Differential and Invertibility Properties of BLAKE

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

[1]FHNW, Windisch, Switzerland

[2]Nanyang Technological University, Singapore

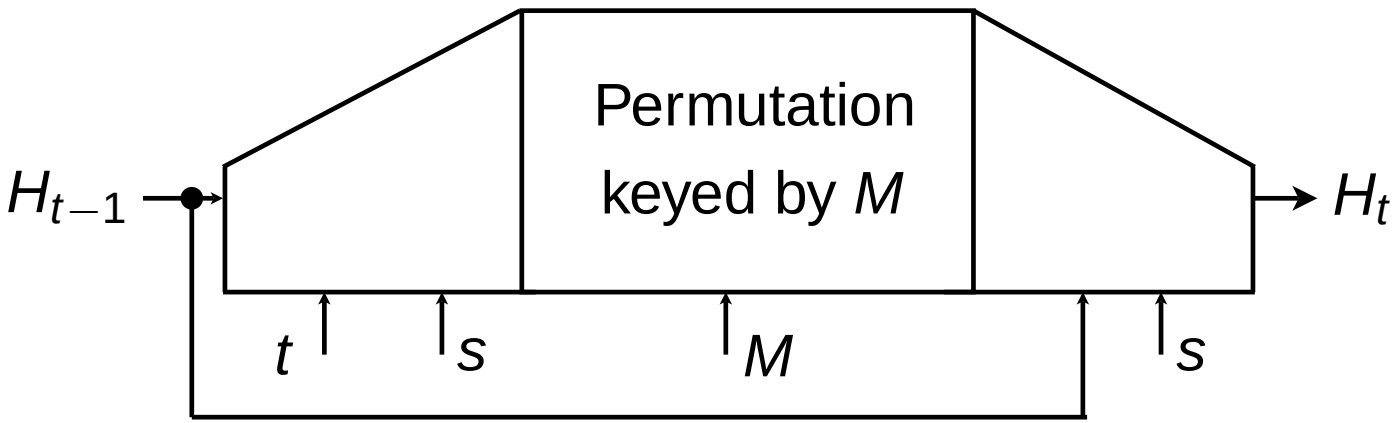
[3]Technical University of Denmark, Denmark

18 Jan 2010

Talk Overview

BLAKE Overview

- One of the 14 second round SHA-3 candiates
- HAIFA-like construction (narrow pipe)
- Local wide-pipe compression function



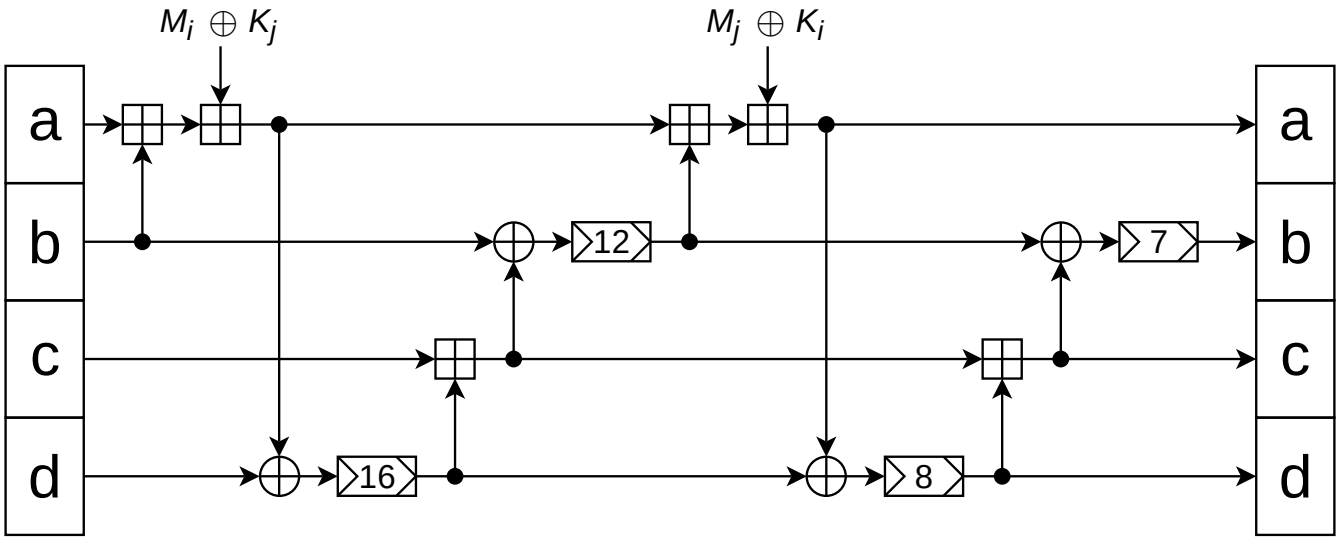
- BLAKE-32: 32-bit word, 512-bit state, 10 rounds, 256-bit digest
- BLAKE-64: 64-bit word, 1024-bit state, 14 rounds, 512-bit digest

