

Related-Key Rectangle Attack of the Full HAS-160 in Encryption Mode

Orr Dunkelman¹, Ewan Fleischmann², Michael Gorski², and Stefan Lucks²

¹ Ecole Normale Supérieure, France

Orr.Dunkelman@ens.fr

² Bauhaus-University Weimar, Germany

{Ewan.Fleischmann, Michael.Gorski, Stefan.Lucks}@uni-weimar.de

Abstract. In this paper we investigate the security of the compression function of HAS-160 in encryption mode. The structure of HAS-160 is similar to SHA-1 besides some modifications. This is the first cryptographic attack that breaks the encryption mode of the full 80-round HAS-160.

We apply a key recovery attack that requires 2^{157} chosen plaintexts and $2^{377.5}$ 80-round HAS-160 encryptions. The attack does not aim for a collision, preimage or 2nd-preimage attack, but it shows that HAS-160's compression function used as a block cipher is not an ideal cipher.

Keywords: differential cryptanalysis, related-key rectangle attack, HAS-160.

1 Introduction

HAS-160 is a hash function that is widely used by the Korean industry, due to its standardization by the Korean government (TTAS.KO-12.0011/R1) [1]. Based on the MERKLE-DAMGÅRD structure [9, 17], it uses a compression function with input size of 512 bits and a chaining and output value of 160 bits. HAS-160 consists of a round function which is applied 80 times for each input message block. The overall design of the compression function is similar to the design of SHA-1 [18] and the MD family [19, 20], except a few modifications in the rotation constants and in the message expansion.

Up to now there are only a few cryptographic results on HAS-160. Yun et al. [24] found a collision on 45-round HAS-160 with complexity 2^{12} by using the techniques introduced by Wang et al. [23]. Cho et al. [7] extended the previous result to break 53-round HAS-160 in time 2^{55} . At ICISC 2007 Mendel and Rijmen [15] improved the attack complexity of the attack in [7] to 2^{35} hash computations and they were able to present a colliding message pair for the 53-round version of HAS-160. They also showed how the attack can be extended to 59-round HAS-160 with a complexity of 2^{55} .

HAS-160 in encryption mode is resistant to many attacks that can be applied to SHACAL-1, since its rotation constants are different and in each round its key schedule (which is equal to the message expansion) does not offer any

sliding properties. Nevertheless, it has a high degree of linearity which makes it vulnerable to related-key attacks.

In this paper we analyze the internal block cipher of HAS-160 and present the first cryptographic result on the full compression function of HAS-160. Using a related-key rectangle attack with four related keys we can break the full 80-rounds, i.e., recovering some key bits faster than exhaustive search. Our attack uses about 2^{157} chosen plaintexts and runs in time of about $2^{377.5}$ 80-round HAS-160 encryptions. For comparison exhaustive key search would require about 2^{512} 80-round HAS-160 encryptions.

The paper is organized as follows: In Section 2 we give a brief description of the HAS-160 compression function in encryption mode. Section 3 discusses some crucial properties of HAS-160. In Section 4 we describe the related-key rectangle attack. Section 5 presents our related-key rectangle attack on the full HAS-160 encryption mode. Section 6 concludes the paper.

2 Description of the HAS-160 Encryption Mode

2.1 Notation

The following notations are used in this paper:

- \oplus : bitwise XOR operation
- \wedge : bitwise AND operation
- \vee : bitwise OR operation
- $X \lll^k$: bit-rotation of X by k positions to the left.
- \boxplus : addition modulo 2^{32} operation
- \neg : bitwise complement operation
- e_i : a 32-bit word with zeros in all positions except for bit i , ($0 \leq i \leq 31$)
- $e_{i_1, \dots, i_l} : e_{i_1} \oplus \dots \oplus e_{i_l}$

The bit positions follow the little endian convention, i.e., for a 32-bit word bit 31 is the most significant bit and bit 0 is the least significant bit.

