Preliminary Analysis of DHA-256*

IAIK Krypto Group

Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology, Austria
http://www.iaik.tugraz.at/research/krypto/

Abstract. DHA-256 was presented at the Cryptographic Hash Workshop hosted by NIST in November 2005. DHA-256 (Double Hash Algorithm) was proposed to enhance the security of SHA-256. We present a preliminary analysis of the message expansion and give an alternative 9-step local collision for DHA-256.

1 Short Description of DHA-256

The structure of DHA-256 [1] is very similar to the one of SHA-256. The differences are a modified message expansion and a modified state update. The main difference is that the expanded message words are used twice in each step of the state update, therefore the name Double Hash Algorithm.

The message expansion is defined as follows:

$$\begin{aligned} W_i &= M_i \quad 0 \le i \le 15 \\ W_i &= \sigma_1(W_{i-1}) + W_{i-9} + \sigma_2(W_{i-15}) + W_{i-16} \quad 16 \le i \le 63 \ , \end{aligned}$$

where $\sigma_1(x) = x \oplus (x \ll 7) \oplus (x \ll 22)$ and $\sigma_2(x) = x \oplus (x \ll 13) \oplus (x \ll 27)$.

The i-th step of the state update is defined as follows:

$$\begin{aligned} H_{i+1} &= A_i + SS_1(D_i) + f(B_i, C_i, D_i) + W_i + K_i \\ B_{i+1} &= C_i \ll 17 \\ D_{i+1} &= E_i + SS_2(H_i) + g(F_i, G_i, H_i) + W_i + K_i \\ F_{i+1} &= G_i \ll 2 \\ A_{i+1} &= B_i \\ C_{i+1} &= D_i \\ E_{i+1} &= F_i \\ G_{i+1} &= H_i \ , \end{aligned}$$

where $SS_1(x) = x \oplus (x \ll 11) \oplus (x \ll 25)$ and $SS_2(x) = x \oplus (x \ll 19) \oplus (x \ll 29)$. The functions $f(x, y, z)$ and $g(x, y, z)$ correspond to the functions $CH(x, y, z)$ and $MAJ(x, y, z)$ of SHA-256 [2]. Also the IVs are the same as for SHA-256.

* The work in this paper has been supported by the Austrian Science Fund (FWF), project P18138.

2 Message Expansion of DHA-256

For the analysis of the message expansion we replace the modular additions by XOR-operations. We search for low-weight differences from step 24 to step 55 by using algorithms from coding theory. The difference with the smallest weight found for the linearized message expansion is given in Table 1. For 32 steps (from step 24 to step 55) we find a minimum weight of 10. In [1] a weight of 63 is presented. The low-weight difference vector given in Table 1 is also valid for the message expansion with the modular additions left in place.

Table 1. 32-step difference for the message expansion of DHA-256.

step	W_i	step	W_i
$i = 24$	0x00000000	$i = 40$	0x00000000
$i = 25$	0x00000000	$i = 41$	0x00000000
$i = 26$	0x00000000	$i = 42$	0x00000000
$i = 27$	0x00000000	$i = 43$	0x00000000
$i = 28$	0x00000000	$i = 44$	0x00000000
$i = 29$	0x00000000	$i = 45$	0x00000000
$i = 30$	0x00000000	$i = 46$	0x00004000
$i = 31$	0x00000000	$i = 47$	0x00000000
$i = 32$	0x00000000	$i = 48$	0x00000000
$i = 33$	0x00000000	$i = 49$	0x00000000
$i = 34$	0x00000000	$i = 50$	0x00000000
$i = 35$	0x00000000	$i = 51$	0x00000000
$i = 36$	0x00000000	$i = 52$	0x08004200
$i = 37$	0x00004000	$i = 53$	0x00004000
$i = 38$	0x00204010	$i = 54$	0x00000000
$i = 39$	0x00000000	$i = 55$	0x00004000
total Hamming weight for 32 steps: 10			

3 9-Step Local Collision for DHA-256

In [1] the authors provide a 9-step local collision, also referred to as *inner collision pattern*, that leads to a real (with modular addition) 9-step collision with probability 2^{-64}. After the introduction of the 1-bit difference W_i (disturbance) the correction pattern in [1] is defined as shown in Table 2.