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

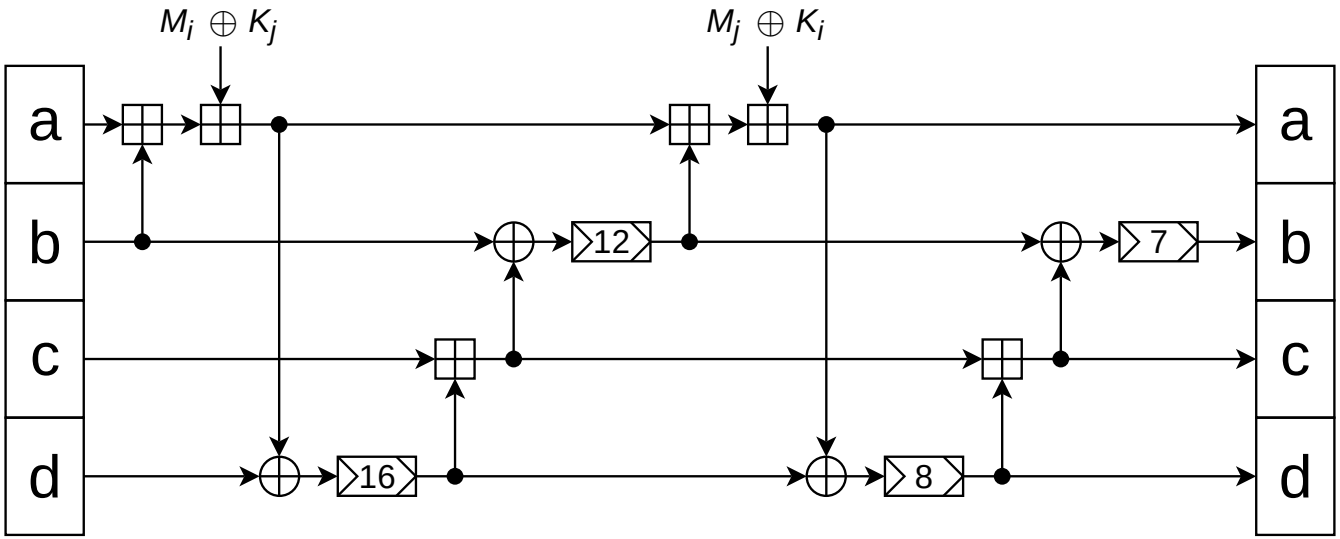


BLAKE's Permutation

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

1 round = 1 column step followed by 1 diagonal step

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

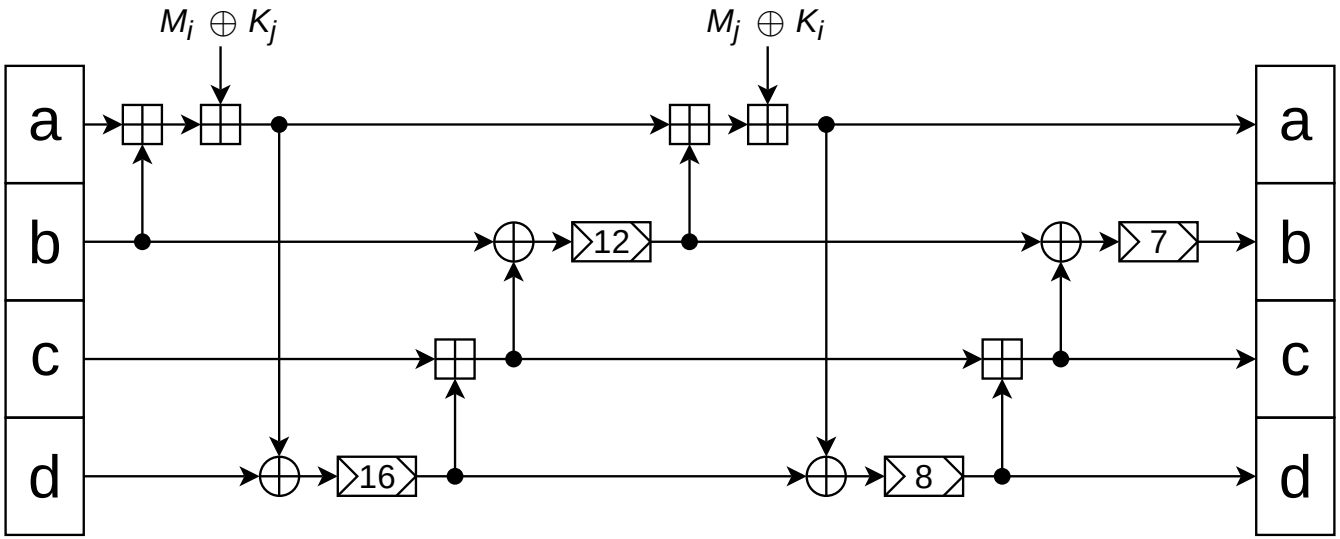


BLAKE's Permutation

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

1 round = 1 column step followed by 1 diagonal step