2.2 HAS-160

Now we describe the structure of HAS-160 and how it can be used as a block cipher. The inner block cipher operates on a 160-bit message block and a 512-bit master key. A 160-bit plaintext $P_0 = A_0 || B_0 || C_0 || D_0 || E_0$ is divided into five 32-bit words A_0, B_0, C_0, D_0, E_0 . HAS-160 consists of 4 passes of 20 rounds each, i.e., the round function is applied 80 times in total. The corresponding ciphertext, P_{80} , is denoted by $A_{80} || B_{80} || C_{80} || D_{80} || E_{80}$. The round function at round i ($i = 1, \dots, 80$) can be described as follows:

$$\begin{aligned}
 A_i &\leftarrow A_{i-1} \lll^{s_{1,i}} \boxplus f_i(B_{i-1}, C_{i-1}, D_{i-1}) \boxplus E_{i-1} \boxplus k_i + c_i, \\
 B_i &\leftarrow A_{i-1}, \\
 C_i &\leftarrow B_{i-1} \lll^{s_{2,i}}, \\
 D_i &\leftarrow C_{i-1}, \\
 E_i &\leftarrow D_{i-1},
 \end{aligned}$$

where c_i and k_i represents the i -th round constant and the i -th round key respectively, while $f_i(\cdot)$ represents a boolean function. The function $f_i(\cdot)$ and the constant c_i of round i can be found in Table 1.

Table 1. Boolean functions and constants

Pass	Round (i)	Boolean function (f_i)	Constant (c_i)
1	1 – 20	$(x \wedge y) \vee (\neg x \wedge z)$	0x00000000
2	21 – 40	$x \oplus y \oplus z$	0x5a827999
3	41 – 60	$(x \vee \neg z) \oplus y$	0x6ed9eba1
4	61 – 80	$x \oplus y \oplus z$	0x8f1bbcdc

The rotation constant $s_{1,i}$ used in round i are given in Table 2.

Table 2. The bit rotation s_1

Round ($i \bmod 20$) + 1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$s_{1,i}$	13	5	11	7	15	6	13	8	14	7	12	9	11	8	15	6	12	9	14	5

The rotation constant $s_{2,i}$ depends on the pass, i.e., it changes the value if the pass is changed but it is constant in each pass. A pass contains 20 rounds of the encryption. The pass-dependent values of $s_{2,i}$ are:

- Pass 1: $s_{2,i} = 10$
- Pass 2: $s_{2,i} = 17$
- Pass 3: $s_{2,i} = 25$
- Pass 4: $s_{2,i} = 30$

The 80 round keys k_i , $i \in \{1, 2, \dots, 80\}$ are derived from the master key K , which consists of sixteen 32-bit words $K = x_0, x_1, \dots, x_{15}$. The round keys k_i are obtained from the key schedule described in Table 3.

Figure 1 shows the round function of HAS-160.

3 Properties of HAS-160

Property 1. (from [10]) Let $Z = X \boxplus Y$ and $Z^* = X^* \boxplus Y^*$ with X, Y, X^*, Y^* being 32-bit words. Then, the following properties hold:

1. If $X \oplus X^* = e_j$ and $Y = Y^*$, then $Z \oplus Z^* = e_{j,j+1,\dots,j+k-1}$ holds with probability 2^{-k} for ($j < 31, k \geq 1$ and $j+k-1 \leq 30$). In addition, if $j = 31$, $Z \oplus Z^* = e_{31}$ holds with probability 1.
2. If $X \oplus X^* = e_j$ and $Y \oplus Y^* = e_j$, then $Z \oplus Z^* = e_{j+1,\dots,j+k-1}$ holds with probability 2^{-k} for ($j < 31, k \geq 1$ and $j+k-1 \leq 30$). In addition, in case $j = 31$, $Z = Z^*$ holds with probability 1.

