On differential and invertibility properties of BLAKE

Jean-Philippe Aumasson

Joint work with Simon Knellwolf and Willi Meier

(to appear at FSE 2010)

Agenda

Differential properties

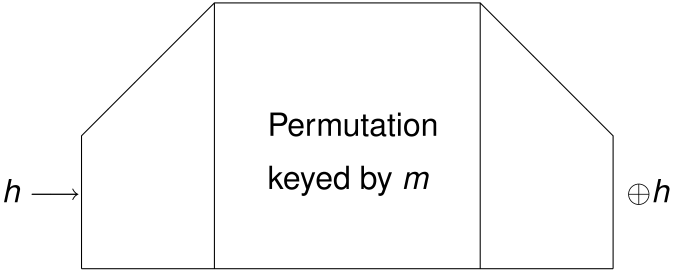
- Of the G transform
- Impossible differentials for 2 rounds and more

Invertibility properties

- The problem: fix initial state, vary block
- Algorithms to invert 1 and 1.5 round

BLAKE

- Second-round SHA-3 candidate
- HAIFA-like construction (narrow-pipe)
- Local wide-pipe compression function



BLAKE-32: 32-bit words, 512-bit state, 10 rounds
BLAKE-64: 64-bit words, 1024-bit state, 14 rounds

BLAKE's permutation

Internal state: $\begin{pmatrix} v_0 & v_1 & v_2 & v_3 \\ v_4 & v_5 & v_6 & v_7 \\ v_8 & v_9 & v_{10} & v_{11} \\ v_{12} & v_{13} & v_{14} & v_{15} \end{pmatrix}$

1 round = 1 **column step** followed by 1 **diagonal step**

Reuse the permutation of the ChaCha stream cipher, based on the G transform

$$\begin{aligned} a &\leftarrow (a+b)+(m_i \oplus k_j) \\ d &\leftarrow (d \oplus a) \ggg 16 \\ c &\leftarrow (c+d) \\ b &\leftarrow (b \oplus c) \ggg 12 \end{aligned} \qquad \begin{aligned} a &\leftarrow (a+b)+(m_j \oplus k_i) \\ d &\leftarrow (d \oplus a) \ggg 8 \\ c &\leftarrow (c+d) \\ b &\leftarrow (b \oplus c) \ggg 7 \end{aligned}$$

BLAKE's permutation

Internal state: $\begin{pmatrix} v_0 & v_1 & v_2 & v_3 \\ v_4 & v_5 & v_6 & v_7 \\ v_8 & v_9 & v_{10} & v_{11} \\ v_{12} & v_{13} & v_{14} & v_{15} \end{pmatrix}$

1 round = 1 **column step** followed by 1 **diagonal step**

Reuse the permutation of the ChaCha stream cipher, based on the *G* transform

$$\begin{aligned} a &\leftarrow (a+b) + (m_i \oplus k_j) \\ d &\leftarrow (d \oplus a) \ggg 16 \\ c &\leftarrow (c+d) \\ b &\leftarrow (b \oplus c) \ggg 12 \end{aligned} \qquad \begin{aligned} a &\leftarrow (a+b) + (m_j \oplus k_i) \\ d &\leftarrow (d \oplus a) \ggg 8 \\ c &\leftarrow (c+d) \\ b &\leftarrow (b \oplus c) \ggg 7 \end{aligned}$$

BLAKE's permutation

Internal state: $\begin{pmatrix} v_0 & v_1 & v_2 & v_3 \\ v_4 & v_5 & v_6 & v_7 \\ v_8 & v_9 & v_{10} & v_{11} \\ v_{12} & v_{13} & v_{14} & v_{15} \end{pmatrix}$

1 round = 1 **column step** followed by 1 **diagonal step**

Reuse the permutation of the ChaCha stream cipher, based on the G transform

$$\begin{array}{rl|rl} a \leftarrow & (a+b) + (m_i \oplus k_j) & a \leftarrow & (a+b) + (m_j \oplus k_i) \\ d \leftarrow & (d \oplus a) \ggg 16 & d \leftarrow & (d \oplus a) \ggg 8 \\ c \leftarrow & (c+d) & c \leftarrow & (c+d) \\ b \leftarrow & (b \oplus c) \ggg 12 & b \leftarrow & (b \oplus c) \ggg 7 \end{array}$$