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

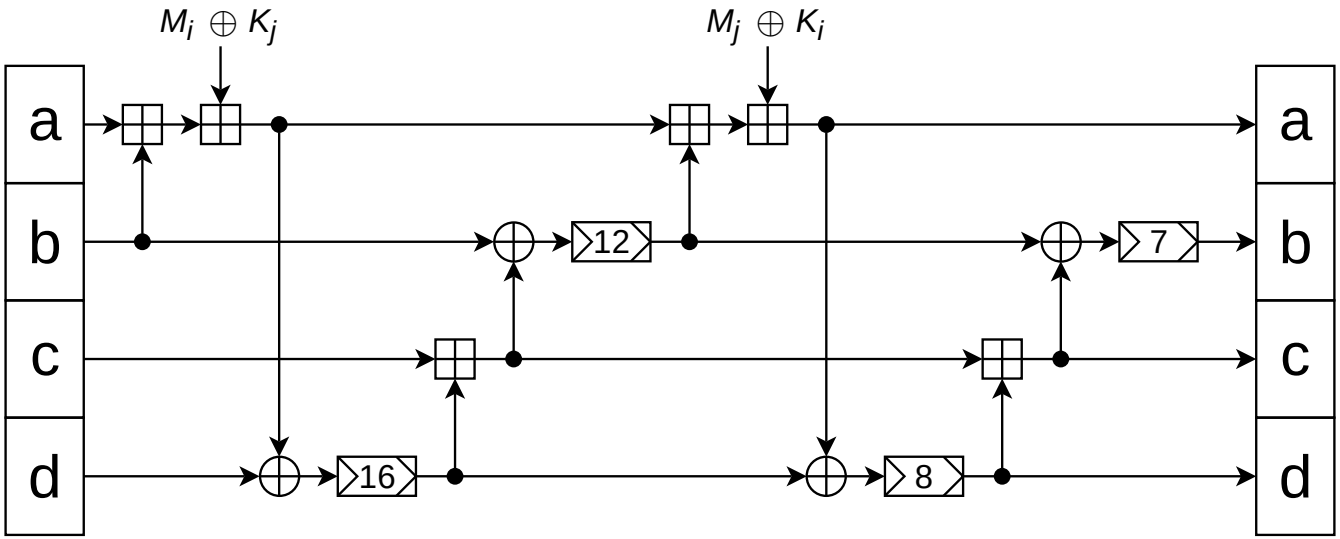


BLAKE's Permutation

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

1 round = 1 column step followed by 1 diagonal step

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

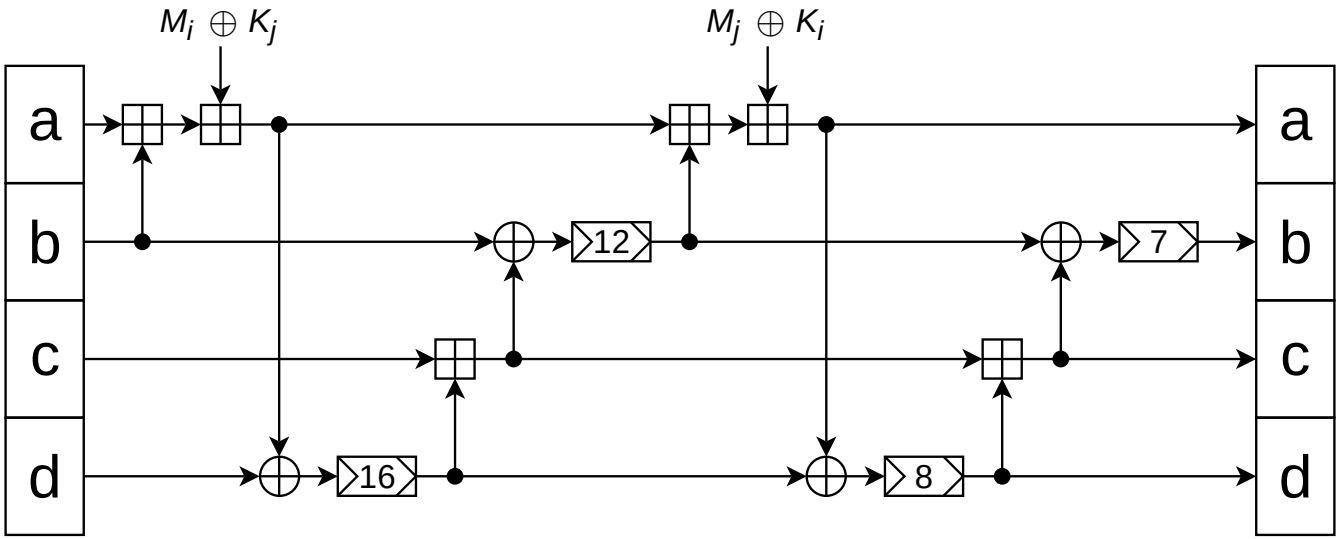


BLAKE's Permutation

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

1 round = 1 column step followed by 1 diagonal step

