New Pseudo-Near-Collision Attack on Reduced-Round of Hamsi-256*

Meiqin Wang[1], Xiaoyun Wang[2], Keting Jia[1], Wei Wang[1]

[1] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan 250100, China
[2] Institutate of Advanced Study, Tsinghua University, Beijing 100084, China
{mqwang, xywang}@sdu.edu.cn, ktjia@mail.sdu.edu.cn

Abstract. Hamsi-256 is designed by Özgül Kücük and it has been a candidate Hash function for the second round of SHA-3. The compression function of Hamsi-256 maps a 256-bit chaining value and a 32-bit message to a new 256-bit chaining value. As hashing a message, Hamsi-256 operates 3-round except for the last message it operates 6-round. In this paper, we will give the pseudo-near-collision for 5-round Hamsi-256. By the message modifying, the pseudo-near-collision for 3, 4 and 5 rounds can be found with 2^5, 2^{32} and 2^{125} compression function computations respectively.

Keywords: hash functions, SHA-3, near collision

1 Introduction

Hamsi[2] is one of the 14 candidate Hash functions in the second round of SHA-3 competition and it is designed by Özgül Kücük. Hamsi includes four kinds of Hash functions, Hamsi-224, Hamsi-256, Hamsi-384 and Hamsi-512.

Ivica Nikolić presented the pseudo-near-collision attack for 3-round Hamsi-256 with the difference in the chaining value instead of the message. However, the pseudo-near-collision attack doesn't produce any essential effect on the security of Hamsi-256. Therefore we try to extend the attack on 6-round Hamsi-256 and this attack can incur the related-key attack on the MAC based on Hamsi-256. As a result, the 5-round pseudo-near-collision for Hamsi-256 with the difference only in the chaining value has been found.

This paper is organized as follows: Sect. 2 briefly details the Hamsi-256 Hash function; Sect. 3 presents our pseudo-near-collision attack on reduced-round of Hamsi-256.

2 The Hamsi-256 Hash Function

Hamsi-256 is one of the 14 candidate Hash functions of the second round SHA-3 competition. Hamsi uses the Concatenate-Permute-Truncate design strategy, and another important design strategy is the special message expansion function. For the Hamsi-256, the input includes a 256-bit chaining value and a 32-bit message, the compression function operates 3-round non-linear round function, and for the last message, the compression function contains 6-round non-linear round function. Firstly the 32-bit message is expanded to 256-bit, concatenate the expanded message and the initial chaining value to produce 512-bit state, operate a 3-round non-linear round function, and truncate the 512-bit state to produce 256-bit output value.

* Supported by 973 Program of China (Grant No.2007CB807902) and National Outstanding Young Scientist fund of China (Grant No. 60525201).

3 Pseudo-Near-Collision for Reduced-Round of Hamsi-256

First, we identify the new pseudo-near-collision for 3-round Hamsi-256 compression function with 23-bit hamming distance. Compared with the pseudo-near-collision in [1], the hamming distance is reduced by 2 bits. Secondly, we further identify such pseudo-near-collision for 4-round and 5-round Hamsi-256 compression function with the probability 2^{-63} and 2^{-156}. Although the probability for the 5-round pseudo-near-collision is less than 2^{-128}, By modifying the input chaining value and the message value to satisfy some conditions, the time complexity can be reduced to 2^{-125}.

3.1 Pseudo-Near-Collision for 3-Round Hamsi-256

Ivica Nikolić presented a pseudo-near-collision for 3-round Hamsi-256 with the probability 2^{-23} and the hamming distance 25-bit. By analyzing the diffusion properties for the 3-round Hamsi-256, we identify another pseudo-near-collision for 3-round Hamsi-256 with the probability 2^{-23} and the hamming distance 23-bit in Table 1.

Table 1. Pseudo-Near-Collision Path for 3-Round Hamsi-256

R		Difference				Pr
R_1	I			2,11		
		2,21	17,24,27,31			
				2,11		
		2,21	17,24,27,31			
	Sbox			11		2^{-23}
		2				
		21	31			
			17,24,27	2		
	Diffusion					1
			24			
			24			
R_2	Sbox					2^{-3}
			24			
	Diffusion	30				1
			25			
R_3	Sbox		25			2^{-5}
		30	25			
		30				
	Diffusion	31	10,11,12,21		4	1
		31	26	7		
					4,6,27	
		5,16				
Truncation and FeedBack		2,11,31	10,11,12,21	2,21	4,17,24,27,31	1
		2,11		2,21	4,6,17,24,21	

3.2 Pseudo-Near-Collision for 4-Round Hamsi-256

We further extend the above 3-round differential to 4-round, so the pseudo-near-collision for 4-round Hamsi-256 with the probability 2^{-63} and the hamming distance 53-bit in Table 2.

