKE with Non-Ideal Compression Function

Elena Andreeva, Atul Luykx, and Bart Mennink (KU Leuven)

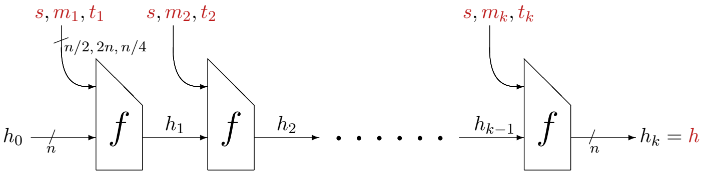
Selected Areas in Cryptography
Windsor, Canada

August 17, 2012

BLAKE

$$\mathcal{H} : \{0,1\}^{n/2} \times \{0,1\}^* \to \{0,1\}^n$$
$$\mathcal{H}(s, M) = h$$

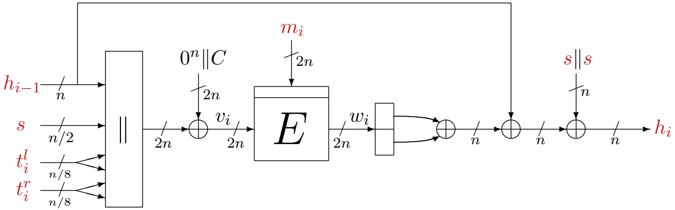
- SHA-3 finalist
- HAIFA design
- $m_1, \ldots, m_k$ padded message blocks of $2n$ bits
- $t_1, \ldots, t_k$ HAIFA-counter blocks of $n/4$ bits



BLAKE

$$f : \{0,1\}^n \times \{0,1\}^{n/2} \times \{0,1\}^{2n} \times \{0,1\}^{n/4} \rightarrow \{0,1\}^n$$
$$f(h_{i-1}, s, m_i, t_i) = h_i$$

- Local wide-pipe design
- f uses $E : \{0,1\}^{2n} \times \{0,1\}^{2n} \rightarrow \{0,1\}^{2n}$



State of the Art

pre f	sec f	col f	pre $\mathcal{H}$	sec $\mathcal{H}$	col $\mathcal{H}$	indiff $\mathcal{H}$
			2^n f ideal	2^n f ideal	$2^{n/2}$ f ideal	$2^{n/2}$ f ideal

- BLAKE follows HAIFA design:
  - $\rightarrow$ pre/sec/col/indiff security for f ideal

State of the Art

pre f	sec f	col f	pre $\mathcal{H}$	sec $\mathcal{H}$	col $\mathcal{H}$	indiff $\mathcal{H}$
			2^n	2^n	$2^{n/2}$	$2^{n/2}$
			f ideal	f ideal	f ideal	f ideal

- BLAKE follows HAIFA design:
  $\rightarrow$ pre/sec/col/indiff security for f ideal

- f lacks security analysis

State of the Art

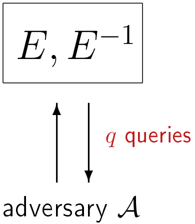
pre f	sec f	col f	pre $\mathcal{H}$	sec $\mathcal{H}$	col $\mathcal{H}$	indiff $\mathcal{H}$
			2^n	2^n	$2^{n/2}$	$2^{n/2}$
			f ideal	f ideal	f ideal	f ideal

- BLAKE follows HAIFA design:
  $\rightarrow$ pre/sec/col/indiff security for f ideal

- f lacks security analysis

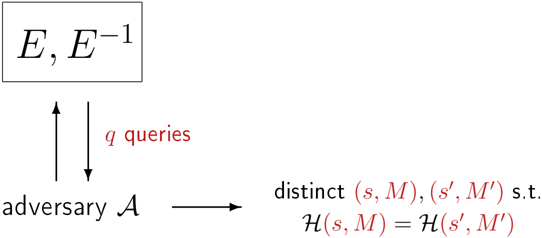
Analysis of BLAKE's $\mathcal{H}$ and f with underlying E ideal

Ideal Model Security: Col/Sec/Pre Resistance



- Ideal cipher model: $E : \{0,1\}^{2n} \times \{0,1\}^{2n} \to \{0,1\}^{2n}$
- $\mathcal{A}$ has query access to E

