Provable Security of BLAKE with Non-Ideal Compression Function

Elena Andreeva, Atul Luykx, and <u>Bart Mennink</u> (KU Leuven)

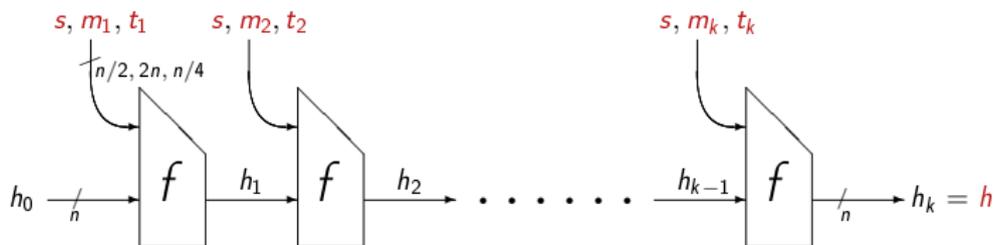Third SHA-3 Candidate Conference, Washington, DC

March 22, 2012

BLAKE

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

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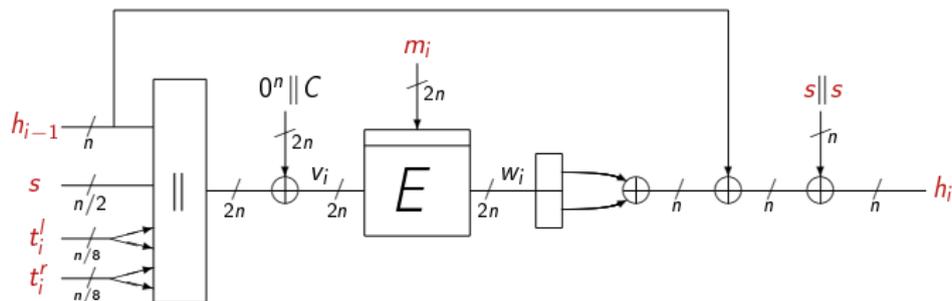- $t_1, \ldots, t_k$ HAIFA-counter blocks of $n/4$ bits

BLAKE

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

- 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	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

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

$$\boxed{E, E^{-1}}$$

q queries

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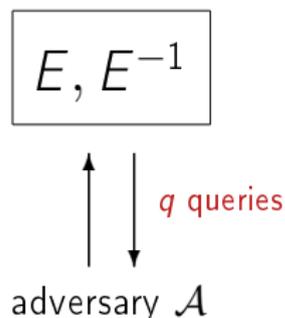
- Ideal cipher model: $E : \{0,1\}^{2n} \times \{0,1\}^{2n} \to \{0,1\}^{2n}$
- $\mathcal{A}$ has query access to E

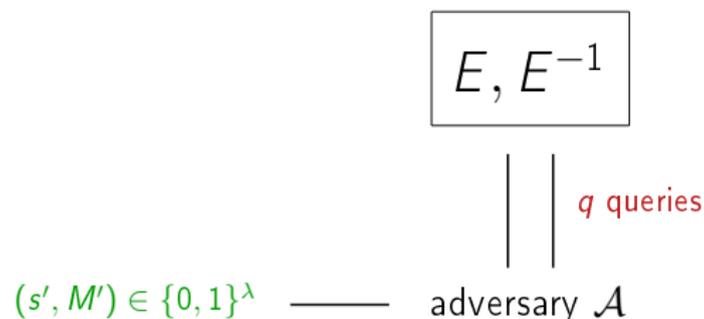# Ideal Model Security: Col/Sec/Pre Resistance

$$\boxed{E, E^{-1}}$$

q queries

adversary $\mathcal{A}$ $\longrightarrow$ distinct $(s, M), (s', M')$ s.t.
$\mathcal{H}(s, M) = \mathcal{H}(s', M')$