BLAKE's permutation

Internal state: $\begin{pmatrix} v_0 & v_1 & v_2 & v_3 \\ v_4 & v_5 & v_6 & v_7 \\ v_8 & v_9 & v_{10} & v_{11} \\ v_{12} & v_{13} & v_{14} & v_{15} \end{pmatrix}$

1 round = 1 **column step** followed by 1 **diagonal step**

Reuse the permutation of the ChaCha stream cipher, based on the G transform

$$\begin{aligned} a &\leftarrow (a+b)+(m_i \oplus k_j) \\ d &\leftarrow (d \oplus a) \ggg 16 \\ c &\leftarrow (c+d) \\ b &\leftarrow (b \oplus c) \ggg 12 \end{aligned} \qquad \begin{aligned} a &\leftarrow (a+b)+(m_j \oplus k_i) \\ d &\leftarrow (d \oplus a) \ggg 8 \\ c &\leftarrow (c+d) \\ b &\leftarrow (b \oplus c) \ggg 7 \end{aligned}$$

BLAKE's permutation

Internal state: $\begin{pmatrix} v_0 & v_1 & v_2 & v_3 \\ v_4 & v_5 & v_6 & v_7 \\ v_8 & v_9 & v_{10} & v_{11} \\ v_{12} & v_{13} & v_{14} & v_{15} \end{pmatrix}$

1 round = 1 **column step** followed by 1 **diagonal step**

Reuse the permutation of the ChaCha stream cipher, based on the G transform

$$\begin{aligned} a &\leftarrow (a+b)+(m_i \oplus k_j) \\ d &\leftarrow (d \oplus a) \ggg 16 \\ c &\leftarrow (c+d) \\ b &\leftarrow (b \oplus c) \ggg 12 \end{aligned} \qquad \begin{aligned} a &\leftarrow (a+b)+(m_j \oplus k_i) \\ d &\leftarrow (d \oplus a) \ggg 8 \\ c &\leftarrow (c+d) \\ b &\leftarrow (b \oplus c) \ggg 7 \end{aligned}$$

BLAKE's permutation

Internal state: $\begin{pmatrix} \color{red}{v_0} & v_1 & v_2 & v_3 \\ v_4 & \color{red}{v_5} & v_6 & v_7 \\ v_8 & v_9 & \color{red}{v_{10}} & v_{11} \\ v_{12} & v_{13} & v_{14} & \color{red}{v_{15}} \end{pmatrix}$

1 round = 1 **column step** followed by 1 **diagonal step**

Reuse the permutation of the ChaCha stream cipher, based on the G transform

$$\begin{aligned} a &\leftarrow (a+b)+(m_i \oplus k_j) \\ d &\leftarrow (d \oplus a) \ggg 16 \\ c &\leftarrow (c+d) \\ b &\leftarrow (b \oplus c) \ggg 12 \end{aligned} \qquad \begin{aligned} a &\leftarrow (a+b)+(m_j \oplus k_i) \\ d &\leftarrow (d \oplus a) \ggg 8 \\ c &\leftarrow (c+d) \\ b &\leftarrow (b \oplus c) \ggg 7 \end{aligned}$$

BLAKE's permutation

Internal state: $\begin{pmatrix} v_0 & v_1 & v_2 & v_3 \\ v_4 & v_5 & v_6 & v_7 \\ v_8 & v_9 & v_{10} & v_{11} \\ v_{12} & v_{13} & v_{14} & v_{15} \end{pmatrix}$

1 round = 1 **column step** followed by 1 **diagonal step**

Reuse the permutation of the ChaCha stream cipher, based on the *G* transform

$$\begin{array}{rl|rl} a \leftarrow & (a+b)+(m_i \oplus k_j) & a \leftarrow & (a+b)+(m_j \oplus k_i) \\ d \leftarrow & (d \oplus a) \ggg 16 & d \leftarrow & (d \oplus a) \ggg 8 \\ c \leftarrow & (c+d) & c \leftarrow & (c+d) \\ b \leftarrow & (b \oplus c) \ggg 12 & b \leftarrow & (b \oplus c) \ggg 7 \end{array}$$