Ideal Model Security: Col/Sec/Pre Resistance

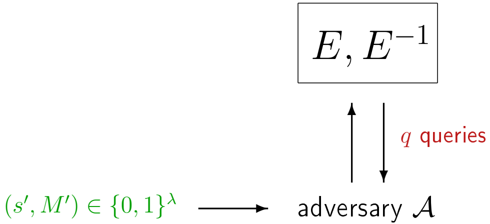


- Ideal cipher model: $E : \{0,1\}^{2n} \times \{0,1\}^{2n} \to \{0,1\}^{2n}$
- $\mathcal{A}$ has query access to E

$$\mathbf{Adv}_{\mathcal{H}}^{\mathrm{col}}(q) = \max_{\mathcal{A}} \text{ success probability } \mathcal{A}$$

(similar definitions if $\mathcal{A}$ attacks f)

Ideal Model Security: Col/Sec/Pre Resistance

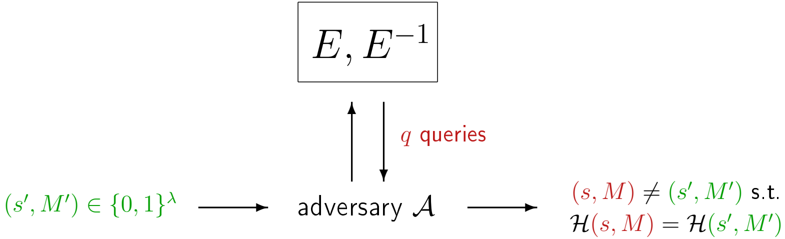


- Ideal cipher model: $E : \{0,1\}^{2n} \times \{0,1\}^{2n} \to \{0,1\}^{2n}$
- $\mathcal{A}$ has query access to E

$$\mathbf{Adv}_{\mathcal{H}}^{\mathrm{col}}(q) = \max_{\mathcal{A}} \text{ success probability } \mathcal{A}$$

(similar definitions if $\mathcal{A}$ attacks f)

Ideal Model Security: Col/Sec/Pre Resistance



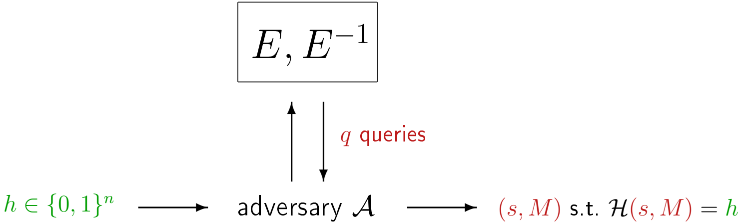
- Ideal cipher model: $E : \{0,1\}^{2n} \times \{0,1\}^{2n} \to \{0,1\}^{2n}$
- $\mathcal{A}$ has query access to E

$$\mathbf{Adv}_{\mathcal{H}}^{\mathrm{col}}(q) = \max_{\mathcal{A}} \text{ success probability } \mathcal{A}$$

$$\mathbf{Adv}_{\mathcal{H}}^{\mathrm{esec}[\lambda]}(q) = \max_{\mathcal{A}} \max_{(s',M') \in \{0,1\}^\lambda} \text{ success probability } \mathcal{A}$$

(similar definitions if $\mathcal{A}$ attacks f)

Ideal Model Security: Col/Sec/Pre Resistance



- Ideal cipher model: $E : \{0,1\}^{2n} \times \{0,1\}^{2n} \to \{0,1\}^{2n}$
- $\mathcal{A}$ has query access to E

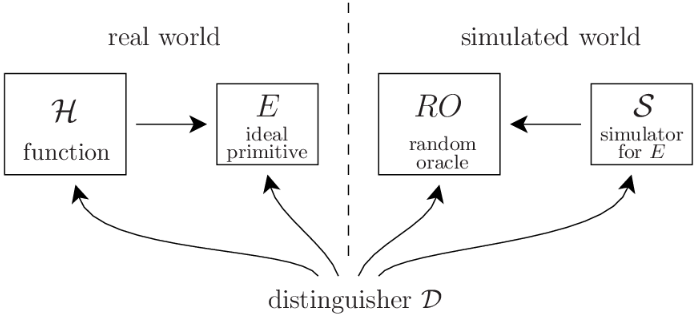
$$\mathbf{Adv}_{\mathcal{H}}^{\mathrm{col}}(q) = \max_{\mathcal{A}} \text{ success probability } \mathcal{A}$$

$$\mathbf{Adv}_{\mathcal{H}}^{\mathrm{esec}[\lambda]}(q) = \max_{\mathcal{A}} \max_{(s',M')\in\{0,1\}^{\lambda}} \text{ success probability } \mathcal{A}$$

$$\mathbf{Adv}_{\mathcal{H}}^{\mathrm{epre}}(q) = \max_{\mathcal{A}} \max_{h\in\{0,1\}^{n}} \text{ success probability } \mathcal{A}$$

