Journal of Computing and Security

October 2016, Volume 3, Number 4 (pp. 211–215)
http://www.jcomsec.org

Multicollision Attack on a Recently Proposed Hash Function vMDC-2

Zahra Zolfaghari [a], Hamid Asadollahi [a], Nasour Bagheri [a,*]

[a] *Department of Electrical Engineering, Shahid Rajaee Teacher Training University, Tehran, Iran*

ARTICLE INFO.

Article history:
Received: 10 December 2016
Revised: 10 December 2017
Accepted: 31 January 2018
Published Online: 01 April 2018

Keywords:
DBL Compression Function, Iterated Hash Function, Multicollision Attack, Collision Attack.

ABSTRACT

In this paper, we describe an attack on a new double block length hash function which was proposed as a variant of MDC-2 and MDC-4. The vMDC-2 compression function is based on two calls to a block cipher that compresses a 3n-bit string to a 2n-bit one. This attack is based on the Joux's multicollision attack, where we show that an adversary wins finding collision game by requesting 2^{70} queries for $n = 128$-bit block cipher that is much less than the complexity of birthday attack.

1 Introduction

Hash function maps from the set of binary sequence of arbitrary length to the set of binary sequences of fixed length. Hash functions are used widely in digital signatures and message authentication codes.In practice, it is not easy to construct a cryptographic function with an input of variable size. So, hash functions can be used in iterated mode that makes use of compression functions. Compression functions are the cryptographic primitives which compress fixed length input messages to the fixed length output values. Merkle-Damgård (MD) design [1, 2] is used for building an iterated hash function.

There exist two ways for constructing compression function, construction based on block cipher or from scratch. The topic of this paper is about the constructions which are based on block ciphers. The sixty-four methods of building a compression function mode from block ciphers have been proposed by Preneel, Govaerts and Vandewalle (PGV) [3] that twelve of them are secured against collision and (second) preimage attacks. The compression functions that has the output length as same as the output length of underlying block cipher, are called single block length (SBL) compression functions. Some compression functions are called Multi block length compression functions that the output length of them is larger than the output length of the block cipher. The double block length (DBL) compression functions is a kind of multi block length compression functions which maps long string to 2n-bit ones.

Hash functions are used widely in digital signatures and message authentication codes.Each cryptographic hash function should be secure against generic attacks such as collision attack. Due to Merkle-Damgård (MD) design [1, 2] theorem, if the length of input is included in the padding procedure and the IV is fixed, the hash function is collision resistant if the compression function is collision resistant. However, Joux [4] and Biham [5] proposed respectively multicollision attack and the multi-block differential on MD5, SHA-0 and SHA-1 which proved that the security of a hash function is not just rely on collision resistant compression function, but also is depended on the resistant of structure against collision attacks.

In this paper we analyze the vMDC-2 hash function recently proposed by Mazumder *et al.* [6] as an efficient construction of a compression function for

* Corresponding author.

Email addresses: `z.zolfaghari71@gmail.com` (Z. Zolfaghari), `Hamid.Asadollahi@gmail.com` (H. Asadollahi), `nbagheri@srttu.edu` (N. Bagheri)

ISSN: 2322-4460 © 2016 JComSec. All rights reserved.

cryptographic hash which is a variant of MDC-2,4 with higher efficiency-rate including a satisfactory collision security bound. The scheme is a compression function which can be used in Merkle-Damgård (MD) design approach to settle a hash function that follows the construction of MDC-2 and MDC-4 which are double block length hash functions. A double block length hash function uses an n-bit block cipher as the building block and out puts 2n-bit string as output.

The proposed scheme requires two calls of blockcipher under single iteration of encryption. Additionally, it has double key scheduling and it's operational mode is parallel. The efficiency-rate (r) of the proposed scheme is $r \approx 1$ and covers some weakness of MDC-2,4 such as symmetric property. The authors proposed a collision security bound with complexity $q = 2^{125.84}$ for the compression function without analyzing the collision resistance of the construction when it builds up to a hash function with iteration of compression functions.

Here we provide a collision attack on vMDC-2 hash function based on Joux multi collision attack which finds a collision beyond the birthday bound. The attack makes no non-standard assumptions on the underlying block cipher. Applying the attack to the vMDC-2 hash function with *e.g.*, a 128-bit block cipher the attack has complexity about 2^{70} which shows that unless the compression function of vMDC-2 is collision resistant up to $2^{125.84}$ but the iterated hash function made by this compression function is much more vulnerable to this kind of collision attack.

