Analysis of BLAKE2

Jian Guo[†] **Pierre Karpman**[†⋆] Ivica Nikolić[†] Lei Wang[†]
Shuang Wu[†]

[†]Nanyang Technological University, Singapore
[⋆]École normale supérieure de Rennes, France

The Cryptographer's Track at the RSA Conference, San Francisco
2014–02–28

The BLAKE hash function family

- One of the five SHA-3 finalists
- Purely ARX round function inspired from ChaCha
- Local wide-pipe compression function in a HAIFA iteration mode
- Four digest sizes: BLAKE-224/256 & BLAKE-384/512
- Very fast in software
- Widely believed to be very secure

BLAKE specifications (compression function)

- Bijectively transforms a $4 \times 4 \times 32/64$-bit state with a $16 \times 32/64$-bit message
- (Uses four parallel applications of a 'G function')
- The output is compressed to form the chaining value
- Initial state:

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

BLAKE specifications (compression function)

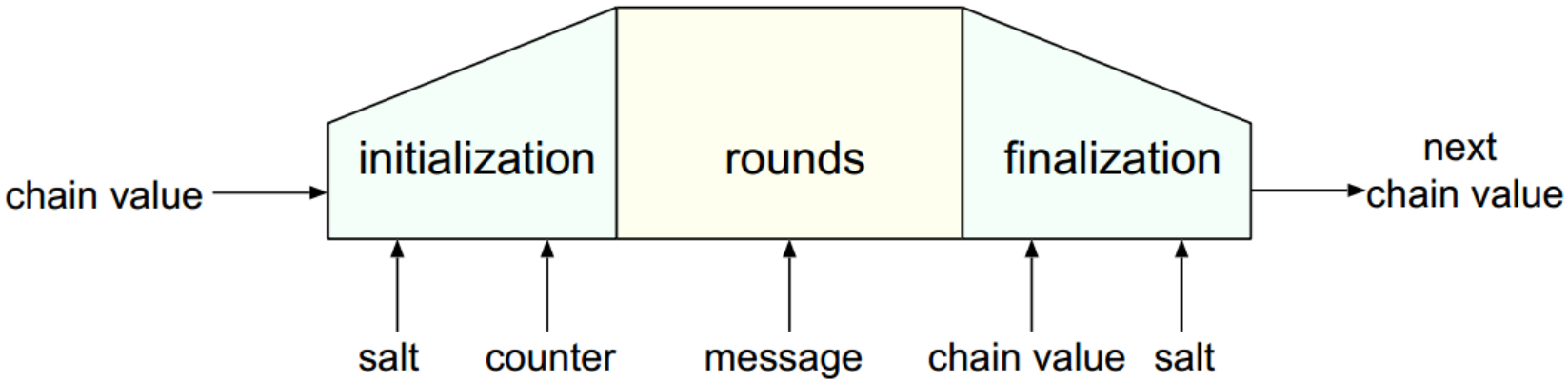

Figure : BLAKE compression function structure (Aumasson *& al.*, 2010)

BLAKE specifications (G function)

- Feistel-like function with four branches
- $\mathbf{G}_{i,j}(a, b, c, d)$ computes:

$$
\begin{aligned}
&1{:}\, a \leftarrow a + b + (m_i \oplus c_j) && 5{:}\, a \leftarrow a + b + (m_j \oplus c_i)\\
&2{:}\, d \leftarrow (d \oplus a) \ggg 32/16 && 6{:}\, d \leftarrow (d \oplus a) \ggg 16/8\\
&3{:}\, c \leftarrow c + d && 7{:}\, c \leftarrow c + d\\
&4{:}\, b \leftarrow (b \oplus c) \ggg 25/12 && 8{:}\, b \leftarrow (b \oplus c) \ggg 11/7
\end{aligned}
$$

BLAKE specifications (G function)