BLAKE's permutation

Internal state: $\begin{pmatrix} v_0 & v_1 & v_2 & v_3 \\ v_4 & v_5 & v_6 & v_7 \\ v_8 & v_9 & v_{10} & v_{11} \\ v_{12} & v_{13} & v_{14} & v_{15} \end{pmatrix}$

1 round = 1 **column step** followed by 1 **diagonal step**

Reuse the permutation of the ChaCha stream cipher, based on the *G* transform

$$\begin{aligned} a &\leftarrow (a+b)+(m_i \oplus k_j) \\ d &\leftarrow (d \oplus a) \ggg 16 \\ c &\leftarrow (c+d) \\ b &\leftarrow (b \oplus c) \ggg 12 \end{aligned} \qquad \begin{aligned} a &\leftarrow (a+b)+(m_j \oplus k_i) \\ d &\leftarrow (d \oplus a) \ggg 8 \\ c &\leftarrow (c+d) \\ b &\leftarrow (b \oplus c) \ggg 7 \end{aligned}$$

BLAKE's permutation

Internal state: $\begin{pmatrix} v_0 & v_1 & v_2 & v_3 \\ v_4 & v_5 & v_6 & v_7 \\ v_8 & v_9 & v_{10} & v_{11} \\ v_{12} & v_{13} & v_{14} & v_{15} \end{pmatrix}$

1 round = 1 **column step** followed by 1 **diagonal step**

Reuse the permutation of the ChaCha stream cipher, based on the *G* transform

$$\begin{aligned} a &\leftarrow (a+b)+(m_i \oplus k_j) \\ d &\leftarrow (d \oplus a) \ggg 16 \\ c &\leftarrow (c+d) \\ b &\leftarrow (b \oplus c) \ggg 12 \end{aligned} \qquad \begin{aligned} a &\leftarrow (a+b)+(m_j \oplus k_i) \\ d &\leftarrow (d \oplus a) \ggg 8 \\ c &\leftarrow (c+d) \\ b &\leftarrow (b \oplus c) \ggg 7 \end{aligned}$$

BLAKE's permutation

1 round = 1 **column step** followed by 1 **diagonal step**

Reuse the permutation of the ChaCha stream cipher, based on the G transform

$$
\begin{array}{rl|rl}
a \leftarrow & (a+b)+(m_i \oplus k_j) & a \leftarrow & (a+b)+(m_j \oplus k_i) \\
d \leftarrow & (d \oplus a) \ggg 16 & d \leftarrow & (d \oplus a) \ggg 8 \\
c \leftarrow & (c+d) & c \leftarrow & (c+d) \\
b \leftarrow & (b \oplus c) \ggg 12 & b \leftarrow & (b \oplus c) \ggg 7
\end{array}
$$

m_i's= message words, k_i's= constants

- Indexes i & j depend on the round index
- Each word appears once in a round
- Never same combination (i, j)

For fixed m, G is a permutation of (a, b, c, d)

G:

$$
\begin{array}{rl|rl}
a \leftarrow & (a+b)+(m_i \oplus k_j) & a \leftarrow & (a+b)+(m_j \oplus k_i) \\
d \leftarrow & (d \oplus a) \ggg 16 & d \leftarrow & (d \oplus a) \ggg 8 \\
c \leftarrow & (c+d) & c \leftarrow & (c+d) \\
b \leftarrow & (b \oplus c) \ggg 12 & b \leftarrow & (b \oplus c) \ggg 7
\end{array}
$$

G^{-1}:

$$
\begin{array}{rl|rl}
b \leftarrow & c \oplus (b \lll 7) & b \leftarrow & c \oplus (b \lll 12) \\
c \leftarrow & c - d & c \leftarrow & c - d \\
d \leftarrow & a \oplus (d \lll 8) & d \leftarrow & a \oplus (d \lll 16) \\
a \leftarrow & a - b - (m_j \oplus k_i) & a \leftarrow & a - b - (m_i \oplus k_j)
\end{array},
$$