In this paper, we focus on the special DBL scheme with the compression function which hash a $3n$-bit string to $2n$-bit string and can make two calls to a block cipher of $2n$-bit key and n-bit block. Tandem-DM [7]and Abreast-DM are based on two calls to the same (2n, n) block ciphers which have been proposed for about two decades. If we consider 128-bit block cipher, the best collision and preimage security bounds for Abreast-DM are $2^{124.42}$ and 2^{246} queries respectively. For the same block ciphers, the best collision and preimage security bounds for Tandem-DM are $2^{120.87}$ [8] and 2^{246} queries respectively.For two different and independent $(2n, n)$ block ciphers Hirose [9] presented a class of DBL hash functions with rate 1/2 which has collision and preimage security bounds for a 128-bit block cipher, $2^{124.55}$ and 2^{251} queries respectively. Fleischmann *et al.* [10] proposed a DBL constructions known as Weimar-DM for which has collision and preimage security bounds, $2^{126.23}$ and $2^{252.5}$. MDC-2 and MDC-4 have been presented in a patent by Brachtl et al over 20 years. The collision and preimage security bounds for MDC-2 and MDC-4 are both $O(2^n)$. Recently, Mazumder *et al.* [6] proposed a variant of MDC-2, 4 with efficiency rate $r = 0.999$ and collision security bound $q = 2^{125.84}$ that has some weaknesses. In following sections, we are describing the attack on proposed scheme by Mazumder *et al.* .

Table 1 gives a comparison on MDC-2,4 and vMDC compression function and hash function collision and preimage security/attack bounds which shows this scheme is not only less secure than MDC-2 and MDC-4 but its collision finding complexity doesn't even reach to their collision security bound .

Outline. Section 2 introduces definitions. Some Technical details of the proposed scheme are given in Section 2.2. In Section 3 we provide an attack on VMDC-2 scheme. Section 4 concludes the paper.

2 Preliminaries

The collision attack presented in this article makes use of Joux's multicollision attack.

2.1 Joux's Multicollision Attack

Joux [4] proposed an efficient attack on iterated hash function which is the most amazing results in the study of generic hash functions. An iterated hash function begins from Initial Values. Then, a different compression function is applied to the original message in each chain, and the final state of all the chains gets fixed as n-bit output. Joux presented how to make a 2^k-multicollision (*i.e.*, The hash function maps all of 2^k different messages to the same hash value) by requesting $k2^{n/2}$ queries to prove that multi chains compression functions are not more secure than a single chain. The complexity of 2^k-multicollision is only slightly larger than the $2^{n/2}$ expected complexity for birthday paradox to find a pairwise collision in the underlying compression function, and much smaller than the $2^k 2^n$ expected complexity of finding such a multicollision in a random non-iterated hash function.Joux's attack first finds a pair of message locks m_1^0 and m_1^1 that collide under the compression function f when starting from the IV, *i.e.*, $f(IV, m_1^0) = f(IV, m_1^1) = h_1$. The attack now proceeds by finding a new pair of message blocks m_2^0 and m_2^1 that collide under the compression function f when starting from the intermediate hash h_1. If we carry on this procedure k times, we can end up with a set containing 2^k messages $M = m_1^{i_1} m_2^{i_2} ... m_k^{i_k} | i_j 0, 1$which all hash to the same value under the iterated hash function F^f . The cost of building the multicollision in an iterated hash function is simply k times the cost of finding a single collision in the underlying compression function f or $k2^{n/2}$.

Table 1. Comparison of MDC-2,4 and vMDC Compression and Hash Functions Collision and Preimage Security/attack Bounds.

Primitive	Collision		Preimage	
	Security	Attack	Security	Attack
f_{MDC-2}	$O(2^{n/2})$(triv)	$O(2^{n/2})$(triv)	$O(2^{n})$(triv)	$O(2^{n})$(triv)
MDC-2	$O(2^{3n/5})$[11]	$O(2^{n}/n)$ [12]	$O(2^{n})$(triv)	$O(2^{n})$ [12]
f_{MDC-4}	$O(2^{n/2})$(triv)	$O(2^{n/2})$(triv)	$O(2^{n})$(triv)	$O(2^{n})$(triv)
MDC-4	$O(2^{5n/8})$[13, 14]	$O(2^{n})$(triv)	$O(2^{n})$ (triv)	$O(2^{n})$[13, 14]
f_{vMDC-2}	$O(2^{n}/\sqrt{12})$[6]	$O(2^{n})$(triv)	$O(2^{n})$(triv)	$O(2^{n})$(triv)
vMDC-2	$O(2^{n/2})$(triv)	$O(\frac{n}{2}2^{n/2})$(Our attack)	$O(2^{n})$(triv)	$O(2^{2n})$(triv)