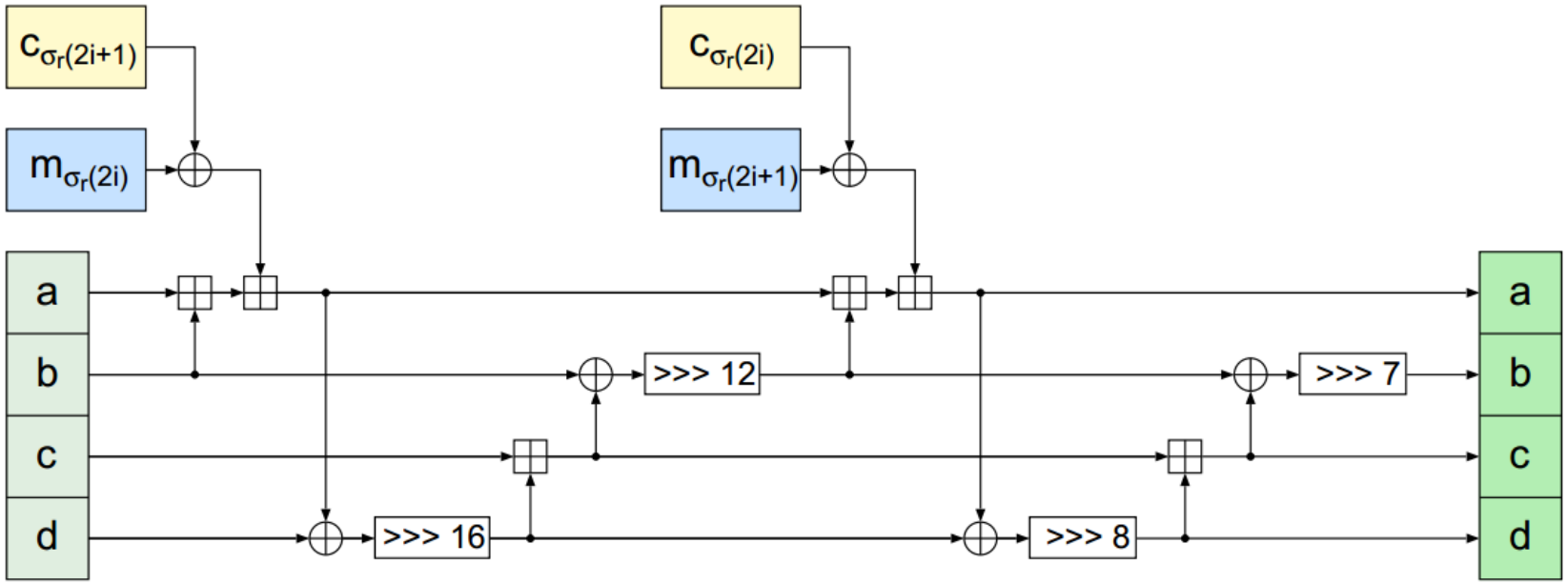

Figure : Diagram of the BLAKE-224/256 G function (Aumasson *& al.*, 2010)

BLAKE specifications (round structure)

- One round alternates a column & a diagonal step
- BLAKE-224/256 use 14 rounds; BLAKE-384/512 use 16

BLAKE specifications (round structure)

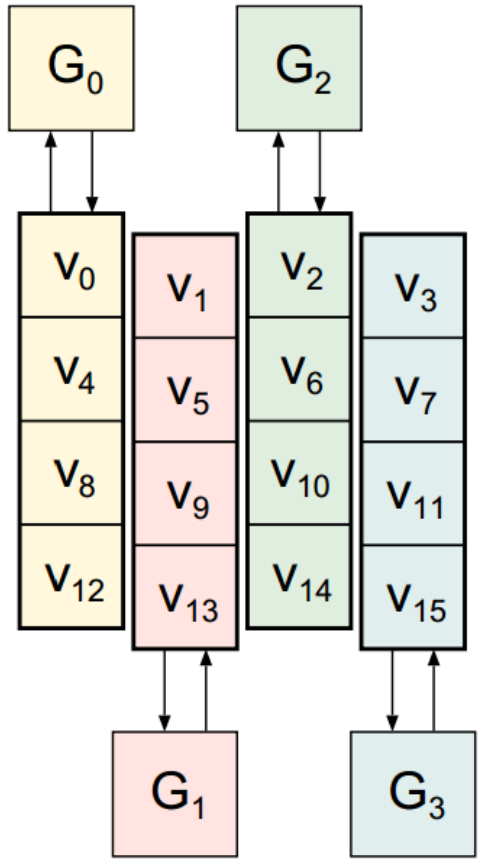

Figure : BLAKE column step (Aumasson *& al.*, 2010)