Properties of G^{-1}:

- The final b and c don't depend on m_i or m_j
- The final b doesn't depend on the initial a

Probability-1 trails

There exist 3 probability-1 trails for G

$$
\begin{array}{rl|rl}
a \leftarrow & (a+b)+(m_i \oplus k_j) & a \leftarrow & (a+b)+(m_j \oplus k_i) \\
d \leftarrow & (d \oplus a) \ggg 16 & d \leftarrow & (d \oplus a) \ggg 8 \\
c \leftarrow & (c+d) & c \leftarrow & (c+d) \\
b \leftarrow & (b \oplus c) \ggg 12 & b \leftarrow & (b \oplus c) \ggg 7
\end{array}
$$

$\Delta = 800\ldots00$

Probability-1 trails

There exist 3 probability-1 trails for G

$$
\begin{array}{ll}
a \leftarrow & (\Delta + b) + (\Delta \oplus k_j) \\
d \leftarrow & (d \oplus a) \ggg 16 \\
c \leftarrow & (c + d) \\
b \leftarrow & (b \oplus c) \ggg 12
\end{array}
\quad\Bigg|\quad
\begin{array}{ll}
a \leftarrow & (a + b) + (m_j \oplus k_i) \\
d \leftarrow & (d \oplus a) \ggg 8 \\
c \leftarrow & (c + d) \\
b \leftarrow & (b \oplus c) \ggg 7
\end{array}
$$

Δ in m_i, a

Probability-1 trails

There exist 3 probability-1 trails for G

$$\begin{array}{rl|rl} \Delta \leftarrow & (a+b)+(\Delta \oplus k_j) & a \leftarrow & (\Delta + b)+(\Delta \oplus k_i) \\ d \leftarrow & (\Delta \oplus \Delta) \ggg 16 & d \leftarrow & (d \oplus a) \ggg 8 \\ c \leftarrow & (c+d) & c \leftarrow & (c+d) \\ b \leftarrow & (b \oplus c) \ggg 12 & b \leftarrow & (b \oplus c) \ggg 7 \end{array}$$

Δ in m_i, m_j, d

Probability-1 trails

There exist 3 probability-1 trails for G

$$
\begin{array}{rl|rl}
\Delta \leftarrow & (\Delta + b) + (m_i \oplus k_j) & a \leftarrow & (\Delta + b) + (\Delta \oplus k_i) \\
d \leftarrow & (\Delta \oplus \Delta) \ggg 16 & d \leftarrow & (d \oplus a) \ggg 8 \\
c \leftarrow & (c + d) & c \leftarrow & (c + d) \\
b \leftarrow & (b \oplus c) \ggg 12 & b \leftarrow & (b \oplus c) \ggg 7
\end{array}
$$

Δ in m_j, a, d

Impossible differentials of G...

...for an **input difference in** m_i **(and possibly** m_j**)**

$$
\begin{array}{rl|rl}
a \leftarrow & (a+b)+(m_i \oplus k_j) & a \leftarrow & (a+b)+(m_j \oplus k_i) \\
d \leftarrow & (d \oplus a) \ggg 16 & d \leftarrow & (d \oplus a) \ggg 8 \\
c \leftarrow & (c+d) & c \leftarrow & (c+d) \\
b \leftarrow & (b \oplus c) \ggg 12 & b \leftarrow & (b \oplus c) \ggg 7
\end{array}
$$

Properties:

- Final a and d can't be both free of difference
- Idem for d and c, b and c

Impossible differentials of G...