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

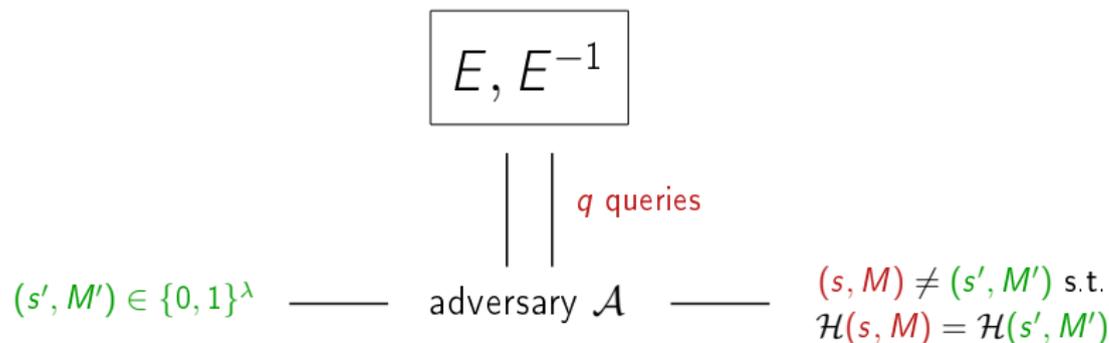$$\mathbf{Adv}_{\mathcal{H}}^{\mathrm{col}}(q) = \max_{\mathcal{A}} \text{ success probability } \mathcal{A}$$

Ideal Model Security: Col/Sec/Pre Resistance

$$E, E^{-1}$$

q queries

$(s', M') \in \{0,1\}^{\lambda}$ —————— adversary $\mathcal{A}$

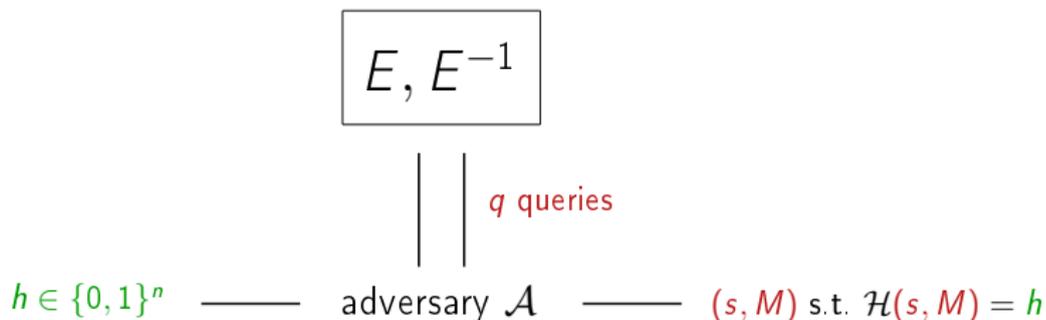- Ideal cipher model: $E : \{0,1\}^{2n} \times \{0,1\}^{2n} \to \{0,1\}^{2n}$
- $\mathcal{A}$ has query access to E

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

Ideal Model Security: Col/Sec/Pre Resistance

$$E, E^{-1}$$

q queries

$(s', M') \in \{0,1\}^\lambda$ —— adversary $\mathcal{A}$ —— $(s, M) \neq (s', M')$ s.t.
$\mathcal{H}(s, M) = \mathcal{H}(s', M')$

- 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)   5 / 12

Ideal Model Security: Col/Sec/Pre Resistance

$$\boxed{E, E^{-1}}$$

q queries

$h \in \{0,1\}^n$ ——— adversary $\mathcal{A}$ ——— (s, M) s.t. $\mathcal{H}(s, M) = h$

