Collisions for Hash Functions

MD4, MD5, HAVAL-128 and RIPEMD

Xiaoyun Wang[1], Dengguo Feng[2], Xuejia Lai[3], Hongbo Yu[1]

The School of Mathematics and System Science, Shandong University, Jinan250100, China[1]

Institute of Software, Chinese Academy of Sciences, Beijing100080, China[2]

Dept. of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai, China[3]

xywang@sdu.edu.cn[1]

August 16, 2004

1 Collisions for MD5

MD5 is the hash function designed by Ron Rivest [9] as a strengthened version of MD4[8]. In 1993 Bert den Boer and Antoon Bosselaers [1] found pseudo-collision for MD5 which is made of the same message with two different sets of initial value. H. Dobbertin[3] found another kind of collision which consists of two different 512-bit messages with a chosen initial value IV_0'.

$$IV_0' : A_0' = 0x12AC2375,\ \mathrm{B}_0' = 0\mathrm{x}3B341042, C_0' = 0x5F62B97C\ , \mathrm{D}_0' = 0x4BA763ED$$

Our attack can find many real collisions which are composed of two 1024-bit messages with the original initial value IV_0 of MD5.

$$IV_0 : A_0 = 0x01234567, B_0 = 0x89abcdef\ , C_0 = 0xfedcba98, D_0 = 0x76543210$$

$$M_k' = M_k + \Delta C_1, \Delta C_1 = (0,0,0,0,2^{31},....2^{15},...2^{31},0), s = 4,11,14$$

$$M_{ki}' = M_{ki} + \Delta C_2, \Delta C_2 = (0,0,0,0,2^{31},.... - 2^{15},...2^{31},0), s = 4,11,14$$

such that

$$MD5(M, N_i) = MD5(M', N_i')$$

On IBM P690 it takes about one hour to find such M and M', after that, it takes only 15 seconds to 5 minutes to find N_i and N_i', so that (M, N_i) and (M', N_i') will produce the same hash same value.

The following are two pairs of 1024-bit messages producing collisions, the two examples have the same 1-st half 512 bits.

X_1	M_1	313838dd	fc2932c7	c030b717	bafc1bae	6673a8d7	9ddcf416	85d70859	99403db0
		634add1	c0736004	9558bd1f	21e10982	ca94c90b	6aae6e69	cbf61bf1	6b0e615
	M_{11}	2e82d48b	16bdf161	ce10bd62	c3c6809d	b6745639	fc0e06c7	6573a914	bef0d753
		537b8755	497b92e8	46f559c2	7d7a347a	511d8b1	98ebeb68	c9ca4559	eb10e037
X_1'	M_1'	313838dd	fc2932c7	c030b717	bafc1bae	e673a8d7	9ddcf416	85d70859	99403db0
		634add1	c0736004	9558bd1f	21e18982	ca94c90b	6aae6e69	4bf61bf1	6b0e615
	M_{11}'	2e82d48b	16bdf161	ce10bd62	c3c6809d	36745639	fc0e06c7	6573a914	bef0d753
		537b8755	497b92e8	46f559c2	7d79b47a	511d8b1	98ebeb68	49ca4559	eb10e037
H		21f15d09	3ef611d2	f9f09bfb	86b9cadf				
X_2	M_1	313838dd	fc2932c7	c030b717	bafc1bae	6673a8d7	9ddcf416	85d70859	99403db0
		634add1	c0736004	9558bd1f	21e10982	ca94c90b	6aae6e69	cbf61bf1	6b0e615
	M_{12}	2882d409	177df16c	bf90fdc1	c406a19a	b43a36af	fd41f967	2835450e	a12506ce
		2973087d	8839e1a0	78646612	9c8dac6d	ef59b8e7	4840474	2afb5bd0	840c546a
X_2'	M_1'	313838dd	fc2932c7	c030b717	bafc1bae	e673a8d7	9ddcf416	85d70859	99403db0
		634add1	c0736004	9558bd1f	21e18982	ca94c90b	6aae6e69	4bf61bf1	6b0e615
	M_{12}'	2882d409	177df16c	bf90fdc1	c406a19a	343a36af	fd41f967	2835450e	a12506ce
		2973087d	8839e1a0	78646612	9c8d2c6d	ef59b8e7	4840474	aafb5bd0	840c546a
H		fa8892f3	49c2111f	477d3217	56ae4e97				

Table 1 Two pairs of collision for MD5

2 Collisions for HAVAL-128

HAVAL is proposed in [10] . HAVAL is a hashing algorithm that can compress messages of any length in 3,4 or 5 passes and produce a variable length output --128-bit,160-bit, 192 or 224-bit fingerprint.