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

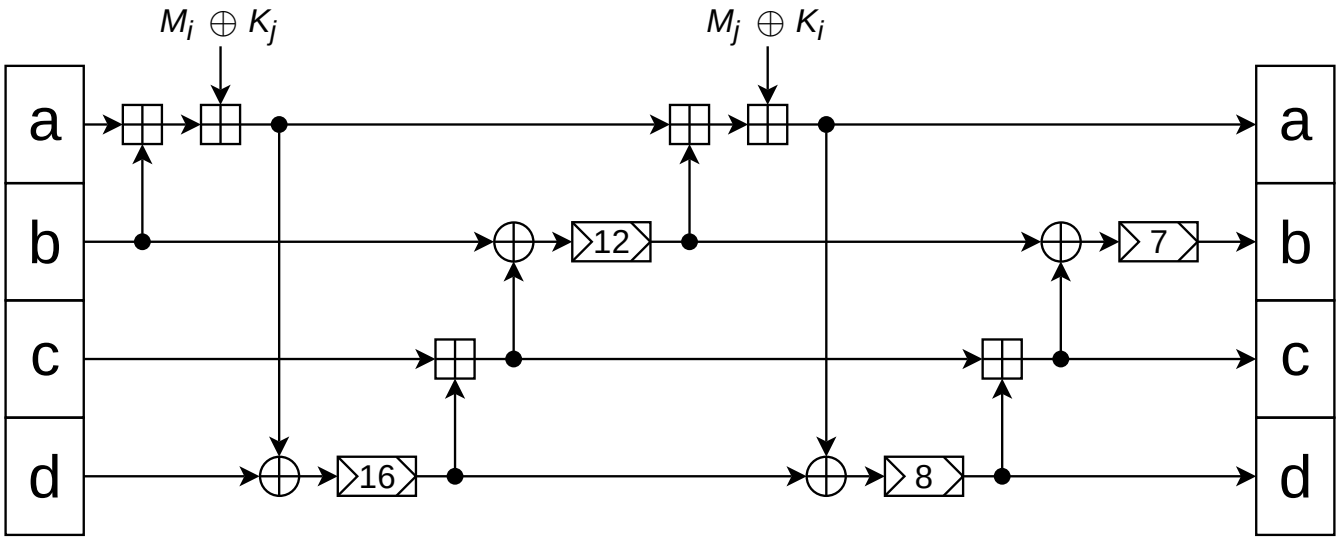


BLAKE's Permutation

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

1 round = 1 column step followed by 1 diagonal step

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

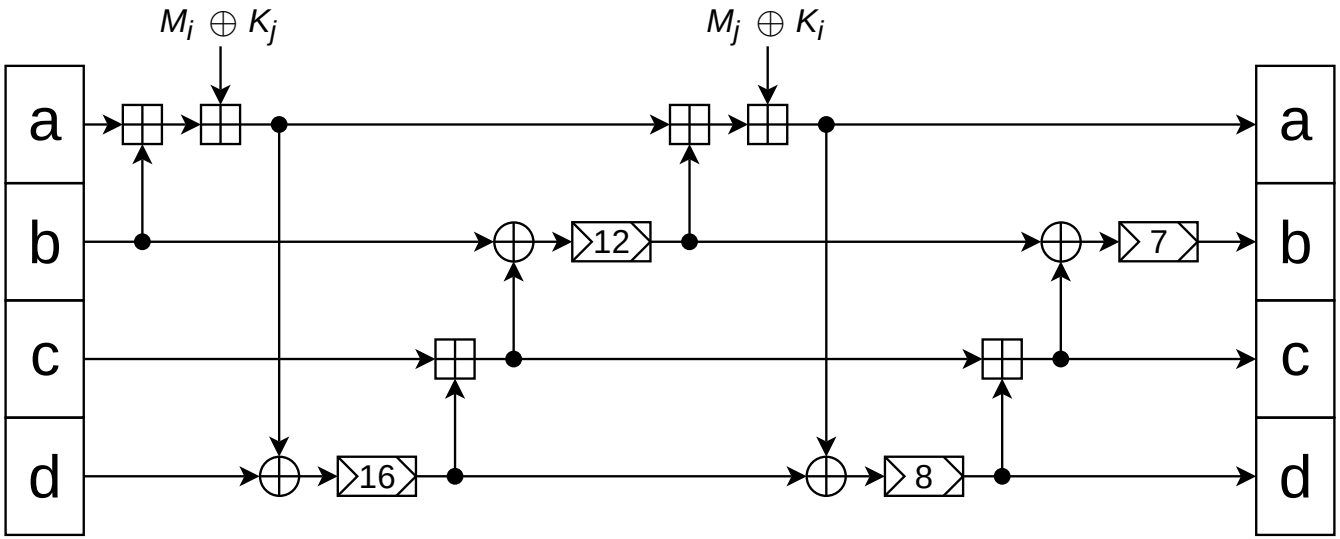


BLAKE's Permutation

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

1 round = 1 column step followed by 1 diagonal step

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

