

Provable Security of BLAKE with Non-Ideal Compression Function

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

Third SHA-3 Candidate Conference, Washington, DC

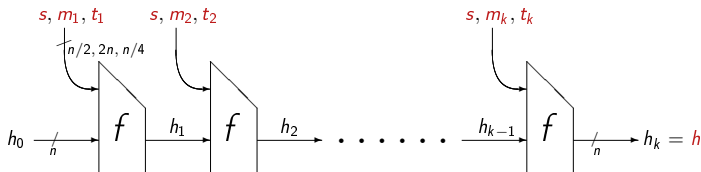
March 22, 2012

BLAKE

$$\mathcal{H} : \{0, 1\}^{n/2} \times \{0, 1\}^* \rightarrow \{0, 1\}^n$$

$$\mathcal{H}(s, M) = h$$

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

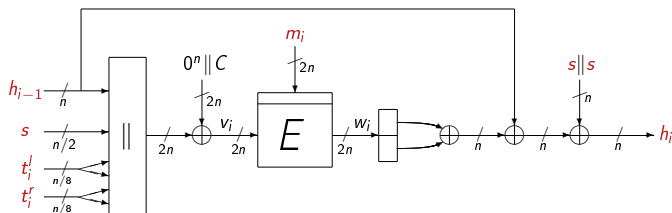


BLAKE

$$f : \{0, 1\}^n \times \{0, 1\}^{n/2} \times \{0, 1\}^{2n} \times \{0, 1\}^{n/4} \rightarrow \{0, 1\}^n$$

$$f(h_{i-1}, s, m_i, t_i) = h_i$$

- 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	2^n	$2^{n/2}$	$2^{n/2}$
			f ideal	f ideal	f ideal	f ideal

- BLAKE follows HAIFA design:
 → 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:
 → pre/sec/col/indiff security for f ideal
- f lacks security analysis

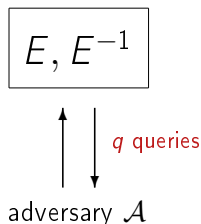
State of the Art

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:
 → pre/sec/col/indiff security for f ideal
- f lacks security analysis

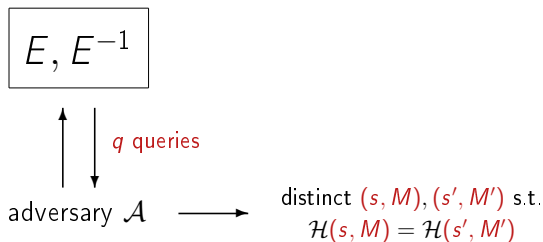
Analysis of BLAKE's \mathcal{H} and f with underlying E ideal

Ideal Model Security: Col/Sec/Pre Resistance



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

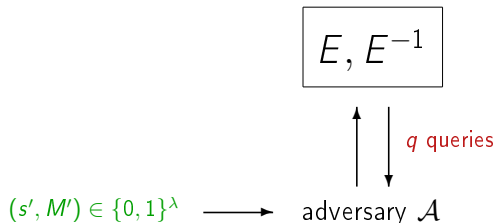
Ideal Model Security: Col/Sec/Pre Resistance



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

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

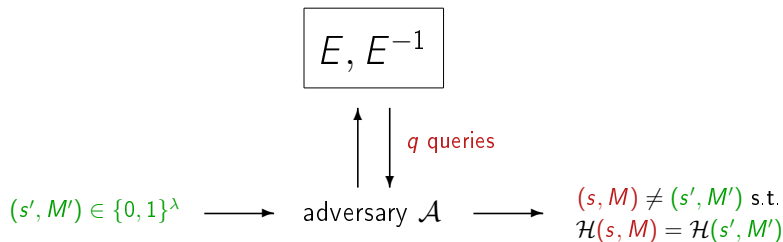
Ideal Model Security: Col/Sec/Pre Resistance



