Boomerang Attacks against ARX Hash Functions

Gaëtan Leurent & Arnab Roy

Gaëtan Leurent
University of Luxembourg
Introduction to Hash Functions
An Ideal Hash Function: the Random Oracle

- Public Random Oracle
- The output can be used as a fingerprint of the document
An Ideal Hash Function: the Random Oracle

- Public Random Oracle
- The output can be used as a fingerprint of the document

G. Leurent (uni.lu),
Boomerang Attacks against ARX Hash Functions
A Concrete Hash Function

- A public function with no structural property.
  - Should behave like a random function.
  - Cryptographic strength without any key!

- $F : \{0, 1\}^* \rightarrow \{0, 1\}^n$

$$0x1d66ca77ab361c6f$$
A Concrete Hash Function

- A public function with no structural property.
  - Should behave like a random function.
  - Cryptographic strength without any key!

- $F : \{0, 1\}^* \rightarrow \{0, 1\}^n$

- $0x1d66ca77ab361c6f$
Using Hash Functions

Hash functions are used in many different contexts:

- To generate **unique identifiers**
  - Hash-and-sign signatures
  - Commitment schemes

- As a **one-way** function
  - One-Time-Passwords
  - Forward security

- To **break the structure** of the input
  - Entropy extractors
  - Key derivation
  - Pseudo-random number generator

- To build **MACs**
  - HMAC
  - Challenge/response authentication
The SHA-3 Competition

After Wang et al.’s attacks on the MD/SHA family, we need new hash functions

The SHA-3 competition

- Organized by NIST
- Similar to the AES competition
- Submission deadline was October 2008: 64 candidates
- 51 valid submissions
- 14 in the second round (July 2009)
- 5 finalists in December 2010:
  - Blake, Grøstl, JH, Keccak, Skein
- Winner in 2012?
Hash Function Design

- Build a small compression function, and iterate.
  - Cut the message in chunks $M_0, \ldots M_k$
  - $H_i = f(M_i, H_{i-1})$
  - $F(M) = H_k$
Boomerang Attacks
Boomerang Attacks

- Introduced by Wagner, many later improvements

- Combine **two short differentials** instead of using a long one.
  - $f = f_b \circ f_a$
  - for $f_a$, $\alpha \rightarrow \alpha'$ with probability $p_a$
  - for $f_b$, $\gamma \rightarrow \gamma'$ with probability $p_b$
  - Interesting when we don’t know how to build iterative differentials.

- Uses an **encryption oracle** together with a **decryption oracle**
  - Adaptive attack
Boomerang Attacks

1. Start with $P^{(0)}, P^{(1)}$
2. Compute $C^{(0)}, C^{(1)}$
3. Build $C^{(2)}, C^{(3)}$
4. Compute $P^{(2)}, P^{(3)}$

$$C = \frac{1}{p_a} \frac{1}{p_b} \frac{1}{p_a}$$

$$P^{(0)} \oplus P^{(1)} = \alpha$$
$$P^{(2)} \oplus P^{(3)} = \alpha$$
$$C^{(0)} \oplus C^{(1)} = \gamma'$$
$$C^{(2)} \oplus C^{(3)} = \gamma'$$
Boomerang Attacks

1. Start with $P^{(0)}$, $P^{(1)}$
2. Compute $C^{(0)}$, $C^{(1)}$
3. Build $C^{(2)}$, $C^{(3)}$
4. Compute $P^{(2)}$, $P^{(3)}$

\[ \Pr[\alpha \rightarrow \alpha'] = p_a \]
\[ \Pr[\gamma \rightarrow \gamma'] = p_b \]

\[ C = \frac{1}{p_a} \frac{1}{p_b^2} \]

\[ P^{(0)} \oplus P^{(1)} = \alpha \]
\[ P^{(2)} \oplus P^{(3)} = \alpha \]
\[ C^{(0)} \oplus C^{(1)} = \gamma' \]
\[ C^{(2)} \oplus C^{(3)} = \gamma' \]
Boomerang Attacks

1. Start with $P^{(0)}, P^{(1)}$
2. Compute $C^{(0)}, C^{(1)}$
3. Build $C^{(2)}, C^{(3)}$
4. Compute $P^{(2)}, P^{(3)}$

$Pr[\alpha \rightarrow \alpha'] = p_a$

$C = \frac{1}{p_a} \frac{1}{p_a^2} \frac{1}{p_b}$

$P^{(0)} \oplus P^{(1)} = \alpha$

$P^{(2)} \oplus P^{(3)} = \alpha$

$C^{(0)} \oplus C^{(1)} = \gamma'$

$C^{(2)} \oplus C^{(3)} = \gamma'$
Boomerang Attacks

1. Start with $P^{(0)}, P^{(1)}$
2. Compute $C^{(0)}, C^{(1)}$
3. Build $C^{(2)}, C^{(3)}$
4. Compute $P^{(2)}, P^{(3)}$

$$C = \frac{1}{p_a} \frac{1}{p_b^2} \frac{1}{p_a}$$

$$P^{(0)} \oplus P^{(1)} = \alpha$$
$$P^{(2)} \oplus P^{(3)} = \alpha$$
$$C^{(0)} \oplus C^{(1)} = \gamma'$$
$$C^{(2)} \oplus C^{(3)} = \gamma'$$