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

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

$$\mathbf{Adv}_{\mathcal{H}}^{\mathrm{esec}[\lambda]}(q) = \max_{\mathcal{A}} \max_{(s', M') \in \{0,1\}^{\lambda}} \text{ success probability } \mathcal{A}$$
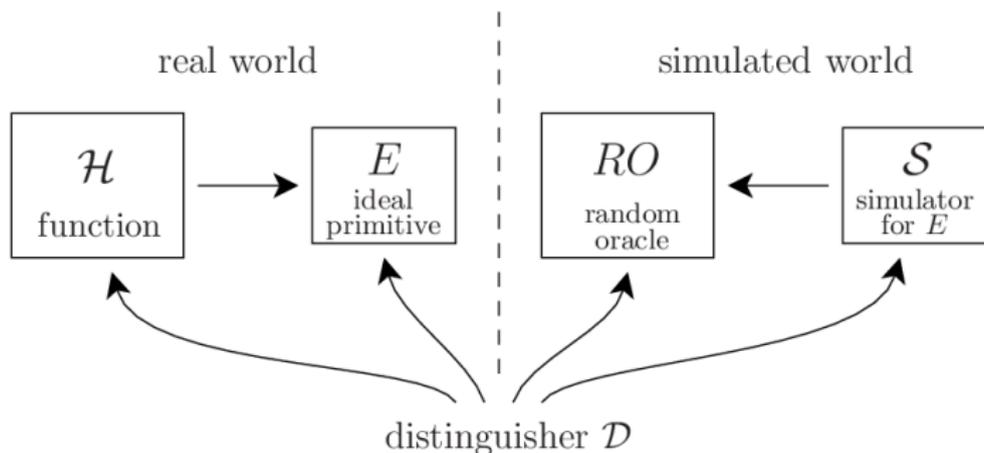
$$\mathbf{Adv}_{\mathcal{H}}^{\mathrm{epre}}(q) = \max_{\mathcal{A}} \max_{h \in \{0,1\}^n} \text{ success probability } \mathcal{A}$$
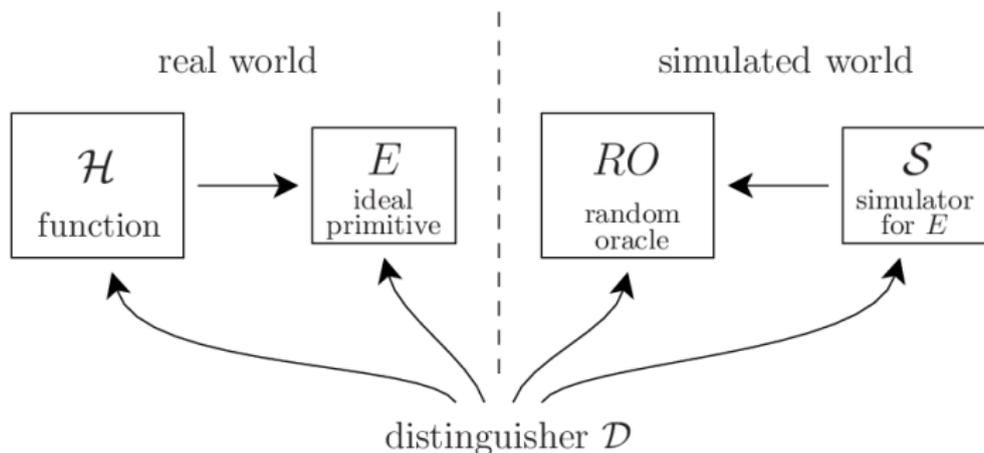
Ideal Model Security: Indifferentiability

- 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

# 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 $\mathcal{H}$

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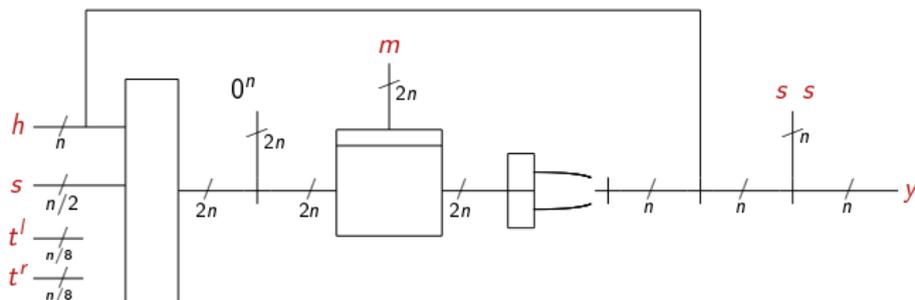
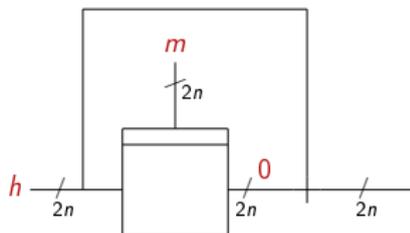f differentiable from RO in $2^{n/}$ queries