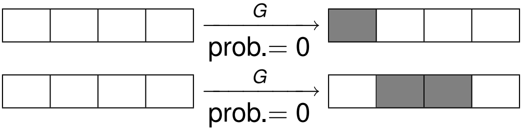
...for an **input difference in m_i (and possibly m_j)**

$$\begin{array}{rl|rl}
a \leftarrow & (a+b)+(m_i \oplus k_j) & a \leftarrow & (a+b)+(m_j \oplus k_i) \\
d \leftarrow & (d \oplus a) \ggg 16 & d \leftarrow & (d \oplus a) \ggg 8 \\
c \leftarrow & (c+d) & c \leftarrow & (c+d) \\
b \leftarrow & (b \oplus c) \ggg 12 & b \leftarrow & (b \oplus c) \ggg 7
\end{array}$$

Properties:

- Final a and d can't be both free of difference
- Idem for d and c, b and c

$\Rightarrow$ Impossible differentials follow, ex:



Impossible differentials of G...

... in the general case (input diff. anywhere)

$$\begin{array}{rl} a \leftarrow & (a+b)+(m_i \oplus k_j) \\ d \leftarrow & (d \oplus a) \ggg 16 \\ c \leftarrow & (c+d) \\ b \leftarrow & (b \oplus c) \ggg 12 \end{array} \quad \Bigg| \quad \begin{array}{rl} a \leftarrow & (a+b)+(m_j \oplus k_i) \\ d \leftarrow & (d \oplus a) \ggg 8 \\ c \leftarrow & (c+d) \\ b \leftarrow & (b \oplus c) \ggg 7 \end{array}$$

Observation on collisions

- $G(a,b,c,d,m_i,m_j) = G(a',b',c',d',m_i',m_j') \Rightarrow (b,c) = (b',c')$

Follows from the property of G^{-1} that a diff. in m_i and/or m_j cannot affect b and c

Impossible differentials follow, ex: $(\Delta, 0, \Delta', \Delta'') \mapsto (0,0,0,0)$

Impossible differentials of one round

Are **impossible**: all differentials with no diff. in the initial state, and an output diff. in a **single diagonal** of one of the following forms:

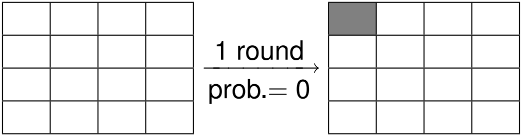
$$(\Delta, 0, 0, 0) \quad (0, \Delta, 0, 0) \qquad\qquad (\Delta, 0, 0, \Delta') \quad (\Delta, 0, \Delta', 0)$$
$$(0, 0, \Delta, 0) \quad (0, 0, 0, \Delta) \qquad\qquad (\Delta, \Delta', 0, 0) \quad (0, \Delta, \Delta', 0)$$

Impossible differentials of one round

Are **impossible**: all differentials with no diff. in the initial state, and an output diff. in a **single diagonal** of one of the following forms:

$$(\Delta, 0, 0, 0) \quad (0, \Delta, 0, 0) \qquad (\Delta, 0, 0, \Delta') \quad (\Delta, 0, \Delta', 0)$$
$$(0, 0, \Delta, 0) \quad (0, 0, 0, \Delta) \qquad (\Delta, \Delta', 0, 0) \quad (0, \Delta, \Delta', 0)$$

Ex, for some nonzero diff. in (m_i, m_j):



Impossible differentials of one round: proof

First case: no diff. introduced in the column step

- Directly follows from the impossible differentials of G

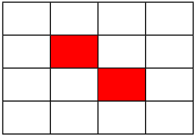
Impossible differentials of one round: proof

First case: no diff. introduced in the column step

- Directly follows from the impossible differentials of G

Second case: diff. introduced in the column step

- A collision for G needs no diff. in b and c, but
- any diff. in m_i or m_j gives diff. in b or c
- Hence, to have diff. only in the central diagonal (say), diff. must be in the 2nd or 3rd columns



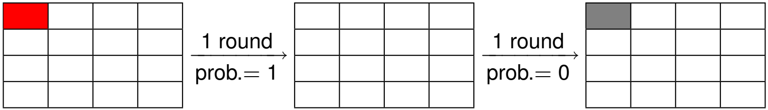
- No diff. in a and d $\Rightarrow$ diff. in a, c, and d after G

Impossible differentials of two rounds

Idea: prepend a probability-1 differential to the 1-round impossible differentials