BLAKE specifications (round structure)

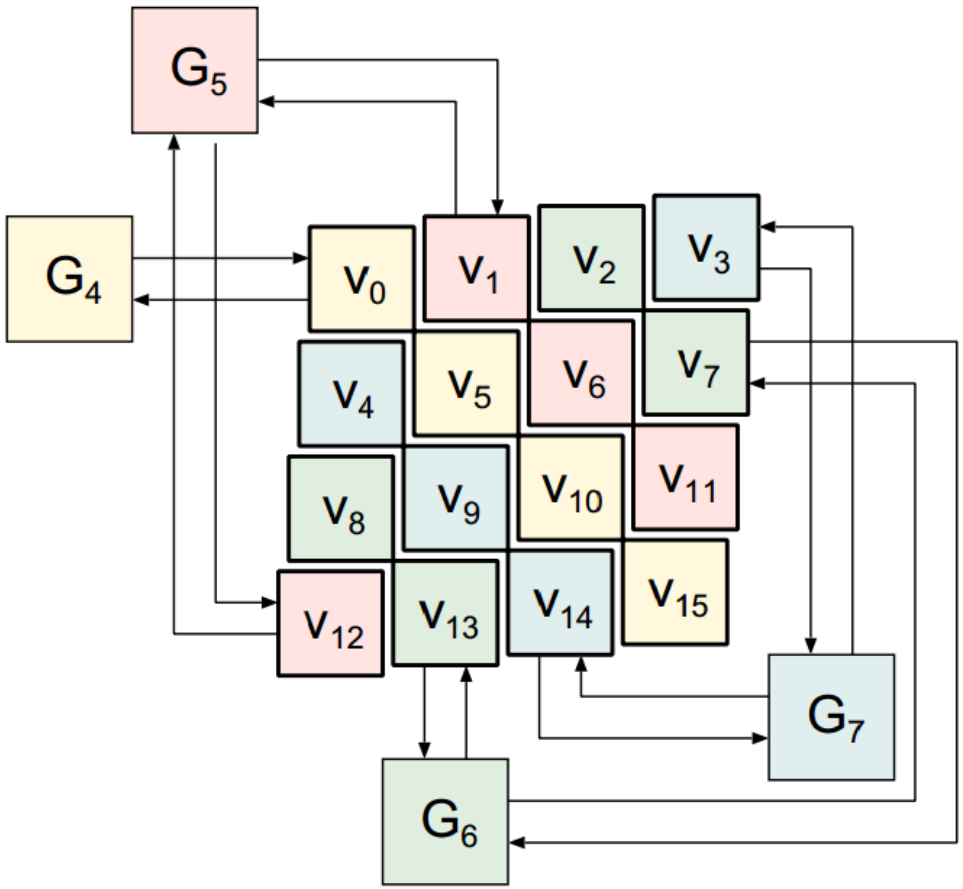

Figure : BLAKE diagonal step (Aumasson *& al.*, 2010)

BLAKE evolves into BLAKE2

- BLAKE2 is an even faster evolution of BLAKE (Aumasson *& al.*, ACNS 2013)
- Already popular
- Some changes made to the G function; initialisation; # of rounds
- No specific security analysis provided

BLAKE2 specifications (compression function)

- Initial state:

$$\begin{pmatrix} v_0 & v_1 & v_2 & v_3 \\ v_4 & v_5 & v_6 & v_7 \\ v_8 & v_9 & v_{10} & v_{11} \\ v_{12} & v_{13} & v_{14} & v_{15} \end{pmatrix} \leftarrow \begin{pmatrix} h_0 & h_1 & h_2 & h_3 \\ h_4 & h_5 & h_6 & h_7 \\ c_0 & c_1 & c_2 & c_3 \\ t_0 \oplus c_4 & t_1 \oplus c_5 & f_0 \oplus c_6 & f_1 \oplus c_7 \end{pmatrix}$$