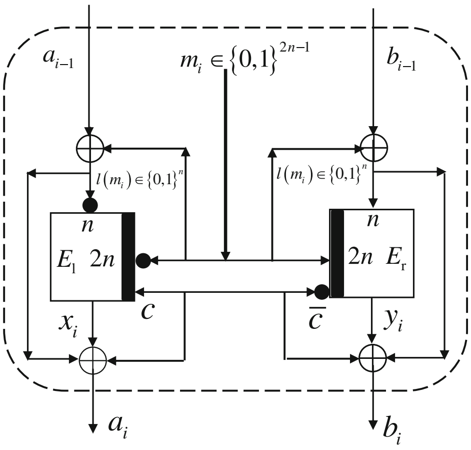


Figure 1. vMDC-2 Construction (A Variant of MDC-2,4)

2.2 Description of vMDC-2 Construction

Usually, there are two methods for increasing efficiency-rate. The first is using three calls of blockcipher. The second is using a pair of chaining values which are containing message in the two blockciphers. Such kind of these methods are used in MDC-2, MDC-4 and variant of MDC-2. Mazumder *et al.* [6] presented a construction that came from the construction of MDC-2 and MDC-4. In proposed scheme, two chaining values are used as input and message is common for two block ciphers which compresses $4n$ bits into $2n$ bits. Some changes are presented in the proposed scheme such as each block cipher uses one constant bit 0 and 1 as one bit of the key for the considered scheme. Figure. 1

Definition 1. let E be a block cipher that is taken from a set of Ideal Block Cipher with k-bit key and n-bit block length that $E_{l,r} = \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$. $E^{dbl} = \{0,1\}^k \times \{0,1\}^{2n} \rightarrow \{0,1\}^{2n}$ is defined as a double block length (dbl) cipher and parallel calling of two independent block ciphers of E_l, E_r such that, [6]

$$x_i = E_l, (\overline{m_i}\|c)\overline{(a_{i-1} \oplus l(m_i))} \tag{1}$$

$$y_i = E_r, (m_i\|\overline{c})(b_{i-1} \oplus l(m_i)) \tag{2}$$

Where $m_i \in \{0,1\}^{2n-1}, (a,b,x,y) \in \{0,1\}^n$ and $l(m_i) = lsb$ of $m_i \in \{0,1\}^n, c = 1$. Thus, the final output is $f_E(a_i, b_i)$ where:

$$a_i = x_i \oplus (a_{i-1} \oplus l(m_i)) \oplus c \tag{3}$$

$$b_i = y_i \oplus (b_{i-1} \oplus l(m_i)) \oplus \overline{c} \tag{4}$$

Definition 2. let $f_E = \{0,1\}^k \times \{0,1\}^{2n} \rightarrow \{0,1\}^{2n}$ be a blockcipher based compression function such as $(a_i, b_i, m_i) = f(a_i, b_i, m_i)$, where, $a_i \in \{0,1\}^n, b_i \in \{0,1\}^n$,$m_i \in \{0,1\}^{2n-1}$, and $c_i \in \{0,1\}$. Therefore, f_E contains ideal block cipher (E) such as: [6]

$$\left\{\begin{array}{l} a_i = f_l(\overline{a_{i-1} \oplus l(m_i)}, \overline{m_i}\|c) \oplus (a_{i-1} \oplus l(m_i)) \oplus c \leftarrow \\ E_l(\overline{a_{i-1} \oplus l(m_i)}, \overline{m_i}\|c) \oplus (a_{i-1} \oplus l(m_i)) \oplus c \end{array}\right\} \tag{5}$$

$$\left\{\begin{array}{l} b_i = f_r(b_{i-1} \oplus l(m_i), \overline{m_i}\|\overline{c}) \oplus (b_{i-1} \oplus l(m_i)) \oplus \overline{c} \leftarrow \\ E_r(b_{i-1} \oplus l(m_i), m_i\|\overline{c}) \oplus (b_{i-1} \oplus l(m_i)) \oplus \overline{c} \end{array}\right\} \tag{6}$$