Ex: MSB difference in m_0 and v_0

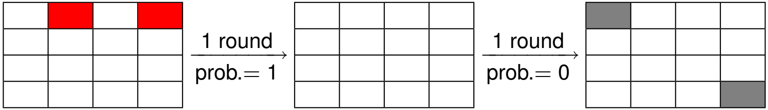
$$
\begin{array}{rl}
a \leftarrow & (a + b) + (m_i \oplus k_j) \\
d \leftarrow & (d \oplus a) \ggg 16 \\
c \leftarrow & (c + d) \\
b \leftarrow & (b \oplus c) \ggg 12
\end{array}
\quad\Bigg|\quad
\begin{array}{rl}
a \leftarrow & (a + b) + (m_j \oplus k_i) \\
d \leftarrow & (d \oplus a) \ggg 8 \\
c \leftarrow & (c + d) \\
b \leftarrow & (b \oplus c) \ggg 7
\end{array}
$$



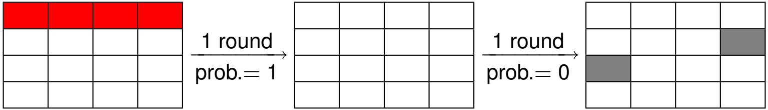
Where ▬ is any nonzero diff.

Impossible differentials of two rounds

MSB diff. in m_2, m_6, v_1, v_3:



MSB diff. in $m_0, m_2, m_4, m_6, v_0, v_1, v_2, v_3$:



Holds for both **BLAKE-32 and BLAKE-64**

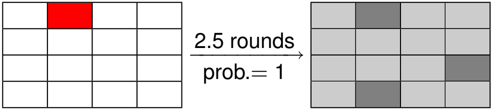
Impossible differentials for more rounds

Apply **miss-in-the-middle** to BLAKE-32

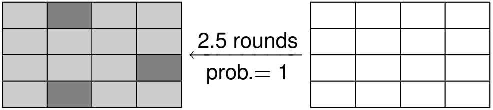
is any diff. (possibly zero)

is any nonzero diff., **partially determined**

From round 1:



From round 5:



There exist contradictions in the probability-1 differences, hence the 5-round differential is impossible

Impossible differentials for more rounds

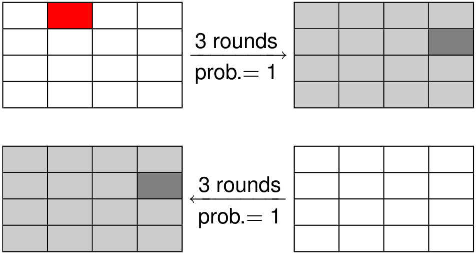
Apply **miss-in-the-middle** to BLAKE-64

is any diff. (possibly zero)

is any nonzero diff., **partially determined**

From round 1:

From round 6:



There exist contradictions in the probability-1 differences, hence the 6-round differential is impossible

Invertibility properties

Internal state: $\begin{pmatrix} v_0 & v_1 & v_2 & v_3 \\ v_4 & v_5 & v_6 & v_7 \\ v_8 & v_9 & v_{10} & v_{11} \\ v_{12} & v_{13} & v_{14} & v_{15} \end{pmatrix}$

1 round = 1 **column step** followed by 1 **diagonal step**

Fix m: permutation of the state

Fix the initial state: permutation of the block?

- Yes, can be shown using differential properties
- No straightforward inversion algorithm,
- even for 1 round only!

Inverting a round: diagonal step

(One round = column step followed by diagonal step)

$$
\begin{array}{rl|rl}
a \leftarrow & (a+b)+(m_i \oplus k_j) & a \leftarrow & (a+b)+(m_j \oplus k_i) \\
d \leftarrow & (d \oplus a) \ggg 16 & d \leftarrow & (d \oplus a) \ggg 8 \\
c \leftarrow & (c+d) & c \leftarrow & (c+d) \\
b \leftarrow & (b \oplus c) \ggg 12 & b \leftarrow & (b \oplus c) \ggg 7
\end{array}
$$

From the final value of (a, b, c, d), one can determine the initial b and c without knowing m_i nor m_j

