Security Analysis of BLAKE2's Modes of Operation

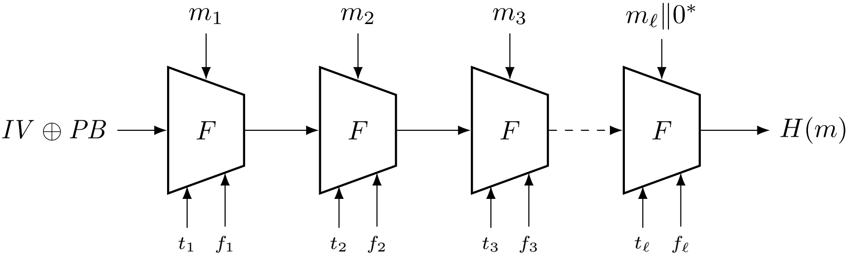
Atul Luykx, Bart Mennink, Samuel Neves

KU Leuven (Belgium) and Radboud University (The Netherlands)

FSE 2017

March 7, 2017

BLAKE2



- Cryptographic hash function
- Aumasson, Neves, Wilcox-O'Hearn, Winnerlein (2013)
- Simplification of SHA-3 finalist BLAKE

BLAKE2

Use in Password Hashing

- Argon2 (Biryukov et al.)
- Catena (Forler et al.)
- Lyra (Almeida et al.)
- Lyra2 (Simplício Jr. et al.)
- Rig (Chang et al.)

Use in Authenticated Encryption

- AEZ (Hoang et al.)

Applications

- Noise Protocol Framework (Perrin)
- Zcash Protocol (Hopwood et al.)
- RAR 5.0 (Roshal)

Security Inheritance?

	BLAKE
cryptanalysis	Aumasson et al. 2010 Biryukov et al. 2011 Dunkelman&K. 2011
generic	Andreeva et al. 2012 Chang et al. 2012

Security Inheritance?

	BLAKE	BLAKE2
cryptanalysis	Aumasson et al. 2010 Biryukov et al. 2011 Dunkelman&K. 2011	Guo et al. 2014 Hao 2014 Khovratovich et al. 2015 Espitau et al. 2015
generic	Andreeva et al. 2012 Chang et al. 2012	

Security Inheritance?

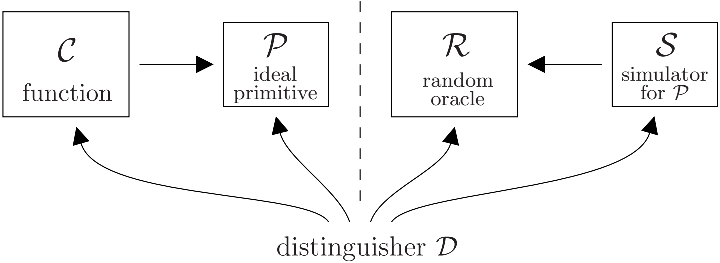
	BLAKE	BLAKE2
cryptanalysis	Aumasson et al. 2010 Biryukov et al. 2011 Dunkelman&K. 2011	Guo et al. 2014 Hao 2014 Khovratovich et al. 2015 Espitau et al. 2015
generic	Andreeva et al. 2012 Chang et al. 2012	???

Security Inheritance?

	BLAKE	BLAKE2
cryptanalysis	Aumasson et al. 2010 Biryukov et al. 2011 Dunkelman&K. 2011	Guo et al. 2014 Hao 2014 Khovratovich et al. 2015 Espitau et al. 2015
generic	Andreeva et al. 2012 Chang et al. 2012	???

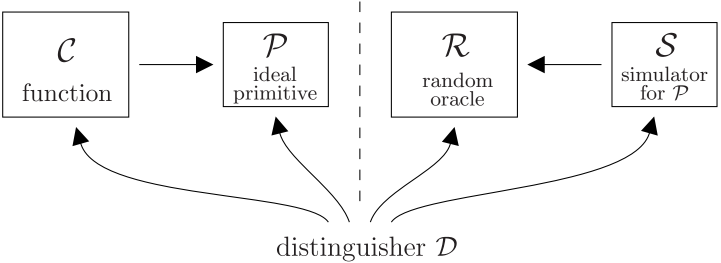
Even slight modifications may make a scheme insecure!