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

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

Ideal Model Security: Col/Sec/Pre Resistance

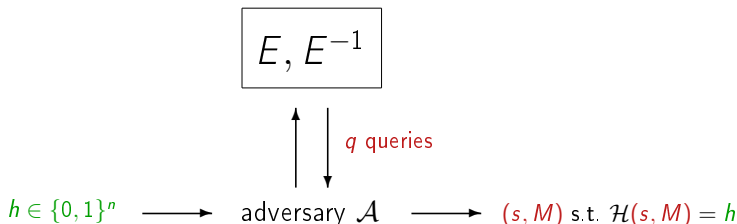


- Ideal cipher model: $E : \{0, 1\}^{2n} \times \{0, 1\}^{2n} \rightarrow \{0, 1\}^{2n}$
- \mathcal{A} has query access to E

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

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

Ideal Model Security: Col/Sec/Pre Resistance



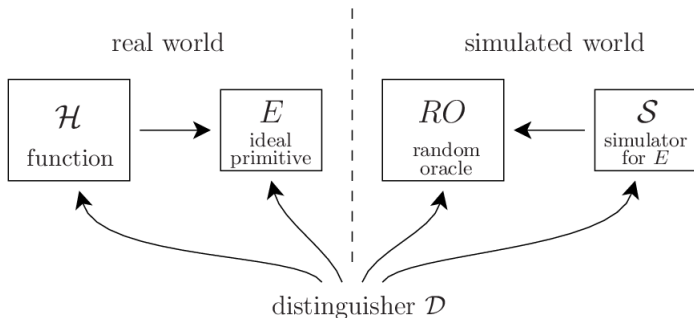
- Ideal cipher model: $E : \{0, 1\}^{2n} \times \{0, 1\}^{2n} \rightarrow \{0, 1\}^{2n}$
- \mathcal{A} has query access to E

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

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

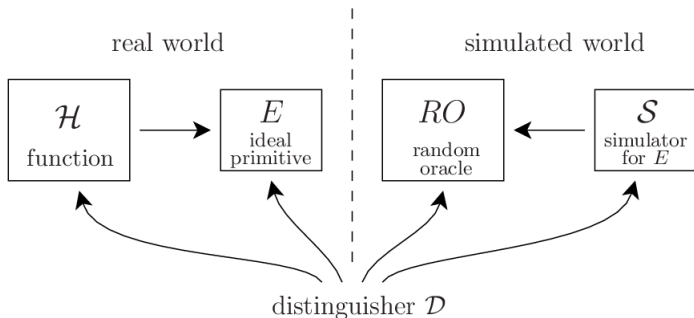
$$\mathbf{Adv}_{\mathcal{H}}^{\text{epre}}(q) = \max_{\mathcal{A}} \max_{h \in \{0, 1\}^n} \text{success probability } \mathcal{A}$$

Ideal Model Security: Indifferentiability



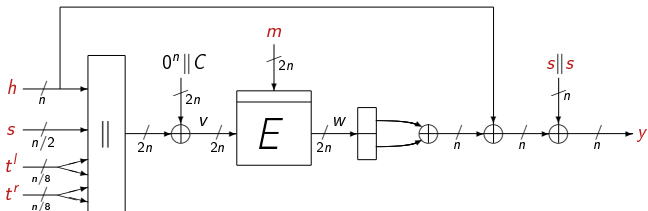
- Indifferentiability of \mathcal{H} from a random oracle
- \mathcal{H}^E is indistinguishable from RO if \exists simulator \mathcal{S} such that (\mathcal{H}, E) and (RO, \mathcal{S}) indistinguishable

Ideal Model Security: Indifferentiability



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

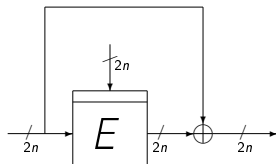
Differentiability Attack f



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

- Differentiability: construct a distinguisher that tricks any simulator

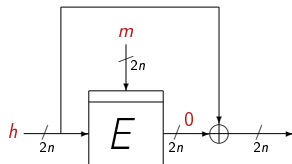
Differentiability Attack f



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

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

Differentiability Attack f



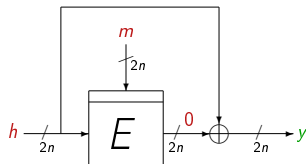
f differentiable from RO in $2^{n/4}$ queries