(similar definitions if $\mathcal{A}$ attacks f)

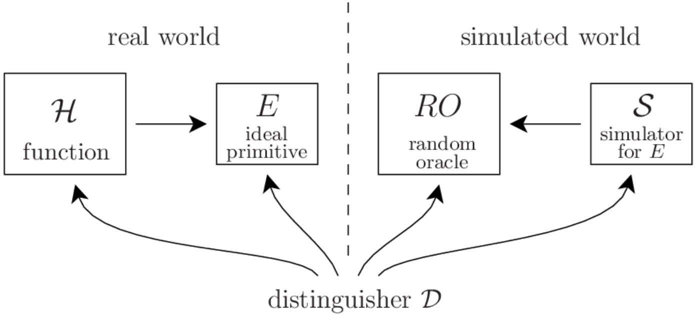
Ideal Model Security: Indifferentiability



- Indifferentiability of $\mathcal{H}$ from a random oracle
- $\mathcal{H}^E$ is indifferentiable from RO if $\exists$ simulator S such that $(\mathcal{H}, E)$ and $(RO, \mathcal{S})$ indistinguishable

(similar definitions if $\mathcal{D}$ attacks f)

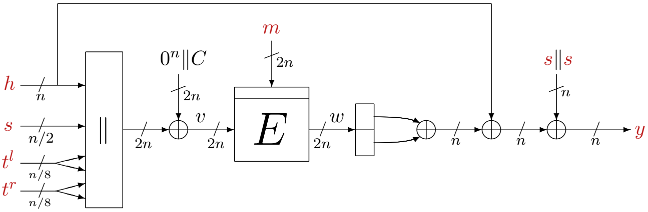
Ideal Model Security: Indifferentiability



- Indifferentiability of $\mathcal{H}$ from a random oracle
- $\mathcal{H}^E$ is indifferentiable from RO if $\exists$ simulator S such that $(\mathcal{H}, E)$ and $(RO, \mathcal{S})$ indistinguishable
- Extension of indistinguishability: $\mathcal{D}$ may know structure of $\mathcal{H}$

(similar definitions if $\mathcal{D}$ attacks f)

Differentiability Attack f

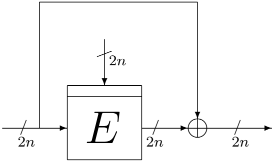


f differentiable from RO in $2^{n/4}$ queries

- Differentiability: construct a distinguisher that tricks any simulator

(independently found by [Chang+11])

Differentiability Attack f

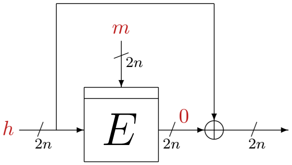


f differentiable from RO in $2^{n/4}$ queries

- Differentiability: construct a distinguisher that tricks any simulator
- Davies-Meyer differentiable in 2 queries

(independently found by [Chang+11])

Differentiability Attack f



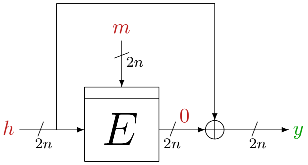
f differentiable from RO in $2^{n/4}$ queries

- Differentiability: construct a distinguisher that tricks any simulator
- Davies-Meyer differentiable in 2 queries

Real world
$\mathcal{D}$ queries $E^{-1}(m, 0) \to h$

(independently found by [Chang+11])

Differentiability Attack f



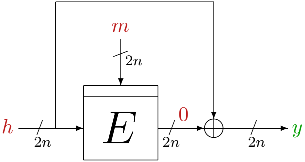
f differentiable from RO in $2^{n/4}$ queries

- Differentiability: construct a distinguisher that tricks any simulator
- Davies-Meyer differentiable in 2 queries

Real world
$\mathcal{D}$ queries $E^{-1}(m, 0) \rightarrow h$ $\mathcal{D}$ queries $DM(h, m) \rightarrow y$

(independently found by [Chang+11])

Differentiability Attack f



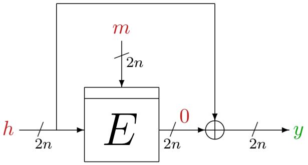
f differentiable from RO in $2^{n/4}$ queries