Table 2. Pseudo-Near-Collision Path for 4-Round Hamsi-256

R		Difference				Pr
R_1	I			2,11		
		2,21	17,24,27,31			
				2,11		
		2,21	17,24,27,31			
	Sbox			11		2^{-23}
		2				
		21	31			
			17,24,27	2		
	Diffusion					1
			24			
			24			
R_2	Sbox					2^{-3}
			24			
	Diffusion	30				1
			25			
R_3	Sbox		25			2^{-5}
		30	25			
		30				
	Diffusion	31	10,11,12,21		4	1
		31	26	7		
					4,6,27	
		5,16				
R_4	Sbox	5,16	26	7		2^{-32}
		31	10,11,12,21,26	7	6,27	
		5,16	10,11,12,21		4,6,27	
	Diffusion	0,1,2,3,7,17,23,24,27	12,17,22,28	3,12,22,23,24,25,26	5	1
		0	11,12,13,19,22,27,30		7,21,28	
		4,7,8,9,20	29	1,3,8,9,10,16,18,19,24	2,7,13	
		12,17,23	17,18,19,28,30		2,11,13,28	
Truncation and FeedBack		0,1,3,7,11,17,23,24,27	12,17,22,28	2,3,12,21,22,23,24,25,26	5,17,24,27,31	1
		2,4,7,8,9,11,20	29	1,2,3,8,9,10,16,18,19,21,24	2,7,13,17,24,27,31	

3.3 Pseudo-Near-Collision for 5-Round Hamsi-256

We further extend the above 4-round differential to 5-round, so the pseudo-near-collision for 5-round Hamsi-256 with the probability 2^{-156} and the hamming distance 111-bit. In Table 3, we only present the output difference from the 4^{th} round to the 5^{th} round, and the final output difference of the feedback and truncation operation.

Table 3. Pseudo-Near-Collision Path for 5-Round Hamsi-256

R		Difference				Pr
R_4	Sbox	5,16	26	7		2^{-32}
		31	10,11,12,21,26	7	6,27	
		5,16	10,11,12,21		4,6,27	
	Diffusion	0,1,2,3,7,17,23,24,27	12,17,22,28	3,12,22,23,24,25,26	5	1
		0	11,12,13,19,22,27,30		7,21,28	
		4,7,8,9,20	29	1,3,8,9,10,16,18,19,24	2,7,13	
		12,17,23	17,18,19,28,30		2,11,13,28	
R_5	Sbox	0,12	11,12,13,18,22,27	3,24	2,11,13,21	2^{-93}
		1, 2, 3, 4, 7, 8, 9, 12, 20, 24, 27	11,13,18,19,27,29,30	1, 8, 9, 10, 12, 16, 18, 19, 22, 23, 25, 26	2, 5, 7, 11, 13, 21, 28	
		1,2,3,24,27	18	12,22,23,25,26	5,11	
		1, 2, 3, 4, 8, 9, 12, 17, 20, 23, 24, 27	17,19,28,29,30	1, 8, 9, 10, 12, 16, 18, 19, 22, 23, 25, 26	2, 5, 13, 28	
	Diffusion	0, 1, 2, 4, 5, 6, 8, 9, 14, 18, 21, 24, 27, 28, 30	0, 3, 5, 7, 20, 21, 22, 23, 25, 26, 28, 29, 31	1, 2, 4, 7, 9, 11, 12, 13, 16, 18, 19, 20, 21, 22, 27, 29	0, 2, 3, 5, 6, 7, 10, 14, 15, 17, 18, 22, 24, 26, 27, 28, 29	1
		2, 4, 5, 8, 9, 10, 13, 16, 21, 22, 27, 28	12, 16, 19, 20, 27, 28, 29, 31	0, 2, 4, 9, 10, 11, 13, 15, 17, 19, 20, 23, 24, 25	3, 5, 6, 7, 8, 12, 14, 17, 22, 28, 29, 31	
		0, 1, 4, 9, 11, 17, 19, 20, 24, 25, 27, 28	1, 9, 10, 11, 16, 20, 22, 23, 24, 26, 30, 31	2, 5, 9, 10, 12, 15, 17, 18, 19, 22, 23, 25, 26, 31	0, 3, 4, 7, 9, 10, 11, 12, 16, 25, 26, 29	
		3, 4, 8, 9, 10, 11, 13, 16, 18, 19, 21, 24, 27, 30, 31	2, 3, 4, 11, 12, 13, 15, 24	0, 1, 2, 4, 8, 12, 15, 16, 17, 19, 23, 26, 28, 29, 30	0, 1, 3, 4, 9, 12, 20, 22, 23	
Truncation and FeedBack		0, 1, 4, 5, 6, 8, 9, 11, 14, 18, 21, 24, 27, 28, 30	0, 3, 5, 7, 20, 21, 22, 23, 25, 26, 28, 29, 31	1, 4, 7, 9, 11, 12, 13, 16, 18, 19, 20, 22, 27, 29	0, 2, 3, 5, 6, 7, 10, 14, 15, 18, 22, 26, 28, 29, 31	1
		0, 1, 2, 4, 9, 17, 19, 20, 24, 25, 27, 28	1, 9, 10, 11, 16, 20, 22, 23, 24, 26, 30, 31	5, 9, 10, 12, 15, 17, 18, 19, 21, 22, 23, 25, 26, 31	0, 3, 4, 7, 9, 10, 11, 12, 16, 17, 24, 25, 26, 27, 29, 31	