3 The Multicollision Attack

This chapter fully describes our attack on the vMDC-2 construction. As shown in Figure 2 vMDC-2 is a construction which has two pipes, each pipe is separated from another one. For example we can apply M_i to i-th iteration and get $H_{i+1} = E(H_i, M_i)$ without interference of $\tilde{H}_i$. So the independence of left and right pipes lets us to put Joux attack on one pipe and use the multicollision results to query on the other

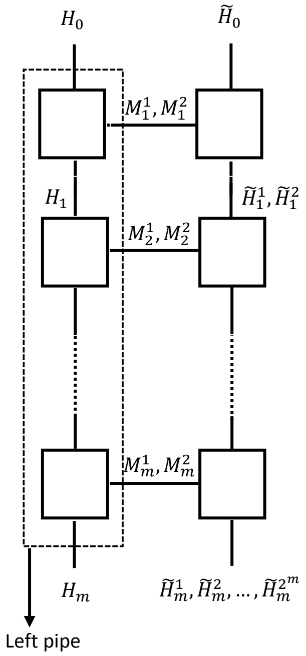

H_0
$\tilde{H}_0$
M_1^1, M_1^2
H_1
$\tilde{H}_1^1, \tilde{H}_1^2$
M_2^1, M_2^2
M_m^1, M_m^2
H_m
$\tilde{H}_m^1, \tilde{H}_m^2, \ldots, \tilde{H}_m^{2^m}$
Left pipe

Figure 2. The Generalized vMDC-2 Construction

pipe. Without loss of generality we use Joux attack to find Multicollision on the left pipe and finalize the attack by computing the probability and complexity of finding collision from m-ouputs of right pipe with single output of left pipe.So the attack is as follows:

First, we assume that the construction is composed of two independent pipes similar to Figure 2, then our attack follows this procedure:

(1) Let consider $H_0, \tilde{H}_0$ as an initial chaining value of hash function.

(2) find two different messages and set H_1 in such a way that

$$H_1 = f(H_0, M_1^1) = f(H_0,, M_1^2) \qquad (7)$$

Note that concurrently two outputs are generated in the right pipe.

(3) for i from 2 to m repeat step 2 by considering the output of each round as an input for next round, such that

$$H_2 = f(H_1, M_2^1) = f(H_1,, M_2^2) \qquad (8)$$

$$H_i = f(H_{i-1}, M_i^1) = f(H_{i-1},, M_i^2) \qquad (9)$$

(4) continue up to round m and output 2^m values

For each round with $2^{n/2}$ we can find a collision then by Joux's attack we can find $2^m.2^{n/2}$ collisions by $m2^{n/2}$ queries. On the other pipe we have $\tilde{H}_m^1 \tilde{H}_m^2, \ldots, \tilde{H}_m^{2^m}$ as the outputs which according to Birthday paradox we can have a collision by more than $2^{n/2}$ outputs, then:

$$\text{if} \quad 2^m = 2^{n/2} \Rightarrow collisionfound \Rightarrow m = n/2 \quad (10)$$

If we set $n = 128$ then for $m = 64$ we have found a collision by $m2^{n/2} = 64(2^{64}) = 2^{70}$ by probability of 1/2.

Thus for a $n = 128$ bit block the adversary could find a collision in 2^{70} queries with probability 0.5 for the hash function.

4 Conclusion

In this paper we presented the first collision attack on the vMDC-2 construction proposed by Mazumder *et al.* [6] having time complexity much less than a birthday attack. The attack applies to other constructions similar to vMDC-2, and does not rely on weaknesses of the underlying block cipher. We proposed multicollision attack for finding collision's game with time complexity $O(n/2 \times 2^{n/2})$ which finds a collision for this hash function in time complexity of 2^{70}.

Acknowledgements

This work was supported by Shahid Rajaee Teacher Training University.

References

[1] Ralph C. Merkle. One Way Hash Functions and DES. In *Advances in Cryptology — CRYPTO' 89 Proceedings*, pages 428–446. Springer New York, 1990. ISBN 978-0-387-34805-6. doi:10.1007/0-387-34805-0_40.

[2] Ivan Bjerre Damgård. A Design Principle for Hash Functions. In *Advances in Cryptology — CRYPTO' 89 Proceedings*, pages 416–427. Springer New York, 1990. ISBN 978-0-387-34805-6. doi:10.1007/0-387-34805-0_39.

[3] Bart Preneel, René Govaerts, and Joos Vandewalle. Hash functions based on block ciphers: a synthetic approach. In *Advances in Cryptology — CRYPTO' 93*, pages 368–378, Berlin, Heidelberg, 1994. Springer Berlin Heidelberg. ISBN 978-3-540-48329-8. doi:10.1007/3-540-48329-2_31.