- Differentiability: construct a distinguisher that tricks any simulator
- Davies-Meyer differentiable in 2 queries

Real world
$\mathcal{D}$ queries $E^{-1}(m, 0) \to h$
$\mathcal{D}$ queries $DM(h, m) \to y$
$h = y$ with probability 1

(independently found by [Chang+11])

Differentiability Attack f



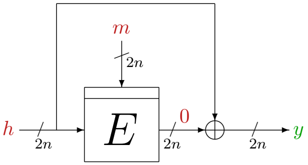
f differentiable from RO in $2^{n/4}$ queries

- Differentiability: construct a distinguisher that tricks any simulator
- Davies-Meyer differentiable in 2 queries

Real world	Simulated world
$\mathcal{D}$ queries $E^{-1}(m, 0) \to h$	$\mathcal{D}$ queries $\mathcal{S}^{-1}(m, 0) \to h$
$\mathcal{D}$ queries $DM(h, m) \to y$	$\mathcal{D}$ queries $RO(h, m) \to y$
$h = y$ with probability 1	

(independently found by [Chang+11])

Differentiability Attack f



f differentiable from RO in $2^{n/4}$ queries

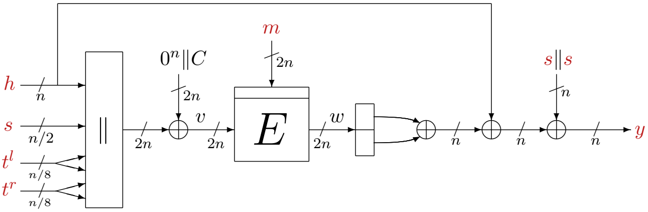
- Differentiability: construct a distinguisher that tricks any simulator
- Davies-Meyer differentiable in 2 queries

Real world
$\mathcal{D}$ queries $E^{-1}(m, 0) \to h$
$\mathcal{D}$ queries $DM(h, m) \to y$
$h = y$ with probability 1

Simulated world
$\mathcal{D}$ queries $\mathcal{S}^{-1}(m, 0) \to h$
$\mathcal{D}$ queries $RO(h, m) \to y$
$h = y$ with probability $O(1/2^{2n})$

(independently found by [Chang+11])

Differentiability Attack f

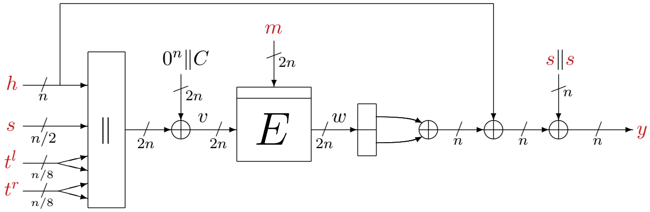


f differentiable from RO in $2^{n/4}$ queries

- Differentiability: construct a distinguisher that tricks any simulator
- Davies-Meyer differentiable in 2 queries

(independently found by [Chang+11])

Differentiability Attack f



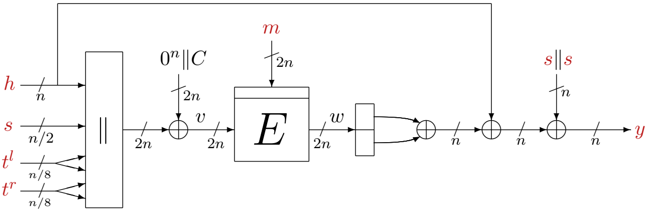
f differentiable from RO in $2^{n/4}$ queries

- Differentiability: construct a distinguisher that tricks any simulator
- Davies-Meyer differentiable in 2 queries

- BLAKE's f: duplicate counter prevents this attack
  - $\mathcal{S}^{-1}$-responses non-compliant with duplicate counter are useless to $\mathcal{D}$
  - After $2^{n/4}$ queries, this gets suspicious

(independently found by [Chang+11])

Differentiability Attack f



f differentiable from RO in $2^{n/4}$ queries

- Differentiability: construct a distinguisher that tricks any simulator
- Davies-Meyer differentiable in 2 queries

- BLAKE's f: duplicate counter prevents this attack
  - $\mathcal{S}^{-1}$-responses non-compliant with duplicate counter are useless to $\mathcal{D}$
  - After $2^{n/4}$ queries, this gets suspicious
- Invalidates assumption "f ideal"