$$\Pr[\alpha \rightarrow \alpha'] = p_a$$
$$\Pr[\gamma \rightarrow \gamma'] = p_b$$
Boomerang Attacks

1. Start with $P^{(0)}, P^{(1)}$
2. Compute $C^{(0)}, C^{(1)}$
3. Build $C^{(2)}, C^{(3)}$
4. Compute $P^{(2)}, P^{(3)}$

$$C = \frac{1}{p_a} \frac{1}{p_b} \frac{1}{p_a}$$

$$P^{(0)} \oplus P^{(1)} = \alpha$$
$$P^{(2)} \oplus P^{(3)} = \alpha$$
$$C^{(0)} \oplus C^{(1)} = \gamma'$$
$$C^{(2)} \oplus C^{(3)} = \gamma'$$
Boomerang Attacks

1. Start with $P^{(0)}, P^{(1)}$
2. Compute $C^{(0)}, C^{(1)}$
3. Build $C^{(2)}, C^{(3)}$
4. Compute $P^{(2)}, P^{(3)}$

\[
C = \frac{1}{p_a} \frac{1}{p_b^2} \frac{1}{p_a}
\]

\[
\begin{align*}
P^{(0)} &\oplus P^{(1)} = \alpha \\
C^{(0)} &\oplus C^{(1)} = \gamma' \\
C^{(2)} &\oplus C^{(3)} = \gamma'
\end{align*}
\]
Boomerang Attacks

1. Start with $P^{(0)}, P^{(1)}$
2. Compute $C^{(0)}, C^{(1)}$
3. Build $C^{(2)}, C^{(3)}$
4. Compute $P^{(2)}, P^{(3)}$

\[
\Pr[\alpha \rightarrow \alpha'] = p_a
\]
\[
\Pr[\gamma \rightarrow \gamma'] = p_b
\]
\[
C = \frac{1}{p_a} \frac{1}{p_b^2} \frac{1}{p_a}
\]
\[
P^{(0)} \oplus P^{(1)} = \alpha
\]
\[
P^{(2)} \oplus P^{(3)} = \alpha
\]
\[
C^{(0)} \oplus C^{(1)} = \gamma'
\]
\[
C^{(2)} \oplus C^{(3)} = \gamma'
\]
Improvements to the Boomerang Attack

1. Amplified probabilities
   - Do not specify $\alpha'$ and $\gamma$
   - $\hat{p}_a = \sqrt{\sum \alpha' \Pr[\alpha \rightarrow \alpha']}$
   - $\hat{p}_b = \sqrt{\sum \gamma \Pr[\gamma \rightarrow \gamma']}$

2. Related-key
   - $p_a = \Pr[\alpha \xrightarrow{\alpha_k} \alpha']$
   - $p_b = \Pr[\gamma \xrightarrow{\gamma_k} \gamma']$
Improvements to the Boomerang Attack

1. Amplified probabilities
   - Do not specify $\alpha'$ and $\gamma$
   - $\hat{p}_a = \sqrt{\sum \alpha' \Pr[\alpha \rightarrow \alpha']}$
   - $\hat{p}_b = \sqrt{\sum \gamma \Pr[\gamma \rightarrow \gamma']}$

2. Related-key
   - $p_a = \Pr[\alpha \xrightarrow{\alpha_k} \alpha']$
   - $p_b = \Pr[\gamma \xrightarrow{\gamma_k} \gamma']$
Boomerang Attacks on Hash Functions

Most hash functions are based on a block cipher:

- Davies-Meyer $f(h, m) = E_m(h) \oplus h$
- Matyas-Meyer-Oseas $f(h, m) = E_h(m) \oplus m$

A (related-key) boomerang attack gives a quartet:

$$\sum P^{(i)} = 0 \quad \sum C^{(i)} = 0 \quad \sum K^{(i)} = 0$$

This is a zero-sum for the compression function:

$$\sum h^{(i)} = 0 \quad \sum m^{(i)} = 0 \quad \sum f(h^{(i)}, m^{(i)}) = 0$$

In general this is hard:

- $\sum f(h, m) = 0$, best attack $2^{n/3}$, lower bound $2^{n/4}$
- $\sum f(h, m) = \sum h = \sum m = 0$, best attack $2^{n/2}$, lower bound $2^{n/3}$

With a known key, one can start from the middle

Message modification
Using Auxiliary Paths

- Divide $f$ in three sub-functions: $f = f_c \circ f_b \circ f_a$
  - for $f_a$, $\alpha \rightarrow \alpha'$ with probability $p_a$
  - for $f_b$, $\beta_j \rightarrow \beta'_j$ with probability $p_b$
  - for $f_c$, $\gamma \rightarrow \gamma'$ with probability $p_c$

1. Start with a boomerang quartet for $f_b$:
   \[
   U^{(1)} = U^{(0)} + \alpha' \quad U^{(3)} = U^{(2)} + \alpha' \\
   V^{(2)} = V^{(0)} + \gamma \quad V^{(2)} = V^{(1)} + \gamma
   \]

2. For each auxiliary path, construct $U^{(i)}_* = U^{(i)} + \beta_j$.
   With probability $p_b^4$, $V^{(i)}_* = V^{(i)} + \beta'_j$, and we have a new quartet:
   \[
   U^{(1)}_* = U^{(0)}_* + \alpha' \quad U^{(3)}_* = U^{(2)}_* + \alpha' \\
   V^{(2)}_* = V^{(0)}_* + \gamma \quad V^{(2)}_* = V^{(1)}_* + \gamma
   \]

3. Check if the $f_a$ and $f_b$ paths are satisfied.
$U(0) \rightarrow U(1) \rightarrow U(2) \rightarrow U(3)$
$V(0) \rightarrow V(1) \rightarrow V(2) \rightarrow V(3)$

$f_a$
$Pr[\alpha \rightarrow \alpha'] = p_a$

$f_b$
$Pr[\beta_j \rightarrow \beta_j'] = p_b$

$f_c$
$Pr[\gamma \rightarrow \gamma'] = p_c$
\[ f_a \Pr[\alpha \rightarrow \alpha'] = p_a \]

\[ f_b \Pr[\beta_j \rightarrow \beta'_j] = p_b \]

\[ f_c \Pr[\gamma \rightarrow \gamma'] = p_c \]
\[ f_a \quad \Pr[\alpha \rightarrow \alpha'] = p_a \]

\[ f_b \quad \Pr[\beta_j \rightarrow \beta'_j] = p_b \]

\[ f_c \quad \Pr[\gamma \rightarrow \gamma'] = p_c \]
$U^{(0)} \rightarrow \alpha' \rightarrow U^{(1)} \rightarrow \beta_j \rightarrow U_*^{(0)} \rightarrow \alpha' \rightarrow U_*^{(1)} \rightarrow \beta_j \rightarrow U_*^{(2)} \rightarrow \beta_j \rightarrow U_*^{(3)} \rightarrow \beta_j' \rightarrow V_*^{(0)} \rightarrow \gamma' \rightarrow V_*^{(1)} \rightarrow \gamma' \rightarrow V_*^{(2)} \rightarrow \gamma' \rightarrow V_*^{(3)} \rightarrow \gamma'$

\[ f_a \Rightarrow \Pr[\alpha \rightarrow \alpha'] = p_a \]

\[ f_b \Rightarrow \Pr[\beta_j \rightarrow \beta_j'] = p_b \]

\[ f_c \Rightarrow \Pr[\gamma \rightarrow \gamma'] = p_c \]
\[
\alpha' \quad \beta_j \quad \alpha' \quad \beta_j \quad \alpha' \quad \beta_j \\
\gamma' \quad \gamma \quad \gamma' \quad \gamma \quad \gamma' \quad \gamma
\]

\[
f_a \quad \Pr[\alpha \rightarrow \alpha'] = p_a \\
f_b \quad \Pr[\beta_j \rightarrow \beta_j'] = p_b \\
f_c \quad \Pr[\gamma \rightarrow \gamma'] = p_c
\]
Using Auxiliary Paths

- Hash function setting allows to start from the middle and to build related quartets (instead of related pairs)

- Complexity: \[
\frac{1}{p_a^2 p_c^2} \left( \frac{C}{b \cdot p_b^4} + 1 \right)
\]
  - Cost C to build an initial quartet
  - \( b \) paths with probability \( p_b \) for \( f_b \)

- Also works with related-key paths
  - New quartet with a different key

- Very efficient with a large family of probability 1 paths
  - We can combine three paths instead of two
Application
Application to ARX Designs

Several recent design are based on the ARX design
  - Use only Addition, Rotation, Xor
  - Skein, Blake are SHA-3 finalists

- Short RK paths with high probability
- Hard to build controlled characteristics

