Threefish

From Wikipedia, the free encyclopedia

This article **relies too much on references to primary sources**. Please improve this article by adding secondary or tertiary sources. *(November 2008)*

Threefish is a symmetric-key tweakable block cipher designed as part of the Skein hash function, an entry in the NIST hash function competition. Threefish uses no S-boxes or other table lookups in order to avoid cache timing attacks;[1] its nonlinearity comes from alternating additions with exclusive ORs. In that respect, it is similar to Salsa20, TEA, and the SHA-3 candidates CubeHash and BLAKE.

Threefish and the Skein hash function were designed by Bruce Schneier, Niels Ferguson, Stefan Lucks, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas, and Jesse Walker.

Threefish

General	
Designers	Bruce Schneier, Niels Ferguson, Stefan Lucks, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas, Jesse Walker
First published	2008
Related to	Blowfish, Twofish
Cipher detail	
Key sizes	256, 512 or 1024 bits (key size is equal to block size)
Block sizes	256, 512 or 1024 bits
Rounds	72 (80 for 1024-bit block size)
Speed	6.1 cpb on Core 2.[1]

Contents [hide]

Description of the cipher[1] [edit]

At first the block, the tweak and the key (of length 256, 512 or 1024 bits) is converted into N_w words of 64 bit length each. These words are treated as 64bit unsigned Little endian integers throughout the cipher. All additions and subtractions are defined modulo 2^{64}

Key schedule [edit]

Threefish uses $\frac{N_r}{4}+1$ different round keys (N_r: Number of rounds). To calculate these keys the original key words $k_0, k_1, \ldots, k_{N_w-1}$ are appended by an additional key word k_{N_w}. The tweak words t_0, t_1 are appended with an additional tweak word too.

$$t_2 = t_0 \oplus t_1$$

$$k_{N_w} = C_{240} \oplus k_0 \oplus k_1 \oplus \ldots \oplus k_{N_w-1}$$

$$C_{240} = \mathrm{0x1BD11BDAA9FC1A22}$$

The round key words $k_{s,i}$ are now defined like this:

$$k_{s,i} = \begin{cases} k_{(s+i) \bmod (N_w+1)} & i = 0, \ldots, N_w-4 \\ k_{(s+i) \bmod (N_w+1)} + t_{s \bmod 3} & i = N_w-3 \\ k_{(s+i) \bmod (N_w+1)} + t_{(s+1) \bmod 3} & i = N_w-2 \\ k_{(s+i) \bmod (N_w+1)} + s & i = N_w-1 \end{cases}$$

Mix function [edit]

The mix function takes a tuple of words (x_0, x_1) and returns another tuple of words (y_0, y_1). The function is

defined like this:

$$y_0 = x_0 + x_1 \mod 2^{64}$$
$$y_1 = (y_1 \lll R_{(d \bmod 8),j}) \oplus y_0$$

$R_{d,j}$ is a fixed set of rotation constants chosen to achieve maximum diffusion.

A full Threefish round [edit]

If $d \bmod 4 == 0$ the round key $k_{\frac{d}{4}}$ is added to the words. Afterwards the mix function is applied to consecutive words and the resulting words are permutated using a fixed permutation.

Threefish256 and Threefish512 apply this round 72 times. Threefish1024 applies it 80 times.

Final operations [edit]

After all rounds are applied the last round key is added to the words and the words are converted back to a string of bytes.

Security [edit]

In October 2010, an attack that combines rotational cryptanalysis with the rebound attack was published. The attack mounts a known-key distinguisher against 53 of 72 rounds in Threefish-256, and 57 of 72 rounds in Threefish-512. It also affects the Skein hash function.[2] This is a follow-up to the earlier attack published in February, which breaks 39 and 42 rounds respectively.[3] In response to this attack, the Skein team tweaked the rotation constants used in Threefish and thereby the key schedule constants for round 3 of the NIST hash function competition.[1]

In 2009, a related key boomerang attack against a reduced round Threefish version was published. For the 32-round version, the time complexity is 2^{226} and the memory complexity is 2^{12}; for the 33-round version, the time complexity is $2^{352.17}$ with a negligible memory usage. The attacks also work against the tweaked version of Threefish: for the 32-round version, the time complexity is 2^{222} and the memory complexity is 2^{12}; for the 33-round version, the time complexity is $2^{355.5}$ with a negligible memory usage.[4]

See also [edit]

- Twofish
- Blowfish (cipher)

References [edit]

1. ^ [a] [b] [c] [d] Ferguson et al. (2010-10-01). "The Skein Hash Function Family" (PDF). The paper in which Threefish was introduced.
2. ^ Dmitry Khovratovich, Ivica Nikolic, Christian Rechberger (2010-10-20). "Rotational Rebound Attacks on Reduced Skein".
3. ^ Dmitry Khovratovich and Ivica Nikolić (2010). "Rotational Cryptanalysis of ARX" (PDF). University of Luxembourg.
4. ^ Jiazhe Chen; Keting Jia (2009-11-01). "Improved Related-key Boomerang Attacks on Round-Reduced Threefish-512".

External links [edit]

- "The Skein Hash Function Family" Homepage of the Skein Hash Function Family.

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 | Free ciphers