(independently found by [Chang+11])

State of the Art, cntd.

pre f	sec f	col f	pre $\mathcal{H}$	sec $\mathcal{H}$	col $\mathcal{H}$	indiff $\mathcal{H}$
			2^n f ideal	2^n f ideal	$2^{n/2}$ f ideal	$2^{n/2}$ f ideal

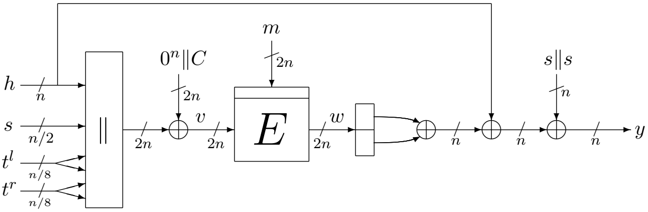
State of the Art, cntd.

pre f	sec f	col f	pre $\mathcal{H}$	sec $\mathcal{H}$	col $\mathcal{H}$	indiff $\mathcal{H}$
			2^n f ideal	2^n f ideal	$2^{n/2}$ f ideal	$2^{n/2}$ f ideal

Differentiability attack on f

pre f	sec f	col f	pre $\mathcal{H}$	sec $\mathcal{H}$	col $\mathcal{H}$	indiff $\mathcal{H}$

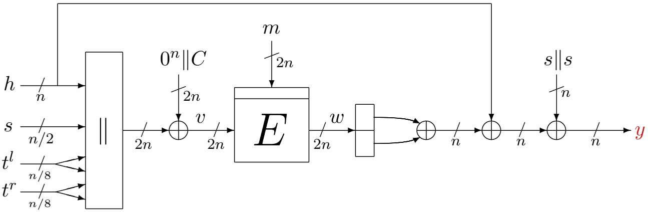
Preimage and Collision Resistance of BLAKE



$$\mathbf{Adv}_{\mathcal{H}}^{\mathrm{epre}}(q) \leq \mathbf{Adv}_{f}^{\mathrm{epre}}(q) = O(q/2^n)$$

- BLAKE preserves "epre"

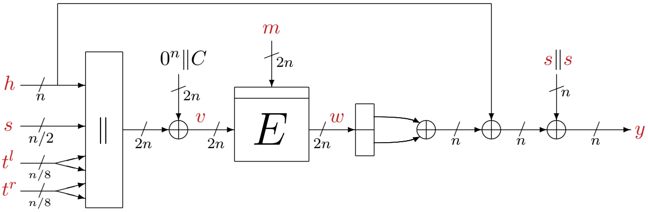
Preimage and Collision Resistance of BLAKE



$$\mathbf{Adv}^{\mathrm{epre}}_{\mathcal{H}}(q) \leq \mathbf{Adv}^{\mathrm{epre}}_{f}(q) = O(q/2^n)$$

- BLAKE preserves “epre”
- Let $y \in \{0,1\}^n$ be target image
- $\mathcal{A}$ makes q queries

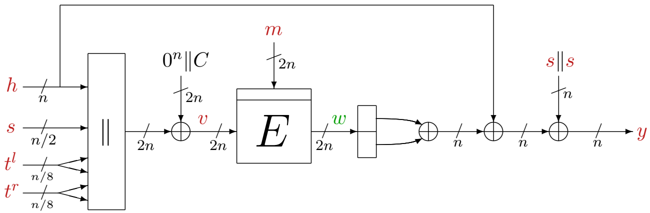
Preimage and Collision Resistance of BLAKE



$$\mathbf{Adv}_{\mathcal{H}}^{\mathrm{epre}}(q) \leq \mathbf{Adv}_{f}^{\mathrm{epre}}(q) = O(q/2^n)$$

- BLAKE preserves "epre"
- Let $y \in \{0,1\}^n$ be target image
- $\mathcal{A}$ makes q queries
- Any E-query (m, v, w): preimage if $w^l \oplus w^r \oplus h \oplus (s\|s) = y$

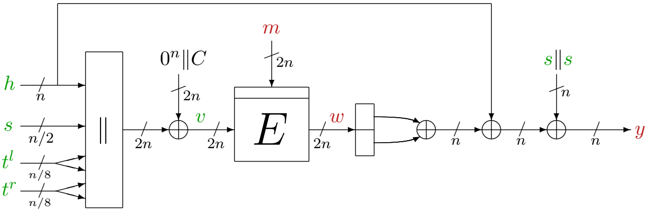
Preimage and Collision Resistance of BLAKE



$$\mathbf{Adv}_{\mathcal{H}}^{\text{epre}}(q) \leq \mathbf{Adv}_{f}^{\text{epre}}(q) = O(q/2^n)$$

