Boomerang attacks on BLAKE-32

Arnab Roy (joint work with Alex Biryukov and Ivica Nikolić)

University of Luxembourg, Luxembourg

February 15, 2011

About BLAKE

- BLAKE is now one of the five finalists in SHA-3 competition anounced by NIST.
- One of the two (Addition-Rotation-Xor)ARX designs in the final round
- It is one of the fastest functions on various platforms in software

Hash function BLAKE-32

Hash function BLAKE-32

- *Initialization*

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

Hash function BLAKE-32

- *Initialization*

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

- Each round is composed of 8 applications of `G` function and
- Compression function iterates a series of 10 rounds

Hash function BLAKE-32

- *Initialization*

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

- Each round is composed of 8 applications of `G` function and
- Compression function iterates a series of 10 rounds
- Each round uses all 16 message words according to permutation table described in the proposal of BLAKE

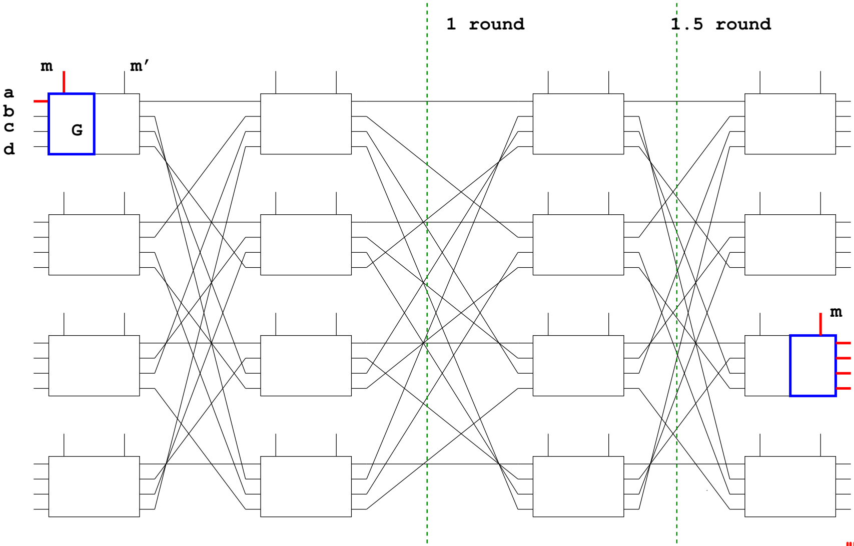
Hash function BLAKE-32

- *Initialization*

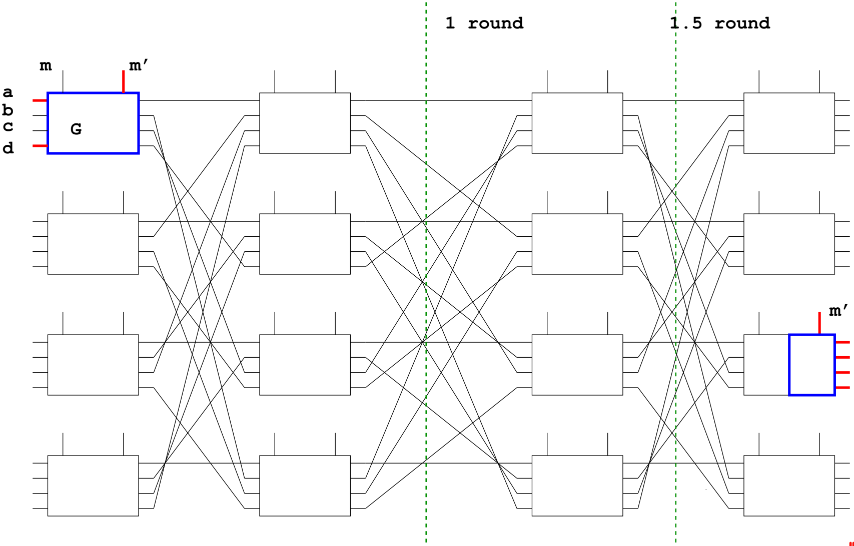
$$\begin{pmatrix} v_0 & v_1 & v_2 & v_3 \\ v_4 & v_5 & v_6 & v_7 \\ v_8 & v_9 & v_{10} & v_{11} \\ v_{12} & v_{13} & v_{14} & v_{15} \end{pmatrix} \leftarrow \begin{pmatrix} h_0 & h_1 & h_2 & h_3 \\ h_4 & h_5 & h_6 & h_7 \\ s_0 \oplus c_0 & s_1 \oplus c_1 & s_2 \oplus c_2 & s_3 \oplus c_3 \\ t_0 \oplus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

- Each round is composed of 8 applications of `G` function and
- Compression function iterates a series of 10 rounds
- Each round uses all 16 message words according to permutation table described in the proposal of BLAKE
- *Finalization* procedure is linear

High probability differential trail



High probability differential trail



High probability differential trails

- We obtain a 2-round differential trail with probability 2^{-1} with active MSB
- 3-round differential trail with probability 2^{-s} where $s = 6, 7, 8$
- 3.5-round differential trail with probability $\geq 2^{-32}$