- Differentiability: construct a distinguisher that tricks any simulator

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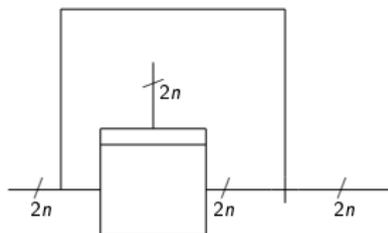
f differentiable from RO in $2^{n/}$ queries

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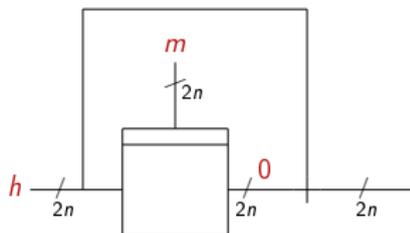
Differentiability Attack f

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

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

Real world

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

Differentiability Attack f

f differentiable from RO in $2^{n/}$ 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 $DM(h, m) \to y$

Differentiability Attack f

f differentiable from RO in $2^{n/}$ queries
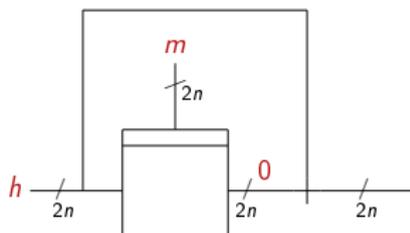
- Differentiability: construct a distinguisher that tricks any simulator
- Davies-Meyer differentiable in 2 queries

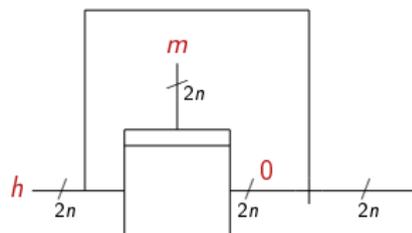| Real world |
| --- |
| $\mathcal{D}$ queries $E^{-1}(m, 0) \rightarrow h$ |
| $\mathcal{D}$ queries $DM(h, m) \rightarrow y$ |
| $h = y$ with probability 1 |

Differentiability Attack f

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

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

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

Differentiability Attack f

f differentiable from RO in $2^{n/}$ 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 $O(1/2^n)$

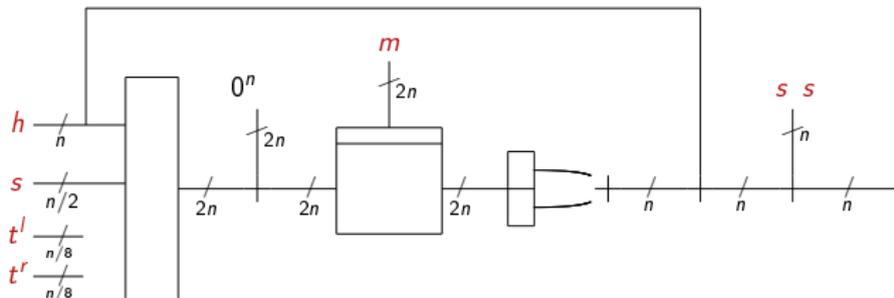(independently found by [Chang+11])   7 / 12