- BLAKE preserves "epre"
- Let $y \in \{0,1\}^n$ be target image
- $\mathcal{A}$ makes q queries
- Any E-query (m, v, w): preimage if $w^l \oplus w^r \oplus h \oplus (s\|s) = y$
    - Forward query: with probability $O(1/2^n)$

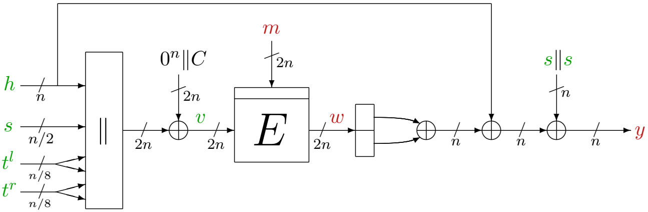
Preimage and Collision Resistance of BLAKE



$$\mathbf{Adv}_{\mathcal{H}}^{\text{epre}}(q) \leq \mathbf{Adv}_{f}^{\text{epre}}(q) = O(q/2^n)$$

- BLAKE preserves "epre"
- Let $y \in \{0,1\}^n$ be target image
- $\mathcal{A}$ makes q queries
- Any E-query (m, v, w): preimage if $w^l \oplus w^r \oplus h \oplus (s\|s) = y$
    - Forward query: with probability $O(1/2^n)$
    - Inverse query: with probability $O(1/2^n)$

Preimage and Collision Resistance of BLAKE

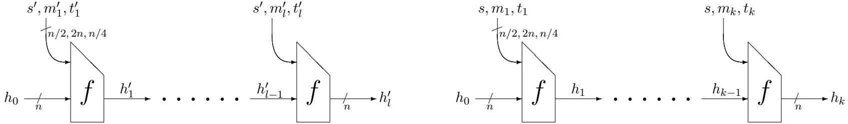


$$\mathbf{Adv}_{\mathcal{H}}^{\mathrm{epre}}(q) \leq \mathbf{Adv}_{f}^{\mathrm{epre}}(q) = O(q/2^n)$$

- BLAKE preserves "epre"
- Let $y \in \{0,1\}^n$ be target image
- $\mathcal{A}$ makes q queries
- Any E-query (m, v, w): preimage if $w^l \oplus w^r \oplus h \oplus (s\|s) = y$
  - Forward query: with probability $O(1/2^n)$
  - Inverse query: with probability $O(1/2^n)$

- Similarly, $\mathbf{Adv}_{\mathcal{H}}^{\mathrm{col}}(q) \leq \mathbf{Adv}_{f}^{\mathrm{col}}(q) = O(q^2/2^n)$

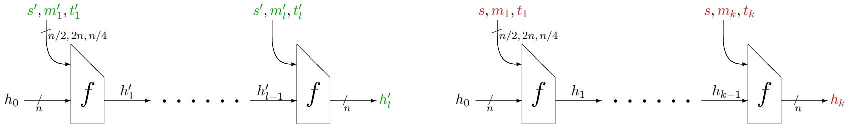
Second Preimage Resistance of BLAKE



$$\mathbf{Adv}_{\mathcal{H}}^{\text{esec}[\lambda]}(q) = O(q/2^n)$$

- "esec" not preserved: $\mathbf{Adv}_{\mathcal{H}}^{\text{esec}[\lambda]}(q) \not\lesssim \mathbf{Adv}_{f}^{\text{esec}[\lambda]}(q)$!

