Information Processing Letters ••• (••••) •••–•••

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

An improved preimage attack against HAVAL-3

Jian Guo [a,*], Chunhua Su [b], Wun-She Yap [c]

[a] Nanyang Technological University, Singapore
[b] Japan Advanced Institute of Science and Technology, Japan
[c] Universiti Tunku Abdul Rahman, Malaysia

ARTICLE INFO

Article history:
Received 2 January 2014
Received in revised form 29 September 2014
Accepted 15 October 2014
Available online xxxx
Communicated by V. Rijmen

Keywords:
Cryptography
Hash function
HAVAL-3
Cryptanalysis
Meet-in-the-middle attack
Splice-and-cut

ABSTRACT

Hash functions play an important role in constructing cryptographic schemes that provide security services, such as confidentiality in an encryption scheme, authenticity in an authentication protocol and integrity in a digital signature scheme and so on. Such hash function is needed to process a challenge, a message, an identifier or a private key. In this paper, we propose an attack against HAVAL-3 hash function, which is used in open source Tripwire and is included in GNU Crypto. Under the meet-in-the-middle (MITM) preimage attack framework proposed by Aoki and Sasaki in 2008, the one-wayness of several (reduced-)hash functions had been broken recently. However, most of the attacks are of complexity close to brute-force search. Focusing on reducing the time complexity of such MITM attacks, we improve the preimage attacks against HAVAL-3 hash function to within lower time complexity and memory requirement, compared with the best known attack proposed by Sasaki and Aoki in ASIACRYPT 2008. Besides the 256-bit variant of HAVAL-3, similar improvements can be applied to some truncated variants as well. Interestingly, due to the low complexity of our attack, the preimage attack applies to the 192-bit variant of HAVAL-3 for the first time.

1. Introduction

A hash function H which is used in cryptography maps a message M of arbitrary length to a short fixed-length hash value h. It is a fundamental component of many cryptographic protocols and applications used in electronic devices such as digital signatures, random number generation in embedded chips, especially for RFID authentication system. To fulfill the security needs from these applications, there are three basic security requirements for hash functions of digest size n bits, *i.e.*,

Collision Resistance: it should be computationally difficult, up to a bound of $2^{n/2}$, to find (M, M') with $M \neq M'$ such that $H(M) = H(M')$.

Second-Preimage Resistance: given a message M, it should be computationally difficult, up to a bound of 2^{n-k} for message of 2^k blocks, to find M' with $M \neq M'$ such that $H(M) = H(M')$.

Preimage Resistance: given a target T, it should be computationally difficult, up to a bound of 2^n, to find M such that $H(M) = T$.

In this paper, we focus on preimage resistance. There are many known attack methods against the hash functions. We pay our attention to the splice-and-cut meet-in-the-middle preimage attack against cryptographic hash function HAVAL-3 designed by Zheng *et al.* in 1992 and improve the previous best time complexity of such attack. We note that HAVAL-3 has already many applications. For example, HAVAL is used in open source Tripwire, a free software security and data integrity tool useful for monitoring and alerting on specific file changes on a range of systems.

* Corresponding author.
E-mail addresses: ntu.guo@gmail.com (J. Guo), suchunhua@gmail.com (C. Su), yapws@utar.edu.my (W.-S. Yap).

http://dx.doi.org/10.1016/j.ipl.2014.10.016
0020-0190/

The meet-in-the-middle (MITM) attack was originated from an attack against double-DES by Diffie and Hellman [9], where they found double-DES (*i.e.*, encrypting a plaintext P using DES twice under different keys to produce a ciphertext $C = \mathrm{DES}_{k2}(\mathrm{DES}_{k1}(P))$) did not provide security as expected, since one can compare $\mathrm{DES}_{k2}^{-1}(C)$ and $\mathrm{DES}_{k1}(P)$ to check whether both outputs match in the middle. One can view this attack works at the level of operating modes since the specification of DES does not play a crucial role in such a generic attack. Similar MITM attacks on operating modes of hash functions were presented in 1992 by Lai and Massey [21]. Later, this attack was generalized to analyze the security of block ciphers, and had been applied to round-reduced AES [7], DES [11] and IDEA [8] block ciphers.