Message Modifying:

In the differential path of the 5-round pseudo-near-collision, there are 23 conditions in the first round, among which the below 15 conditions can be satisfied by modifying the message,

$$\begin{array}{l} {s^0}_{0,2} = 1, {s^0}_{8,2} = 0, {s^0}_{0,21} = 1, {s^0}_{8,21} = 1, {s^0}_{1,31} = 1, {s^0}_{9,31} = 1, {s^0}_{1,17} = 1, {s^0}_{9,17} = 0, \\ {s^0}_{1,24} = 1, {s^0}_{9,24} = 0, {s^0}_{1,27} = 1, {s^0}_{9,27} = 0, {s^0}_{6,2} = 1, {s^0}_{14,2} = 0, {s^0}_{6,11} = 1. \end{array} \quad (1)$$

where ${s^i}_{j,k}$ represents the k^{th} bit variable of the j^{th} word for the input of the i^{th} round.

By searching 2^{15} messages, there are averagely one message satisfying the above 15 conditions, then we fix the message. The remained below 8 conditions can be satisfied by modifying the chaining value,

$$\begin{array}{l} {s^0}_{4,2} = {s^0}_{12,2}, {s^0}_{4,21}! = {s^0}_{12,21}, {s^0}_{5,31}! = {s^0}_{13,31}, {s^0}_{5,17}! = {s^0}_{13,17}, \\ {s^0}_{5,24}! = {s^0}_{13,24}, {s^0}_{5,27}! = {s^0}_{13,27}, {s^0}_{2,2} = {s^0}_{10,2}, {s^0}_{2,11}! = {s^0}_{10,11}. \end{array} \quad (2)$$

We can identify 2^{15} structures satisfying the above 8 conditions, each with the fixed value in the above related 16-bit input chaining variables and any value for others bits.

There are 3 conditions in the third round as follows,

$${s^1}_{1,24} = 0, {s^1}_{5,24} = 1, {s^1}_{9,24} = {s^1}_{13,24}. \quad (3)$$

${s^1}_{1,24}$ is related to the following 28 bits input of the first round,

$${s^0}_{4i,12}, {s^0}_{4i+1,5}, {s^0}_{4i+1,6}, {s^0}_{4i+1,28}, {s^0}_{4i+2,18}, {s^0}_{4i+3,9}, {s^0}_{4i+3,15}, (0 \le i \le 3). \quad (4)$$

which includes 14-bit chaining variables and 14-bit expanded messages. In order to make the input chaining value of the first round satisfying the conditions, there should be 2^{13} structures, each with the fixed value in the above related 14-bit input chaining variables and any value for others bits. ${s^1}_{5,24}$ is related to the following 12 bits input of the first round,

$${s^0}_{4i,10}, {s^0}_{4i+1,23}, {s^0}_{4i+2,20}, (0 \le i \le 3). \quad (5)$$

which includes 6-bit chaining variable and 6-bit expanded messages. There should be 2^5 structures, each with the fixed value in the above related 6-bit input chaining variables and any value for others bits.