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

Real world

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

Differentiability Attack f



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

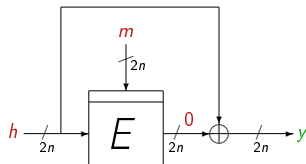
- Differentiability: construct a distinguisher that tricks any simulator
- Davies-Meyer differentiable in 2 queries

Real world

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

\mathcal{D} queries $DM(h, m) \rightarrow y$

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

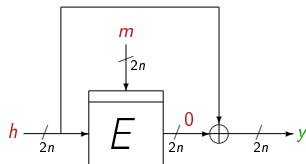
Real world

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

\mathcal{D} queries $DM(h, m) \rightarrow y$

$h = y$ with probability 1

Differentiability Attack f



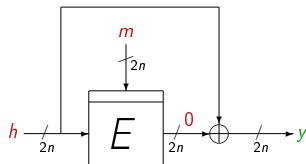
f differentiable from RO in $2^{n/4}$ queries

- 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 $DM(h, m) \rightarrow y$
$h = y$ with probability 1

Simulated world
\mathcal{D} queries $\mathcal{S}^{-1}(m, 0) \rightarrow h$
\mathcal{D} queries $RO(h, m) \rightarrow y$

Differentiability Attack f



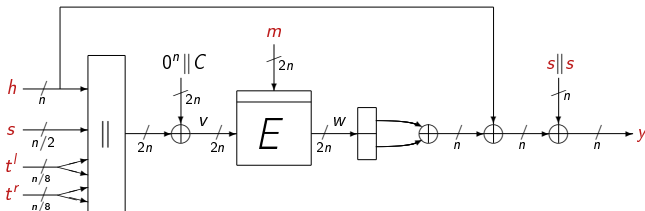
f differentiable from RO in $2^{n/4}$ queries

- 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 $DM(h, m) \rightarrow y$
$h = y$ with probability 1

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

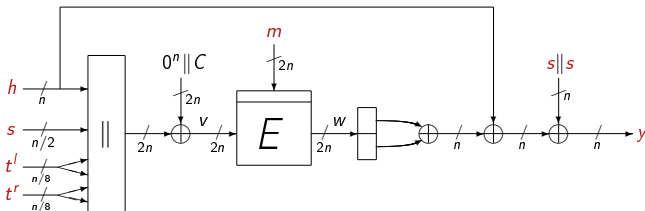
Differentiability Attack f



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

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

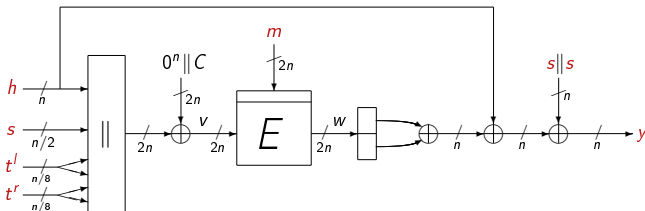
Differentiability Attack f



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

Differentiability Attack f



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

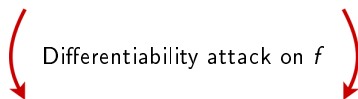
- Differentiability: construct a distinguisher that tricks any simulator
- Davies-Meyer differentiable in 2 queries
- BLAKE's f : duplicate counter prevents this attack
 - \mathcal{S}^{-1} -responses non-compliant with duplicate counter are useless to \mathcal{D}
 - After $2^{n/4}$ queries, this gets suspicious
- Invalidates assumption “ f ideal”

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

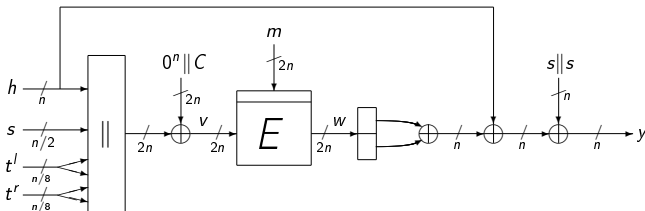
State of the Art, cntd.

