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
- 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)
<table>
<thead>
<tr>
<th>Security Inheritance?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BLAKE</strong></td>
</tr>
</tbody>
</table>
| **cryptanalysis** | Aumasson et al. 2010  
| | Biryukov et al. 2011  
| | Dunkelman & K. 2011 |
| **generic** | Andreeva et al. 2012  
| | Chang et al. 2012 |
Security Inheritance?

<table>
<thead>
<tr>
<th></th>
<th>BLAKE</th>
<th>BLAKE2</th>
</tr>
</thead>
<tbody>
<tr>
<td>cryptanalysis</td>
<td>Aumasson et al. 2010</td>
<td>Guo et al. 2014</td>
</tr>
<tr>
<td></td>
<td>Biryukov et al. 2011</td>
<td>Hao 2014</td>
</tr>
<tr>
<td></td>
<td>Dunkelman &amp; K. 2011</td>
<td>Khovratovich et al. 2015</td>
</tr>
<tr>
<td>generic</td>
<td>Andreeva et al. 2012</td>
<td>Espitau et al. 2015</td>
</tr>
<tr>
<td></td>
<td>Chang et al. 2012</td>
<td></td>
</tr>
</tbody>
</table>
## Security Inheritance?

<table>
<thead>
<tr>
<th></th>
<th>BLAKE</th>
<th>BLAKE2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>cryptanalysis</strong></td>
<td>Aumasson et al. 2010</td>
<td>Guo et al. 2014</td>
</tr>
<tr>
<td></td>
<td>Biryukov et al. 2011</td>
<td>Hao 2014</td>
</tr>
<tr>
<td></td>
<td>Dunkelman&amp;K. 2011</td>
<td>Khovratovich et al. 2015</td>
</tr>
<tr>
<td><strong>generic</strong></td>
<td>Andreeva et al. 2012</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Chang et al. 2012</td>
<td>???</td>
</tr>
</tbody>
</table>

Even slight modifications may make a scheme insecure!
## Security Inheritance?

<table>
<thead>
<tr>
<th>Cryptanalysis</th>
<th>BLAKE</th>
<th>BLAKE2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Aumasson et al. 2010</td>
<td>Guo et al. 2014</td>
</tr>
<tr>
<td></td>
<td>Biryukov et al. 2011</td>
<td>Hao 2014</td>
</tr>
<tr>
<td></td>
<td>Dunkelman &amp; K. 2011</td>
<td>Khovratovich et al. 2015</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Espitau et al. 2015</td>
</tr>
<tr>
<td>Generic</td>
<td>Andreeva et al. 2012</td>
<td>???</td>
</tr>
<tr>
<td></td>
<td>Chang et al. 2012</td>
<td></td>
</tr>
</tbody>
</table>

Even slight modifications may make a scheme insecure!
Indifferentiability

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

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

(i) First hash-function indierentiability results
- Chop-/PF-MD with ideal $F$ → indierentiable

(ii) Most obvious second step (composition)
- But (e.g.) Davies-Meyer with ideal $E$ → dierentiable

(iii) Researchers focused on direct proofs
- Chop-/PF-MD with Davies-Meyer and ideal $E$ → indierentiable
(i) First hash-function indifferentiability results

- Chop-/PF-MD with ideal $F \rightarrow$ indifferentiable
Composition

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

(ii) Most obvious second step (composition)
   - But (e.g.) Davies-Meyer with ideal \( E \rightarrow \) differentiable
(i) First hash-function indifferentiability results
   - Chop-/PF-MD with ideal $F \rightarrow$ indifferentiable

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

(iii) Researchers focused on direct proofs
   - Chop-/PF-MD with Davies-Meyer and ideal $E \rightarrow$ indifferentiable
(i) First hash-function indifferentiability results
   • Chop-/PF-MD with ideal $F \rightarrow$ indifferentiable

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

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

\[
\begin{pmatrix}
k & k & k & k \\
k & k & k & k \\
k & k & k & k \\
k & k & k & k \\
\end{pmatrix}
\]

\[
\begin{pmatrix}
\begin{pmatrix}
a & a & a & a \\
b & b & b & b \\
c & c & c & c \\
d & d & d & d \\
\end{pmatrix} \rightarrow
\begin{pmatrix}
a' & a' & a' & a' \\
b' & b' & b' & b' \\
c' & c' & c' & c' \\
d' & d' & d' & d' \\
\end{pmatrix}
\end{pmatrix}
\]