Differentiability Attack f

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

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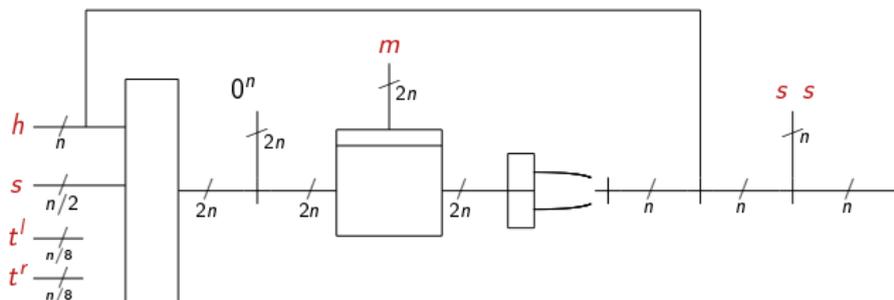- Davies-Meyer differentiable in 2 queries

Differentiability Attack f

f differentiable from RO in $2^{n/}$ 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
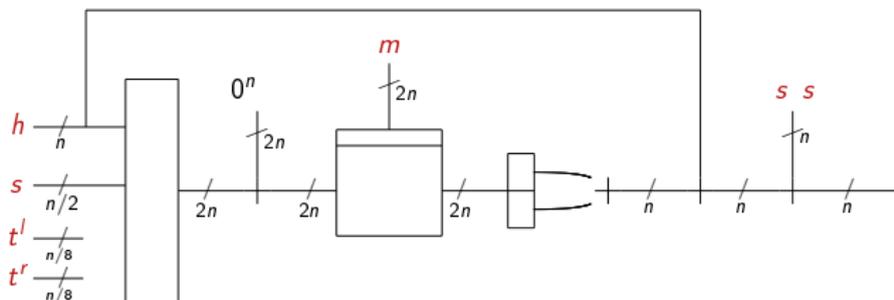
Differentiability Attack f

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

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	2^n	$2^{n/2}$	$2^{n/2}$
			f ideal	f ideal	f ideal	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	2^n	$2^{n/2}$	$2^{n/2}$
			f ideal	f ideal	f ideal	f ideal
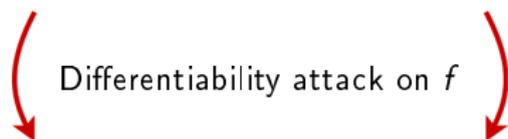
Differentiability attack on f

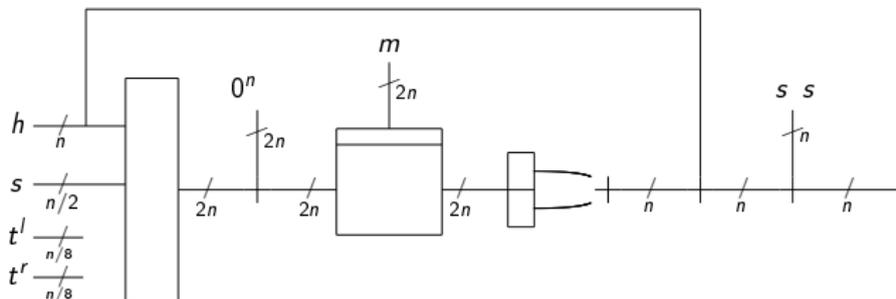| pre f	sec f	col f	pre $\mathcal{H}$	sec $\mathcal{H}$	col $\mathcal{H}$	indiff $\mathcal{H}$

Preimage and Collision Resistance of BLAKE
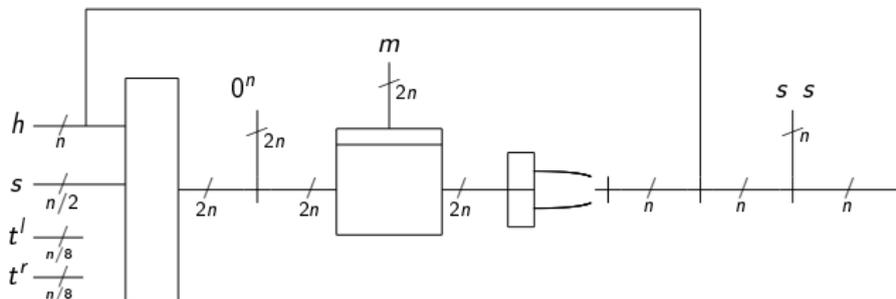
$$\mathbf{Adv}_{\mathcal{H}}^{\mathrm{epre}}(q) \leq \mathbf{Adv}_{f}^{\mathrm{epre}}(q) = O(q/2^n)$$