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

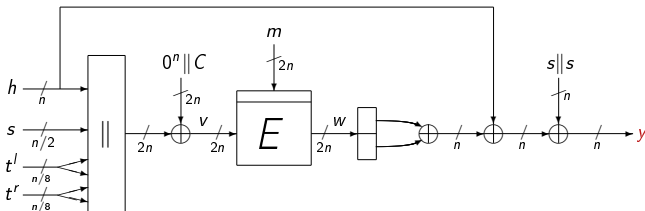
Preimage and Collision Resistance of BLAKE



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

- BLAKE preserves “epre”

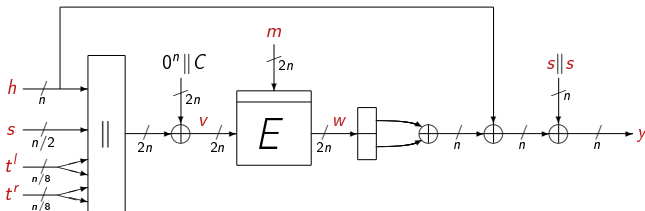
Preimage and Collision Resistance of BLAKE



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

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

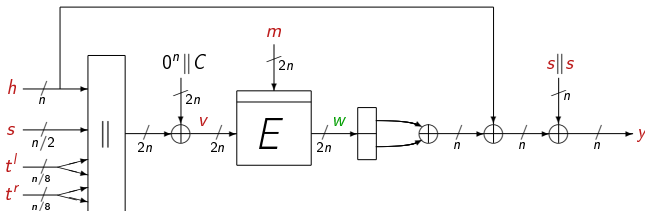
Preimage and Collision Resistance of BLAKE



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

- 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 $w^l \oplus w^r \oplus h \oplus (s || s) = y$

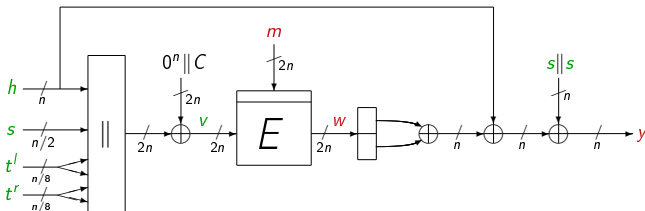
Preimage and Collision Resistance of BLAKE



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

- 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 $w^l \oplus w^r \oplus h \oplus (s \parallel s) = y$
 - Forward query: with probability $O(1/2^n)$

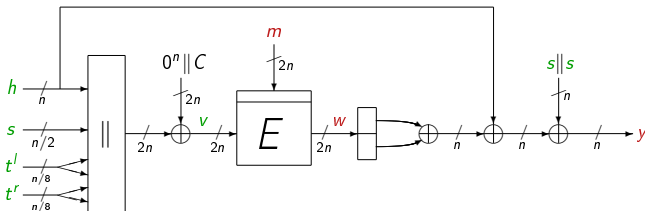
Preimage and Collision Resistance of BLAKE



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

- 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 $w^l \oplus w^r \oplus h \oplus (s \parallel s) = y$
 - Forward query: with probability $O(1/2^n)$
 - Inverse query: with probability $O(1/2^n)$

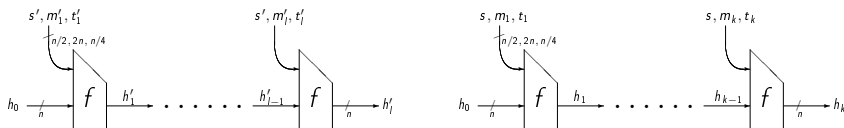
Preimage and Collision Resistance of BLAKE



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

- 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 $w^l \oplus w^r \oplus h \oplus (s \parallel s) = y$
 - Forward query: with probability $O(1/2^n)$
 - Inverse query: with probability $O(1/2^n)$
- Similarly, $\mathbf{Adv}_{\mathcal{H}}^{\text{col}}(q) \leq \mathbf{Adv}_f^{\text{col}}(q) = O(q^2/2^n)$

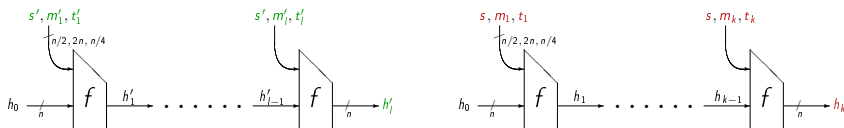
Second Preimage Resistance of BLAKE



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

- “esec” not preserved: $\text{Adv}_{\mathcal{H}}^{\text{esec}[\lambda]}(q) \not\leq \text{Adv}_f^{\text{esec}[\lambda]}(q)!$