Table 3. The key schedule

Round $(i \bmod 20) + 1$	Pass 1	Pass 2	Pass 3	Pass 4
1	$x_8 \oplus x_9$ $\oplus x_{10} \oplus x_{11}$	$x_{11} \oplus x_{14}$ $\oplus x_1 \oplus x_4$	$x_4 \oplus x_{13}$ $\oplus x_6 \oplus x_{15}$	$x_{15} \oplus x_{10}$ $\oplus x_5 \oplus x_0$
2	x_0	x_3	x_{12}	x_4
3	x_1	x_6	x_5	x_2
4	x_2	x_9	x_{14}	x_{13}
5	x_3	x_{12}	x_7	x_8
6	$x_{12} \oplus x_{13}$ $\oplus x_{14} \oplus x_{15}$	$x_7 \oplus x_{10}$ $\oplus x_{13} \oplus x_0$	$x_8 \oplus x_1$ $\oplus x_{10} \oplus x_3$	$x_{11} \oplus x_6$ $\oplus x_1 \oplus x_{12}$
7	x_4	x_{15}	x_0	x_3
8	x_5	x_2	x_9	x_{14}
9	x_6	x_5	x_2	x_9
10	x_7	x_8	x_{11}	x_4
11	$x_0 \oplus x_1$ $\oplus x_2 \oplus x_3$	$x_3 \oplus x_6$ $\oplus x_9 \oplus x_{12}$	$x_{12} \oplus x_5$ $\oplus x_{14} \oplus x_7$	$x_7 \oplus x_2$ $\oplus x_{13} \oplus x_8$
12	x_8	x_{11}	x_4	x_{15}
13	x_9	x_{14}	x_{13}	x_{10}
14	x_{10}	x_{14}	x_6	x_5
15	x_{11}	x_4	x_{15}	x_0
16	$x_4 \oplus x_5$ $\oplus x_6 \oplus x_7$	$x_{15} \oplus x_2$ $\oplus x_5 \oplus x_8$	$x_0 \oplus x_9$ $\oplus x_2 \oplus x_{11}$	$x_3 \oplus x_{14}$ $\oplus x_9 \oplus x_4$
17	x_{12}	x_7	x_8	x_{11}
18	x_{13}	x_{10}	x_1	x_6
19	x_{14}	x_{13}	x_{10}	x_1
20	x_{15}	x_0	x_3	x_{12}

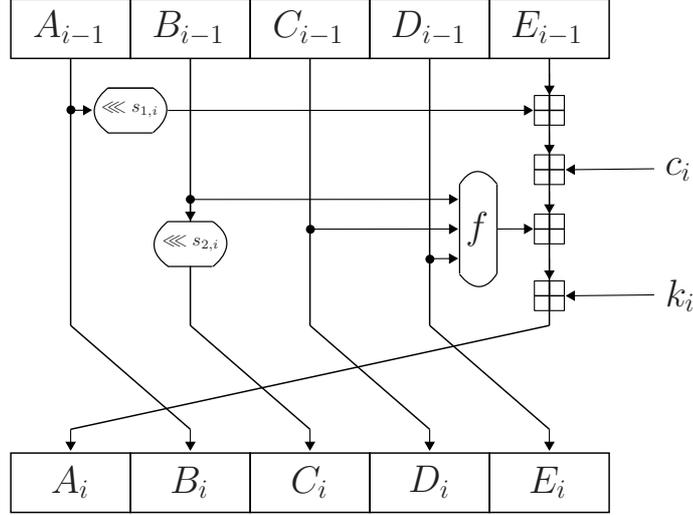


Fig. 1. The round function of HAS-160

A more general description of these properties can be derived from the following theorem.

Theorem 1. (from [14]) Given three 32-bit XOR differences $\Delta X, \Delta Y$ and ΔZ . If the probability $\Pr[(\Delta X, \Delta Y) \stackrel{\boxplus}{\rightarrow} \Delta Z] > 0$, then

$$\Pr[(\Delta X, \Delta Y) \stackrel{\boxplus}{\rightarrow} \Delta Z] = 2^{-k},$$

where the integer k is given by $k = \#\{i | 0 \leq i \leq 30, \text{ not } ((\Delta X)_i = (\Delta Y)_i = (\Delta Z)_i)\}$.