High probability differential trails

- We obtain a 2-round differential trail with probability 2^{-1} with active MSB
- 3-round differential trail with probability 2^{-s} where $s = 6, 7, 8$
- 3.5-round differential trail with probability $\geq 2^{-32}$
- 2-round differential trail with probability $2^{-(3t-1)}$ or 2^{-3t}or $2^{-(3t+1)}$ where t is number of active bits (excluding MSB)

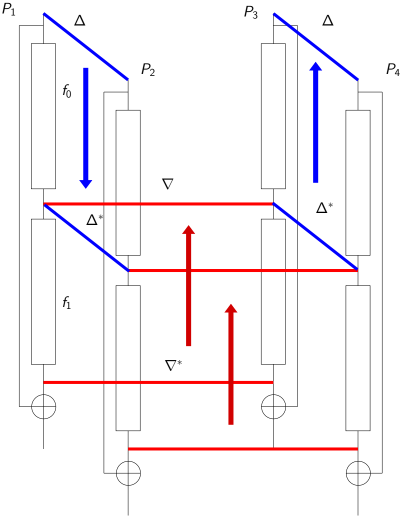
High probability differential trails

- We obtain a 2-round differential trail with probability 2^{-1} with active MSB
- 3-round differential trail with probability 2^{-s} where $s = 6, 7, 8$
- 3.5-round differential trail with probability $\geq 2^{-32}$
- 2-round differential trail with probability $2^{-(3t-1)}$ or 2^{-3t}or $2^{-(3t+1)}$ where t is number of active bits (excluding MSB)
- 3-round differential trail consistent with the counters t_0, t_1 which has probability 2^{-21}

High probability differential trails

- We obtain a 2-round differential trail with probability 2^{-1} with active MSB
- 3-round differential trail with probability 2^{-s} where $s = 6, 7, 8$
- 3.5-round differential trail with probability $\geq 2^{-32}$
- 2-round differential trail with probability $2^{-(3t-1)}$ or 2^{-3t}or $2^{-(3t+1)}$ where t is number of active bits (excluding MSB)
- 3-round differential trail consistent with the counters t_0, t_1 which has probability 2^{-21}
- 2-round differential trail with ith and $(i+16)$th bit active with probability 2^{-9}(when ith bit is MSB) otherwise probability is $\geq 2^{-14}$

Boomerang attack on Compression Function



$Pr[\Delta \to \Delta^*] = p$

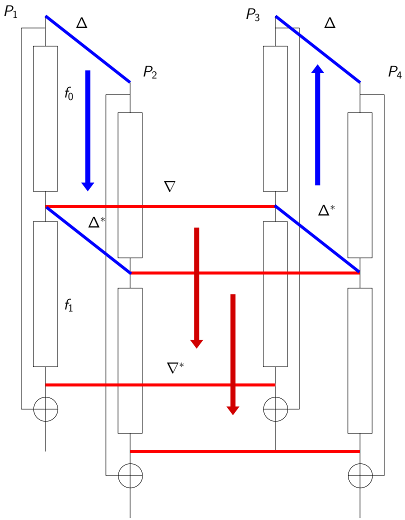
$Pr[\nabla \to \nabla^*] = q$

$f = f_1 \circ f_0$

$f(P_1) \oplus f(P_3) = \nabla^*$

$f(P_2) \oplus f(P_4) = \nabla^*$

Boomerang attack on Compression Function



$Pr[\Delta \to \Delta^*] = p$

$Pr[\nabla \to \nabla^*] = q$

$f = f_1 \circ f_0$

$f(P_1) \oplus f(P_3) = \nabla^*$

$f(P_2) \oplus f(P_4) = \nabla^*$

Boomerang distinguisher

- Let $F(H) = f(H) \oplus H$ where $f = f_1 \circ f_0$.

Boomerang distinguisher

- Let $F(H) = f(H) \oplus H$ where $f = f_1 \circ f_0$.
- For the boomerang quartet (P_1, P_2, P_3, P_4) we obtain:

$$P_1 \oplus P_2 = \Delta, \tag{1}$$

$$P_3 \oplus P_4 = \Delta, \tag{2}$$

$$[F(P_1) \oplus P_1] \oplus [F(P_3) \oplus P_3] = \nabla^*, \tag{3}$$

$$[F(P_2) \oplus P_2] \oplus [F(P_4) \oplus P_4] = \nabla^* \tag{4}$$

Boomerang distinguisher

- Let $F(H) = f(H) \oplus H$ where $f = f_1 \circ f_0$.
- For the boomerang quartet (P_1, P_2, P_3, P_4) we obtain:

$$P_1 \oplus P_2 = \Delta, \tag{1}$$

$$P_3 \oplus P_4 = \Delta, \tag{2}$$

$$[F(P_1) \oplus P_1] \oplus [F(P_3) \oplus P_3] = \nabla^*, \tag{3}$$

$$[F(P_2) \oplus P_2] \oplus [F(P_4) \oplus P_4] = \nabla^* \tag{4}$$

- For a random n-bit compression function finding such quartet will have complexity 2^n(with a fixed difference)