Weakenly 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`)
Underlying Block Cipher

\[
\begin{pmatrix}
  k & k & k & k \\
  k & k & k & k \\
  k & k & k & k \\
  k & k & k & k \\
\end{pmatrix}
\]

\[
\begin{pmatrix}
  a & a & a & a \\
  b & b & b & b \\
  c & c & c & c \\
  d & d & d & d \\
\end{pmatrix}
\xrightarrow{2n}
\begin{pmatrix}
  a' & a' & a' & a' \\
  b' & b' & b' & b' \\
  c' & c' & c' & c' \\
  d' & d' & d' & d' \\
\end{pmatrix}
\]

Weakly Ideal Cipher Model

- \( E \) is an ideal cipher modulo above property
Underlying Block Cipher

\[
\begin{pmatrix}
k & k & k & k \\
k & k & k & k \\
k & k & k & k \\
k & k & k & k \\
\end{pmatrix}
\]

\[
\begin{pmatrix}
a & a & a & a \\
b & b & b & b \\
c & c & c & c \\
d & d & d & d \\
\end{pmatrix}
\rightarrow
\begin{pmatrix}
a' & a' & a' & a' \\
b' & b' & b' & b' \\
c' & c' & c' & c' \\
d' & d' & d' & d' \\
\end{pmatrix}
\]

Weakly Ideal Cipher Model

- \( E \) is an ideal cipher modulo above property
- Weak- and strong-subspace invariance for weak keys
Underlying Block Cipher

\[
\begin{pmatrix}
k & k & k & k \\
k & k & k & k \\
k & k & k & k \\
k & k & k & k \\
\end{pmatrix}
\]

\[
\begin{pmatrix}
a & a & a & a \\
b & b & b & b \\
c & c & c & c \\
d & d & d & d \\
\end{pmatrix}
\rightarrow
E
\rightarrow
\begin{pmatrix}
a' & a' & a' & a' \\
b' & b' & b' & b' \\
c' & c' & c' & c' \\
d' & d' & d' & d' \\
\end{pmatrix}
\]

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 $S$:

\begin{align*}
&\text{Input matches legitimate } F^E\text{-call?} \\
&\text{consult } \text{Yes} \\
&\text{input weak?} \\
&\text{reply like weak permutation } \text{Yes} \\
&\text{reply uniformly at random } \text{No} \\
&\text{Indifferent } F^E, S(q) = \Theta(q^2 n/2) \\
&\rightarrow \text{collision in uniformly random responses} \\
&\rightarrow \text{inverse query hits 0-block} \\
\end{align*}
Proof Idea

Construction $F^E$:

Simulator $S$:

- **input matches legitimate $F$-call?**
  - yes
  - no

- consult $R$
Proof Idea

Construction $F^E$:

Simulator $S$:

- input matches legitimate $F$-call?
  - yes: consult $R$
  - no: input weak?
    - yes: reply like weak permutation
    - no: reply uniformly at random
Proof Idea

Construction $F^E$:

Simulator $S$:

input matches legitimate $F$-call?  
yes → consult $R$  
no → input weak?  
yes → reply like weak permutation  
no → reply uniformly at random

collision in uniformly random responses
Proof Idea

**Construction** $F^E$:

- **Simulator** $S$:
  - input matches legitimate $F$-call?
  - yes, consult $R$
  - no
  - input weak?
    - yes
      - reply like weak permutation
    - no
      - reply uniformly at random

- inverse query hits 0-block
- collision in uniformly random responses

\[
\begin{align*}
E_n &
\end{align*}
\]
Proof Idea

**Construction** $F^E$: 

**Simulator** $S$: 

\[
\text{Indiff}_{F^E,S}(q) = \Theta \left( \frac{q}{2^{n/2}} \right)
\]
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 $m_1 \parallel \cdots \parallel m_\ell$
- $t_1 \parallel \cdots \parallel t_\ell$ are counter values, $f_1 \parallel \cdots \parallel f_\ell$ are flags
- $PB$ is a parameter block

Prefix-Free Merkle-Damgård?
BLAKE2 Hashing Modes

- $PB$ is largely freely choosable by user
  → Essentially just an extra message block $m_0$
BLAKE2 Hashing Modes

- $PB$ is largely freely choosable by user
  → 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
  → 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

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

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

\[
\begin{pmatrix}
  k & k & k & k \\
  k & k & k & k \\
  k & k & k & k \\
  k & k & k & k \\
\end{pmatrix}
\]

\[
\begin{pmatrix}
a & e & a & e \\
b & f & b & f \\
c & g & c & g \\
d & h & d & h \\
\end{pmatrix}
\]

\[
\begin{pmatrix}
a' & e' & a' & e' \\
b' & f' & b' & f' \\
c' & g' & c' & g' \\
d' & h' & d' & h' \\
\end{pmatrix}
\]

“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