Inverting a round: diagonal step

(One round = column step followed by diagonal step)

$$
\begin{array}{ll|ll}
a \leftarrow & (a+b)+(m_i \oplus k_j) & a \leftarrow & (a+b)+(m_j \oplus k_i) \\
d \leftarrow & (d \oplus a) \ggg 16 & d \leftarrow & (d \oplus a) \ggg 8 \\
{\color{red}c} \leftarrow & (c+d) & c \leftarrow & (c+d) \\
{\color{red}b} \leftarrow & (b \oplus c) \ggg 12 & b \leftarrow & (b \oplus c) \ggg 7
\end{array}
$$

From the final value of (a, b, c, d), one can determine the initial b and c without knowing m_i nor m_j

$\Rightarrow$ doing this for each diagonal, recover half the **intermediate state**

$$
\begin{pmatrix}
v_0 & v_1 & v_2 & v_3 \\
{\color{red}v_4} & {\color{red}v_5} & {\color{red}v_6} & {\color{red}v_7} \\
{\color{red}v_8} & {\color{red}v_9} & {\color{red}v_{10}} & {\color{red}v_{11}} \\
v_{12} & v_{13} & v_{14} & v_{15}
\end{pmatrix}
$$

Inverting a round: column step

State after the column step (known):

$$\begin{pmatrix} v_0 & v_1 & v_2 & v_3 \\ v_4 & v_5 & v_6 & v_7 \\ v_8 & v_9 & v_{10} & v_{11} \\ v_{12} & v_{13} & v_{14} & v_{15} \end{pmatrix}$$

From the final (b, c) and the initial (a, b, c, d), one can compute efficiently m_i and m_j for each G of the column step

Inverting a round: column step

State after the column step (known):

$$\begin{pmatrix} v_0 & v_1 & v_2 & v_3 \\ v_4 & v_5 & v_6 & v_7 \\ v_8 & v_9 & v_{10} & v_{11} \\ v_{12} & v_{13} & v_{14} & v_{15} \end{pmatrix}$$

From the final (b, c) and the initial (a, b, c, d), one can compute efficiently m_i and m_j for each G of the column step

One can then determine all the intermediate state...

$$\begin{pmatrix} v_0 & v_1 & v_2 & v_3 \\ v_4 & v_5 & v_6 & v_7 \\ v_8 & v_9 & v_{10} & v_{11} \\ v_{12} & v_{13} & v_{14} & v_{15} \end{pmatrix}$$

and use it to determine the rest of the message

Inverting 1.5 round

A bit more complicated…

Inverting 1.5 round

A bit more complicated...

1. Guess 3 message words and 1 state word
2. Recover words of the state at various steps of the computation
3. Combine them to recover the rest of the message
4. Check the correctness of the guess

Gives a **preimage attack** for the compression function of BLAKE-32 in 2^{128} (improves on Ji/Liangyu's 2^{192})

Complexity 2^{256} for BLAKE-64 (1024-bit state)

Guess of 4 words seems optimal...

Summary

We identified **impossible differentials**:

- For the internal permutation
- Large classes for up to 2 rounds
- Particular differentials for 5/6 rounds

$\Rightarrow$ distinguisher for the reduced permutation

Not relevant for the compression function

Summary

We identified **impossible differentials**:

- For the internal permutation
- Large classes for up to 2 rounds
- Particular differentials for 5/6 rounds

$\Rightarrow$ distinguisher for the reduced permutation

Not relevant for the compression function

Invertibility properties for fixed initial state

- 1 and 1.5 rounds **are** a permutation of a block
- But probably not 2 or more rounds
- Straightforward preimages for 1-round BLAKE
- $2^{128}/2^{256}$ preimages for 2-round BLAKE-32/64

Previous and future work

- Free-start collisions on 2.5 rounds (Ji/Liangyu) in $2^{112}/2^{240}$
- Preimages on 2.5 rounds (Ji/Liangyu) in $2^{241}/2^{481}$
- Near-collision for rounds 6–9 (Guo/Matusiewicz) in 2^{42}

- Better exploit *G*'s properties?
- MITM strategy (as for MD5 preimages)?
- Rotational cryptanalysis?