Complexity

Rounds
Application to ARX Designs

- Several recent design are based on the ARX design
  - Use only Addition, Rotation, Xor
  - Skein, Blake are SHA-3 finalists

- Short RK paths with high probability

- Using auxiliary paths

\[ \text{Complexity} \]

\[ \text{Rounds} \]
Skein

- SHA-3 finalist
- ARX design
  - 64-bit words
  - $\text{MIX}_r(a, b) := ((a \oplus b), (b \ll r) \oplus c)$
  - Word permutations
  - Key addition every four rounds

- Threefish-256:
  - 256-bit key: $K_0, K_1, K_2, K_3$
  - 128-bit tweak: $T_0, T_1$
  - 256-bit text

G. Leurent (uni.lu),
Boomerang Attacks against ARX Hash Functions
Skein: Differential Trails

Key schedule (Threefish-256):

- 256-bit key: $K_0, K_1, K_2, K_3$
- 128-bit tweak: $T_0, T_1$
- $K_4 := K_0 \oplus K_1 \oplus K_2 \oplus K_3 \oplus C$
- $T_2 := T_0 \oplus T_1$

<table>
<thead>
<tr>
<th>Round</th>
<th>$K_0$</th>
<th>$K_1 + T_0$</th>
<th>$K_2 + T_1$</th>
<th>$K_3 + 0$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$K_0$</td>
<td>$K_1 + T_0$</td>
<td>$K_2 + T_1$</td>
<td>$K_3 + 0$</td>
</tr>
<tr>
<td>4</td>
<td>$K_1$</td>
<td>$K_2 + T_1$</td>
<td>$K_3 + T_2$</td>
<td>$K_4 + 1$</td>
</tr>
<tr>
<td>8</td>
<td>$K_2$</td>
<td>$K_3 + T_2$</td>
<td>$K_4 + T_0$</td>
<td>$K_0 + 2$</td>
</tr>
<tr>
<td>12</td>
<td>$K_3$</td>
<td>$K_4 + T_0$</td>
<td>$K_0 + T_1$</td>
<td>$K_1 + 3$</td>
</tr>
<tr>
<td>16</td>
<td>$K_4$</td>
<td>$K_0 + T_1$</td>
<td>$K_1 + T_2$</td>
<td>$K_2 + 4$</td>
</tr>
</tbody>
</table>

- Use a difference in the tweak and in the key so that they cancel out
- One key addition without any difference
Skein: Differential Trails

Key schedule (Threefish-256):

- 256-bit key: $K_0, K_1, K_2, K_3$
- 128-bit tweak: $T_0, T_1$
- $K_4 := K_0 \oplus K_1 \oplus K_2 \oplus K_3 \oplus C$
- $T_2 := T_0 \oplus T_1$

<table>
<thead>
<tr>
<th>Round</th>
<th>$K_0$</th>
<th>$K_1 + T_0$</th>
<th>$K_2 + T_1$</th>
<th>$K_3 + 0$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$K_0$</td>
<td>$K_1 + T_0$</td>
<td>$K_2 + T_1$</td>
<td>$K_3 + 0$</td>
</tr>
<tr>
<td>4</td>
<td>$K_1$</td>
<td>$K_2 + T_1$</td>
<td>$K_3 + T_2$</td>
<td>$K_4 + 1$</td>
</tr>
<tr>
<td>8</td>
<td>$K_2$</td>
<td>$K_3 + T_2$</td>
<td>$K_4 + T_0$</td>
<td>$K_0 + 2$</td>
</tr>
<tr>
<td>12</td>
<td>$K_3$</td>
<td>$K_4 + T_0$</td>
<td>$K_0 + T_1$</td>
<td>$K_1 + 3$</td>
</tr>
<tr>
<td>16</td>
<td>$K_4$</td>
<td>$K_0 + T_1$</td>
<td>$K_1 + T_2$</td>
<td>$K_2 + 4$</td>
</tr>
</tbody>
</table>

- Use a difference in the tweak and in the key so that they cancel out
- One key addition without any difference
Skein: Differential Trails

- 16-round trail:

\[
\begin{align*}
\Delta_0 & \xrightarrow[]{} \Delta^T + \Delta_0 \\
\Delta_1 & \xrightarrow[]{} \Delta^T \\
0 & \xrightarrow[]{} \Delta_1 \\
0 & \xrightarrow[]{} 0 \\
0 & \xrightarrow[]{} 0 \\
\Delta_3 & \xrightarrow[]{} 0 \\
\Delta^\perp & \xrightarrow[]{} \Delta_3 \\
\Delta^\perp + \Delta & \xrightarrow[]{} 0
\end{align*}
\]

\[
\Pr[\Delta^T \leftarrow \Delta_1] = 2^{-33} \quad \text{and} \quad \Pr[\Delta_3 \rightarrow \Delta^\perp] = 2^{-6}
\]

