

[article](#) [discussion](#) [edit this page](#) [history](#)



WIKIPEDIA
The Free Encyclopedia

navigation

- [Main page](#)
- [Contents](#)
- [Featured content](#)
- [Current events](#)
- [Random article](#)

search

interaction

- [About Wikipedia](#)
- [Community portal](#)
- [Recent changes](#)
- [Contact Wikipedia](#)
- [Donate to Wikipedia](#)
- [Help](#)

toolbox

- [What links here](#)
- [Related changes](#)
- [Upload file](#)
- [Special pages](#)
- [Printable version](#)
- [Permanent link](#)
- [Cite this page](#)

languages

- [Français](#)
- [Simple English](#)
- [Русский](#)

Avalanche effect

From Wikipedia, the free encyclopedia



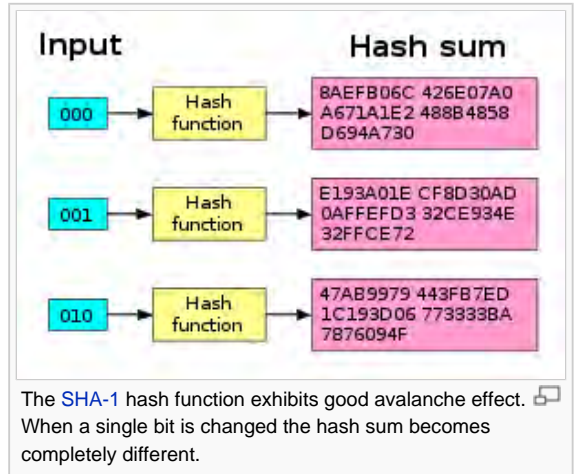
This article includes a [list of references](#), related reading or [external links](#), but **its sources remain unclear because it lacks inline citations**. Please [improve](#) this article by introducing more precise citations [where appropriate](#). *(July 2009)*

This article is about [cryptography](#); for other meanings, see [snowball effect](#) and [avalanche \(disambiguation\)](#).

In [cryptography](#), the **avalanche effect** refers to a desirable property of cryptographic [algorithms](#), typically [block ciphers](#) and [cryptographic hash functions](#). The avalanche effect is evident if, when an input is changed slightly (for example, flipping a single bit) the output changes significantly (e.g., half the output bits flip). In the case of quality block ciphers, such a small change in either the [key](#) or the [plaintext](#) should cause a drastic change in the [ciphertext](#). The actual term was first used by [Horst Feistel](#),^[1] although the concept dates back to at least [Shannon's diffusion](#).

If a block cipher or cryptographic hash function does not exhibit the avalanche effect to a significant degree, then it has poor randomization, and thus a [cryptanalyst](#) can make predictions about the input, being given only the output. This may be sufficient to partially or completely break the algorithm. Thus, the avalanche effect is a desirable condition from the point of view of the designer of the cryptographic algorithm or device.

Constructing a cipher or hash to exhibit a substantial avalanche effect is one of the primary design objectives. This is why most block ciphers are [product ciphers](#). It is also why hash functions have large data blocks. Both of these features allow small changes to propagate rapidly through iterations of the algorithm, such that every [bit](#) of the output should depend on every bit of the input before the algorithm terminates.



Contents

- 1 [Strict avalanche criterion](#)
- 2 [Bit independence criterion](#)
- 3 [See also](#)
- 4 [References](#)

Strict avalanche criterion

[\[edit\]](#)

The **strict avalanche criterion (SAC)** is a generalization of the avalanche effect. It is satisfied if, whenever a single input bit is [complemented](#), each of the output bits changes with a probability of one half. The SAC builds on the concepts of [completeness](#) and avalanche and was introduced by Webster and Tavares in 1985.^[2]

[\[edit\]](#)

Bit independence criterion

The **bit independence criterion (BIC)** states that output bits *j* and *k* should change independently when any single input bit *i* is inverted, for all *i*, *j* and *k*.

