Call for Challenge: Challenging A Different 1-Block Collision Attack on MD5

Announced by: [1,2]Tao Xie, [1]Dengguo Feng

[1]State Key Lab of Information Security, Chinese Academy of Sciences, Beijing, China

[2]The Center for Soft-Computing and Cryptology, NUDT, Changsha, China

(hamishxie@vip.sina.com)

So far, all the differential attacks on MD5 were constructed through multi-block collision method. Can collisions for MD5 be found using just a single block of message (i.e. 512-bit)? This has been an open problem since the first 2-block collision attack was given. However, a paper titled "How To Find Weak Input Differences For MD5 Collision Attacks" (Cryptology ePrint Archive (2009/223), http://eprint.iacr.org/) listed all the practically possible weak differences that can be used to make attacks on MD5, in the Table1 of that paper, only an 1-block message difference ($m_{5,10}, m_{10,31}$) was included in and suggested in the end of the paper to be able to be exploited to construct a practical collision attack on MD5. A hint was later given in EUROCRYPT2009's poster paper tilted "Could The 1-MSB Input Difference Be The Fastest Collision Attack For MD5? " (LNCS 5479, the poster session of EUROCRYPT 2009. Cryptology ePrint Archive (2008/391), http://eprint.iacr.org/) that, 1-block collision attack on MD5 is possible if a more efficient searching algorithm can be developed using evolutionary approaches. Today, in the last month (Dec,) of 2010, we would like to make public a result of our 1-block collision attacks on MD5 in Table 1 as below, which was infact obtained in the beginning of 2010, but for security reasons, the techniques are not allowed to be made public at the moment.

Table 1. An 1-Block Collision Example With Its MD5 Digest (Underlined Bits With Difference）

M_0	0x6165300e,0x87a79a55,0xf7c60bd0,0x34febd0b,0x6503cf04,0x854f709e,0xfb0fc034,0x874c9c65, 0x2f94cc40,0x15a12deb,0x5c15f4a3,0x490786bb,0x6d658673,0xa4341f7d,0x8fd75920,0xefd18d5a
M_0^*	0x6165300e,0x87a79a55,0xf7c60bd0,0x34febd0b,0x6503cf04,0x854f7<u>4</u>9e,0xfb0fc034,0x874c9c65, 0x2f94cc40,0x15a12deb,0x<u>d</u>c15f4a3,0x490786bb,0x6d658673,0xa4341f7d,0x8fd75920,0xefd18d5a
MD5	0xf999c8c9　0xf7939ab6　0x84f3c481　0x1457cb23

Here, we are calling for a challenge to the cryptology community that, any one who first gives a new different 1-block collision attack on MD5 will win 10,000 US dollars (about 50,000 RMB in Chinese Yuan) as a reward for his (her) excellent work. This call for challenge will be ended on Jan 1st, 2013. This announcement's first affiliated unit will be responsible for this amount of reward when a new different 1-block collision attack is received and verified.