- Use a MSB difference for best probability

- Use any difference for auxiliary paths
  - \(2^{64}\) 8-round paths with probability 1

G. Leurent (uni.lu),
Boomerang Attacks against ARX Hash Functions
Skein: Description of the Attack

   \[ \text{cost: } 2^{18} \]

2. Extend to rounds 12–20 using random keys.
   \[ \text{cost: } 2^{18} \]

3. Use auxiliary paths to generate quartets.
   \[ \text{amortized cost: } 2^0 \]

Top path (0–12)

Middle part (12–20)

Bottom path (20–32)
Skein: Description of the Attack

   - Top path (0–12)
   - Middle part (12–20)
   - Bottom path (20–32)
   - Cost: $2^{18}$

2. Extend to rounds 12—20 using random keys.
   - Cost: $2^{18}$

3. Use auxiliary paths to generate quartets.
   - Amortized cost: $2^0$
Skein: Description of the Attack

   - Top path (0–12)
   - cost: $2^{18}$

2. Extend to rounds 12—20 using random keys.
   - Middle part (12–20)
   - cost: $2^{18}$

3. Use auxiliary paths to generate quartets.
   - Bottom path (20–32)
   - amortized cost: $2^0$
Limitations of the Technique

Why not attack more rounds?

Paths are incompatible!
Limitations of the Technique

Why not attack more rounds?

Paths are incompatible!
Incompatible Characteristics
Incompatibilities in Boomerang Paths

> For a Boomerang attack, we usually assume that the path are independent

> We are building a quartet $X^{(0)}, X^{(1)}, X^{(2)}, X^{(3)}$:

\[
\begin{align*}
X^{(1)} &= X^{(0)} + \alpha' \\
X^{(2)} &= X^{(0)} + \gamma \\
X^{(3)} &= X^{(2)} + \alpha' \\
X^{(2)} &= X^{(1)} + \gamma
\end{align*}
\]

We expect:

\[
\begin{align*}
(X^{(0)}, X^{(1)}) &\xleftarrow{f_a} \alpha \\
(X^{(0)}, X^{(2)}) &\xrightarrow{f_b} \gamma' \\
(X^{(2)}, X^{(3)}) &\xleftarrow{f_a} \alpha \\
(X^{(1)}, X^{(3)}) &\xrightarrow{f_b} \gamma'
\end{align*}
\]

> But these events are not independent!  

[Murphy 2011]
Boomerang Incompatibility

\[ \delta a = -x, \quad \delta b = -x \]

\[ \delta u = \quad \]

\[ u = a + b \]

Top path: \((a^{(0)}, b^{(0)}; a^{(2)}, b^{(2)}) (a^{(1)}, b^{(1)}; a^{(3)}, b^{(3)})\)

Bottom path: \((a^{(0)}, b^{(0)}; a^{(1)}, b^{(1)}) (a^{(2)}, b^{(2)}; a^{(3)}, b^{(3)})\)

\[
\begin{array}{cccc}
\text{x}(0) & \text{x}(1) & \text{x}(2) & \text{x}(3) \\
\hline
a & 0 & 1 & 1 & 0 \\
b & 1 & 0 & 0 & 1 \\
\end{array}
\]

- Wlog, assume \(a^{(0)} = 0\)
- Compute \(a^{(i)}\), deduce sign of \(b\)
- Contradiction for \(b\)!
Boomerang Incompatibility

\[ \delta a = -x \quad \delta b = --- \]

Top path: \((a^{(0)}, b^{(0)}; a^{(2)}, b^{(2)}) \) \((a^{(1)}, b^{(1)}; a^{(3)}, b^{(3)})\)

\[ \delta a = -x \quad \delta b = -x \]

Bottom path: \((a^{(0)}, b^{(0)}; a^{(1)}, b^{(1)}) \) \((a^{(2)}, b^{(2)}; a^{(3)}, b^{(3)})\)

\[ \delta u = --- \]

\[ u = a + b \]

\[ \begin{array}{cccc}
   x^{(0)} & x^{(1)} & x^{(2)} & x^{(3)} \\
   a & 0 & 1 & 1 & 0 \\
   b & 1 & 0 & 0 & 1 \\
\end{array} \]

- Wlog, assume \(a^{(0)} = 0\)
- Compute \(a^{(i)}\), deduce sign of \(b\)
- Contradiction for \(b\)!
Boomerang Incompatibility

\[ \delta a = -x^- \quad \delta b = --- \]

**Top path:** \((a^{(0)}, b^{(0)}; a^{(2)}, b^{(2)}) (a^{(1)}, b^{(1)}; a^{(3)}, b^{(3)})\)

\[ \delta a = -x^- \quad \delta b = -x^- \]