- BLAKE preserves "epre"

Preimage and Collision Resistance of BLAKE

$$\mathcal{H}(\ ) \leq \qquad (\ ) = O(\ /2^n)$$

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

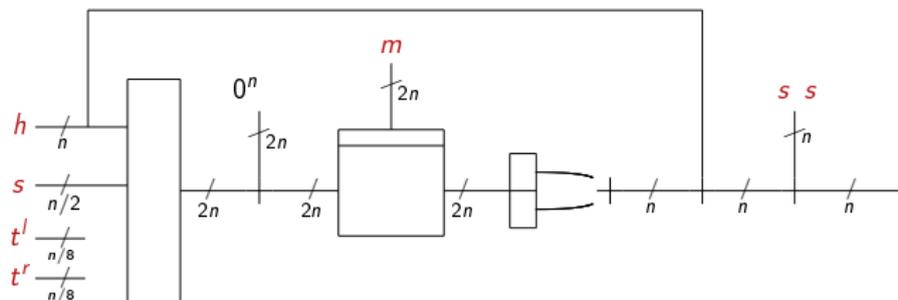# Preimage and Collision Resistance of BLAKE

$$\mathcal{H}\ (\ ) \leq \qquad (\ ) = O(\ /2^n)$$

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

Preimage and Collision Resistance of BLAKE

$$\mathcal{H} \ (\ ) \leq \qquad (\ ) = O(\ /2^n)$$

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

Preimage and Collision Resistance of BLAKE

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

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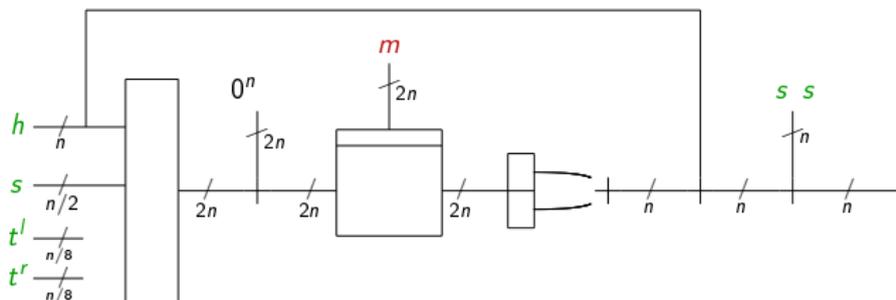- Any E-query (m, t, c): preimage if $c^l \oplus c^r \oplus h \oplus (s \| s) = W$
  - Forward query: with probability $O(1/2^n)$
  - Inverse query: with probability $O(1/2^n)$

Preimage and Collision Resistance of BLAKE

$$\mathbf{Adv}_{\mathcal{H}}^{epre}(q) \le \mathbf{Adv}_E^{epre}(q) = O(q/2^n)$$

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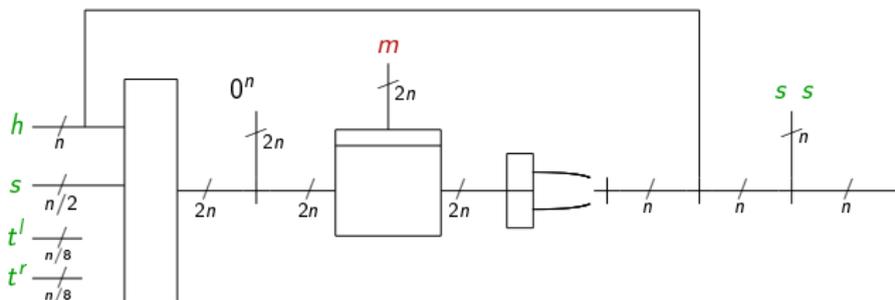 - Forward query: with probability $O(1/2^n)$
  - Inverse query: with probability $O(1/2^n)$