- $\Longrightarrow$ Less freedom for the attacker (salt goes somewhere else)
- BLAKE2s uses 10 rounds; BLAKE2b uses 12

BLAKE2 specifications (G function)

- $\mathbf{G}_{i,j}(a,b,c,d)$ computes:

$1{:}a \leftarrow a+b+m_i$	$5{:}a \leftarrow a+b+m_j$
$2{:}d \leftarrow (d \oplus a) \ggg 32/16$	$6{:}d \leftarrow (d \oplus a) \ggg 16/8$
$3{:}c \leftarrow c+d$	$7{:}c \leftarrow c+d$
$4{:}b \leftarrow (b \oplus c) \ggg 24/12$	$8{:}b \leftarrow (b \oplus c) \ggg 63/7$

- Self-difference only in the message words
- 'Similar' rotations for BLAKE2s & BLAKE2b

Soooo.... what can we do?

Figure : Calvin & Hobbes (Watterson, 1985–1995)

Rotational distinguishers for the (keyed) permutation

- Introduced by (Khovratovich & Nikolić, FSE 2010)
- Distinguish a function F by $\mathrm{F}(x) \lll r = \mathrm{F}(x \lll r)$
- Exploits the absence of constants & 'small' number of '+' ops in **G**
- $\Pr[\mathbf{G}(a, b, c, d, m_i, m_j) \lll 1 = \mathbf{G}(a \lll 1, b \lll 1, c \lll 1, d \lll 1, m_i \lll 1, m_j \lll 1)] = 2^{6 \cdot (-1.4)}$ (th.) / $2^{-9.1}$ (exp.)
- $\Longrightarrow$ distinguish BLAKE2b's permutation in $\approx 2^{-876}$!!
- Not applicable to the compression/hash function

Fixed point partial collision for the compression function chosen IV

- Try to find a valid (iterative) differential pair for a fixed point of **G**
- $\Longrightarrow$ Iterates for free, for any # rounds
- ? Only 2^{64} trials available to find the pair

- Non-trivial fixed-points for **G** : $\approx 2^{64}$, each costs $\approx 2^{25}$ to find
- Search for differential characteristics unsuccessful
- Use rotationals again!
- Total cost of $\approx 2^{61}$ $\Rightarrow$ partial collisions on 304 chosen bits

Impossible differentials for all the BLAKE & BLAKE2

- New prob. 1 differential paths for BLAKE-224/256, BLAKE-384/512, BLAKE2s, BLAKE2b
- 0.5 + 2.5 forward path; 3.5 backward path
- $\Longrightarrow$ 6.5-round miss-in-the-middle ID for all (keyed) permutations
- Improves the best known results on BLAKE

Forward path (BLAKE-224/256 & BLAKE2s)

- Starts with a diff. in the MSB of m_{13} & v_2 @ round 3
- Non-trivial prob. 1 diff. @ round 5.5:

v_0: ????????????????????????????x---
v_3: ????????????????????x----------
v_7: ???x---?????????????????????????
v_{11}: ????????????????????????????x---
v_{12}: ????x---?????????????????????????
v_{15}: --------????????????????????x---

Forward path (BLAKE-224/256 & BLAKE2s)

0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	14	10	4	8	9	15	13	6	1	12	0	2	11	7	5	3
2	11	8	12	0	5	2	15	13	10	14	3	6	7	1	9	4
3	7	9	3	1	13	12	11	14	2	6	5	10	4	0	15	8
4	9	0	5	7	2	4	10	15	14	1	11	12	6	8	3	13
5	2	12	6	10	0	11	8	3	4	13	7	5	15	14	1	9
6	12	5	1	15	14	13	4	10	0	7	6	3	9	2	8	11
7	13	11	7	14	12	1	3	9	5	0	15	4	8	6	2	10
8	6	15	14	9	11	3	0	8	12	2	13	7	1	4	10	5
9	10	2	8	4	7	6	1	5	15	11	9	14	3	12	13	0

Figure : Difference propagation in the forward path
(□ means no diff.; ■ means corrected diff.; ■ means controlled diff.)