Indifferentiability



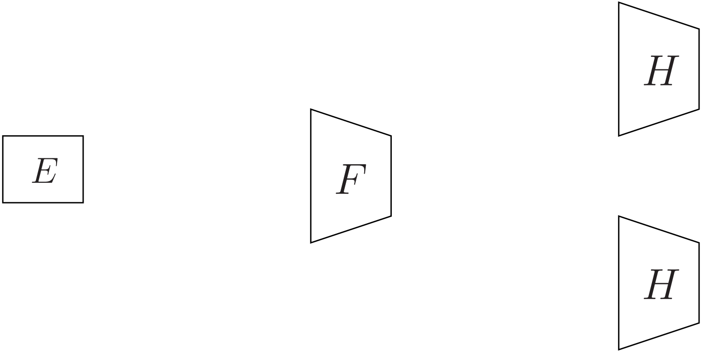
- Indifferentiability of function $\mathcal{C}$ from a random oracle
- $\mathcal{C}^{\mathcal{P}}$ is indifferentiable from $\mathcal{R}$ if $\exists$ simulator $\mathcal{S}$ such that $(\mathcal{C}, \mathcal{P})$ and $(\mathcal{R}, \mathcal{S})$ indistinguishable

Indifferentiability

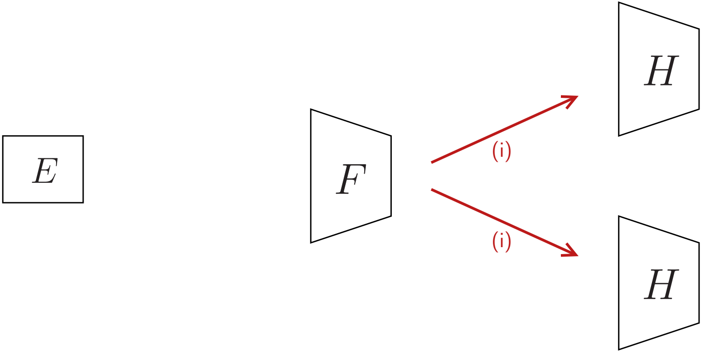


- Indifferentiability of function $\mathcal{C}$ from a random oracle
- $\mathcal{C}^{\mathcal{P}}$ is indifferentiable from $\mathcal{R}$ if $\exists$ simulator $\mathcal{S}$ such that $(\mathcal{C}, \mathcal{P})$ and $(\mathcal{R}, \mathcal{S})$ indistinguishable
- No structural design flaws
- Well-suited for composition

Composition



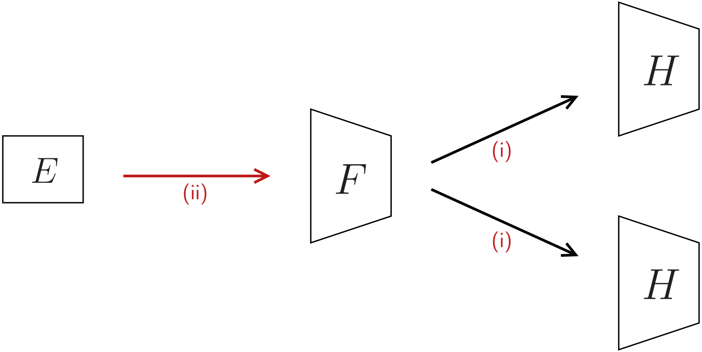
Composition



(i) First hash-function indifferentiability results

- Chop-/PF-MD with ideal $F \longrightarrow$ indifferentiable

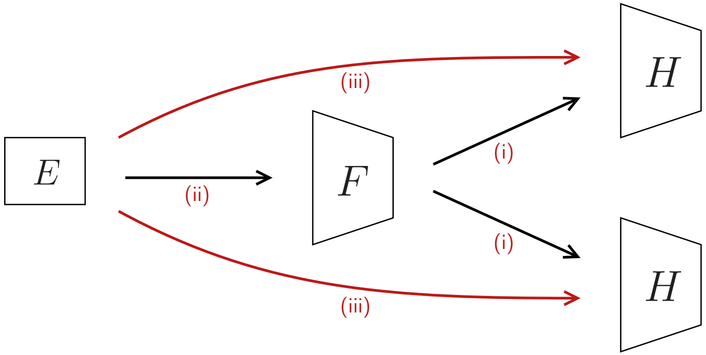
Composition



(i) First hash-function indifferentiability results
- Chop-/PF-MD with ideal $F \longrightarrow$ indifferentiable

