Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export
Create a book
Download as PDF
Printable version

Languages
Català
Čeština
Deutsch
Español
فارسی
Français
Bahasa Indonesia
Italiano
עברית
Nederlands
日本語
Polski
Русский
Simple English
Suomi
Svenska
Тоҷикӣ
Українська
中文
Edit links

Twofish

From Wikipedia, the free encyclopedia

In cryptography, **Twofish** is a symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits. It was one of the five finalists of the Advanced Encryption Standard contest, but it was not selected for standardization. Twofish is related to the earlier block cipher Blowfish.

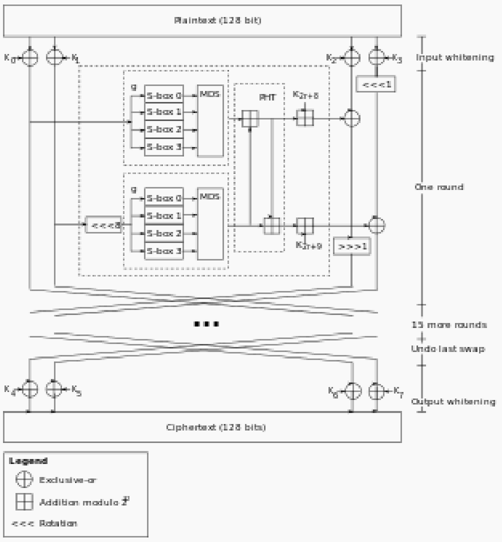
Twofish's distinctive features are the use of pre-computed key-dependent S-boxes, and a relatively complex key schedule. One half of an n-bit key is used as the actual encryption key and the other half of the n-bit key is used to modify the encryption algorithm (key-dependent S-boxes). Twofish borrows some elements from other designs; for example, the pseudo-Hadamard transform (PHT) from the SAFER family of ciphers. Twofish has a Feistel structure like DES.

On most software platforms Twofish was slightly slower than Rijndael (the chosen algorithm for Advanced Encryption Standard) for 128-bit keys, but it is somewhat faster for 256-bit keys.[3]

Twofish was designed by Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson; the "extended Twofish team" who met to perform further cryptanalysis of Twofish and other AES contest entrants included Stefan Lucks, Tadayoshi Kohno, and Mike Stay.

The Twofish cipher has not been patented and the reference implementation has been placed in the public domain. As a result, the Twofish algorithm is free for anyone to use without any restrictions whatsoever. It is one of a few ciphers included in the OpenPGP standard (RFC 4880). However, Twofish has seen less widespread usage than Blowfish, which has been available longer.

Twofish



The Twofish algorithm

General	
Designers	Bruce Schneier
First published	1998
Derived from	Blowfish, SAFER, Square
Related to	Threefish
Certification	AES finalist
Cipher detail	
Key sizes	128, 192 or 256 bits
Block sizes	128 bits
Structure	Feistel network
Rounds	16
Best public cryptanalysis	

Truncated differential cryptanalysis requiring roughly 2^{51} chosen plaintexts.[1]
Impossible differential attack that breaks 6 rounds out of 16 of the 256-bit key version using 2^{256} steps.[2]

Contents [hide]

Cryptanalysis [edit]

In 1999, Niels Ferguson published an impossible differential attack that breaks six rounds out of 16 of the 256-bit key version using 2^{256} steps.[2]

As of 2000, the best published cryptanalysis on the Twofish block cipher is a truncated differential cryptanalysis of the full 16-round version. The paper claims that the probability of truncated differentials is $2^{-57.3}$ per block and that it will take roughly 2^{51} chosen plaintexts (32 petabytes worth of data) to find a good pair of truncated differentials.[1]

Bruce Schneier responds in a 2005 blog entry that this paper does not present a full cryptanalytic attack, but only some hypothesized differential characteristics: "But even from a theoretical perspective, Twofish isn't even remotely broken. There have been no extensions to these results since they were published in 2000."[4]

See also [edit]

- Threefish
- Advanced Encryption Standard
- Data Encryption Standard

References [edit]

1. ^ a b Shiho Moriai, Yiqun Lisa Yin (2000). "Cryptanalysis of Twofish (II)" (PDF). Retrieved 2013-01-14.
2. ^ a b Niels Ferguson (1999-10-05). "Impossible differentials in Twofish" (PDF). Retrieved 2013-01-14.
3. ^ After Rijndael was chosen as the Advanced Encryption Standard, Twofish has become much slower than Rijndael on the CPUs that support the AES instruction set. Bruce Schneier, Doug Whiting (2000-04-07). "A Performance Comparison of the Five AES Finalists" (PDF/PostScript). Retrieved 2013-01-14.
4. ^ Schneier, Bruce (2005-11-23). "Twofish Cryptanalysis Rumors". Schneier on Security blog. Retrieved 2013-01-14.

Articles [edit]

- Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson (1998-06-15). "The Twofish Encryption Algorithm" (PDF/PostScript). Retrieved 2013-01-14.
- Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson (1999-03-22). *The Twofish Encryption Algorithm: A 128-Bit Block Cipher*. New York City: John Wiley & Sons. ISBN 0-471-35381-7.

External links [edit]

- Twofish web page, with full specifications, free source code, and other Twofish resources by Bruce Schneier
- 256bit Ciphers - TWOFISH Reference implementation and derived code
- Products that Use Twofish by Bruce Schneier
- Better algorithm: Rijndael or TwoFish? by sci.crypt
- Standard Cryptographic Algorithm Naming: Twofish

v · t · e	**Block ciphers (security summary)**
Common algorithms	AES · Blowfish · DES (Internal Mechanics, Triple DES) · Serpent · **Twofish**
Less common algorithms	Camellia · CAST-128 · IDEA · RC2 · RC5 · SEED · ARIA · Skipjack · TEA · XTEA
Other algorithms	3-Way · Akelarre · Anubis · BaseKing · BassOmatic · BATON · BEAR and LION · CAST-256 · Chiasmus · 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 · LOKI (97, 89/91) · Lucifer · M6 · M8 · MacGuffin · Madryga · MAGENTA · MARS · Mercy · MESH · MISTY1 · MMB · MULTI2 · MultiSwap · New Data Seal · NewDES · Nimbus · NOEKEON · NUSH · PRESENT · Q · RC6 · REDOC · Red Pike · S-1 · SAFER · SAVILLE · SC2000 · SHACAL · SHARK · Simon · SMS4 · Speck · Spectr-H64 · Square · SXAL/MBAL · Threefish · Treyfer · UES · Xenon · xmx · XXTEA · Zodiac
Design	Feistel network · Key schedule · Lai-Massey scheme · Product cipher · S-box · P-box · SPN · Avalanche effect · Block size · Key size · Key whitening (Whitening transformation)
Attack (cryptanalysis)	Brute-force (EFF DES cracker) · MITM (Biclique attack, 3-subset MITM attack) · Linear (Piling-up lemma) · Differential (Impossible · Truncated · Higher-order) · Differential-linear · Integral/Square · Boomerang · Mod *n* · Related-key · Slide · Rotational · Timing · XSL · Interpolation · Partitioning · Davies' · Rebound · Weak key · Tau · Chi-square · Time/memory/data tradeoff
Standardization	AES process · CRYPTREC · NESSIE
Utilization	Initialization vector · Mode of operation · Padding
v · t · 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: Block ciphers | Feistel ciphers | Free ciphers