Boomerang distinguisher

- Let $F(H) = f(H) \oplus H$ where $f = f_1 \circ f_0$.
- For the boomerang quartet (P_1, P_2, P_3, P_4) we obtain:

$$P_1 \oplus P_2 = \Delta, \tag{1}$$

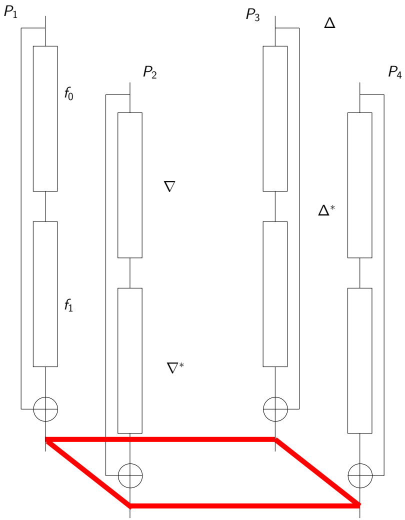
$$P_3 \oplus P_4 = \Delta, \tag{2}$$

$$[F(P_1) \oplus P_1] \oplus [F(P_3) \oplus P_3] = \nabla^*, \tag{3}$$

$$[F(P_2) \oplus P_2] \oplus [F(P_4) \oplus P_4] = \nabla^* \tag{4}$$

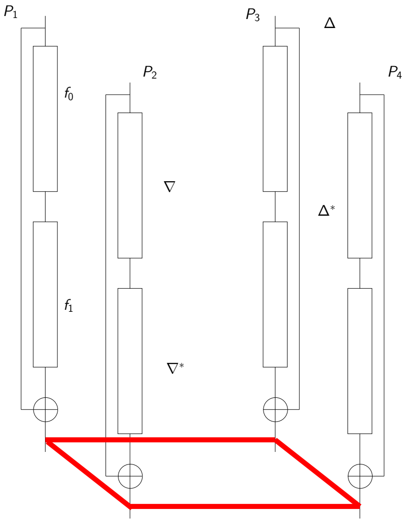
- For a random n-bit compression function finding such quartet will have complexity 2^n(with a fixed difference)
- To get a boomerang distinguisher for compression function F we need $p^2q^2 > 2^{-n}$

Zero-sum distinguisher



- From the last equations we get: $F(P_1) \oplus F(P_2) \oplus F(P_3) \oplus F(P_4) = 0$

Zero-sum distinguisher



- From the last equations we get: $F(P_1) \oplus F(P_2) \oplus F(P_3) \oplus F(P_4) = 0$
- For a random permutation complexity is $2^{n/4}$. But with fixed difference the complexity rises to $2^{n/2}$

Boomerang attack on BLAKE-32

- The real probability of the Boomerang is $\hat{p}^2\hat{q}^2$, where $\hat{p}, \hat{q}$ are the amplified probability defined as:
  $\hat{p} = \sqrt{\sum_{\Delta^*} Pr[\Delta \to \Delta^*]^2}$, $\hat{q} = \sqrt{\sum_{\nabla} Pr[\nabla \to \nabla^*]^2}$

- The real probability of the Boomerang is $\hat{p}^2\hat{q}^2$, where $\hat{p}, \hat{q}$ are the amplified probability defined as:
  $\hat{p} = \sqrt{\sum_{\Delta^*} Pr[\Delta \rightarrow \Delta^*]^2}$, $\hat{q} = \sqrt{\sum_{\nabla} Pr[\nabla \rightarrow \nabla^*]^2}$
- But getting these probabilities is hard in some cases. So we run computer simulation

Boomerang attack on BLAKE-32

- The real probability of the Boomerang is $\hat{p}^2\hat{q}^2$, where $\hat{p}, \hat{q}$ are the amplified probability defined as:
  $\hat{p} = \sqrt{\sum_{\Delta^*} Pr[\Delta \to \Delta^*]^2}$, $\hat{q} = \sqrt{\sum_{\nabla} Pr[\nabla \to \nabla^*]^2}$
- But getting these probabilities is hard in some cases. So we run computer simulation
- For the attack on Hash function, the returned pairs are consistent if $v_{12} \oplus v_{13}$ and $v_{14} \oplus v_{15}$ are fixed. This increases the complexity of the attack by a factor of 2^{64}

Summary of our attack

CF/KP[1]	Rounds	CF/KP calls
CF	4	2^{67}
CF	5	$2^{71.2}$
CF	6	2^{102}
CF	6.5	2^{184}
CF	7	2^{232}
KP	4	2^{3}
KP	5	$2^{7.2}$
KP	6	$2^{11.75}$
KP	7	2^{122}
KP	8	2^{242}

[1] CF = Compression Function, KP = Keyed Permutation

Conclusion

- Application of the concept of boomerang distinguisher to compression function
- Shown such distinguisher for CF of BLAKE-32
- Classical boomerang distinguisher for KP of BLAKE-32
- Attack works for 2/3 of the total number of rounds of the CF and 4/5 of the total number of rounds of the KP
- The attack can be equally applied to other versions of BLAKE
- BLAKE-32 has been tweaked to 15 rounds in the final round

THANK YOU!