**Bottom path:** \((a^{(0)}, b^{(0)}; a^{(1)}, b^{(1)}) (a^{(2)}, b^{(2)}; a^{(3)}, b^{(3)})\)

\[ \delta u = --- \]

\[ u = a + b \]

\[ \begin{array}{cccc}
   & x^{(0)} & x^{(1)} & x^{(2)} & x^{(3)} \\
   a & 0 & 1 & 1 & 0 \\
b & 1 & 0 & 0 & 1
\end{array} \]

- Wlog, assume \(a^{(0)} = 0\)
- Compute \(a^{(i)}\), deduce sign of \(b\)
- Contradiction for \(b\)!
Boomerang Incompatibility

\[ \delta a = -x^- \quad \delta b = -x^- \]

\[ \delta u = --- \]

\[ u = a + b \]

**Top path:** \((a^{(0)}, b^{(0)}; a^{(2)}, b^{(2)}) (a^{(1)}, b^{(1)}; a^{(3)}, b^{(3)})\)

**Bottom path:** \((a^{(0)}, b^{(0)}; a^{(1)}, b^{(1)}) (a^{(2)}, b^{(2)}; a^{(3)}, b^{(3)})\)

<table>
<thead>
<tr>
<th>(x^{(0)})</th>
<th>(x^{(1)})</th>
<th>(x^{(2)})</th>
<th>(x^{(3)})</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>b</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

- Wlog, assume \(a^{(0)} = 0\)
- Compute \(a^{(i)}\), deduce sign of \(b\)
- Contradiction for \(b\)!
Boomerang Incompatibility

\[ \delta a = -x \quad \delta b = --- \]

\[ \begin{align*}
\delta a &= -x \\
\delta b &= -x
\end{align*} \]

Top path: \((a^{(0)}, b^{(0)}; a^{(2)}, b^{(2)}) (a^{(1)}, b^{(1)}; a^{(3)}, b^{(3)})\)

\[ \delta u = --- \]

\[ u = a + b \]

Bottom path: \((a^{(0)}, b^{(0)}; a^{(1)}, b^{(1)}) (a^{(2)}, b^{(2)}; a^{(3)}, b^{(3)})\)

\[
\begin{array}{c|cccc}
 & x^{(0)} & x^{(1)} & x^{(2)} & x^{(3)} \\
\hline
a & 0 & 1 & 1 & 0 \\
b & 1 & 0 & 0 & 1
\end{array}
\]

- Wlog, assume \(a^{(0)} = 0\)
- Compute \(a^{(i)}\), deduce sign of \(b\)
- Contradiction for \(b\)!
Many "natural" characteristics are in fact incompatible.

- Previous boomerang attacks on Skein-512 do not work
- Works on Skein-256
## Results on Skein

<table>
<thead>
<tr>
<th>Attack</th>
<th>CF/KP</th>
<th>Rounds</th>
<th>CF/KP calls</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown Key</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Near collisions (Skein-256)</td>
<td>CF</td>
<td>24</td>
<td>$2^{60}$</td>
<td>[CANS ’10]</td>
</tr>
<tr>
<td>Boomerang dist. (Threefish-512)</td>
<td>KP</td>
<td>32</td>
<td>$2^{189}$</td>
<td>[ISPEC ’10]</td>
</tr>
<tr>
<td>Key Recovery (Threefish-512)</td>
<td>KP</td>
<td>34</td>
<td>$2^{474.4}$</td>
<td>[ISPEC ’10]</td>
</tr>
<tr>
<td>Key Recovery (Threefish-512)</td>
<td>KP</td>
<td>32</td>
<td>$2^{312}$</td>
<td>[AC ’09]</td>
</tr>
<tr>
<td>Open key</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Boomerang dist. (Threefish-512)</td>
<td>KP</td>
<td>35</td>
<td>$2^{478}$</td>
<td>[AC ’09]</td>
</tr>
<tr>
<td>Near collisions (Skein-256)</td>
<td>CF</td>
<td>32</td>
<td>$2^{105}$</td>
<td>[ePrint ’11]</td>
</tr>
<tr>
<td>Boomerang dist. (Skein-256)</td>
<td>CF and KP</td>
<td>24</td>
<td>$2^{18}$</td>
<td></td>
</tr>
<tr>
<td>Boomerang dist. (Threefish-256)</td>
<td>KP</td>
<td>28</td>
<td>$2^{21}$</td>
<td></td>
</tr>
<tr>
<td>Boomerang dist. (Skein-256)</td>
<td>CF</td>
<td>28</td>
<td>$2^{24}$</td>
<td></td>
</tr>
<tr>
<td>Boomerang dist. (Threefish-256)</td>
<td>KP</td>
<td>32</td>
<td>$2^{57}$</td>
<td></td>
</tr>
<tr>
<td>Boomerang dist. (Skein-256)</td>
<td>CF</td>
<td>32</td>
<td>$2^{114}$</td>
<td></td>
</tr>
</tbody>
</table>
Conclusion

