

# Analysis of Reduced MD6 – Abstract

Thomas Hodanek

Graz University of Technology, Austria.

thomas.hodanek@student.tugraz.at

## 1 Introduction

Advances in the cryptanalysis of popular hash functions like MD5 and SHA-1 [2,4,5,6,7,9,15,16,17,18,19] led to the SHA-3 competition. MD6 is one of the candidates, designed by a team around Ronald Rivest [14]. Analysis of MD6 appears in [1,8,10,11].

In this paper, we describe collision attacks on round-reduced variants of MD6, combining approaches which were initially applied to SHA-1 [12,13] with new speed-up techniques developed specifically for MD6.

## 2 Short description of MD6

Hash functions of the MD6 family are comprised of two main components: the MD6 compression function and the MD6 mode of operation [14]. These parts are explained in more detail in the following.

### MD6 compression function

The MD6 compression function works on binary words of length  $w = 64$  bits. It maps 89 words of input down to 16 words of output. The number of input words to the compression function  $f$  are composed of 15 fixed words  $Q$ , an 8-word key  $K$ , 2 auxiliary information words and a 64-word data block  $B$ . For our attacks we consider the actual constant  $Q$  used in MD6 and set  $K, U, V$  to zero.

---

#### Algorithm 1 MD6 compression function

---

**Input:** input data array  $N$  of  $n = 89$  words; a positive number of rounds  $r$

**Output:** output array  $C$  of  $c = 16$  words

Set  $t = c \cdot r$

Set an inner working array  $A[0\dots t+n-1]$  of length  $n+t$  words

$A[0\dots n-1] \leftarrow N[0\dots n-1]$

**for**  $i = n$  **to**  $t+n-1$  **do**

$word = S_i \oplus A_{i-n} \oplus A_{i-17}$  /\* linear part \*/  
 $word = word \oplus (A_{i-31} \wedge A_{i-67}) \oplus (A_{i-18} \wedge A_{i-21})$  /\* nonlinear part \*/  
 $word = word \oplus (word \gg rs_{i-n})$  /\* right shift \*/  
 $A_i = word \oplus (word \ll ls_{i-n})$  /\* left shift \*/

**end for**

$C[0\dots c-1] \leftarrow A[t+n-c\dots t+n-1]$

---

The MD6 compression function works on a controllable number of rounds, whereas each round corresponds to 16 steps. Each step computes a one-word value. This main loop is followed by a truncation operation, which truncates the final result to 16 words (see Algorithm 1).

### MD6 mode of operation

The MD6 mode of operation describes how the compression function  $f$  can be applied repeatedly in order to create a fixed-length digest from an arbitrarily long message input. The standard mode of operation is a bottom-up, tree-based mode, which is parametrizable by a so-called *maximum level* parameter  $L$ . If  $L = 0$  then a sequential mode of operation is used, similar to standard Merkle-Damgård processing.

## 3 Methods

For our attacks we mainly concentrate on the MD6 compression function. Thereto we construct differential collision attacks by first trying to find a characteristic with high probability, and then try to find a conforming message pair. For the search for characteristics we use the framework of [12,13] to map the problem of finding a good characteristic to the problem of finding a low-weight codeword in a linear code. For the problem at hand, we propose a variant of a search algorithm due to Canteaut and Chabaud [3]. For the search of a message pair, we use an ad-hoc technique that speeds-up message search considerably compared to random trials. In the final version of the paper, more details will be given.

## 4 Results

The preliminary results of the characteristic search are summarized in Table 1. There, the attack complexities refer to naive random trials for conforming message pairs. As an example for the more clever version of the search for message pairs, we consider MD6 reduced to 16 steps. There, the speed to find a collision for MD6 reduced to 16 rounds is  $2^{17}$ .

**Table 1.** Summary of founded weights

number of rounds	lowest weights
10	16
12	29
16	80
20	114
25	229
30	378

## References

1. Jean-Philippe Aumasson and Willi Meier. Personal communication (nonrandomness on the reduced-round compression function). Reported in the supporting documentation, 2008.
2. Eli Biham, Rafi Chen, Antoine Joux, Patrick Carribault, Christophe Lemuet, and William Jalby. Collisions of SHA-0 and Reduced SHA-1. In *EUROCRYPT*, pages 36–57, 2005.
3. Anne Canteaut and Florent Chabaud. A new algorithm for finding minimum-weight words in a linear code: application to McEliece’s cryptosystem and to BCH codes of length 511. In *Information Theory. 1997. Proceedings., 1997 IEEE International Symposium on*, pages 367–378, 1997.

4. Christophe De Cannière, Florian Mendel, and Christian Rechberger. Collisions for 70-Step SHA-1: On the Full Cost of Collision Search. In *Selected Areas in Cryptography*, pages 56–73, 2007.
5. Christophe De Cannière and Christian Rechberger. Finding SHA-1 Characteristics: General Results and Applications. In *ASIACRYPT*, pages 1–20, 2006.
6. Christophe De Cannière and Christian Rechberger. Preimages for Reduced SHA-0 and SHA-1. In *CRYPTO*, pages 179–202, 2008.
7. Bert den Boer and Antoon Bosselaers. Collisions for the Compression Function of MD5. In *EUROCRYPT*, pages 293–304, 1993.
8. Itai Dinur and Adi Shamir. Personal communication (key recovery on the reduced-round compression function). Reported in the supporting documentation, 2008.
9. Hans Dobbertin. Cryptanalysis of MD5 Compress, 1996.
10. Shahram Khazaei and Willi Meier. Collisions for 16-round MD6. NIST mailing list (local link), 2009.
11. Dmitry Khovratovich. Nonrandomness of the 33-round MD6. FSE 2009 rump session, slides only, 2009.
12. Norbert Pramstaller, Christian Rechberger, and Vincent Rijmen. Exploiting Coding Theory for Collision Attacks on SHA-1. In Nigel P. Smart, editor, *IMA Int. Conf.*, volume 3796 of *Lecture Notes in Computer Science*, pages 78–95. Springer, 2005.
13. Vincent Rijmen and Elisabeth Oswald. Update on SHA-1. In *CT-RSA*, pages 58–71, 2005.
14. Ronald L. Rivest. The MD6 hash function – A proposal to NIST for SHA-3. Submission to NIST, 2008.
15. Marc Stevens, Arjen K. Lenstra, and Benne de Weger. Chosen-Prefix Collisions for MD5 and Colliding X.509 Certificates for Different Identities. In *EUROCRYPT*, pages 1–22, 2007.
16. Xiaoyun Wang, Xuejia Lai, Dengguo Feng, Hui Chen, and Xiuyuan Yu. Cryptanalysis of the Hash Functions MD4 and RIPEMD. In *EUROCRYPT*, pages 1–18, 2005.
17. Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding Collisions in the Full SHA-1. In *CRYPTO*, pages 17–36, 2005.
18. Xiaoyun Wang and Hongbo Yu. How to Break MD5 and Other Hash Functions. In *EUROCRYPT*, pages 19–35, 2005.
19. Xiaoyun Wang, Hongbo Yu, and Yiqun Lisa Yin. Efficient Collision Search Attacks on SHA-0. In *CRYPTO*, pages 1–16, 2005.