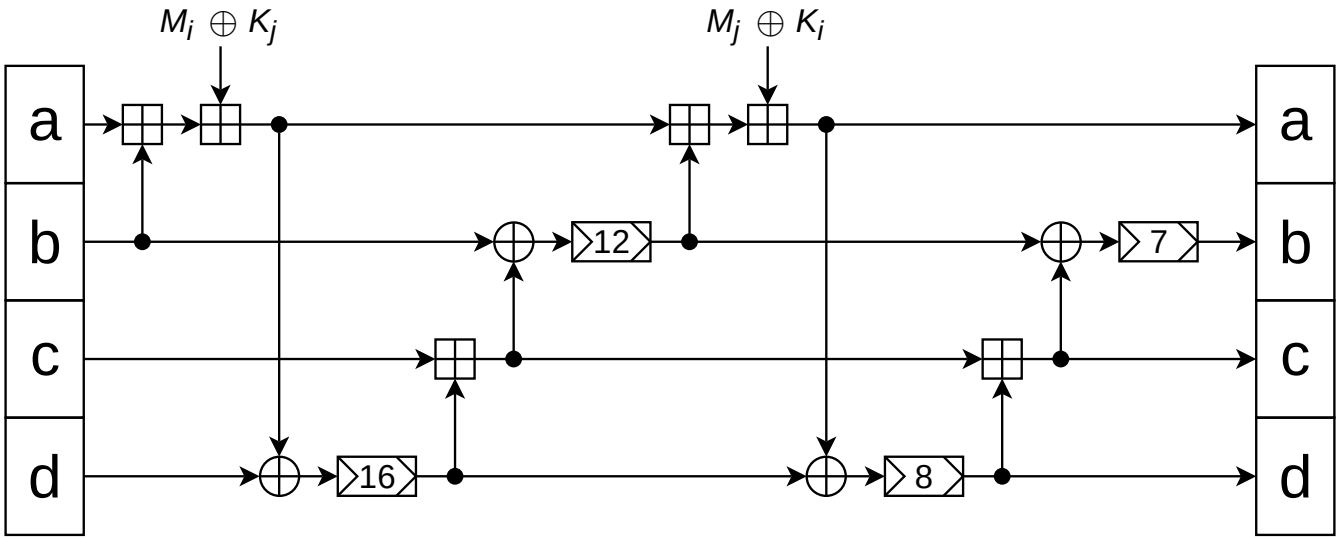


BLAKE's Permutation

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

1 round = 1 column step followed by 1 diagonal step

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

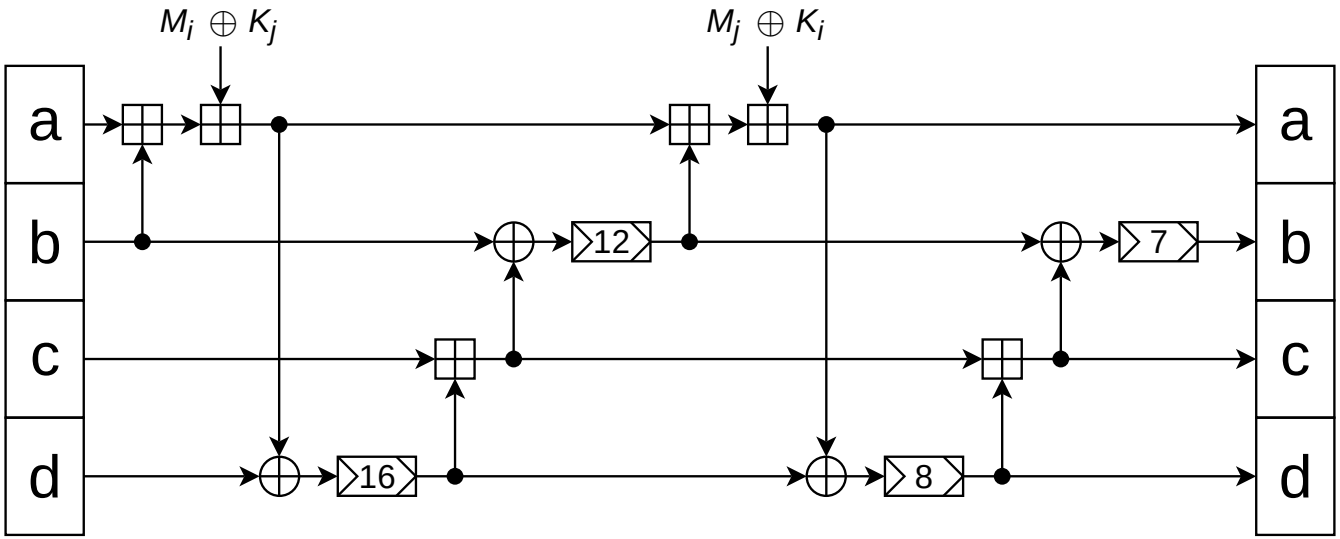


BLAKE's Permutation

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

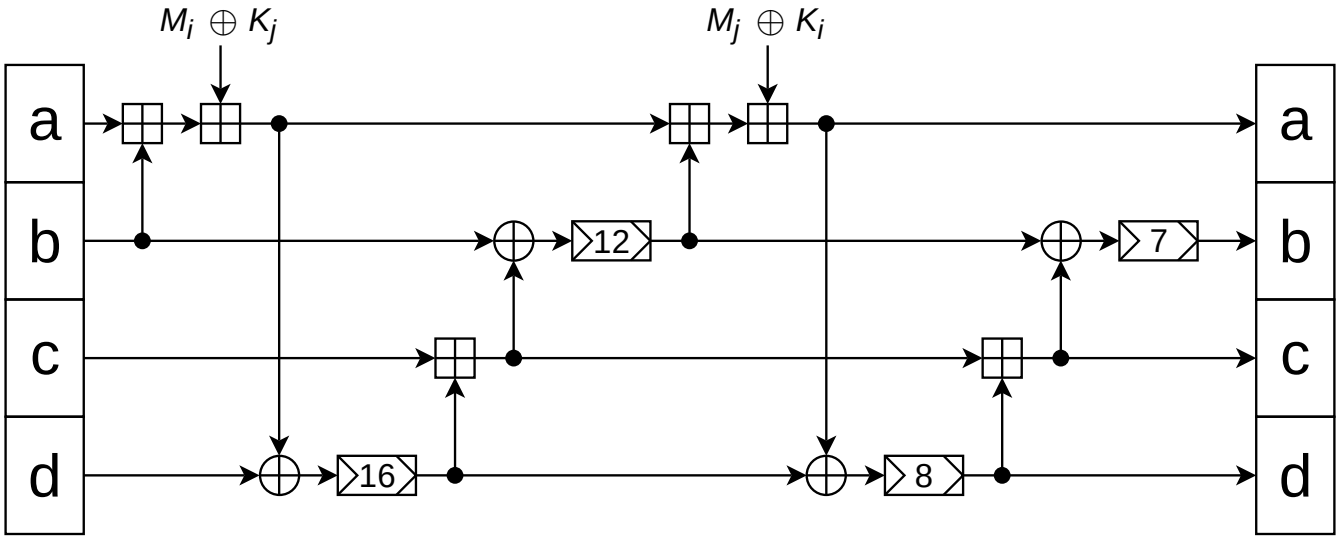
1 round = 1 column step followed by 1 diagonal step