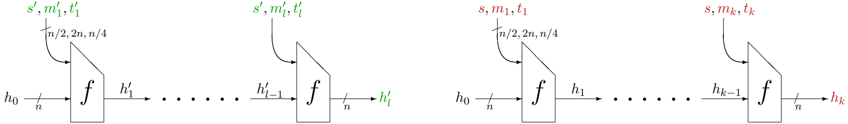
Second Preimage Resistance of BLAKE



$$\mathbf{Adv}_{\mathcal{H}}^{\text{esec}[\lambda]}(q) = O(q/2^n)$$

- "esec" not preserved: $\mathbf{Adv}_{\mathcal{H}}^{\text{esec}[\lambda]}(q) \not\lesssim \mathbf{Adv}_{f}^{\text{esec}[\lambda]}(q)$!
- Let (s', M') be target preimage and (s, M) response by $\mathcal{A}$

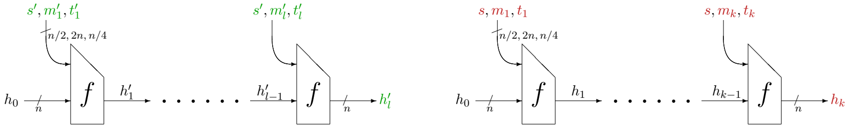
Second Preimage Resistance of BLAKE



$$\mathbf{Adv}_{\mathcal{H}}^{\mathrm{esec}[\lambda]}(q) = O(q/2^n)$$

- "esec" not preserved: $\mathbf{Adv}_{\mathcal{H}}^{\mathrm{esec}[\lambda]}(q) \not\lesssim \mathbf{Adv}_{f}^{\mathrm{esec}[\lambda]}(q)$!
- Let (s', M') be target preimage and (s, M) response by $\mathcal{A}$
- $\exists$ f-coll $f(h_{i-1}, s, m_i, t_i) \in \{h'_1, \ldots, h'_l\}$
  $\rightarrow$ Any E-query: f-coll with probability $O(l/2^n)$

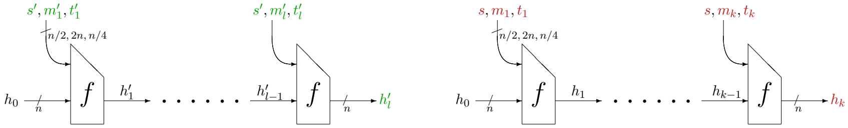
Second Preimage Resistance of BLAKE



$$\mathbf{Adv}_{\mathcal{H}}^{\mathrm{esec}[\lambda]}(q) = O(q/2^n)$$

- "esec" not preserved: $\mathbf{Adv}_{\mathcal{H}}^{\mathrm{esec}[\lambda]}(q) \not\lesssim \mathbf{Adv}_{f}^{\mathrm{esec}[\lambda]}(q)$!
- Let (s', M') be target preimage and (s, M) response by $\mathcal{A}$
- $\exists$ f-coll $f(h_{i-1}, s, m_i, t_i) \in \{h'_1, \ldots, h'_l\}$
  $\rightarrow$ Any E-query: f-coll with probability $O(l/2^n)$
- BLAKE achieves better second preimage resistance!
  $\rightarrow$ t_i fixes particular target state value from $\{h'_1, \ldots, h'_l\}$

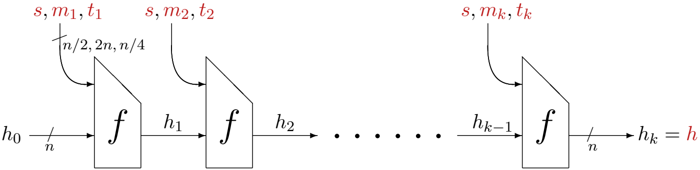
Second Preimage Resistance of BLAKE



$$\mathbf{Adv}_{\mathcal{H}}^{\mathrm{esec}[\lambda]}(q) = O(q/2^n)$$

- "esec" not preserved: $\mathbf{Adv}_{\mathcal{H}}^{\mathrm{esec}[\lambda]}(q) \not\lesssim \mathbf{Adv}_{f}^{\mathrm{esec}[\lambda]}(q)$!
- Let (s', M') be target preimage and (s, M) response by $\mathcal{A}$
- $\exists$ f-coll $f(h_{i-1}, s, m_i, t_i) \in \{h'_1, \ldots, h'_l\}$
  $\rightarrow$ Any E-query: f-coll with probability $O(l/2^n)$
- BLAKE achieves better second preimage resistance!
  $\rightarrow$ t_i fixes particular target state value from $\{h'_1, \ldots, h'_l\}$
  $\rightarrow$ Any E-query: f-coll with probability $O(1/2^n)$

Indifferentiability of BLAKE



$$\mathbf{Adv}_{\mathcal{H}}^{\text{indiff}}(\mathcal{D}) = O((Kq)^2/2^n)$$

(where $\mathcal{D}$ makes at most q queries of length at most K blocks)