1. Boomerang attack on hash functions
   - Start from the middle
   - Use auxiliary path to avoid middle rounds
   - Significant improvement over previous results
   - New result: also works on Blake

2. Analysis of differentials paths
   - Problems found in several previous works
Appendix
Related work

▶ Similar to “Boomerang” of Joux and Peyrin (auxiliary paths)
  ▶ In the context of collision attacks

▶ Similar to message modifications for Boomerang attacks
  ▶ Blake [BNR ’11]
  ▶ SHA-2 [ML ’11]
  ▶ HAVAL [Sasaki ’11]
  ▶ Skein/Threefish [ACMPV ’09, Chen & Jia ’10]

▶ Auxiliary paths allow to skip more rounds
New Result: Application to Blake

- The same technique can be applied to **Blake**
  - Another ARX SHA-3 finalist

- **Significant improvement** over previous results [FSE ’11]

- **Compression function** attack:
  - 6.5 rounds: $2^{140}$ (vs. $2^{184}$)
  - 7 rounds: $2^{183}$ (vs. $2^{232}$)

- **Keyed-permutation** attacks (Open-key vs. Unknown-key)
  - 7 rounds: $2^{32}$ (vs. $2^{122}$)
  - 8 rounds: $2^{1xx}$ (vs. $2^{242}$)
Blake

- State is 4 × 4 matrix:

<table>
<thead>
<tr>
<th>a₀</th>
<th>a₁</th>
<th>a₂</th>
<th>a₃</th>
</tr>
</thead>
<tbody>
<tr>
<td>b₀</td>
<td>b₁</td>
<td>b₂</td>
<td>b₃</td>
</tr>
<tr>
<td>c₀</td>
<td>c₁</td>
<td>c₂</td>
<td>c₃</td>
</tr>
<tr>
<td>d₀</td>
<td>d₁</td>
<td>d₂</td>
<td>d₃</td>
</tr>
</tbody>
</table>

- Column step:
  - $G(a₀, b₀, c₀, d₀)$
  - $G(a₁, b₁, c₁, d₁)$
  - $G(a₂, b₂, c₂, d₂)$
  - $G(a₃, b₃, c₃, d₃)$

- Diagonal step:
  - $G(a₀, b₁, c₂, d₃)$
  - $G(a₁, b₂, c₃, d₀)$
  - $G(a₂, b₃, c₀, d₁)$
  - $G(a₃, b₀, c₁, d₂)$
Blake

- State is $4 \times 4$ matrix:
  
<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$a_0$</td>
<td>$a_1$</td>
<td>$a_2$</td>
<td>$a_3$</td>
</tr>
<tr>
<td>$b_0$</td>
<td>$b_1$</td>
<td>$b_2$</td>
<td>$b_3$</td>
</tr>
<tr>
<td>$c_0$</td>
<td>$c_1$</td>
<td>$c_2$</td>
<td>$c_3$</td>
</tr>
<tr>
<td>$d_0$</td>
<td>$d_1$</td>
<td>$d_2$</td>
<td>$d_3$</td>
</tr>
</tbody>
</table>

- Column step:
  
  $G(a_0, b_0, c_0, d_0)$
  $G(a_1, b_1, c_1, d_1)$
  $G(a_2, b_2, c_2, d_2)$
  $G(a_3, b_3, c_3, d_3)$

- Diagonal step:
  
  $G(a_0, b_1, c_2, d_3)$
  $G(a_1, b_2, c_3, d_0)$
  $G(a_2, b_3, c_0, d_1)$
  $G(a_3, b_0, c_1, d_2)$
Blake

- **State is $4 \times 4$ matrix:**
  
  \[
  \begin{array}{cccc}
  a_0 & a_1 & a_2 & a_3 \\
  b_0 & b_1 & b_2 & b_3 \\
  c_0 & c_1 & c_2 & c_3 \\
  d_0 & d_1 & d_2 & d_3 \\
  \end{array}
  \]

- **Column step:**
  
  \[G(a_0, b_0, c_0, d_0)\]
  \[G(a_1, b_1, c_1, d_1)\]
  \[G(a_2, b_2, c_2, d_2)\]
  \[G(a_3, b_3, c_3, d_3)\]

- **Diagonal step:**
  
  \[G(a_0, b_1, c_2, d_3)\]
  \[G(a_1, b_2, c_3, d_0)\]
  \[G(a_2, b_3, c_0, d_1)\]
  \[G(a_3, b_0, c_1, d_2)\]
Blake: Differential Trails