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



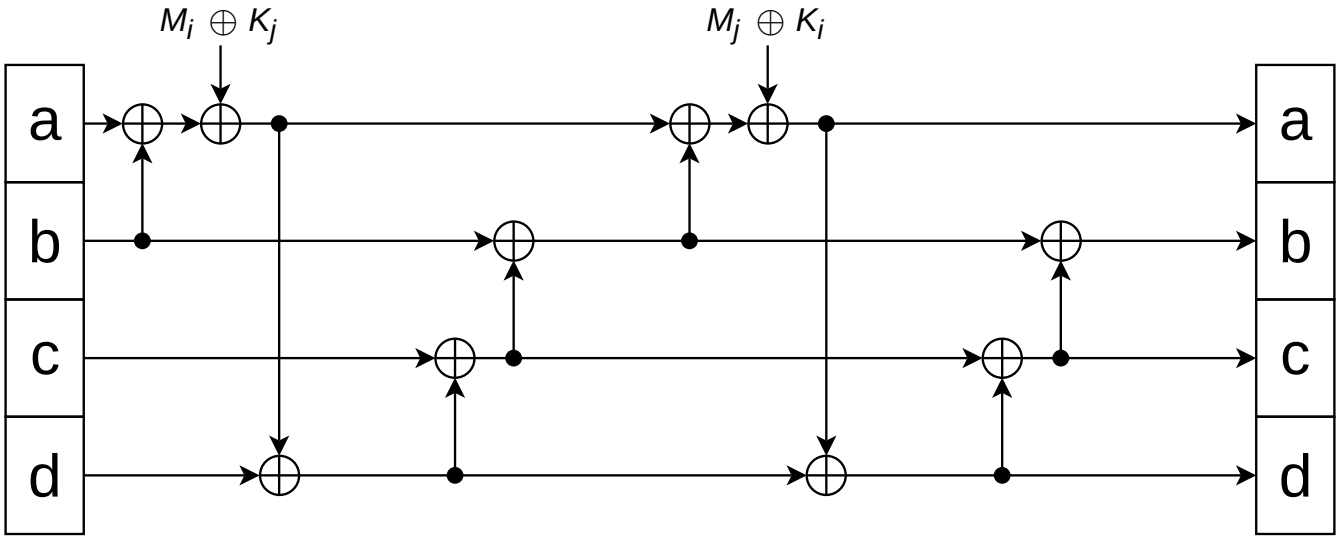
Linearization for BLAKE-32

- $\Delta = 0x88888888$, invariant of ratations by 4
- Linearization: replace addition by xor
- No-difference goes through $\ggg 7$
- 1.5 rounds for fee using message modification

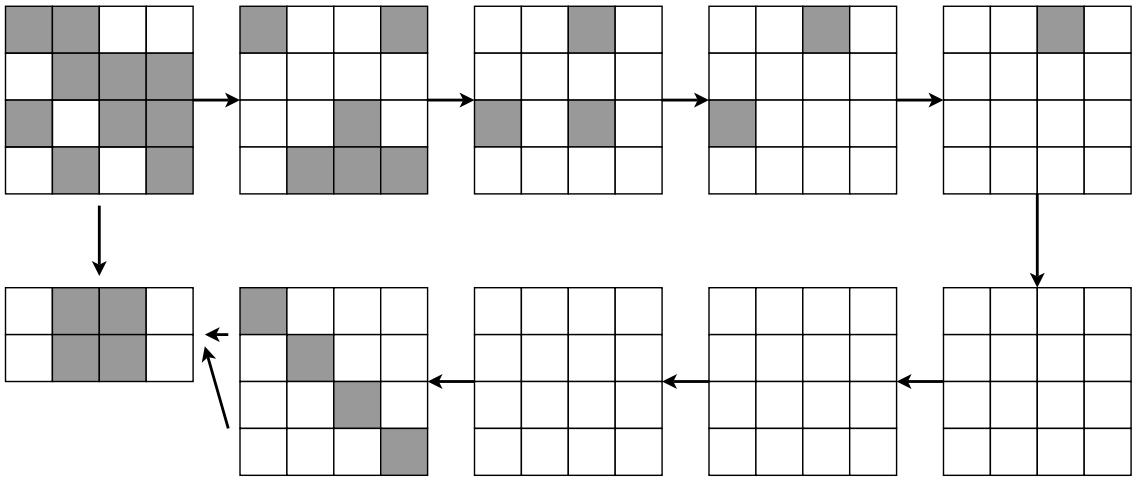


Linearization - linearized G

- $\Delta = 0x88888888$, invariant of ratations by 4
- Linearization: replace addition by xor
- No-difference goes through $\ggg 7$
- 1.5 rounds for fee using message modification



4-Round Near Collisions for BLAKE-32



- Rounds 6 - 9
- Time Complexiy: 2^{42}, with negligible memory

Impossible Differentials

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

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

Impossible Differentials

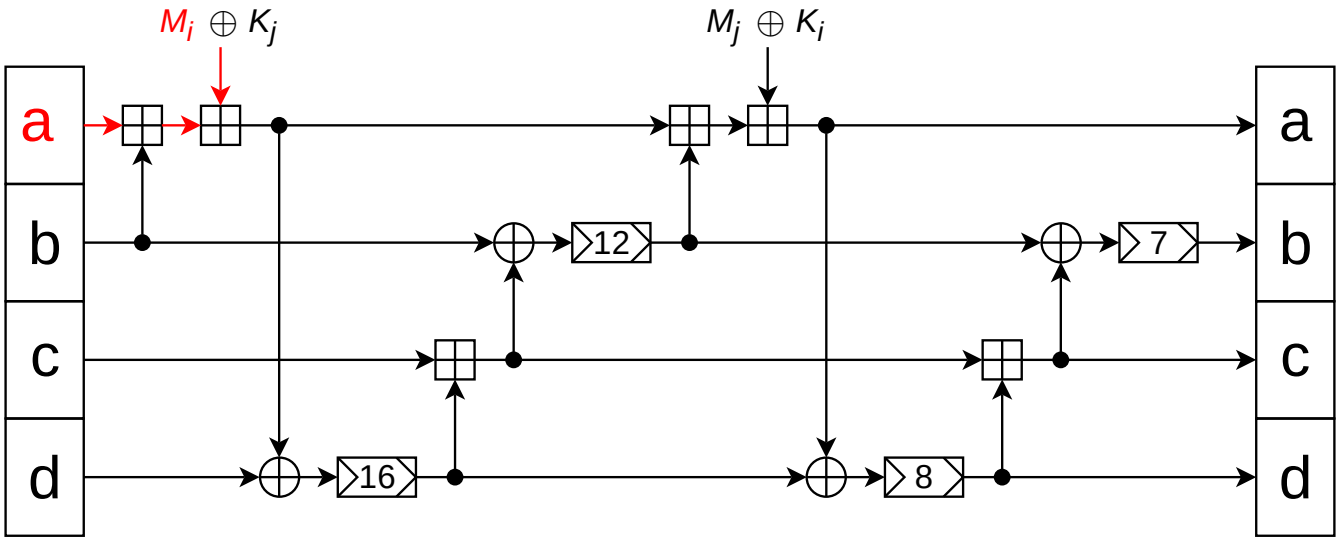
Miss-in-the-Middle:
proof by contradiction that ($\alpha \rightarrow \gamma$) can not occur,