In the CRYPTO 2008 rump session, Sasaki and Aoki [28] presented an MITM preimage attack framework to attack the compression functions of Davies–Meyer hash functions, named *splice-and-cut* MITM attacks. With a generic unbalanced MITM approach, one can convert these pseudo-preimages on compression functions to preimages of hash functions. For a given hash h and a compression function CF, pseudo-preimage is a pair of (v, M), $v \neq$ initial value IV, such that $CF(v, M) = h$. If we can construct many distinguished pairs (H_{i-1}, M_i), such that all produce the same value as the given target h, followed by a message block search, which links the IV to one of the H_{i-1}s, then a full preimage of the hash function is found. Subsequently, this framework has been applied to many narrow-pipe designs such as full or round-reduced MD4 [12], MD5 [29], SHA-0/1 [2,20], SHA-2 [1], HAS-160 [26,16], HAVAL [27,24], RIPEMD [30,33], Tiger [12] and also some SHA-3 candidates [18].

Many useful techniques have been developed through these attacks. In general, there are two streams, one aims to attack more steps, since MITM is generally difficult to achieve for full hash functions due to multiple passes and key schedules. On the other hand, most time complexities of such attacks are very close to brute-force search, thus few techniques have been developed to reduce the time complexities [1,12].

Interestingly, these techniques developed on hash functions are found to be useful to analyze some existing block ciphers such as XTEA [32], also for very recent designs such as KTANTAN [4,36].

In 2011, besides the Davies–Meyer construction, the MITM preimage framework is also applied to other modes of operation [25], with example of AES in different hashing modes. This attack is special since it does not use any key words (or message words in hash functions) as neutral words, but only some state values.

Another research line on finding preimages is to explore special properties and dedicated algorithms for both finding pseudo-preimages and conversion to preimages, *e.g.*, [22,3,5]. However, it is interesting to note that both attacks on MD4 [22] and HAVAL-3 [3] can also be re-explained under the MITM preimage framework. Yet, the dedicated algorithms work much faster when converting pseudo-preimages to preimages.

Besides attacks against primitives like hash functions and block ciphers, variants of MITM attacks have been used to analyze applications of these primitives, such as message authentication codes (MACs) based on block ciphers [37], and MACs based on hash functions [35,34,14,13].

1.1. Our contribution

We observe that there are some new techniques, in particular indirect partial matching (IPM) from [1] and multi-target pseudo-preimages (MTPP) from [12], developed after the best known preimage attacks against HAVAL-3 were found in [24]. We apply some of these techniques together with the MITM preimage framework to HAVAL-3 and improve the attack complexities in terms of time and memory. These improvements apply to not only the 256-bit variant, but also some truncated variants of HAVAL-3 including 224-bit and 192-bit. Interestingly, due to the low time complexity of the attack, this is the first preimage attack against the 192-bit variant of HAVAL-3. A detailed comparison of our results and existing (pseudo-)preimage attacks against HAVAL-3 is shown in Table 1.

1.2. Organization

The rest of the paper is organized as follows. Section 2 describes the details of HAVAL. Section 3 gives an introduction on the details of MITM preimage attacks. We apply the MITM preimage attack to HAVAL-3 and to its small variants in Section 4. Finally, we conclude and give some open problems in Section 5.

2. Description of HAVAL-3

HAVAL [38] is a hash function family designed by Zheng *et al.* in 1992, which compresses a message up to $2^{64} - 1$ bits into 128, 160, 192, 224, 256 bits digest (a.k.a. hash h). It consists of three versions for each hash function with 3, 4, 5 passes (HAVAL-x denotes the version with x passes), following Merkle–Damgård structure. A message is padded by a '1' and many '0's so that the length becomes 944 mod 1024. Then a 3-bit version number, 3-bit indicating number of passes used, 10-bit output length, 64-bit original message length are padded, the final length is multiple of 1024. Then the message is divided into blocks of 1024 bits $(B_0, B_1, \ldots, B_{n-1})$, and the hash can be computed from the initial value (IV) and compression function ($CF : \{0,1\}^{256} \times \{0,1\}^{1024} \to \{0,1\}^{256}$):

(i) $H_0 \leftarrow IV$,
(ii) $H_{i+1} \leftarrow CF(H_i, B_i)$ for $0 \leq i < n$.

H_n is the final hash output of the 256-bit variant. For each message block B_j, the block is divided into 32 words $M_0, M_1, \ldots, M_{31}$, and the compression function proceeds as follows:

(i) $p_0 \leftarrow H_j$
(ii) $p_{i+1} \leftarrow R_i(p_i, M_{\pi(i)})$ for $0 \leq i < 32x$ for x-pass version ($x = 3, 4, 5$). Here R_i is round function at step i and π is the message permutation as defined in Table 2.

Please cite this article in press as: J. Guo, C. Su, W.-S. Yap, An improved preimage attack against HAVAL-3, Inf. Process. Lett. (2014), http://dx.doi.org/10.1016/j.ipl.2014.10.016