Differential and Invertibility Properties of BLAKE

Jean-Philippe Aumasson[1], Jian Guo[2], Simon Knellwolf[3], Krystian Matusiewicz[4], Willi Meier[3]

[1]Nagravision SA, Cheseaux, Switzerland

[2]Nanyang Technological University, Singapore

[3]FHNW, Windisch, Switzerland

[4]Technical University of Denmark, Denmark

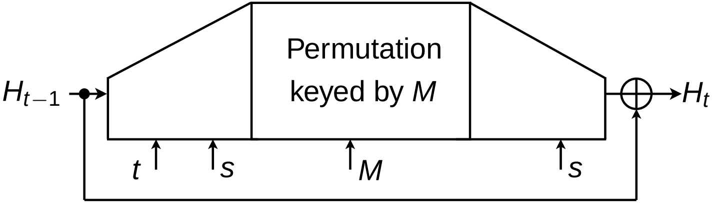
FSE 2010, 09 Feb 2010

Talk Overview

1. Description of BLAKE
2. Results
   - Round-Reduced Near-Collisions
   - Impossible Differentials
   - Invertibility and Preimage Attacks
   - More Results
3. Conclusions

BLAKE Overview

- Designed by Aumasson et al.
- One of the 14 second round SHA-3 candidates
- HAIFA structure
- Local wide-pipe compression function



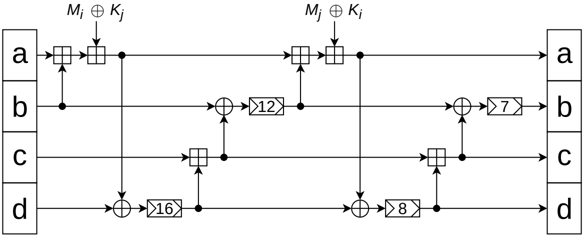
- BLAKE-32: 32-bit word, 512-bit state, 10 rounds, 256-bit digest
- BLAKE-64: 64-bit word, 1024-bit state, 14 rounds, 512-bit digest