- Similarly $\mathbf{Adv}_{\mathcal{H}}^{col}(q) \le \mathbf{Adv}_E^{col}(q) = O(q^2/2^n)$

Second Preimage Resistance of BLAKE

$$\mathbf{Sec}[\lambda]_{\mathcal{H}}(\ ) = O(\ /2^n)$$

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

Second Preimage Resistance of BLAKE

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

- "esec" not preserved: $\mathbf{Adv}_{\mathcal{H}}^{\mathrm{esec}[\lambda]}(\ ) \not\leq \mathbf{Adv}^{\mathrm{esec}[\lambda]}(\ )$!

- Let (s', M') be target preimage and (s, M) response by $\mathcal{A}$

Second Preimage Resistance of BLAKE

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

- "esec" not preserved: $\mathrm{esec}[\lambda]_{\mathcal{H}}(\ ) \not\le \mathrm{esec}[\lambda](\ )$!

- Let (s', M') be target preimage and (s, M) response by $\mathcal{A}$

- $\exists$ f-coll $f(h_{i-1}, s, m_i, t_i) \in \{h'_1, \dots, h'_l\}$
  $\rightarrow$ Any E-query: f-coll with probability $O(l/2^n)$

Second Preimage Resistance of BLAKE
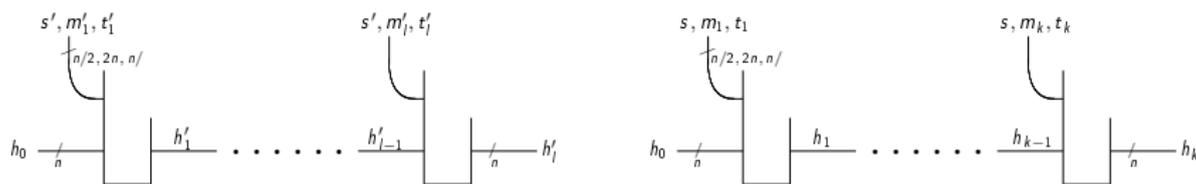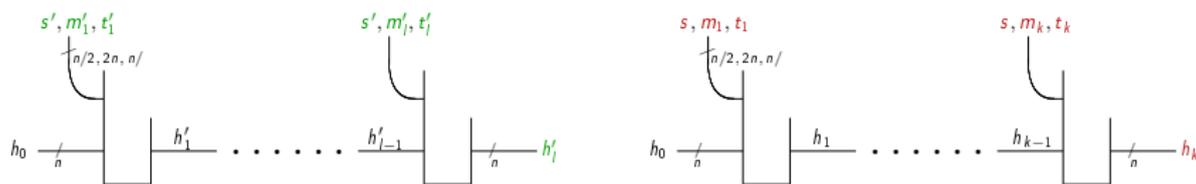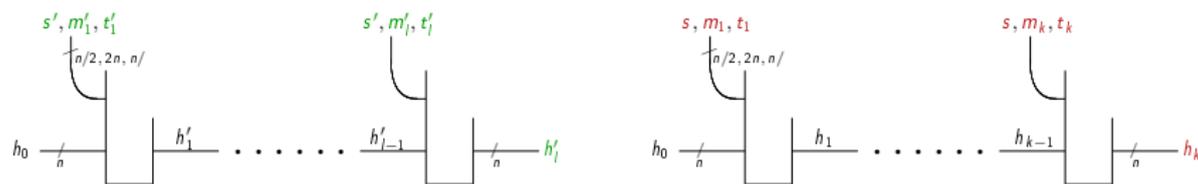
$$\underset{\mathcal{H}}{\text{esec}[\lambda]}(\ ) = O(\ /2^n)$$

- "esec" not preserved: $\quad \underset{\mathcal{H}}{\text{esec}[\lambda]}(\ ) \not\lesssim \quad \text{esec}[\lambda](\ )!$

- 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 preimage resistance!
  - $\rightarrow$ t_i fixes particular target state value from $\{h'_1, \ldots, h'_l\}$

Second Preimage Resistance of BLAKE

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

- "esec" not preserved: $\mathop{\mathrm{esec}[\lambda]}_{\mathcal{H}}(\ ) \not\leq \mathop{\mathrm{esec}[\lambda]}(\ )$!