(ii) Most obvious second step (composition)
- But (e.g.) Davies-Meyer with ideal $E \longrightarrow$ differentiable

Composition

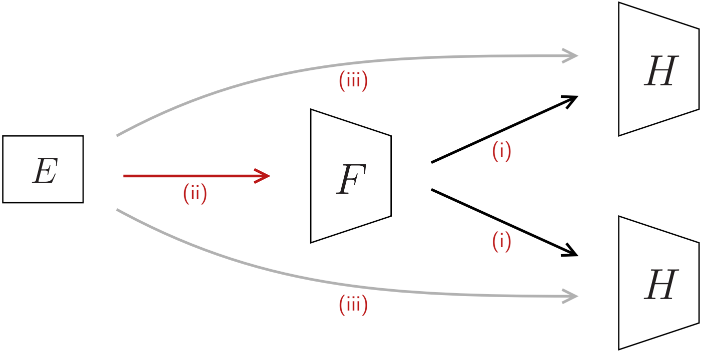


(i) First hash-function indifferentiability results
- Chop-/PF-MD with ideal $F \longrightarrow$ indifferentiable

(ii) Most obvious second step (composition)
- But (e.g.) Davies-Meyer with ideal $E \longrightarrow$ differentiable

(iii) Researchers focused on direct proofs
- Chop-/PF-MD with Davies-Meyer and ideal $E \longrightarrow$ indifferentiable

Composition



(i) First hash-function indifferentiability results
- Chop-/PF-MD with ideal $F \longrightarrow$ indifferentiable

(ii) Most obvious second step (composition)
- But (e.g.) Davies-Meyer with ideal $E \longrightarrow$ differentiable

(iii) Researchers focused on direct proofs
- Chop-/PF-MD with Davies-Meyer and ideal $E \longrightarrow$ indifferentiable

Our Results

Compression Level Indifferentiability

- BLAKE2 indifferentiable at compression function level
- Immediately implies
  - indifferentiability of sequential hash mode
  - indifferentiability of tree/parallel hash mode
  - multi-key PRF security of keyed BLAKE2 mode
- One proof fits all!

Our Results

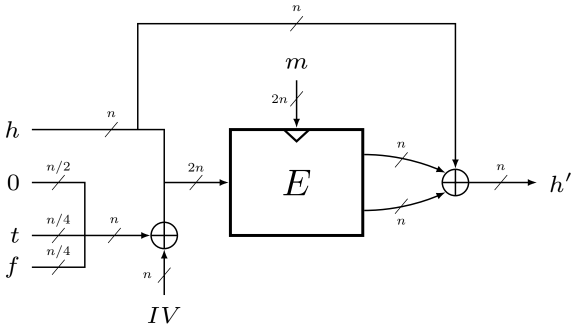
Compression Level Indifferentiability

- BLAKE2 indifferentiable at compression function level
- Immediately implies
  - indifferentiability of sequential hash mode
  - indifferentiability of tree/parallel hash mode
  - multi-key PRF security of keyed BLAKE2 mode
- One proof fits all!

Weakly Ideal Cipher Model

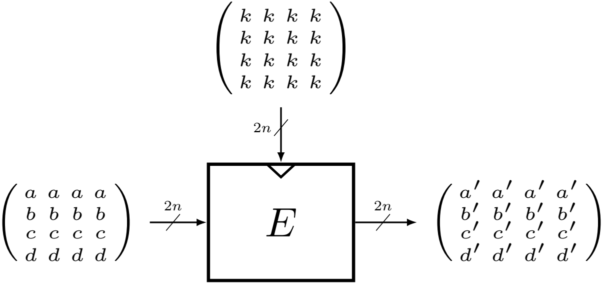
- BLAKE2 cipher has known, but harmless, properties
- Analysis tolerates these properties