Attack on a reduced version for HAVAL was given by P. R. Kasselman and W T Penzhorn [7], which consists of last rounds for HAVAL-128. We break the full HAVAL-128 with only about the 2^6 HAVAL computations. Here we give two examples of collisions of HAVAL-128, where

$$M' = M + \Delta C, \Delta C = (2^{i-1},0,0,0,2^{i-12},....2^{i-8},0,...,0), s = 0,11,18$$

$$i = 0,1,2,...31$$

$$HAVAL(M) = HAVAL(M')$$

M_1	6377448b	d9e59f18	f2aa3cbb	d6cb92ba	ee544a44	879fa576	1ca34633	76ca5d4f
	a67a8a42	8d3adc8b	b6e3d814	5630998d	86ea5dcd	a739ae7b	54fd8e32	acbb2b36
	38183c9a	b67a9289	c47299b2	27039ee5	dd555e14	839018d8	aabbd9c9	d78fc632
	fff4b3a7	40000096	7f466aac	fffffbc0	5f4016d2	5f4016d0	12e2b0	f4307f87

M_1'	6377488b	d9e59f18	f2aa3cbb	d6cb92ba	ee544a44	879fa576	1ca34633	76ca5d4f
	a67a8a42	8d3adc8b	b6e3d814	d630998d	86ea5dcd	a739ae7b	54fd8e32	acbb2b36
	38183c9a	b67a9289	c47299ba	27039ee5	dd555e14	839018d8	aabbd9c9	d78fc632
	fff4b3a7	40000096	7f466aac	fffffbc0	5f4016d2	5f4016d0	12e2b0	f4307f87
H	95b5621c	ca62817a	a48dacd8	6d2b54bf				
M_2	6377448b	d9e59f18	f2aa3cbb	d6cb92ba	ee544a44	879fa576	1ca34633	76ca5d4f
	a67a8a42	8d3adc8b	b6e3d814	5630998d	86ea5dcd	a739ae7b	54fd8e32	acbb2b36
	38183c9a	b67a9289	c47299b2	27039ee5	dd555e14	839018d8	aabbd9c9	d78fc632
	fff4b3a7	40000096	7f466aac	fffffbc0	5f4016d2	5f4016d0	12e2b0	f5b16963
M_2'	6377488b	d9e59f18	f2aa3cbb	d6cb92ba	ee544a44	879fa576	1ca34633	76ca5d4f
	a67a8a42	8d3adc8b	b6e3d814	d630998d	86ea5dcd	a739ae7b	54fd8e32	acbb2b36
	38183c9a	b67a9289	c47299ba	27039ee5	dd555e14	839018d8	aabbd9c9	d78fc632
	fff4b3a7	40000096	7f466aac	fffffbc0	5f4016d2	5f4016d0	12e2b0	f5b16963
H	b0e99492	d64eb647	5149ef30	4293733c				

Table 2 Two pairs of collision, where i=11 and these two examples differ only at the last word

3 Collisions for MD4

MD4 is designed by R. L. Rivest[8] . Attack of H. Dobbertin in Eurocrypto'96[2] can find collision with probability $1/2^{22}$. Our attack can find collision with hand calculation, such trhat

$$M' = M + \Delta C, \Delta C = (0,2^{31},-2^{28}+2^{31},0,....,0,-2^{16},0,...,0), i = 1,2,12$$

$$MD4(M) = MD4(M')$$

M_1	4d7a9c83	56cb927a	b9d5a578	57a7a5ee	de748a3c	dcc366b3	b683a020	3b2a5d9f
	c69d71b3	f9e99198	d79f805e	a63bb2e8	45dd8e31	97e31fe5	2794bf08	b9e8c3e9
M_1'	4d7a9c83	d6cb927a	29d5a578	57a7a5ee	de748a3c	dcc366b3	b683a020	3b2a5d9f
	c69d71b3	f9e99198	d79f805e	a63bb2e8	45dc8e31	97e31fe5	2794bf08	b9e8c3e9
H	5f5c1a0d	71b36046	1b5435da	9b0d807a				
M_2	4d7a9c83	56cb927a	b9d5a578	57a7a5ee	de748a3c	dcc366b3	b683a020	3b2a5d9f
	c69d71b3	f9e99198	d79f805e	a63bb2e8	45dd8e31	97e31fe5	f713c240	a7b8cf69
M_2'	4d7a9c83	d6cb927a	29d5a578	57a7a5ee	de748a3c	dcc366b3	b683a020	3b2a5d9f
	c69d71b3	f9e99198	d79f805e	a63bb2e8	45dc8e31	97e31fe5	f713c240	a7b8cf69
H	e0f76122	c429c56c	ebb5e256	b809793				