[4] Antoine Joux. Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions. In *Advances in Cryptology – CRYPTO 2004*, pages 306–316. Springer Berlin Heidelberg, 2004. ISBN 978-3-540-28628-8. doi:10.1007/978-3-540-28628-8_19.

[5] Eli Biham, Rafi Chen, Antoine Joux, Patrick Carribault, Christophe Lemuet, and William Jalby. Collisions of SHA-0 and Reduced SHA-1. In *Ad-*

vances in Cryptology – EUROCRYPT 2005*, pages 36–57. Springer Berlin Heidelberg, 2005. ISBN 978-3-540-32055-5. doi:10.1007/11426639_3.

[6] Rashed Mazumder, Atsuko Miyaji, and Chunhua Su. An Efficient Construction of a Compression Function for Cryptographic Hash. In *Availability, Reliability, and Security in Information Systems*, pages 124–140. Springer International Publishing, 2016. ISBN 978-3-319-45507-5. doi:10.1007/978-3-319-45507-5_9.

[7] Xucjia Lai and James L. Massey. Hash Functions Based on Block Ciphers. In *Advances in Cryptology — EUROCRYPT' 92*, pages 55–70, Berlin, Heidelberg, 1993. Springer Berlin Heidelberg. ISBN 978-3-540-47555-2. doi:10.1007/3-540-47555-9_5.

[8] Jooyoung Lee, Martijn Stam, and John Steinberger. The Collision Security of Tandem-DM in the Ideal Cipher Model. In *Advances in Cryptology – CRYPTO 2011*, pages 561–577. Springer Berlin Heidelberg, 2011. ISBN 978-3-642-22792-9. doi:10.1007/978-3-642-22792-9_32.

[9] Shoichi Hirose. Some Plausible Constructions of Double-Block-Length Hash Functions. In *Fast Software Encryption*, pages 210–225, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg. ISBN 978-3-540-36598-3. doi:10.1007/11799313_14.

[10] Ewan Fleischmann, Christian Forler, Stefan Lucks, and Jakob Wenzel. Weimar-DM: A Highly Secure Double-Length Compression Function. In *Information Security and Privacy*, pages 152–165, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg. ISBN 978-3-642-31448-3. doi:10.1007/978-3-642-31448-3_12.

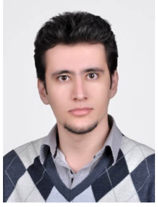
[11] John P. Steinberger. The Collision Intractability of MDC-2 in the Ideal-Cipher Model. In Moni Naor, editor, *Advances in Cryptology - EUROCRYPT 2007*, pages 34–51. Springer Berlin Heidelberg, 2007. ISBN 978-3-540-72540-4. doi:10.1007/978-3-540-72540-4_3.

[12] Lars R. Knudsen, Florian Mendel, Christian Rechberger, and Søren S. Thomsen. Cryptanalysis of MDC-2. In *Advances in Cryptology - EUROCRYPT 2009*, pages 106–120. Springer Berlin Heidelberg, 2009. ISBN 978-3-642-01001-9. doi:10.1007/978-3-642-01001-9_6.

[13] Bart Mennink. On the collision and preimage security of MDC-4 in the ideal cipher model. *Designs, Codes and Cryptography*, 73(1):121–150, Oct 2014. ISSN 1573-7586. doi:10.1007/s10623-013-9813-8.

[14] Ewan Fleischmann, Christian Forler, and Stefan Lucks. The Collision Security of MDC-4. In *Progress in Cryptology - AFRICACRYPT 2012*, pages 252–269. Springer Berlin Heidelberg, 2012. ISBN 978-3-642-31410-0. doi:10.1007/978-3-642-31410-0_16.

Zahra Zolfaghari holds a M.Sc. in Communication Systems from Electrical Engineering Department, Shahid Rajaee Teacher Training University, Tehran, Iran. Her research interest includes cryptology and network security.



Hamid Asadollahi holds a M.Sc. in Communication Systems from Electrical Engineering Department, Shahid Rajaee Teacher Training University, Tehran, Iran. His research interest includes cryptology and network security.

Nasour Bagheri is an associate professor at Electrical Engineering Department, Shahid Rajaee Teacher Training University, Tehran, Iran. He is the author of over 80 articles in information security and cryptology. A record of his publications is available at google scholar.