

Template:Comparison of SHA functions

Comparison of SHA functions

Algorithm and variant		Output size (bits)	Internal state size (bits)	Block size (bits)	Rounds	Operations	Security (in bits) against collision attacks	Capacity against length extension attacks	Performance on Skylake (median cpb) ^[1]		First Published					
									long messages	8 bytes						
MD5 (as reference)		128	128 (4 × 32)	512	64	And, Xor, Rot, Add (mod 2 ³²), Or	≤18 (collisions found) ^[2]	0	4.99	55.00	1992					
SHA-0		160	160 (5 × 32)	512	80	And, Xor, Rot, Add (mod 2 ³²), Or	<34 (collisions found)	0	≈ SHA-1	≈ SHA-1	1993					
SHA-1									3.47	52.00	1995					
SHA-2	<i>SHA-224</i> <i>SHA-256</i>	224 256	256 (8 × 32)	512	64	And, Xor, Rot, Add (mod 2 ³²), Or, Shr	112 128	32 0	7.62 7.63	84.50 85.25	2004 2001					
	<i>SHA-384</i> <i>SHA-512</i>	384 512					512 (8 × 64)		1024	80	And, Xor, Rot, Add (mod 2 ⁶⁴), Or, Shr	192 256	128 (≤ 384) 0	5.12 5.06	135.75 135.50	2001
	<i>SHA-512/224</i> <i>SHA-512/256</i>	224 256										112 128	288 256	≈ SHA-384	≈ SHA-384	2012
SHA-3	<i>SHA3-224</i> <i>SHA3-256</i> <i>SHA3-384</i> <i>SHA3-512</i>	224 256 384 512	1600 (5 × 5 × 64)	1152 1088 832 576	24 ^[4]	And, Xor, Rot, Not	112 128 192 256	448 512 768 1024	8.12 8.59 11.06 15.88	154.25 155.50 164.00 164.00	2015					
	<i>SHAKE128</i> <i>SHAKE256</i>	<i>d</i> (arbitrary) <i>d</i> (arbitrary)					1344 1088	min(<i>d</i> /2, 128) min(<i>d</i> /2, 256)	256 512	7.08 8.59		155.25 155.50				

References

These references will appear in the article, but this list appears only on this page.

- "Measurements table" (<http://bench.cryp.to/results-hash.html#amd64-skylake>). *bench.cryp.to*.
- Xie Tao; Fanbao Liu & Dengguo Feng (2013) "Fast Collision Attack on MD5" (<https://eprint.iacr.org/2013/170.pdf>) (PDF).
- "Announcing the first SHA1 collision" (<https://securitygoogleblog.com/2017/02/announcing-first-sha1-collision.html>) Retrieved 2017-02-23.
- "The Keccak sponge function family" (http://keccak.noekeon.org/specs_summary.html). Retrieved 2016-01-27.

Retrieved from https://en.wikipedia.org/w/index.php?title=Template:Comparison_of_SHA_functions&oldid=858510526

This page was last edited on 7 September 2018, at 18:04 (UTC).

Text is available under the [Creative Commons Attribution-ShareAlike License](#); additional terms may apply. By using this site, you agree to the [Terms of Use](#) and [Privacy Policy](#). Wikipedia® is a registered trademark of the [Wikimedia Foundation, Inc.](#), a non-profit organization.