- Let (s', M') be target preimage and (s, M) response by $\mathcal{A}$

- $\exists$ f-coll $f(h_{i-1}, s, m_i, t_i) \in \{h'_1, \ldots, h'_l\}$
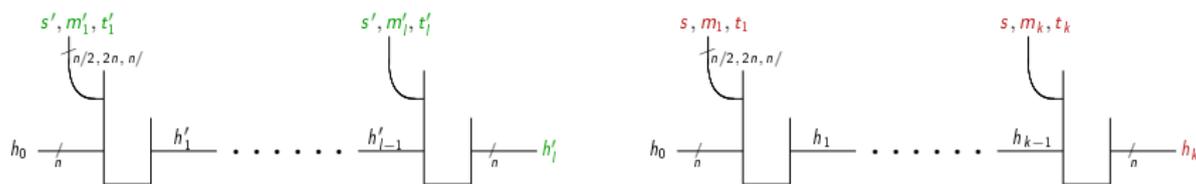 - $\to$ Any E-query: f-coll with probability $O(l/2^n)$

- BLAKE achieves better preimage resistance!
  - $\to$ t_i fixes particular target state value from $\{h'_1, \ldots, h'_l\}$
  - $\to$ Any E-query: f-coll with probability $O(1/2^n)$

Indifferentiability of BLAKE
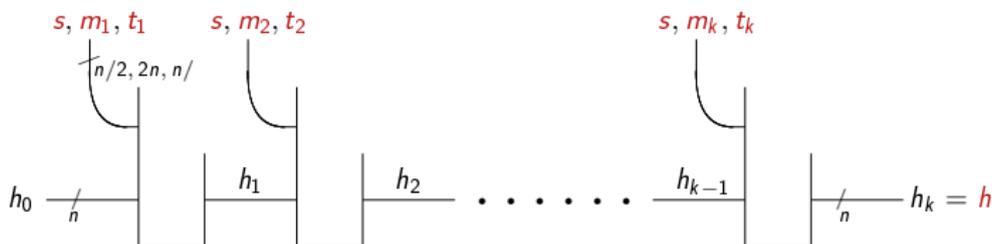
$$\mathcal{H}^{\mathrm{indiff}}(\mathcal{D}) = O((Kq)^2/2^n)$$

(where $\mathcal{D}$ makes at most   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

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

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
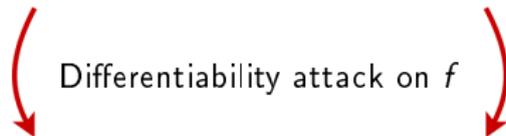
Differentiability attack on f

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

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

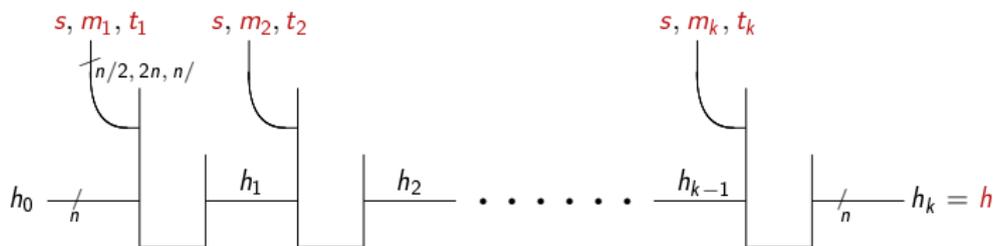| pre f	sec f	col f	pre $\mathcal{H}$	sec $\mathcal{H}$	col $\mathcal{H}$	indiff $\mathcal{H}$

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

Supporting Slides

SUPPORTING SLIDES

Indifferentiability of BLAKE

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

(where $\mathcal{D}$ makes at most   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