- We restore old indifferentiability bound of BLAKE in ICM
- High-level proof idea
  - $\mathcal{S}$ maintains graph: edges correspond to f-evaluations
  - Complete paths should be in correspondence with RO
- Technical details in paper

(independently found by [Chang+11])

Conclusions

pre f	sec f	col f	pre $\mathcal{H}$	sec $\mathcal{H}$	col $\mathcal{H}$	indiff $\mathcal{H}$
			2^n f ideal	2^n f ideal	$2^{n/2}$ f ideal	$2^{n/2}$ f ideal

Conclusions

pre f	sec f	col f	pre $\mathcal{H}$	sec $\mathcal{H}$	col $\mathcal{H}$	indiff $\mathcal{H}$
			2^n f ideal	2^n f ideal	$2^{n/2}$ f ideal	$2^{n/2}$ f ideal

Differentiability attack on f

pre f	sec f	col f	pre $\mathcal{H}$	sec $\mathcal{H}$	col $\mathcal{H}$	indiff $\mathcal{H}$

Conclusions

pre f	sec f	col f	pre $\mathcal{H}$	sec $\mathcal{H}$	col $\mathcal{H}$	indiff $\mathcal{H}$
			2^n	2^n	$2^{n/2}$	$2^{n/2}$
			f ideal	f ideal	f ideal	f ideal

Differentiability attack on f

pre f	sec f	col f	pre $\mathcal{H}$	sec $\mathcal{H}$	col $\mathcal{H}$	indiff $\mathcal{H}$

Fix in ideal cipher model

pre f	sec f	col f	pre $\mathcal{H}$	sec $\mathcal{H}$	col $\mathcal{H}$	indiff $\mathcal{H}$
2^n		$2^{n/2}$	2^n	2^n	$2^{n/2}$	$2^{n/2}$
E ideal		E ideal	E ideal	E ideal	E ideal	E ideal

Comparison of SHA-3 Finalists [AMPS12]

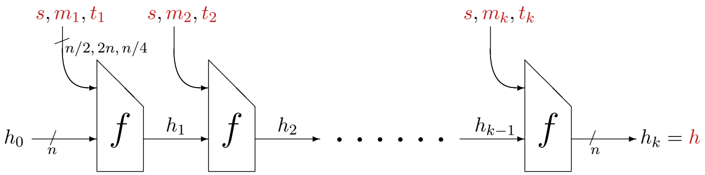
	l	m	pre	sec	col	indiff	assumption
BLAKE-256	256	512	256	256	128	128	E ideal
Grøstl-256	512	512	256	256–L	128	128	P, Q ideal
JH-256	1024	512	256	256	128	256	P ideal
Keccak-256	1600	1088	256	256	128	256	P ideal
Skein-256	512	512	256	256	128	256	E ideal
NIST's requirements			256	256–L	128	—	

	l	m	pre	sec	col	indiff	assumption
BLAKE-512	512	1024	512	512	256	256	E ideal
Grøstl-512	1024	1024	512	512–L	256	256	P, Q ideal
JH-512	1024	512	256	256	256	256	P ideal
Keccak-512	1600	576	512	512	256	512	P ideal
Skein-512	512	512	512	512	256	256	E ideal
NIST's requirements			512	512–L	256	—	

Supporting Slides

SUPPORTING SLIDES

Indifferentiability of BLAKE



$$\mathbf{Adv}_{\mathcal{H}}^{\mathrm{indiff}}(\mathcal{D}) = O((Kq)^2/2^n)$$

(where $\mathcal{D}$ makes at most q queries of length at most K blocks)

- Indifferentiability: construct a simulator that tricks any distinguisher
- $\mathcal{S}$ maintains graph: edges correspond to f-evaluations
  - Any $\mathcal{S}$-query defines at most one edge $h \xrightarrow{s\|m\|t} h'$
- Complete path: $h_0 \xrightarrow{s\|m_1\|t_1} h_1 \cdots \xrightarrow{s\|m_k\|t_k} h_k$ for correctly padded $(m_1, \ldots, m_k)$, $(t_1, \ldots, t_k)$

Indifferentiability of BLAKE

Forward Query $\mathcal{S}(m, v)$
if new query creates complete path **then**
(new query likely results in at most 1 complete path)
generate w in accordance with RO
else
generate w uniformly at random
end if
add new edge to graph

Inverse Query $\mathcal{S}^{-1}(m, w)$
(new query likely results in no complete path)
generate v uniformly at random
add new edge to graph