

Toy versions of BLAKE

Jean-Philippe Aumasson Luca Henzen Willi Meier Raphael C.-W. Phan

To encourage analysis of BLAKE, we describe four variants that should be considered as toy versions, on which we make no security claims.

Below we describe the difference(s) of those variants with the original BLAKE. Reduced-round versions may be considered as well.

BLOKE

Permutations $\sigma_0, \dots, \sigma_9$ are Only the identity.

FLAKE

The compression function makes no Feedforward, so the finalization of FLAKE-32 is just

$$\begin{aligned}h'_0 &\leftarrow v_0 \oplus v_8 \\h'_1 &\leftarrow v_1 \oplus v_9 \\h'_2 &\leftarrow v_2 \oplus v_{10} \\h'_3 &\leftarrow v_3 \oplus v_{11} \\h'_4 &\leftarrow v_4 \oplus v_{12} \\h'_5 &\leftarrow v_5 \oplus v_{13} \\h'_6 &\leftarrow v_6 \oplus v_{14} \\h'_7 &\leftarrow v_7 \oplus v_{15}\end{aligned}$$

BLAZE

Constants are Zeroed in the G_i function. So in BLAZE-32, at round r , G_i computes

$$\begin{aligned}a &\leftarrow a + b + m_{\sigma_r(2i)} \\d &\leftarrow (d \oplus a) \ggg 16 \\c &\leftarrow c + d \\b &\leftarrow (b \oplus c) \ggg 12 \\a &\leftarrow a + b + m_{\sigma_r(2i+1)} \\d &\leftarrow (d \oplus a) \ggg 8 \\c &\leftarrow c + d \\b &\leftarrow (b \oplus c) \ggg 7\end{aligned}$$

BRAKE

All the three above changes, so this variant may be easy to break.