${s^1}_{9,24}$ and ${s^1}_{13,24}$ are related to the following 28 bits input of the first round,

$${s^0}_{4i,14}, {s^0}_{4i+1,17}, {s^0}_{4i+1,24}, {s^0}_{4i+1,31}, {s^0}_{4i+2,1}, {s^0}_{4i+2,27}, {s^0}_{4i+3,11}, (0 \le i \le 3). \quad (6)$$

which includes 14-bit chaining variables and 14-bit expanded messages. There should be 2^{13} structures, each with the fixed value in the above related 16-bit input chaining variables and any value for others bits.

If we choose the value of the above $16+14+6+14 = 50$ bits input chaining variables from these structure, the conditions in the first round and the second round have been satisfied.

There are five conditions for the input of the third round as follows,

$${s^2}_{4,30} = 1, {s^2}_{8,30} = 0, {s^2}_{12,30} = 1, {s^2}_{1,25} = {s^2}_{9,25}, {s^2}_{1,25} = {s^2}_{13,25}. \quad (7)$$

There are seven variables involved in the above five conditions. However, we found that 48 input bits of the first round are still unrelated to any of the above seven chaining variables. Among them, 24-bit is the input chaining variable and 24-bit is the expanded message variables, and here we only list 24-bit input chaining variable as follows,

$$\begin{array}{l} {s^0}_{2,5}, {s^0}_{2,7}, {s^0}_{2,11}, {s^0}_{2,13}, {s^0}_{2,17}, {s^0}_{2,31}, {s^0}_{3,6}, {s^0}_{3,8}, {s^0}_{4,0}, {s^0}_{4,7}, {s^0}_{5,2}, {s^0}_{5,12}, \\ {s^0}_{10,5}, {s^0}_{10,7}, {s^0}_{10,11}, {s^0}_{10,13}, {s^0}_{10,17}, {s^0}_{10,31}, {s^0}_{11,6}, {s^0}_{11,8}, {s^0}_{12,0}, {s^0}_{12,7}, {s^0}_{13,2}, {s^0}_{13,12}, \end{array} \quad (8)$$

It means that the conditions in the third round are related to $256-24 = 232$ input chaining variables of the first round. In modifying the conditions of the first round and the second round, 52-bit input chaining variables have been given the value, so other $232 - 50 = 182$ bits variables can be used to further modify the five conditions in the third round. Among 2^5 values for them, there is averagely one value satisfying the five conditions. We need to identify 2^{101} values satisfying the five conditions. When I identify one value, we can further choose the value for the above unrelated 24-bit input variables. In total, there should be $2^{101} \cdot 2^{24} = 2^{125}$ input values satisfying the conditions from the first round to the third round. Due to the probability of the differential path from the fourth round to the fifth round is $2^{-32} \cdot 2^{-93} = 2^{-125}$, on average there should be one value satisfying the 5-round differential path.

The detailed modifying process is as follows,

Step 1: Search 2^{15} messages and identify one message satisfying the 15 conditions in equations (1). Fix the message value.
Step 2: Set the value of 16-bit input chaining variables involved in equations (2) to satisfy the 8 conditions in equation (2).
Step 3: Search 2 values for the 14-bit in equation (4) and identify one values satisfying the first condition in equation (3).
Step 4: Search 2 values for the 6-bit in equation (5) and identify 2 values satisfying the second condition in equation (3).
Step 5: Search 2 values for the 14-bit in equation (6) and identify 2 values satisfying the third condition in equation (3).
Step 6: Search 2^5 values for the 182-bit variable(described in the above paragraph) and identify one value satisfying the five conditions in equation (7).
Step 7: Search 2^{24} values for the 24-bit in equation (8) and compute the compressive value of the 5-round, verify if it is a near collision. If not, go to Step 6.

The time complexity for searching the 5-round Hamsi-256 pseudo-near-collision is about $2^{101} \cdot (2^5 + 2^{24}) \approx 2^{125}$ 5-round Hamsi-256 implementations.

With the modifying process, the time complexity for searching the 3-round Hamsi-256 pseudo-near-collision is about 2^5 3-round Hamsi-256 computations and 2^{15} message expansion computations, and the time complexity for searching the 4-round Hamsi-256 pseudo-near-collision is about $2^8 \cdot (2^5 + 2^{24}) = 2^{32}$ 4-round Hamsi-256 computations.

References

1. Ivica Nikolić, Near Collisions for the Compression Function of Hamsi-256, CRYPTO'2009 rump session, http://rump2009.cr.yp.to/936779b3afb9b48a404b487d6865091d.pdf, 2009.
2. Özgül Kücük, The Hash function Hamsi, Submission to NIST, 2008.