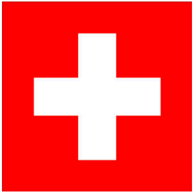
BLAKE

status quo



BLAKE-32

32-bit words, 32-byte digests

64-bit CPU

7.77 cycles/byte on a Core 2 Quad (berlekamp)
15.25 cycles/byte on an AMD Phenom (ranger)
6.97 cycles/byte on a Core 2 Duo (matsui)

32-bit CPU

8.12 cycles/byte on a Core 2 Quad (berlekamp)
16.77 cycles/byte on an AMD Phenom (ranger)
23.23 cycles/byte on a Pentium 3 (manneke)

BLAKE-64

64-bit words, 64-byte digests

64-bit CPU

9.46 cycles/byte on a Core 2 Quad (berlekamp)
11.10 cycles/byte on an AMD Phenom (ranger)
9.61 cycles/byte on a Core 2 Duo (matsui)

32-bit CPU

14.29 cycles/byte on a Core 2 Quad (berlekamp)
24.28 cycles/byte on an AMD Phenom (ranger)
64.43 cycles/byte on a Pentium 3 (manneke)

BLAKE-32

32-bit words, 32-byte digests

ASIC

13.6 kGE 135 Mbps in 180 nm (Henzen et al.)
38.0 kGE 15 Gbps in 90 nm (Henzen et al.)

FPGA

56 slices 225 Mbps in Virtex 5 (Beuchat et al.)
124 slices 216 Mbps in Virtex 4 (Beuchat et al.)
124 slices 115 Mbps in Spartan 3 (Beuchat et al.)

BLAKE-64

64-bit words, 64-byte digests

ASIC

20.6 kGE 181 Mbps in 180 nm (Henzen et al.)
79.0 kGE 19 Gbps in 90 nm (Henzen et al.)

FPGA

108 slices 314 Mbps in Virtex 5 (Beuchat et al.)
230 slices 219 Mbps in Virtex 4 (Beuchat et al.)
229 slices 138 Mbps in Spartan 3 (Beuchat et al.)

Thomas Pornin `(plain C code)`
Chris Drost `(Javascript code)`
Samuel Neves `(SSSE3 C code)`
Peter Schwabe `(SSE2 C code)`
Daniel Otte `(AVR benchmarks)`
eBASH `(benchmarks)`

Jean-Luc Beuchat et al. `(FPGA impl.)`
Kazuyuki Kobayashi et al. `(SASEBO FPGA impl.)`
Stefan Tillich et al. `(ASIC impl.)`
A. H. Namin, M. A. Hasan `(FPGA evaluation)`
Integrated Systems Laboratory of the ETH Zurich

Best attacks on BLAKE-32
(out of 10 rounds)

Preimages on **2.5** rounds (2^{241})
(Li, Xu, IACR ePrint 2009/238)

Impossible differential on **5** rounds
of the internal permutation
(Aumasson et al., FSE 2010)

Nearly near collisions on **4** rounds
of the compression function (2^{21})
(Su et al., IACR ePrint 2010/355)

Best attacks on BLAKE-64 (out of 14 rounds)

Preimages on **2.5** rounds (2^{481})
(Li, Xu, IACR ePrint 2009/238)

Impossible differential on **6** rounds
of the internal permutation
(Aumasson et al., FSE 2010)

Nearly near collisions on **5** rounds
of the compression function (2^{216})
(Su et al., IACR ePrint 2010/355)

Best attacks on the toy versions

Collisions for BLOKE (only identity permutations) and for the compression function of BRAKE (Vidali, Nose, Pasalic, Inf. Proc. Let., 2010)

How to break FLAKE (no feedforward)?

How to break BLAZE (zero constants)?

How to break BRAKE (all 3 tweaks)?

Not an attack: rotational cryptanalysis

$$(x + y) \ggg n \approx (x \ggg n) + (y \ggg n)$$

`Applied to (reduced) BMW, SIMD, Skein, Shabal`

`Ineffective against BLAKE`

`BLAKE's constants break bit symmetries`

$$(x+(y\oplus\texttt{243F6A88})) \ggg n \neq (x \ggg n)+((y \ggg n)\oplus\texttt{243F6A88})$$

Other attacks tried on BLAKE

`My-pipe-is-bigger-than-yours cryptanalysis`

`Related-definition cryptanalysis`

`Related-rules cryptanalysis`

Other attacks tried on BLAKE

`My-pipe-is-bigger-than-yours cryptanalysis`

`Related-definition cryptanalysis`

`Related-rules cryptanalysis`

More seriously…

Why BLAKE as SHA-3?

Fastest hash with unattacked compression (SW)

Plain C implementation almost as fast as SSE$\star$

Simple speed/area tradeoffs in HW

Very easy to implement

Resistant to new attacks
(rebound, zero-sum, rotational)

Confidence-inspiring design
(no ‘‘banana’’)

BLAKE

status quo