- Key schedule: permutation based
  \[\sigma_3 : 7 \ 3 \ 13 \ 11 \ 9 \ 1 \ 12 \ 14 \ 2 \ 5 \ 4 \ 15 \ 6 \ 10 \ 0 \ 8\]
  \[\sigma_4 : 9 \ 5 \ 2 \ 10 \ 0 \ 7 \ 4 \ 15 \ 14 \ 11 \ 6 \ 3 \ 1 \ 12 \ 8 \ 13\]

- Choose a message word used
  - at the beginning of a round
  - at the end of the next round

- 4-round trail:

\[
\begin{align*}
\Delta_T^{m_{13}} & \rightarrow \Delta_1^{m_{13}} & \Delta_3 & \rightarrow \Delta_{\perp}
\end{align*}
\]

\[
\Pr\left[\Delta_T^{m_{13}} \leftrightarrow \Delta_1^{m_{13}}\right] = 2^{-6} \cdot 2^{-42}
\]
\[
p = 1
\]
\[
\Pr\left[\Delta_3 \rightarrow \Delta_{\perp}\right] = 2^{-24}
\]

G. Leurent (uni.lu),
Boomerang Attacks against ARX Hash Functions
Blake: Differential Trails

Key schedule: permutation based

\[ \sigma_3 : 7 \ 3 \ 13 \ 11 \ 9 \ 1 \ 12 \ 14 \ 2 \ 5 \ 4 \ 15 \ 6 \ 10 \ 0 \ 8 \]

\[ \sigma_4 : 9 \ 5 \ 2 \ 10 \ 0 \ 7 \ 4 \ 15 \ 14 \ 11 \ 6 \ 3 \ 1 \ 12 \ 8 \ 13 \]

Choose a message word used
- at the beginning of a round
- at the end of the next round

4-round trail:

\[
\begin{align*}
\Pr[\Delta^T \leftrightarrow \Delta_1] &= 2^{-6} \cdot 2^{-42} \\
p &= 1 \\
\Pr[\Delta_3 \rightarrow \Delta_{\perp}] &= 2^{-24}
\end{align*}
\]
Blake: Differential Trails

- Key schedule: permutation based
  \[ \sigma_3 : \begin{array}{cccccccccccccccccc} 7 & 3 & 13 & 11 & 9 & 1 & 12 & 14 & 2 & 5 & 4 & 15 & 6 & 10 & 0 & 8 \end{array} \]
  \[ \sigma_4 : \begin{array}{cccccccccccccccccc} 9 & 5 & 2 & 10 & 0 & 7 & 4 & 15 & 14 & 11 & 6 & 3 & 1 & 12 & 8 & 13 \end{array} \]

- Choose a message word used
  - at the beginning of a round
  - at the end of the next round

- 4-round trail:
  \[ \Pr \left[ \Delta_1 \right] = 2^{-6} \cdot 2^{-42} \]
  \[ p = 1 \quad \Pr \left[ \Delta_3 \rightarrow \Delta_{\perp} \right] = 2^{-24} \]
  \[ p = 1/2 \]
Blake: Description of the Attack

The hard part is the **middle round**

- Column step is part of the top path
- Diagonal step is part of the bottom path

1. Find (state, message) candidates for each diagonal G function
   - Start with middle quartets with all differences fixed

2. Look for combinations of candidates that follow the first part of the diagonal step
   - Use the message to randomize

3. Look for candidates that follow the full diagonal step
   - Use the message to randomize
## Blake-256: Results

<table>
<thead>
<tr>
<th>Attack</th>
<th>CF/KP</th>
<th>Rounds</th>
<th>CF/KP calls</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unknown Key</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Boomerang dist.</td>
<td>KP</td>
<td>7</td>
<td>$2^{122}$</td>
<td>[FSE ’11]</td>
</tr>
<tr>
<td>Boomerang dist.</td>
<td>KP</td>
<td>8</td>
<td>$2^{242}$</td>
<td>[FSE ’11]</td>
</tr>
<tr>
<td><strong>Open Key</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Boomerang dist.</td>
<td>CF w/ Init</td>
<td>7</td>
<td>$2^{232}$</td>
<td>[FSE ’11]</td>
</tr>
<tr>
<td>Boomerang dist.</td>
<td>CF w/ Init</td>
<td>7</td>
<td>$2^{183}$</td>
<td></td>
</tr>
<tr>
<td>Boomerang dist.</td>
<td>KP</td>
<td>7</td>
<td>$2^{32}$</td>
<td></td>
</tr>
<tr>
<td>Boomerang dist.</td>
<td>KP</td>
<td>8</td>
<td>$2^{1xx}$</td>
<td></td>
</tr>
</tbody>
</table>