BLAKE2 Compression Function

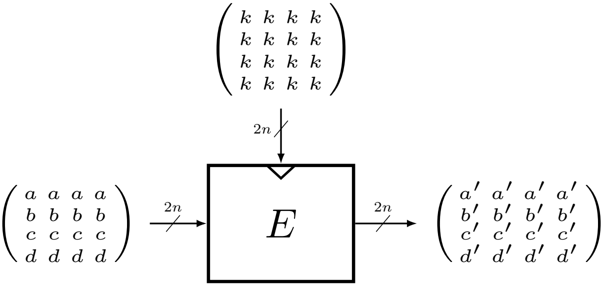


- h is state, m is message, t is counter, f is flag
- IV is initialization value

Underlying Block Cipher



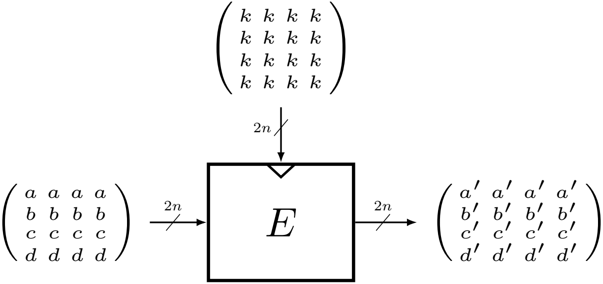
Underlying Block Cipher



Weakly Ideal Cipher Model

- E is an ideal cipher modulo above property

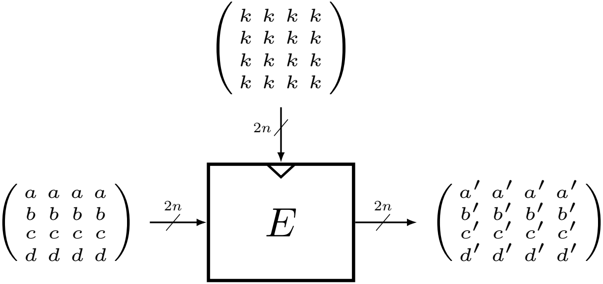
Underlying Block Cipher



Weakly Ideal Cipher Model

- E is an ideal cipher modulo above property
- Weak- and strong-subspace invariance for weak keys

Underlying Block Cipher

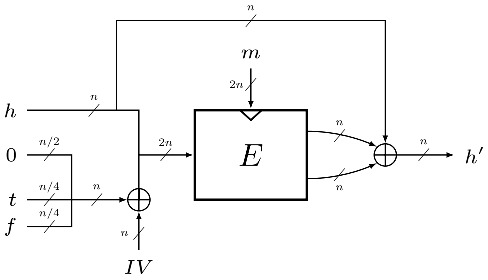


Weakly Ideal Cipher Model

- E is an ideal cipher modulo above property
- Weak- and strong-subspace invariance for weak keys
- Evaluation of E in BLAKE2 is never weak
  (as left half of IV is not of the form $cccc$)

Proof Idea

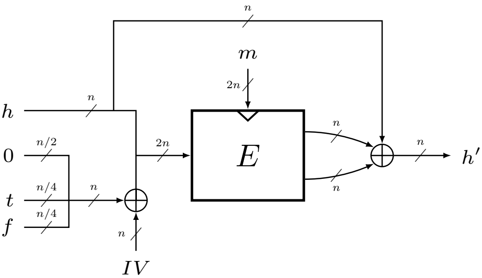
Construction F^E:



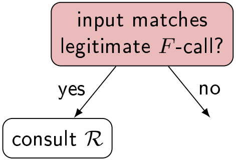
Simulator $\mathcal{S}$:

Proof Idea

Construction F^E:

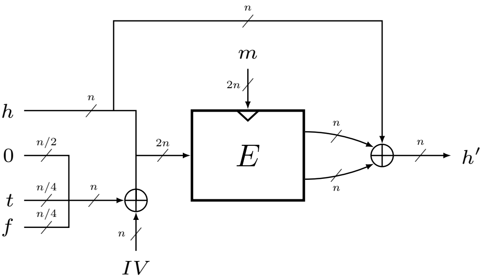


Simulator $\mathcal{S}$:

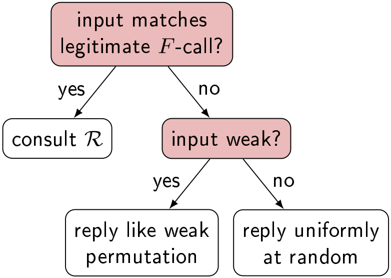


Proof Idea

Construction F^E:

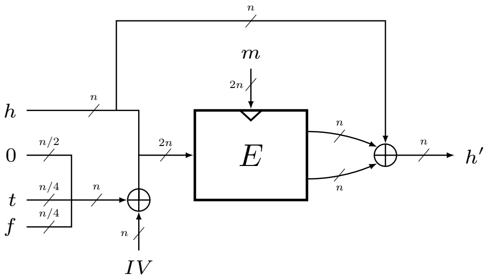


Simulator $\mathcal{S}$:

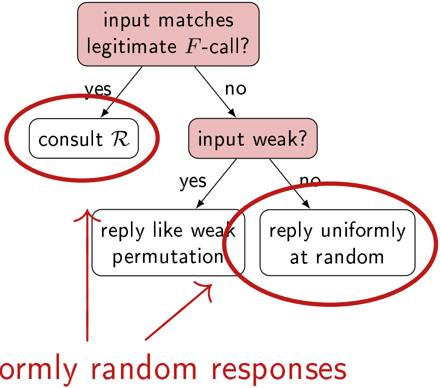


Proof Idea

Construction F^E:

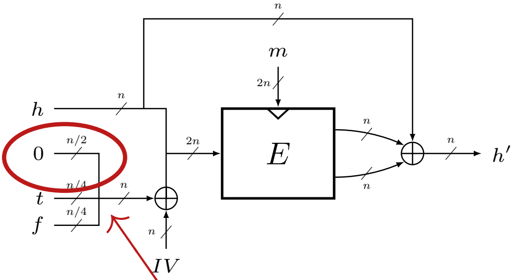


Simulator $\mathcal{S}$:



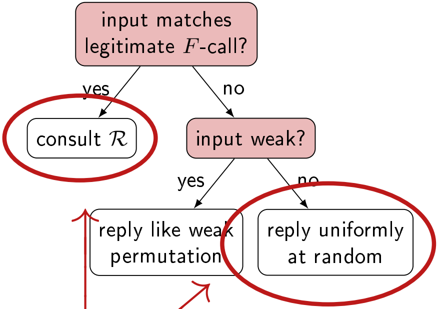
Proof Idea

Construction F^E:



inverse query hits 0-block

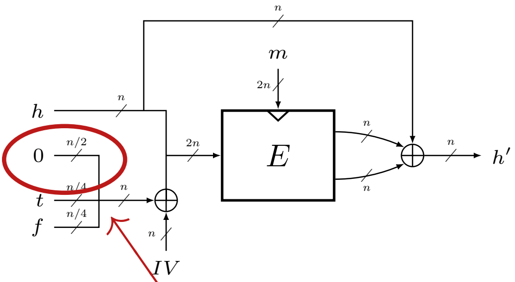
Simulator $\mathcal{S}$:



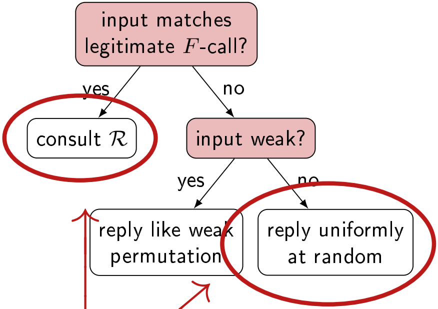
collision in uniformly random responses

Proof Idea

Construction F^E:



Simulator $\mathcal{S}$:

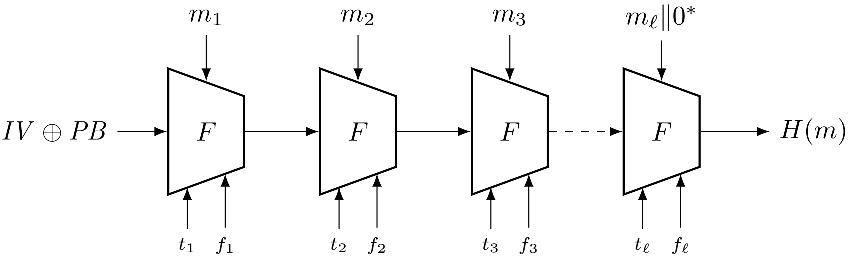


inverse query hits 0-block

collision in uniformly random responses

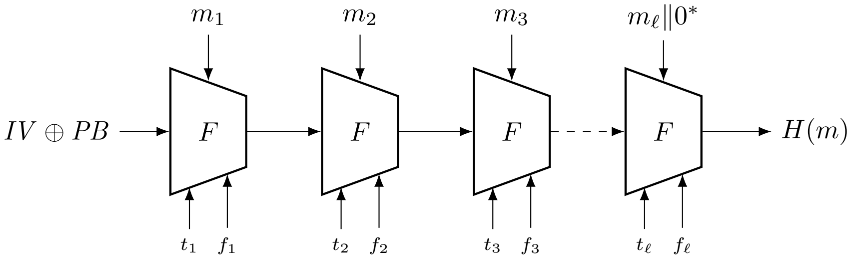
$$\mathsf{Indiff}_{F^E,\mathcal{S}}(q) = \Theta\left(\frac{q}{2^{n/2}}\right)$$

BLAKE2 Hashing Modes



- Message m padded into $m_1 \| \cdots \| m_\ell$
- $t_1 \| \cdots \| t_\ell$ are counter values, $f_1 \| \cdots \| f_\ell$ are flags
- PB is a parameter block

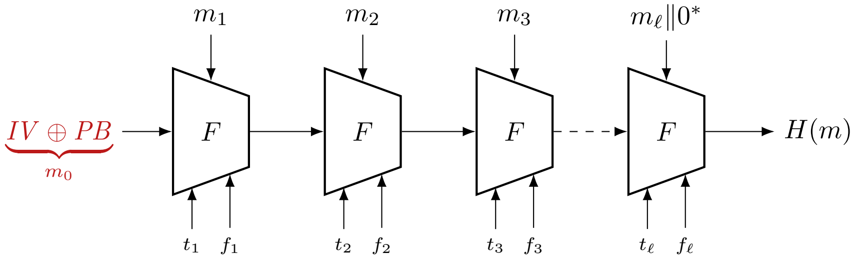
BLAKE2 Hashing Modes



- Message m padded into $m_1 \| \cdots \| m_\ell$
- $t_1 \| \cdots \| t_\ell$ are counter values, $f_1 \| \cdots \| f_\ell$ are flags
- PB is a parameter block

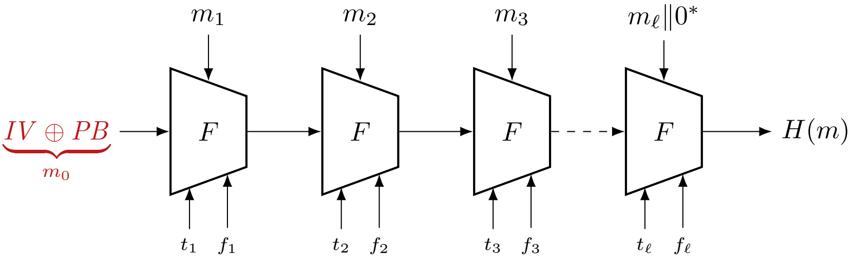
Prefix-Free Merkle-Damgård?

BLAKE2 Hashing Modes



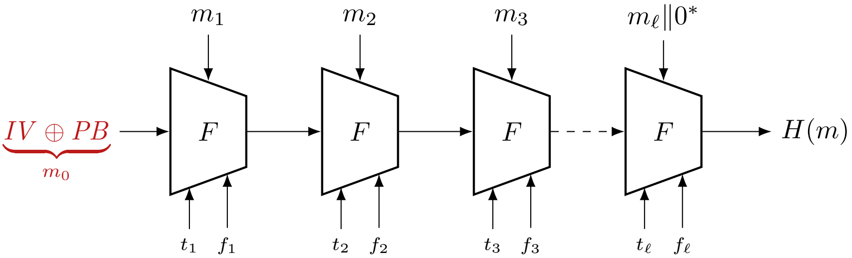
- PB is largely freely choosable by user
  $\rightarrow$ Essentially just an extra message block m_0

BLAKE2 Hashing Modes



- PB is largely freely choosable by user
  $\rightarrow$ Essentially just an extra message block m_0
- Captured by generalized design of Bertoni et al. 2014