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

Construct long impossible differentials by concatenating:

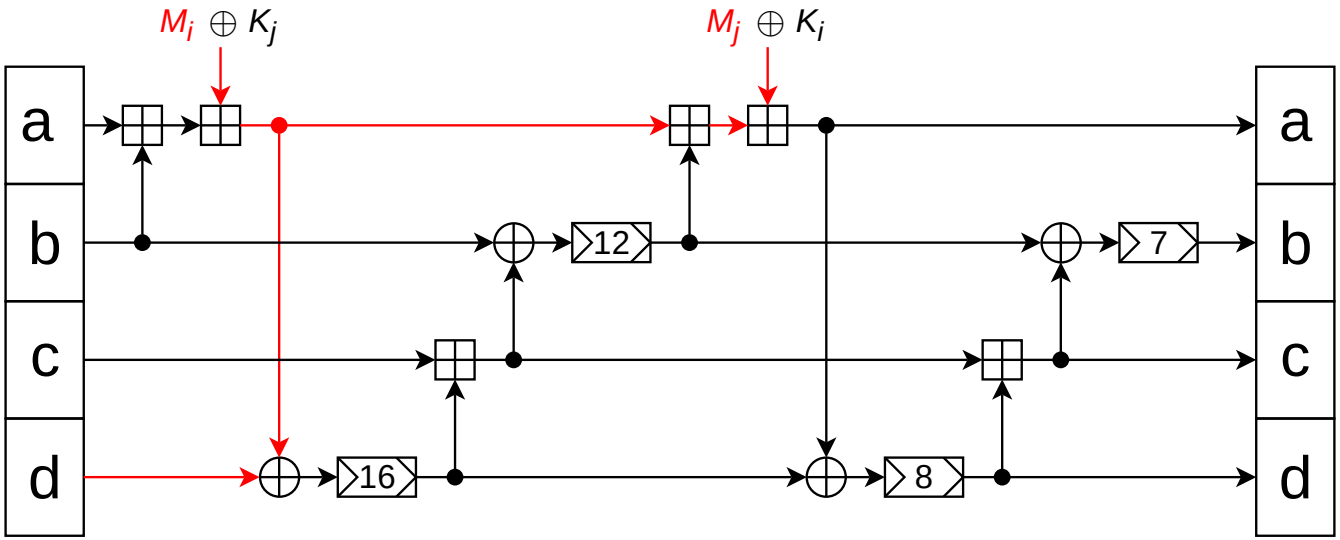
- probablity 1 differentials
- impossible differentials

