Whirlpool (cryptography)

From Wikipedia, the free encyclopedia
(Redirected from WHIRLPOOL)

This article is about the hash function. For other uses, see Whirlpool (disambiguation).

In computer science and cryptography, **Whirlpool** (sometimes styled **WHIRLPOOL**) is a cryptographic hash function. It was designed by Vincent Rijmen (co-creator of the Advanced Encryption Standard) and Paulo S. L. M. Barreto, who first described it in 2000. The hash has been recommended by the NESSIE project. It has also been adopted by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) as part of the joint ISO/IEC 10118-3 international standard.

Whirlpool

General	
Designers	Vincent Rijmen, Paulo S. L. M. Barreto
First published	2000
Derived from	Square, AES
Certification	NESSIE
Detail	
Digest sizes	512 bits
Structure	Miyaguchi-Preneel
Rounds	10

Best public cryptanalysis

In 2009, a rebound attack was announced that presents full collisions against 4.5 rounds of Whirlpool in 2^{120} operations, semi-free-start collisions against 5.5 rounds in 2^{120} time and semi-free-start near-collisions against 7.5 rounds in 2^{128} time.[1]

Contents [hide]

Design features [edit]

Whirlpool is a hash designed after the Square block cipher. Whirlpool is a Miyaguchi-Preneel construction based on a substantially modified Advanced Encryption Standard (AES). It takes a message of any length less than 2^{256} bits and returns a 512-bit message digest.[3]

The authors have declared that "WHIRLPOOL is not (and will never be) patented. It may be used free of charge for any purpose."[2]

The Whirlpool Galaxy (M51), which inspired the name of the algorithm.[2]

Version changes [edit]

The original Whirlpool will be called *Whirlpool-0*, the first revision of Whirlpool will be called *Whirlpool-T* and the latest version will be called *Whirlpool* in the following test vectors.

- In the first revision in 2001, the s-box was changed from a randomly generated one with good cryptographic properties to one which has better cryptographic properties and is easier to implement in hardware.
- In the second revision (2003), a flaw in the diffusion matrix was found that lowered the estimated security of the algorithm below its potential.[4] Changing the 8x8 rotating matrix constants from (1, 1, 3, 1, 5, 8, 9, 5) to (1, 1, 4, 1, 8, 5, 2, 9) solved this issue.

Internal structure [edit]

The Whirlpool hash function is a Merkle–Damgård construction based on an AES-like block cipher W in Miyaguchi-Preneel mode.[2] The block cipher W consists of an 8×8 state matrix S of bytes, for a total of 512 bits. The encryption process consists of updating the state with four round functions over 10 rounds. The four round functions are SubBytes (SB), ShiftColumns (SC), MixRows (MR) and AddRoundKey (AK). During each

Wikipedia The Free Encyclopedia

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
Deutsch
Español
Français
Nederlands
日本語
Polski
Português
Русский
Svenska
Yorùbá
Edit links

round the new state is computed as $S = AK \circ MR \circ SC \circ SB(S)$.

SubBytes [edit]

The **SubBytes** operation applies a non-linear permutation (the S-box) to each byte of the state independently. The 8-bit S-box is composed of 3 smaller 4-bit S-boxes.

ShiftColumns [edit]

The **ShiftColumns** operation cyclically shifts each byte in each column of the state. Column *j* has its bytes shifted downwards by *j* positions.

MixRows [edit]

The **MixRows** operation is a right-multiplication of each row by an 8×8 matrix over $\mathbb{F}_{2^8}$. The matrix is chosen such that the branch number (an important property when looking at resistance to differential cryptanalysis) is 9, which is maximal.

AddRoundKey [edit]

The **AddRoundKey** operation uses bitwise xor to add a key calculated by the key schedule to the current state. The key schedule is identical to the encryption itself, except the AddRoundKey function is replaced by an **AddRoundConstant** function that adds a predetermined constant in each round.

Whirlpool hashes [edit]

The Whirlpool algorithm has undergone two revisions since its original 2000 specification.

People incorporating Whirlpool will most likely use the most recent revision of Whirlpool; while there are no known security weaknesses in earlier versions of Whirlpool, the most recent revision has better hardware implementation efficiency characteristics, and is also likely to be more secure. As mentioned earlier, it is also the version adopted in the ISO/IEC 10118-3 international standard.

The 512-bit (64-byte) Whirlpool hashes (also termed *message digests*) are typically represented as 128-digit hexadecimal numbers. The following demonstrates a 43-byte ASCII input and the corresponding Whirlpool hashes:

```
Whirlpool-0("The quick brown fox jumps over the lazy dog") =
4F8F5CB531E3D49A61CF417CD133792CCFA501FD8DA53EE368FED20E5FE0248C
3A0B64F98A6533CEE1DA614C3A8DDEC791FF05FEE6D971D57C1348320F4EB42D

Whirlpool-T("The quick brown fox jumps over the lazy dog") =
3CCF8252D8BBB258460D9AA999C06EE38E67CB546CFFCF48E91F700F6FC7C183
AC8CC3D3096DD30A35B01F4620A1E3A20D79CD5168544D9E1B7CDF49970E87F1

Whirlpool("The quick brown fox jumps over the lazy dog") =
B97DE512E91E3828B40D2B0FDCE9CEB3C4A71F9BEA8D88E75C4FA854DF36725F
D2B52EB6544EDCACD6F8BEDDFEA403CB55AE31F03AD62A5EF54E42EE82C3FB35
```