The given complexity of 2^{-64} corresponds to a disturbance in the MSB, *i.e.* $W_i =$ 0x80000000. In order to construct a 9-step local collision with the pattern given in Table 2 it is required that input differences to the functions f and g are 'blocked', *i.e.* conditions are set such that a input difference does not propagate through f and g. However, this differential property can not always be guaranteed. For instance if the input difference to f is $B'_{i,j} = 0$, $C'_{i,j} = 1$, and $D'_{i,j} = 1$ the output difference of f is always 1. According to our computations,

Table 2. Disturbance and correction pattern for a 9-step local collision given in [1].

step	**input**	**description**
i	W_i	1-bit disturbance
$i+1$	$W_{i+1} = 0$	
$i+2$	$W_{i+2} = SS_2(SS_1(W_i))$	correction
$i+3$	$W_{i+3} = 0$	
$i+4$	$W_{i+4} = 0$	
$i+5$	$W_{i+5} = SS_1(W_i \ll 17) \oplus SS_2(W_i \ll 2)$	correction
$i+6$	$W_{i+6} = 0$	
$i+7$	$W_{i+7} = 0$	
$i+8$	$W_{i+8} = W_i \ll 19$	correction

this situation occurs exactly in step $i+2$ where the difference in bit position 31 of both chaining variables C_{i+2} and D_{1+2} is 1. Hence the output difference of f in bit position 31 will be 1 too. This difference propagates to H_{i+3} with probability one and we cannot correct it anymore. Despite this fact, also in step $i+5$ the correction has to be different, namely $SS_1(W_i \ll 2) \oplus SS_2(W_i \ll 17)$.

However, with some modification we can construct a 9-step local collision. Since we cannot avoid a difference in bit position 31 at the output of the f function in step $i+2$, we have to cancel it out with a difference in W_{i+2}. Since this difference occurs in bit position 31 we can cancel it out with probability one. Our 9-step local collision is given in Table 3 with the probability of each step. The probability of the 9-step local collision for DHA-256 is 2^{-63}.

Table 3. Correct disturbance-correction pattern for DHA-256.

step	**input**	**probability**	**description**
i	W_i	1	1-bit disturbance
$i+1$	$W_{i+1} = 0$	2^{-6}	
$i+2$	$W_{i+2} = SS_2(SS_1(W_i)) \oplus W_i$	2^{-21}	correction
$i+3$	$W_{i+3} = 0$	2^{-8}	
$i+4$	$W_{i+4} = 0$	2^{-8}	
$i+5$	$W_{i+5} = SS_1(W_i \ll 2) \oplus SS_2(W_i \ll 17)$	2^{-14}	correction
$i+6$	$W_{i+6} = 0$	2^{-2}	
$i+7$	$W_{i+7} = 0$	2^{-2}	
$i+8$	$W_{i+8} = W_i \ll 19$	2^{-2}	correction
	total probability	$\mathbf{2^{-63}}$	

4 Conclusion

We have presented a preliminary analysis of DHA-256 by looking at the message expansion and a 9-step local collision. We presented a low-weight difference

for the linearized message expansion with weight 10. Furthermore, we gave an alternative 9-step local collision with probability 2^{-63}, which is higher than the probability for the local collision given by the designers of DHA-256. This is work in progress.

References

1. Jesang Lee, Donghoon Chang, Hyun Kim, Eunjin Lee, Deukjo Hong, Jaechul Sung, Seokhie Hong, Sangjin Lee. A New 256-bit Hash Function DHA-256 : Enhancing the Security of SHA-256, Presented at the Cryptographic Hash Workshop hosted by NIST, November 2005. Available online at `http://www.csrc.nist.gov/pki/HashWorkshop/2005/Nov1_Presentations/ChangD_DHA256.pdf`.
2. National Institute of Standards and Technology. Secure Hash Standard (SHS). FIPS 180-2, August 2002.