Round-Reduced Near-Collisions of BLAKE-32

Jian Guo[1] and Krystian Matusiewicz[2]

Nanyang Technological University, Singapore

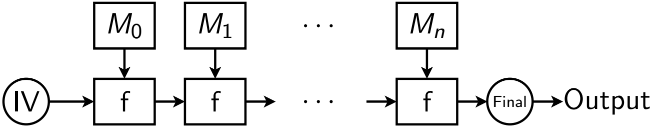
Technical University of Denmark

07 July 2009

Table of contents

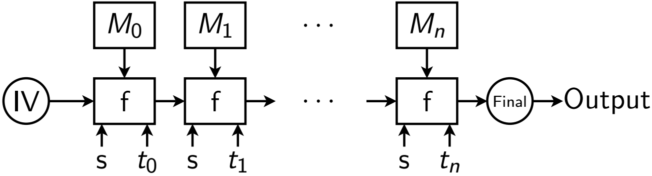
1. Introduction
   - HAIFA
   - BLAKE
2. Differential Attack
   - Differential Path
   - 4-Round Near Collisions
3. Conclusions

MD structure



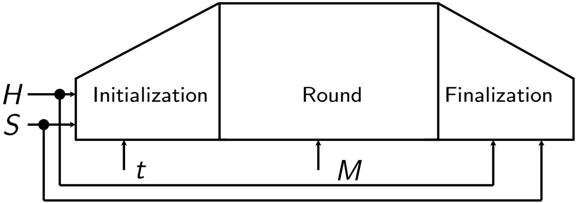
- M_i: i-th Message Block
- f: Compression Function
- IV: Initial Value
- Final: Finalization

HAIFA



- s: salts
- t: block index – number of bits/bytes compressed so far

Overview of BLAKE



- H: chaining (8 words)
- S: salts (4 words)
- t: block index (2 words)
- Internal Wide-Pipe Design

Initialization

$$\begin{pmatrix} v_0 & v_1 & v_2 & v_3 \\ v_4 & v_5 & v_6 & v_7 \\ v_8 & v_9 & v_{10} & v_{11} \\ v_{12} & v_{13} & v_{14} & v_{15} \end{pmatrix} \longleftarrow \begin{pmatrix} h_0 & h_1 & h_2 & h_3 \\ h_4 & h_5 & h_6 & h_7 \\ s_0 \oplus c_0 & s_1 \oplus c_1 & s_2 \oplus c_2 & s_3 \oplus c_3 \\ t_0 \oplus c_4 & t_0 \oplus c_5 & t_1 \oplus c_6 & t_1 \oplus c_7 \end{pmatrix}$$

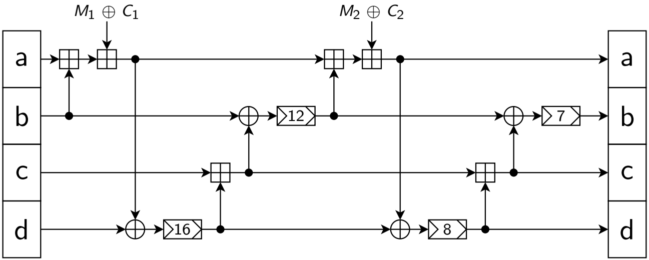
- c: constants

ProcessMessage

$$
\begin{array}{ll}
\text{//column half-round} & \text{//diagonal half-round} \\
G(v_0, v_4, v_8, v_{12}) & G(v_0, v_5, v_{10}, v_{15}) \\
G(v_1, v_5, v_9, v_{13}) & G(v_1, v_6, v_{11}, v_{12}) \\
G(v_2, v_6, v_{10}, v_{14}) & G(v_2, v_7, v_8, v_{13}) \\
G(v_3, v_7, v_{11}, v_{15}) & G(v_3, v_4, v_9, v_{14})
\end{array}
$$

- 10 rounds for BLAKE-32/28
- 14 rounds for BLAKE-64/48

BLAKE-32 – G Function



Difference with BLAKE-64:

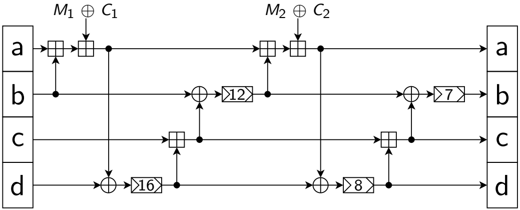
- word size
- number of bits totation

Finalization

$$
\begin{aligned}
h'_0 &\leftarrow h_0 \oplus s_0 \oplus v_0 \oplus v_8\\
h'_1 &\leftarrow h_1 \oplus s_1 \oplus v_1 \oplus v_9\\
h'_2 &\leftarrow h_2 \oplus s_2 \oplus v_2 \oplus v_{10}\\
h'_3 &\leftarrow h_3 \oplus s_3 \oplus v_3 \oplus v_{11}\\
h'_4 &\leftarrow h_4 \oplus s_0 \oplus v_4 \oplus v_{12}\\
h'_5 &\leftarrow h_5 \oplus s_1 \oplus v_5 \oplus v_{13}\\
h'_6 &\leftarrow h_6 \oplus s_2 \oplus v_6 \oplus v_{14}\\
h'_7 &\leftarrow h_7 \oplus s_3 \oplus v_7 \oplus v_{15}
\end{aligned}
$$

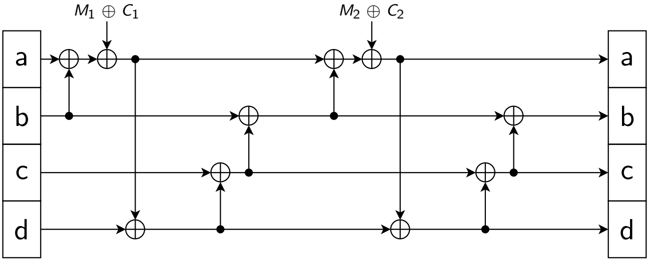
- feedforward
- output from Compression Function
- salts

Observations



- BLAKE-32, number of bits rotations are multiple of 4 with one exception.
- Differences like 0x88888888 are ration invariant with number of bits multiple of 4.
- NOT suitable for BLAKE-64

Linearized G Function



Model under $\mathbb{F}_2$:

- **1** - there is difference (0x88888888)
- **0** - no difference
- Each Additon gives probablity 2^{-7}

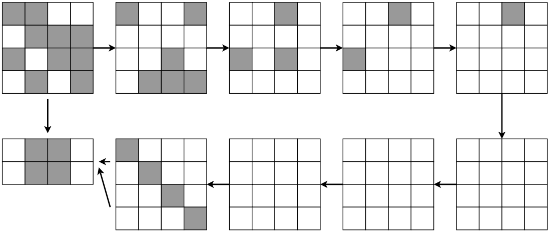
Constraint: **No differences in** b

Fast Search for Collisions

- 16 input chaining + 16 message words
- No difference in output of G
- Minimize number of additon linearization
- 2^{32} configurations
- MAGMA to eliminate poor configurations fast.
- Free 1.5 rounds using freedom of 16 message words.

Result: good configurations for up to 4 steps with 6 additions.

(Near) Collisions of 4-Round BLAKE-32



Conclusions

- Collisions for 3.5 rounds
- Near-Collisions for 4 rounds with complexity 2^{42}

Open Questions

- Cancadinate two 4-rounds configurations to get 8 or more rounds collisions
- Nonrandomness for more than 4 rounds
- Two block full collisions
- (Second) Preimages
- Combinations of differences 0x80808080 and 0x08080808 to reduce complexity.

END

THANK YOU!
QUESTIONS?