See also

[\[edit\]](#)

- [Confusion and diffusion](#)

References

[\[edit\]](#)

- ↑ Horst Feistel, "Cryptography and Computer Privacy." *Scientific American*, Vol. 228, No. 5, 1973. (JPEG format scanned)
- ↑ A. F. Webster and [Stafford E. Tavares](#), "On the design of S-boxes", *Advances in Cryptology - Crypto '85* (Lecture Notes in Computer Science), vol. 219, pp. 523-534, 1985.

v d e	Block ciphers (security summary)
Common algorithms	AES · Blowfish · DES · Triple DES · Serpent · Twofish
Less common algorithms	CAST-128 · IDEA · RC2 · RC5 · SEED · Skipjack · TEA · XTEA
Other algorithms	3-Way · ABC · Akelarre · Anubis · ARIA · BaseKing · BassOmatic · BATON · BEAR and LION · Camellia · CAST-256 · CIKS-1 · CIPHERUNICORN-A · CIPHERUNICORN-E · CLEFIA · CMEA · Cobra · COCONUT98 · Crab · Cryptomeria/C2 · CRYPTON · CS-Cipher · DEAL · DES-X · DFC · E2 · FEAL · FEA-M · FROG · G-DES · GOST · Grand Cru · Hasty Pudding cipher · Hierocrypt · ICE · IDEA NXT · Intel Cascade Cipher · Iraqi · KASUMI · KeeLoq · KHAZAD · Khufu and Khafre · KN-Cipher · Ladder-DES · Libelle · LOKI97 · LOKI89/91 · Lucifer · M6 · M8 · MacGuffin · Madryga · MAGENTA · MARS · Mercy · MESH · MISTY1 · MMB · MULTI2 · MultiSwap · New Data Seal · NewDES · Nimbus · NOEKEON · NUSH · Q · RC6 · REDOC · Red Pike · S-1 · SAFER · SAVILLE · SC2000 · SHACAL · SHARK · SMS4 · Spectr-H64 · Square · SXAL/MBAL · Threefish · Treyfer · UES · Xenon · xmx · XXTEA · Zodiac
Design	Feistel network · Key schedule · Product cipher · S-box · P-box · SPN
Attack (Cryptanalysis)	Brute force · Linear · Differential (Impossible · Truncated) · Integral · Boomerang · Mod <i>n</i> · Related-key · Slide · Rotational · Timing · XSL
Standardization	AES process · CRYPTREC · NESSIE
Misc	Avalanche effect · Block size · IV · Key size · Modes of operation · Piling-up lemma · Weak key · EFF DES cracker · Key whitening
v d e	Cryptographic hash functions and message authentication codes (MACs)
Widely used functions: MD5 SHA-1 SHA-2	Other: FSB ECOH GOST HAS-160 HAVAL LM hash MDC-2 MD2 MD4 N-Hash RadioGatún RIPEMD Snefru SWIFFT Tiger VSH WHIRLPOOL crypt(3) DES
SHA-3 candidates: BLAKE Blue Midnight Wish CubeHash ECHO Fugue Grøstl Hamsi JH Keccak Luffa SHAvite-3 SIMD Shabal Skein	
MAC algorithms: DAA CBC-MAC HMAC OMAC/CMAC PMAC UMAC Poly1305-AES	
Authenticated encryption modes: CCM CWC EAX GCM OCB	
Attacks: Collision attack Birthday attack Preimage attack Rainbow table Side channel attack Brute force attack	
Misc: Avalanche effect Hash collision Merkle-Damgård construction	Standardization: CRYPTREC NESSIE NIST hash function competition
v d e	Cryptography
	History of cryptography · Cryptanalysis · Cryptography portal · Outline of cryptography
	Symmetric-key algorithm · Block cipher · Stream cipher · Public-key cryptography · Cryptographic hash function ·

[Message authentication code](#) · [Random numbers](#) · [Steganography](#)

Categories: [Cryptography](#)



This page was last modified on 5 April 2010 at 20:31.



Text is available under the [Creative Commons Attribution-ShareAlike License](#); additional terms may apply. See [Terms of Use](#) for details.

Wikipedia® is a registered trademark of the [Wikimedia Foundation, Inc.](#), a non-profit organization.

[Contact us](#) [Privacy policy](#) [About Wikipedia](#) [Disclaimers](#)