BLAKE's Permutation

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

1 round = 1 column step followed by 1 diagonal step

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

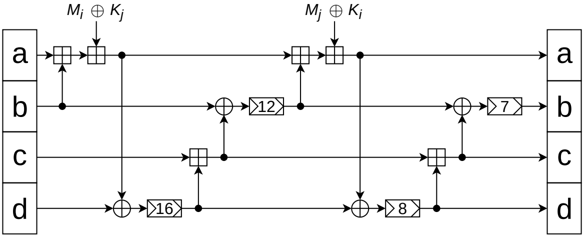


BLAKE’s Permutation

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

1 round = 1 column step followed by 1 diagonal step

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

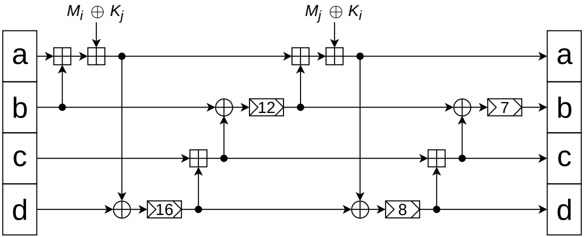


BLAKE's Permutation

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

1 round = 1 column step followed by 1 diagonal step

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

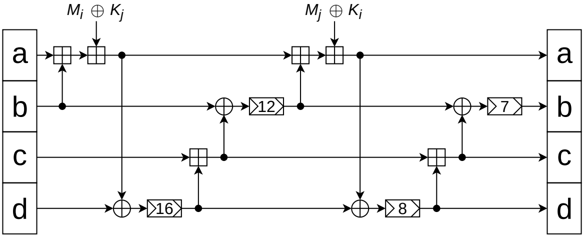


BLAKE’s Permutation

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

1 round = 1 column step followed by 1 diagonal step

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

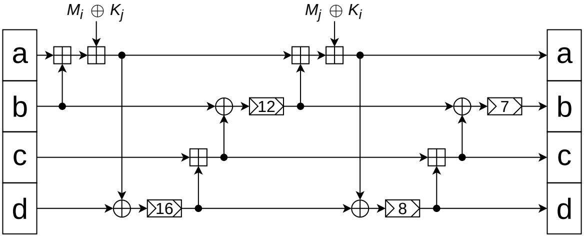


BLAKE's Permutation

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

1 round = 1 column step followed by 1 diagonal step

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

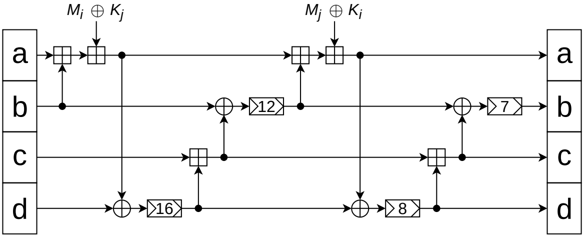


BLAKE’s Permutation

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

1 round = 1 column step followed by 1 diagonal step

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

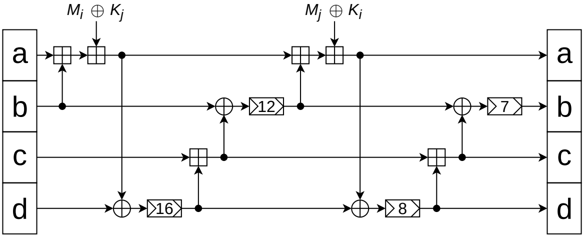


BLAKE’s Permutation

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

1 round = 1 column step followed by 1 diagonal step

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

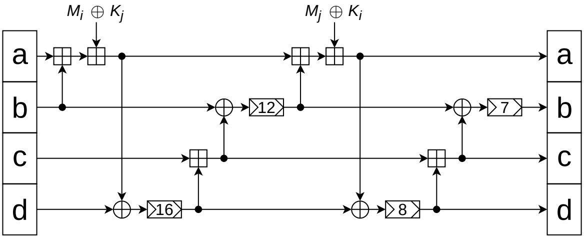


BLAKE’s Permutation

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

1 round = 1 column step followed by 1 diagonal step

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

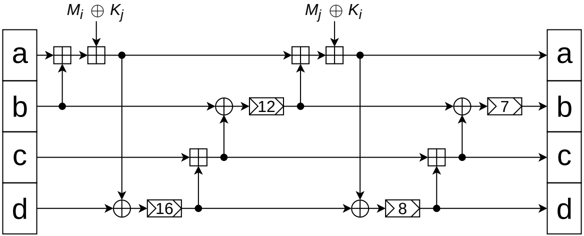


BLAKE’s Permutation

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

1 round = 1 column step followed by 1 diagonal step

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

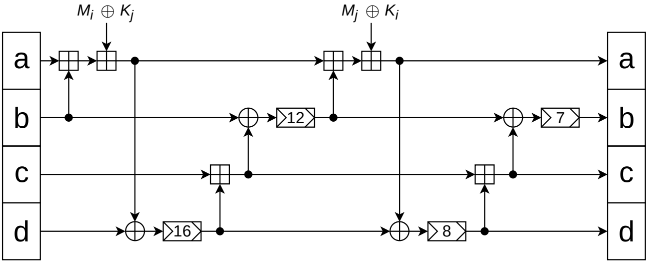


Main Results

- Round-Reduced Near-Collisions up to 4 Rounds for BLAKE-32
- 5/6-Round Impossible Differentials for BLAKE-32/64
- Improved Preimage Attack on 1.5-Round
- More bounds

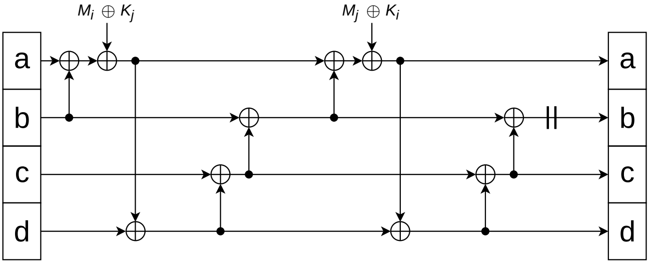
Linearization for BLAKE-32

- $\Delta = 0x88888888$, invariant w.r.t. rotation by 4
- Linearization: replace addition by xor
- No-difference goes through $\ggg 7$