Even a small change in the message will (with an extremely high probability of $1 - 10^{-154}$) result in a different hash, which will usually look completely different just like two unrelated random numbers do. The following demonstrates the result of changing the previous input by a single letter (a single bit, even, in ASCII-compatible encodings), replacing `d` with `e`:

```
Whirlpool-0("The quick brown fox jumps over the lazy eog") =
228FBF76B2A93469D4B25929836A12B7D7F2A0803E43DABA0C7FC38BC11C8F2A
9416BBCF8AB8392EB2AB7BCB565A64AC50C26179164B26084A253CAF2E012676

Whirlpool-T("The quick brown fox jumps over the lazy eog") =
C8C15D2A0E0DE6E6885E8A7D9B8A9139746DA299AD50158F5FA9EECDDEF744F9
1B8B83C617080D77CB4247B1E964C2959C507AB2DB0F1F3BF3E3B299CA00CAE3

Whirlpool("The quick brown fox jumps over the lazy eog") =
C27BA124205F72E6847F3E19834F925CC666D0974167AF915BB462420ED40CC5
0900D85A1F923219D832357750492D5C143011A76988344C2635E69D06F2D38C
```

The hash of a zero-length string is:

```
Whirlpool-0("") =
B3E1AB6EAF640A34F784593F2074416ACCD3B8E62C620175FCA0997B1BA23473
39AA0D79E754C308209EA36811DFA40C1C32F1A2B9004725D987D3635165D3C8

Whirlpool-T("") =
470F0409ABAA446E49667D4EBE12A14387CEDBD10DD17B8243CAD550A089DC0F
EEA7AA40F6C2AAAB71C6EBD076E43C7CFCA0AD32567897DCB5969861049A0F5A

Whirlpool("") =
19FA61D75522A4669B44E39C1D2E1726C530232130D407F89AFEE0964997F7A7
3E83BE698B288FEBCF88E3E03C4F0757EA8964E59B63D93708B138CC42A66EB3
```

Implementations [edit]

The authors provide reference implementations of the WHIRLPOOL algorithm, including a version written in C and a version written in Java.[2] These reference implementations have been released into the public domain.[2]

Two of the first widely used mainstream cryptographic programs that started using Whirlpool were FreeOTFE, followed by TrueCrypt in 2005.

See also [edit]

- Digital timestamping
- Hashcash

References [edit]

1. ^ Florian Mendel1, Christian Rechberger, Martin Schläffer, Søren S. Thomsen (2009-02-24). "Cryptanalysis of Reduced Whirlpool and Grøstl" (PDF). *Fast Software Encryption: 16th International Workshop*.
2. ^ *a b c d e* "The Whirlpool Hash Function". Retrieved 20 December 2011.
3. ^ Barreto, Paulo S.L.M. and Rijmen, Vincent (2003). "The WHIRLPOOL Hashing Function" (PDF). Retrieved 2009-08-01.
4. ^ Kyoji, Shibutani and Shirai, Taizo (2003). "On the diffusion matrix employed in the Whirlpool hashing function" (PDF). Retrieved 2007-11-21.

External links [edit]

- Whirlpool homepage Includes detailed algorithm information, C and Java implementations, the paper, etc.
- A Java implementation of all three revisions of Whirlpool
- An open source Go implementation of the latest revision of Whirlpool
- A Matlab Implementation of the Whirlpool Hashing Function
- CHK Freeware Checksum Utility with GUI and WHIRLPOOL support
- RHash, an open source command-line tool, which can calculate and verify Whirlpool hash.
- Perl Whirlpool module at CPAN
- Ruby Whirlpool library
- Ironclad: a Common Lisp cryptography package containing a Whirlpool implementation
- The ISO/IEC 10118-3 standard
- Test vectors for the Whirlpool hash from the NESSIE project
- Managed C# implementation

v · t · e	**Hash functions & message authentication codes**
	Security summary
Common functions	MD5 · SHA-1 · SHA-2 · SHA-3/Keccak
SHA-3 finalists	BLAKE · Grøstl · JH · Skein · Keccak (winner)
Other functions	FSB · ECOH · GOST · HAS-160 · HAVAL · LM hash · MDC-2 · MD2 · MD4 · MD6 · N-Hash · RadioGatún · RIPEMD · SipHash · Snefru · Streebog · SWIFFT · Tiger · VSH · **WHIRLPOOL** · crypt(3) (DES)
MAC algorithms	DAA · CBC-MAC · HMAC · OMAC/CMAC · PMAC · VMAC · UMAC · Poly1305-AES
Authenticated encryption modes	CCM · CWC · EAX · GCM · IAPM · OCB
Attacks	Collision attack · Preimage attack · Birthday attack · Brute force attack · Rainbow table · Distinguishing attack · Side-channel attack · Length extension attack
	Avalanche effect · Hash collision · Merkle–Damgård construction

Design	
Standardization	CRYPTREC · NESSIE · NIST hash function competition
Utilization	Salt · Key stretching · Message authentication

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

v · t · e **ISO standards** by standard number [show]

Categories: Cryptographic hash functions