Property 2. Consider the difference $\Delta P_i = (\Delta A_i, \Delta B_i, \Delta C_i, \Delta D_i, \Delta E_i)$ of a message pair in round i . Then we know some 32-bit differences in round $i + 1, i + 2, i + 3$ and $i + 4$. The known word differences are as follows:

$$\begin{aligned} (\Delta B_{i+1}, \Delta C_{i+1}, \Delta D_{i+1}, \Delta E_{i+1}) &= (\Delta A_i, \Delta B_i \lll s_{2,i+1}, \Delta C_i, \Delta D_i), \\ (\Delta C_{i+2}, \Delta D_{i+2}, \Delta E_{i+2}) &= (\Delta A_i \lll s_{2,i+2}, \Delta B_i \lll s_{2,i+1}, \Delta C_i), \\ (\Delta D_{i+3}, \Delta E_{i+3}) &= (\Delta A_i \lll s_{2,i+2}, \Delta B_i \lll s_{2,i+1}), \\ (\Delta E_{i+4}) &= (\Delta A_i \lll s_{2,i+2}) \end{aligned}$$

4 The Related-Key Rectangle Attack

The boomerang attack [21] is an extension to differential cryptanalysis [5] using adaptive chosen plaintexts and ciphertexts to attack block ciphers. The amplified boomerang attack [12] transforms the ordinary boomerang attack into a chosen

plaintext attack. A more detailed analysis along some improvements resulted in the rectangle attack [3]. The related-key rectangle attack is published in [4, 11, 13]. It is an adaptation of the rectangle attack into the related-key framework [2]. The attack can be described as follows.

A block cipher $E : \{0, 1\}^n \times \{0, 1\}^k \rightarrow \{0, 1\}^n$ with $E_K(\cdot) := E(K, \cdot)$ is treated as a cascade of two sub-ciphers $E_{K^i}(P) = E1_{K^i}(E0_{K^i}(P))$, where P is a plaintext encrypted under the key K^i . It is assumed that there exists a related-key differential $\alpha \rightarrow \beta$ which holds with probability p for $E0$, i.e., $\Pr[E0_{K^a}(P^a) \oplus E0_{K^b}(P^b) = \beta | P^a \oplus P^b = \alpha] = p$, where K^a and $K^b = K^a \oplus \Delta K^*$ are two related keys and ΔK^* is a known key difference (the same holds for $\Pr[E0_{K^c}(P^c) \oplus E0_{K^d}(P^d) = \beta | P^c \oplus P^d = \alpha] = p$, where K^c and $K^d = K^c \oplus \Delta K^*$ are two related keys). Let $X^i = E0_{K^i}(P^i)$, $i \in \{a, b, c, d\}$ be an intermediate encryption value. We assume that there is a related-key differential $\gamma \rightarrow \delta$ which holds with probability q for $E1$, i.e., $\Pr[E1_{K^a}(X^a) \oplus E1_{K^c}(X^c) = \delta | X^a \oplus X^c = \gamma] = q$, where the keys K^a and K^c are related as $K^a \oplus K^c = \Delta K'$ and $\Delta K'$ is a known key difference (the same holds for $\Pr[E1_{K^b}(X^b) \oplus E1_{K^d}(X^d) = \delta | X^b \oplus X^d = \gamma] = q$ where the keys K^b and K^d are related as $K^b \oplus K^d = \Delta K'$). In our attack we use four different keys but one can also apply the attack with more or less keys.

We discuss plaintext quartets (P^a, P^b, P^c, P^d) , for which $P^a \oplus P^b = \alpha = P^c \oplus P^d$, where P^i is encrypted under the key K^i , $i \in \{a, b, c, d\}$. Out of N pairs of plaintexts with the related-key difference α , about $N \cdot p$ pairs have an output difference β after $E0$. These pairs can be combined into $(N \cdot p)^2$ quartets, such that each quartet satisfies $E0_{K^a}(P^a) \oplus E0_{K^b}(P^b) = \beta$ and $E0_{K^c}(P^c) \oplus E0_{K^d}(P^d) = \beta$. We assume that the intermediate values after $E0$ distribute uniformly over all possible values. Thus, $E0_{K^a}(P^a) \oplus E0_{K^c}(P^c) = \gamma$ holds with probability 2^{-n} . If this occurs, $E0_{K^b}(P^b) \oplus E0_{K^d}(P^d) = \gamma$ holds as well, since the following condition holds:

$$\begin{aligned} (E0_{K^a}(P^a) \oplus E0_{K^b}(P^b)) \oplus (E0_{K^c}(P^c) \oplus E0_{K^d}(P^d)) \\ \oplus (E0_{K^a}(P^a) \oplus E0_{K^c}(P^c)) = \\ (X^a \oplus X^b) \oplus (X^c \oplus X^d) \oplus (X^a \oplus X^c) = \\ \beta \oplus \beta \oplus \gamma = \gamma \end{aligned}$$