Probablity 1 Differential - 1st



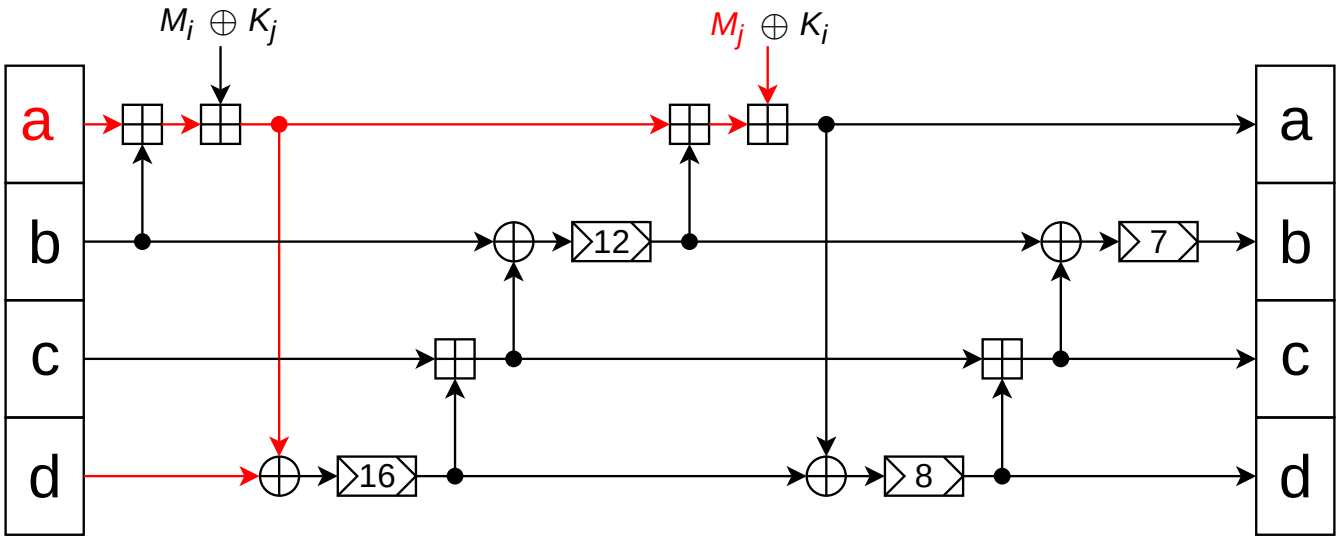
$\Delta = 0x800\ldots00$, prob = 1

Probablity 1 Differential - 2nd



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

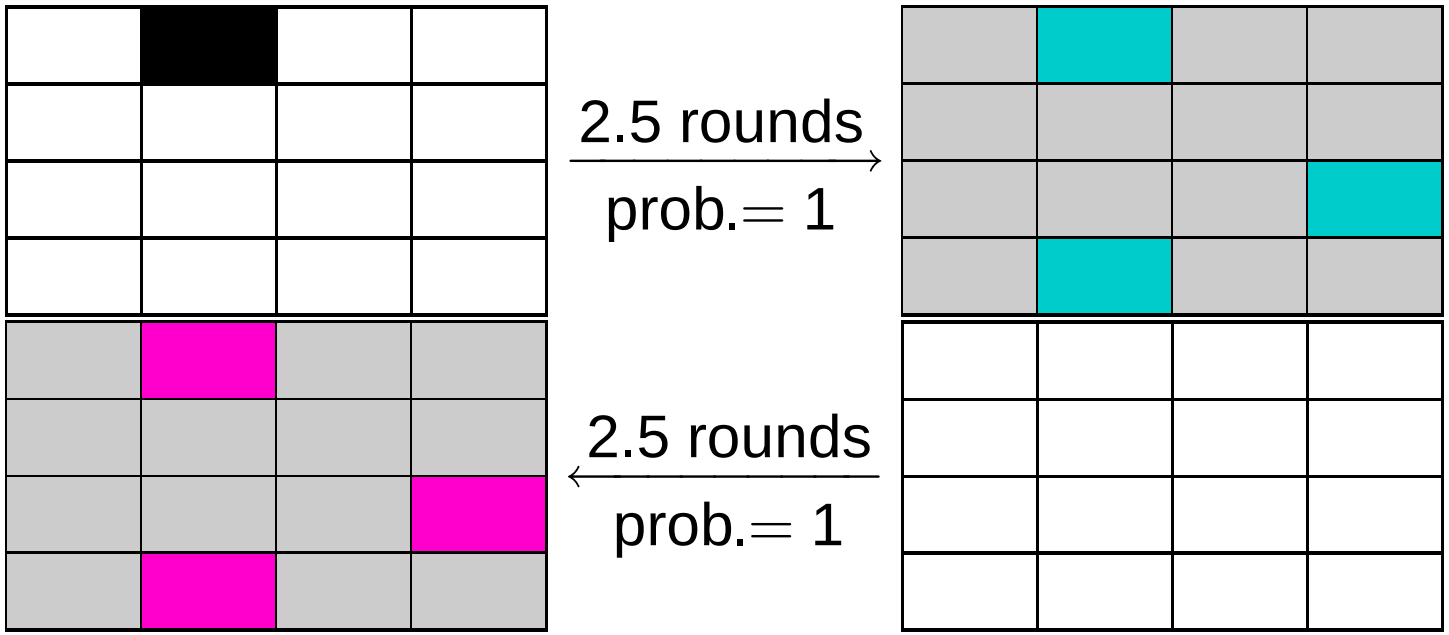
Probablity 1 Differential - 3rd



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

5-round impossible differential for BLAKE-32

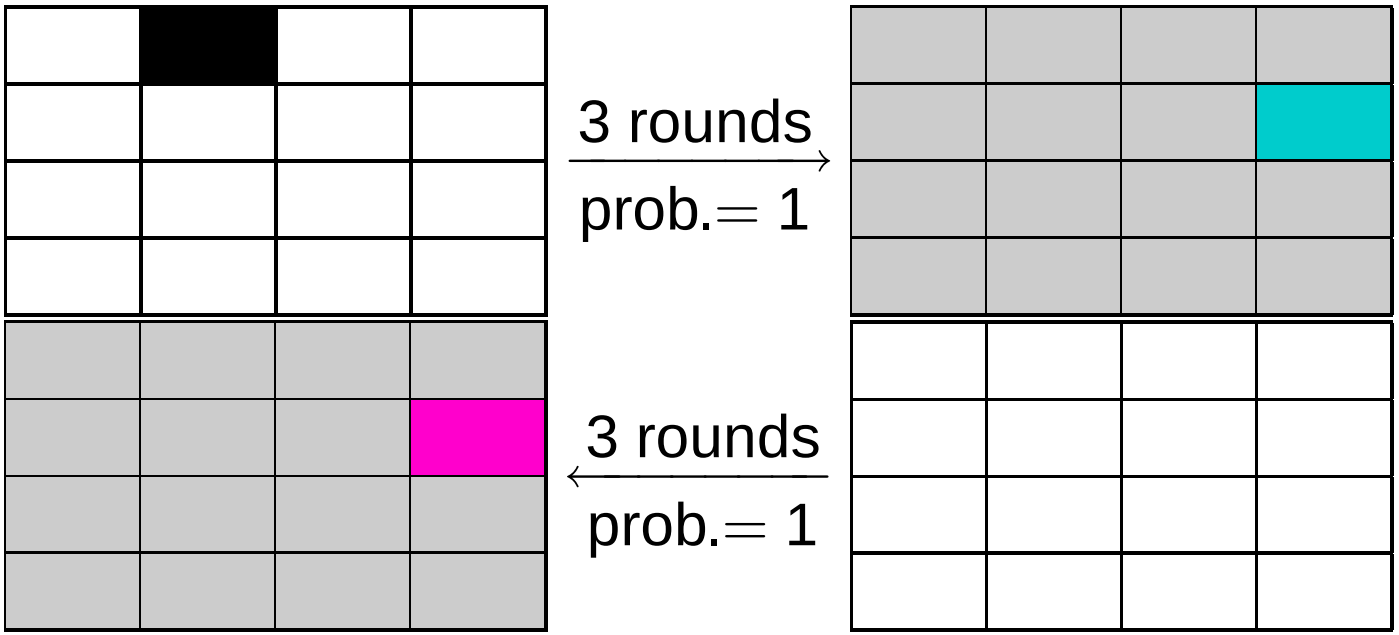
Apply miss-in-the-middle to BLAKE-32:



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

Conclusions

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