Backward path (BLAKE-224/256 & BLAKE2s)

- Starts with @ the inverse of round 8 with:

  v_4 : x---------------0-----------n---
  v_9 : ---n-------x---x-------x-------x
  v_{14} : ----n---n-------n1------n---0---
  v_3 : ----n---n-------00------n-------

- Non-trivial prob. 1 diff. @ round 5.5:

  v_0: ??????????????????????x-------
  v_3: --------??????????????x-------
  v_7: ??????????????????????x-------
  v_{12}: ??????????????????????x-------
  v_{15}: --------------------------------

Backward path (BLAKE-224/256 & BLAKE2s)

0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	14	10	4	8	9	15	13	6	1	12	0	2	11	7	5	3
2	11	8	12	0	5	2	15	13	10	14	3	6	7	1	9	4
3	7	9	3	1	13	12	11	14	2	6	5	10	4	0	15	8
4	9	0	5	7	2	4	10	15	14	1	11	12	6	8	3	13
5	2	12	6	10	0	11	8	3	4	13	7	5	15	14	1	9
6	12	5	1	15	14	13	4	10	0	7	6	3	9	2	8	11
7	13	11	7	14	12	1	3	9	5	0	15	4	8	6	2	10
8	6	15	14	9	11	3	0	8	12	2	13	7	1	4	10	5
9	10	2	8	4	7	6	1	5	15	11	9	14	3	12	13	0

Figure : Difference propagation in the backward path
(□ means no diff.; ■ means corrected diff.; ■ means controlled diff.)

Impossible differentials : last details

- Contradiction between the paths in *e.g.*:

  v_{15}: `--------????????????????????x---` (forward)

  $\neq$

  v_{15}: `----------------------------------` (backward)

- One 0.5-round forward extension using (MSB, 0, MSB, MSB $\oplus$ MSB $\lll 64/32$) $\rightarrow$ (MSB, 0, 0, 0)
- Similar paths for BLAKE-384/512 & BLAKE2b

Differential analysis

- Focus on yet unattacked models: compression & hash function of BLAKE2b
- Builds on previous analysis on BLAKE-256 (Guo & Matusiewicz, 2009), (Dunkelman & Khovratovich, 2011)
- The rotations on BLAKE2b are 'similar' to the ones of BLAKE-256 (all rotations div. by 8 or close to be, 3 out of 4 div. by 16 or close to be)
- BLAKE2b has a bigger state $\Longrightarrow$ lower probs. possible

Differential analysis (cont.)

- Automated search for rotation-friendly characteristics
- With diffs:
  - $\delta = \overline{04}$
  - $2 \times \delta = \overline{08}$
  - $3 \times \delta = \overline{0c}$
- $\Longrightarrow$ characteristic of prob. 2^{-344} on 3-round hash function / 2^{-367} on 4-round compression function
- And:
  - $\nabla = \overline{0004}$
  - $2 \times \nabla = \overline{0008}$
  - $3 \times \nabla = \overline{000c}$
- $\Longrightarrow$ characteristic of prob. 2^{-198} on 2-round hash function / 2^{-336} on 3-round compression function

Conclusion

- Building blocks of BLAKE2 quite more vulnerable than ones of BLAKE (rotational diffs., fixed points, etc.)
- Not so much a concern in practice
- The stronger initialisation makes attacks on the compression & hash function harder

Summary of results

Framework	Type	# Rounds	Complexity
BLAKE2s perm.	imp. diff.	6.5	—
	rotational	7	2^{511}
BLAKE2b perm.	imp. diff.	6.5	—
	rotational	**12**	2^{876}
	differential	5.5	2^{928}
BLAKE2s cf. ch. IV	collision	**10**	2^{64}
BLAKE2b cf. ch. IV	partial collision	**12**	2^{61}
	2^{64} weak preimages	**12**	1
BLAKE2b cf.	differential	4.5	2^{495}
BLAKE2b	differential	3.5	2^{480}