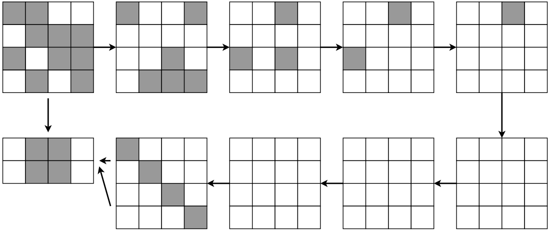


Linearization - linearized G

- $\Delta = 0x88888888$, invariant w.r.t. rotation by 4
- Linearization: replace addition by xor
- No-difference goes through $\ggg 7$



4-Round Near Collisions for BLAKE-32



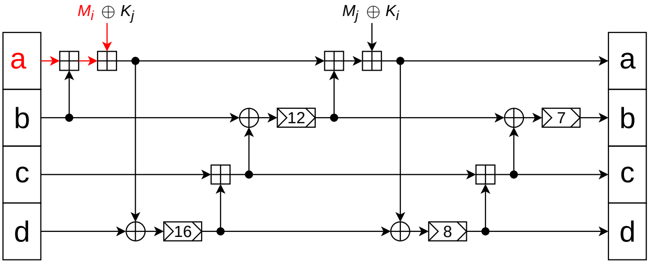
- Rounds 6 - 9
- 1.5 rounds for free using message modification
- Time Complexity: 2^{42}, with negligible memory

Impossible Differentials

Miss-in-the-Middle:
proof by contradiction that ($\alpha \rightarrow \gamma$) can not occur,

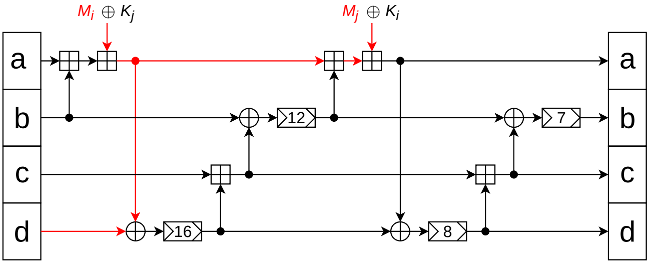
$$\alpha \xrightarrow{\textit{prob}.1} \beta \neq \delta \xleftarrow{\textit{prob}.1} \gamma$$