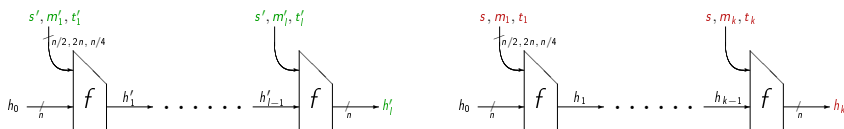
Second Preimage Resistance of BLAKE



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

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

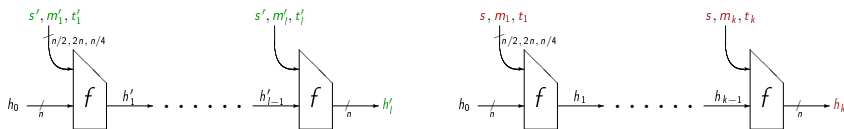
Second Preimage Resistance of BLAKE



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

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

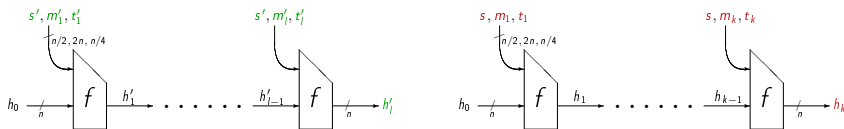
Second Preimage Resistance of BLAKE



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

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

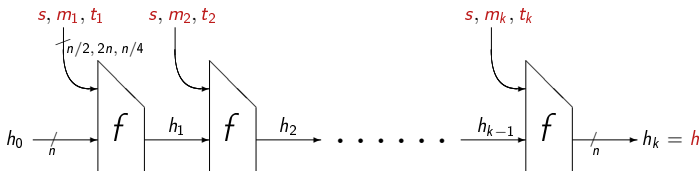
Second Preimage Resistance of BLAKE



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

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

Indifferentiability of BLAKE



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

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

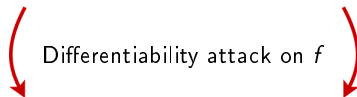
- We restore old indifferentiability bound of BLAKE in ICM
- High-level proof idea
 - \mathcal{S} maintains graph: edges correspond to f -evaluations
 - Complete paths should be in correspondence with RO
- Technical details in paper

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

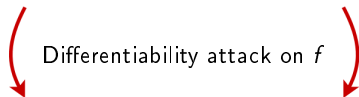
pre f	sec f	col f	pre \mathcal{H}	sec \mathcal{H}	col \mathcal{H}	indiff \mathcal{H}
			2^n f ideal	2^n f ideal	$2^{n/2}$ f ideal	$2^{n/2}$ f ideal


 Differentiability attack on f

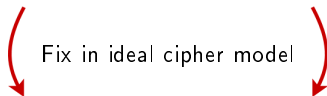
pre f	sec f	col f	pre \mathcal{H}	sec \mathcal{H}	col \mathcal{H}	indiff \mathcal{H}

Conclusions

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

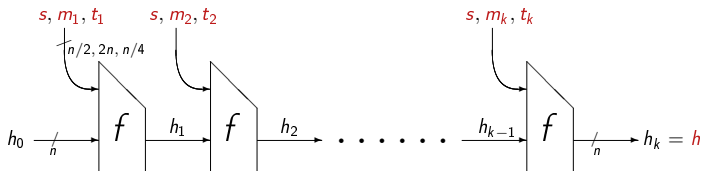

 Fix in ideal cipher model

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

Supporting Slides

SUPPORTING SLIDES

Indifferentiability of BLAKE



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

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

- 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 $h \xrightarrow{s \parallel m \parallel t} h'$
- Complete path: $h_0 \xrightarrow{s \parallel m_1 \parallel t_1} h_1 \dots \xrightarrow{s \parallel m_k \parallel t_k} h_k$ for correctly padded $(m_1, \dots, m_k), (t_1, \dots, t_k)$

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