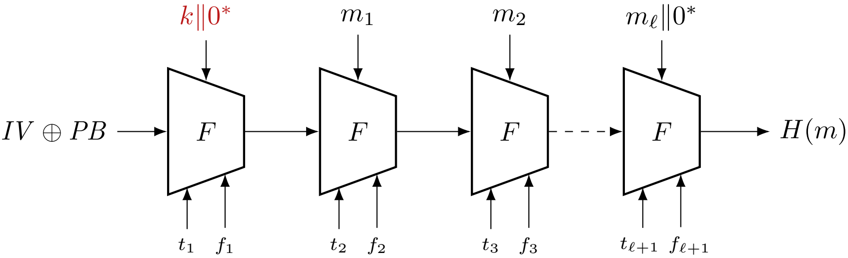
BLAKE2 Hashing Modes



- PB is largely freely choosable by user
  $\rightarrow$ Essentially just an extra message block m_0
- Captured by generalized design of Bertoni et al. 2014

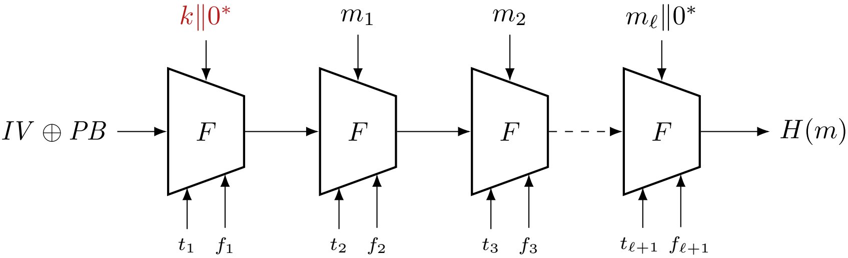
- Same reasoning for tree and parallel modes of BLAKE2

Keyed BLAKE2 Mode



- Key k as first message block, rest unchanged

Keyed BLAKE2 Mode

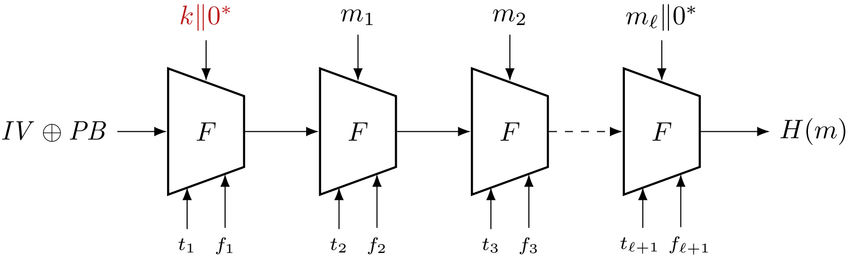


- Key k as first message block, rest unchanged

1. Multi-key PRF security if BLAKE2 is random oracle

$$\mathsf{Prf}_{KH^E}(q) = \frac{\mu q}{2^\kappa} + \frac{\binom{\mu}{2}}{2^\kappa}$$

Keyed BLAKE2 Mode



- Key k as first message block, rest unchanged

1. Multi-key PRF security if BLAKE2 is random oracle
2. Indifferentiability of BLAKE2 with weakly ideal cipher

$$\mathsf{Prf}_{KH^E}(q) = \frac{\mu q}{2^\kappa} + \frac{\binom{\mu}{2}}{2^\kappa} + \Theta\left(\frac{q}{2^{n/2}}\right)$$

Conclusion

Indifferentiability of BLAKE2

- Short compression function indifferentiability proof
- Security of hashing modes due to composition

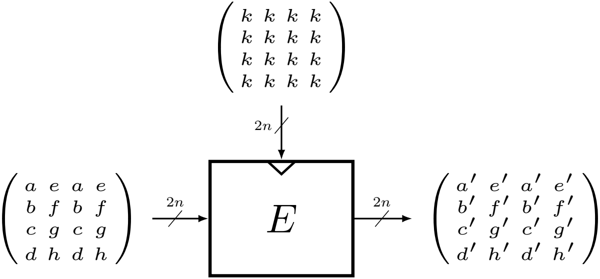
Optimality?

- Birthday bound security in the end
- Improved analysis for (second) preimage resistance?
- PRF security: direct analysis could give better result

Thank you for your attention!

Supporting Slides

Underlying Block Cipher



"Cryptanalysis of NORX v2.0" by Chaigneau et al.

- An unexpected structural property of E
- Analysis easily extends to this property
- Left half of IV is not of the form $cgcg$ either