A near-collision attack on BLENDER-256

Vlastimil Klima,
http://cryptography.hyperlink.cz

We will describe here a near-collision attack on hash function BLENDER with 256-bit output [1]. This attack demonstrates only how to explore one weakness in the design of this hash function family.

The weakness: When we choose the length of the message carefully, we minimize "padding, filling, parsing and appending" the message according to BLENDER description. In such a way the last message block is processed by a small number of rounds (4 rounds here).

In the example we chose the first message with the length 927 bits and the second one with the same value, but one bit shorter. BLENDER prepares 32 32-bit words W[0],..,W[31] from the message, using "padding, filling, parsing and appending" processes.

For the message lengths such as 926 bits, the "padding, filling, parsing and appending" is minimal. In the example the first 28 words (of 32 bits) W[0],..,W[27] are the same for both messages. The word W[28] differs in the most significant bit (it corresponds to the change in "padding" bit 928). The word W[29] differs in one bit due to the length difference. The words W[30] and W[31] contain checksums of the previous words and could differ in a couple of bits.

These changes are propagated in the last four rounds only, what gives a near collision with high probability. The unoptimized trial program found a near-collision in 30 minutes on a notebook (225 equal bits from 256).

Example

BLENDER, Hash algorithm for 256-bit message digests

Message 1, 927 bits:
hex:
A5 25 24 D5 F3 87 F5 66 5F 8B 43 B3 51 BD BE F4 B0 B6 63 60 B3 61 F6 35 0C
2C 7B CB 9E 3F 97 03 5D FF B4 41 52 F1 A2 18 64 E3 B4 43 CC C9 0D C6 C4 68
84 18 05 F7 B7 42 98 CB 91 10 03 39 78 19 AE A7 64 75 DD 59 A0 1A CC 4D 38
64 A3 91 D7 02 51 55 9A F1 98 C1 EC FB F5 37 C4 6A A4 1D 3D 03 1C E8 4C 40
54 19 94 72 2E 84 6F 70 9F 14 D8 CB 40 21 0B 5A
binary:
10100101 10100100 00100100 10101011 11001111 11100001 10101111 01100110
11111010 11010001 11000010 11001101 10001010 10111101 01111101 00101111
00001101 01101101 11000110 00000110 11001101 10000110 01101111 10101100
00110000 00110100 11011110 11010011 01111001 11111100 11101001 11000000
10111010 11111111 00101101 10000010 01001010 10001111 01000101 00011000
00100110 11000111 00101101 11000010 00110011 10010011 10110000 01100011
00100011 00010110 00100001 00011000 10100000 11101111 11101101 01000010
00011001 11010011 10001001 00001000 11000000 10011100 00011110 10011000
01110101 11100101 00100110 10101110 10111011 10011010 00000101 01011000
00110011 10110010 00011100 00100110 11000101 10001001 11101011 01000000
10001010 10101010 01011001 10001111 00011001 10000011 00110111 11011111
10101111 11101100 00100011 01010110 00100101 10111000 10111100 11000000
00111000 00010111 00110010 00000010 00101010 10011000 00101001 01001110
01110100 00100001 11110110 00001110 11111001 00101000 00011011 11010011
00000010 10000100 11010000 0101101

Message 2 = the first 926 bits of Message1

BLENDER-256(Message1)=
hex.:
91 32 2B C9 72 AD 9D 02 BF F5 37 18 67 BE 47 50 CC FA 89 B2 5C 1D A0 7C ED
54 70 BD 35 E7 98 D1
binary:
10001001 01001100 11010100 10010011 01001110 10110101 10111001 01000000
11111101 10101111 11101100 00011000 11100110 01111101 11100010 00001010
00110011 01011111 10010001 01001101 00111010 10111000 00000101 00111110
10110111 00101010 00001110 10111101 10101100 11100111 00011001 100010

BLENDER-256(Message2)=
hex:
90 2F 2A C9 76 A9 9D 00 BE F6 36 18 67 BE 45 52 CD F9 88 B2 58 1D A1 7C EC
53 72 BC 34 E7 99 D2
binary:
00001001 11110100 01010100 10010011 01101110 10010101 10111001 00000000
01111101 01101111 01101100 00011000 11100110 01111101 10100010 01001010
10110011 10011111 00010001 01001101 00011010 10111000 10000101 00111110
00110111 11001010 01001110 00111101 00101100 11100111 10011001 01001011

BLENDER-256(Message1) XOR BLENDER-256(Message2)=
hex:
01 1D 01 00 04 04 00 02 01 03 01 00 00 00 02 02 01 03 01 00 04 00 01 00 01
07 02 01 01 00 01 03
binary:
10000000 10111000 10000000 00000000 00100000 00100000 00000000 01000000
10000000 11000000 10000000 00000000 00000000 00000000 01000000 01000000
10000000 11000000 10000000 00000000 00100000 00000000 10000000 00000000
10000000 11100000 01000000 10000000 10000000 00000000 10000000 11000000

Hamming weight of the difference: 31

References
[1] Colin Bradbury: BLENDER, A Proposed New Family of Cryptographic Hash Algorithms, 25th October, 2008
http://ehash.iaik.tugraz.at/uploads/5/5e/Blender.pdf
http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/documents/Blender.zip