Table 3 Two pairs of collisions for MD4

4 Collisions for RIPEMD

RIPEMD was developed for the RIPE project (RACE Integrrity Primitives Evalustion, 1988-1992). In

1995, H. Dobbertin proved that the reduced version RIPEMD with two rounds is not collision-free[4]. We prove that the full RIPEMD also isn't collision-free. The following are two pairs of collisions for RIPEMD.

$$RIPEMD(M) = RIPEMD(M')$$

where $M' = M + \Delta C, \Delta C = (0,0,0,2^{20},....2^{18} + 2^{31},...,2^{31}), i = 3,10,15$

M_1	579faf8e	9ecf579	574a6aba	78413511	a2b410a4	ad2f6c9f	b56202c	4d757911
	bdeaae7	78bc91f2	47bc6d7d	9abdd1b1	a45d2015	817104ff	264758a8	61064ea5
M'	579faf8e	9ecf579	574a6aba	78513511	a2b410a4	ad2f6c9f	b56202c	4d757911
	bdeaae7	78bc91f2	c7c06d7d	9abdd1b1	a45d2015	817104ff	264758a8	e1064ea5
H	1fab152 1654a31b 7a33776a 9e968ba7							
M_2	579faf8e	9ecf579	574a6aba	78413511	a2b410a4	ad2f6c9f	b56202c	4d757911
	bdeaae7	78bc91f2	47bc6d7d	9abdd1b1	a45d2015	a0a504ff	b18d58a8	e70c66b6
M_2'	579faf8e	9ecf579	574a6aba	78513511	a2b410a4	ad2f6c9f	b56202c	4d757911
	bdeaae7	78bc91f2	c7c06d7d	9abdd1b1	a45d2015	a0a504ff	b18d58a8	670c66b6
H	1f2c159f	569b31a6	dfcaa51a	25665d24				

Table 4 The collisions for RIPEMD

5 Remark

Besides the above hash functions we break, there are some other hash functions not having ideal security. For example, collision of SHA-0 [6] can be found within the running-time of about 2^{40} SHA-0 algorithms, and HAVAL-160 can be found a collision with probability $1/2^{32}$.

1 B. den Boer, Antoon Bosselaers, Collisions for the Compression Function of MD5, Eurocrypto,93.

2 H. Dobbertin, Cryptanalysis of MD4, Fast Software Encryption, LNCS 1039, D. , Springer-Verlag, 1996.

3 H. Dobbertin, Cryptanalysis of MD5 compress, presented at the rump session of EurocrZpt'96.

4 Hans Dobbertin, RIPEMD with Two-round Compress Function is Not Collision-Free, J. Cryptology 10(1), 1997.

5 H. Dobbertin, A. Bosselaers, B. Preneel, "RIPMEMD-160: A Strengthened Version of RIPMMD," Fast Software EncrZption, LNCS 1039, D.Gollmann, Ed., Springer-Verlag, 1996, pp. 71-82.

6 FIPS 180-1, Secure hash standard, NIST, US Department of Commerce, Washington D. C., April 1995.

7 P. R. Kasselman, W T Penzhorn , Cryptananlysis od reduced version of HAVAL, Vol. 36, No. 1, Electronic Letters, 2000.

8 R. L Rivest, The MD4 Message Digest Algorithm, Request for Comments (RFC)1320, Internet Activities Board, Internet Privacy Task Force, April 1992.

9 R. L Rivest, The MD5 Message Digest Algorithm, Request for Comments (RFC)1321, Internet Activities Board, Internet PrivacZ Task Force, April 1992.3RIPEMD-1281

10 Y. Zheng, J. Pieprzyk, J. Seberry, HAVAL--A One-way Hashing Algorithm with Variable Length of Output, Auscrypto'92.