Probability 1 Differential - 1st



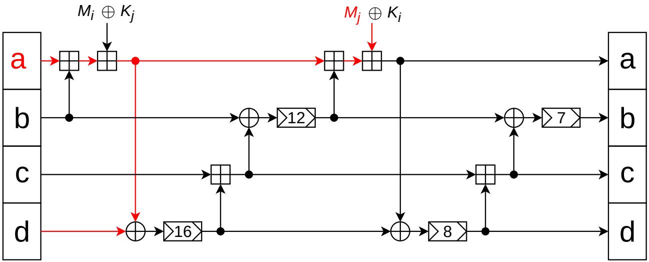
$\Delta = 0x800\ldots00$, prob = 1

Probability 1 Differential - 2nd



$\Delta = 0x800\ldots00$, prob = 1

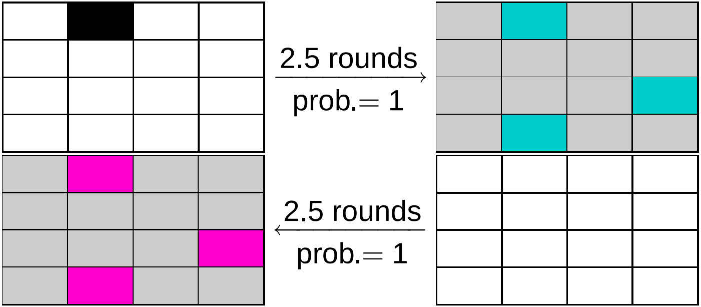
Probability 1 Differential - 3rd



$\Delta = 0x800\ldots00$, prob = 1

5-round impossible differential for BLAKE-32

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



2.5 rounds

prob.$=$ 1

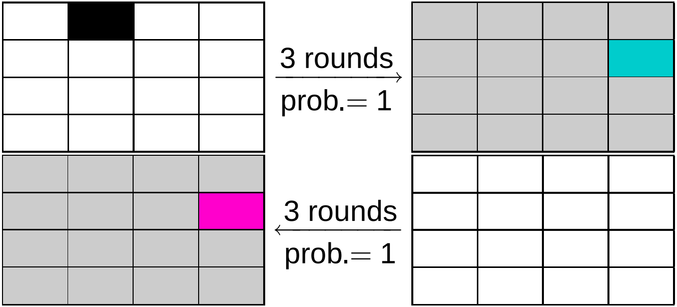
2.5 rounds

prob.$=$ 1

- Start with $\Delta = 0x800\ldots00$ in v_1 and M_2
- Differences after 2.5 rounds DO NOT match

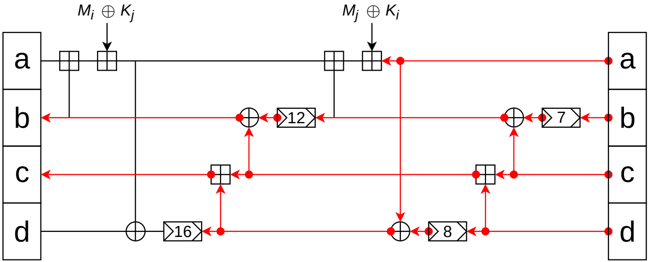
6-round impossible differential for BLAKE-64

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



- Start with $\Delta = 0x800\ldots00$ in v_2 and M_1
- Differences after 3 rounds DO NOT match

Inverting G



Compute two words without knowing the message!

Inverting the Permutation

From output, get 8 words of intermediate state for free.

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

Inverting the Permutation

From output, get 8 words of intermediate state for free.

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

Determine rest state words in forward direction from input, followed by all message words.

Inverting the Permutation

From output, get 8 words of intermediate state for free.

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

Determine rest state words in forward direction from input, followed by all message words.

This applies to 1.5-round, but a bit more complicated ...

Inverting the Permutation

From output, get 8 words of intermediate state for free.

$$\begin{pmatrix} v_0 & v_1 & v_2 & v_3 \\ \color{red}{v}_4 & \color{red}{v}_5 & \color{red}{v}_6 & \color{red}{v}_7 \\ \color{red}{v}_8 & \color{red}{v}_9 & \color{red}{v}_{10} & \color{red}{v}_{11} \\ v_{12} & v_{13} & v_{14} & v_{15} \end{pmatrix}$$

Determine rest state words in forward direction from input, followed by all message words.
This applies to 1.5-round, but a bit more complicated ...

- 1 and 1.5-round are permutation of message
- Preimage attacks on 1.5-round, in $2^{128}/2^{256}$ for BLAKE-32/64, compared with $2^{192}/2^{384}$ (Li & Xu, eprint 2009/238)

More Results

- Large class of 2-round impossible differentials
- Conjecture on maximum 5-round against the MitM preimage attack. Refer to free-start (without Initialization) 4.5-round attack by Wang-Ohta-Sakiyama at Asiacrypt 2009 rump session
- Collision in $2^{n/4}$ for the variant with same constants.
- More bounds on probability of any differential characteristics

Results and Future Work

Results:

- 2^{42} 4-round near collisions
- Impossible differentials for 5/6-rounds
- $2^{128}/2^{256}$ preimages for 1.5-round BLAKE-32/64
- More bounds ...

None of these threat the full BLAKE.

Results and Future Work

Results:

- 2^{42} 4-round near collisions
- Impossible differentials for 5/6-rounds
- $2^{128}/2^{256}$ preimages for 1.5-round BLAKE-32/64
- More bounds ...

None of these threat the full BLAKE.

Future Work:

- Nonlinear connector for collision with more rounds?
- Rotational Cryptanalysis? Too many constants to be successful?
- More properties of G?

End of Talk

Thank You!