The expected number of quartets satisfying both $E1_{K^a}(X^a) \oplus E1_{K^c}(X^c) = \delta$ and $E1_{K^b}(X^b) \oplus E1_{K^d}(X^d) = \delta$ is

$$\sum_{\beta, \gamma} (N \cdot p)^2 \cdot 2^{-n} \cdot q^2 = N^2 \cdot 2^{-n} \cdot (p \cdot q)^2.$$

For a random cipher, the expected number of correct quartets is about $N^2 \cdot 2^{-2n}$. Therefore, if $p \cdot q > 2^{-n/2}$ and N is sufficiently large, the related-key rectangle distinguisher can distinguish between E and a random cipher. Figure 2 visualizes the structure of the related-key rectangle distinguisher.

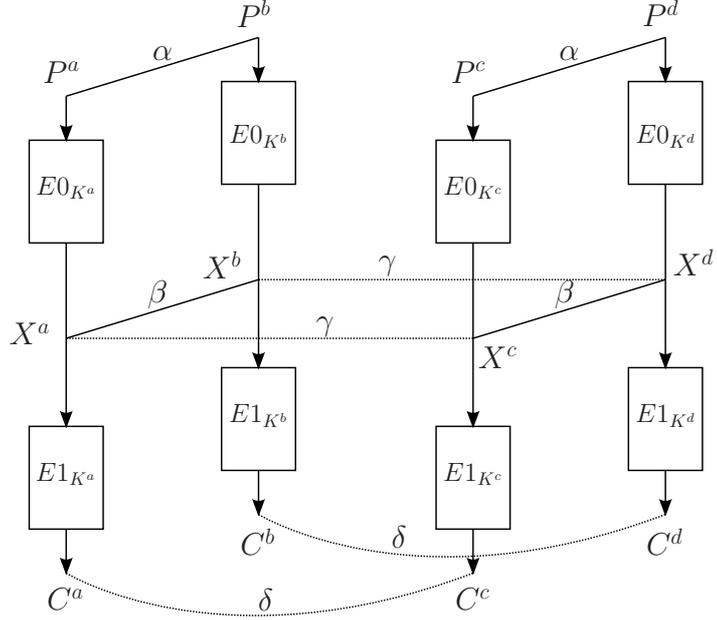


Fig. 2. The related-key rectangle distinguisher

5 Related-Key Rectangle Attack on the full Compression Function of HAS-160 in Encryption Mode

In this section, we give a 71-round related-key rectangle distinguisher, which can be used to mount a related-key rectangle attack on the full 80-round HAS-160 in encryption mode. We can use Property 2 to partially determine whether a candidate quartet is a right one or not. A wrong quartet can be discarded during the stepwise computation, which reduces the complexity of the subsequent steps and also the overall complexity of the attack. Thus, our attack uses the early abort technique.

5.1 A 71-Round Related-Key Rectangle Distinguisher

Let K be a master key which can be written as $K = x_0, x_1, \dots, x_{15}$, where x_i is a 32-bit word. We use four different – but related – master keys K^a, K^b, K^c and K^d to mount our related-key rectangle attack on the full HAS-160 encryption mode. The master key differences are as follows:

$$\begin{aligned} \Delta K^* &= K^a \oplus K^b = K^c \oplus K^d = (e_{31}, 0, 0, 0, 0, 0, 0, 0, 0, 0, e_{31}, 0, 0, 0, 0, 0), \quad (1) \\ \Delta K' &= K^a \oplus K^c = K^b \oplus K^d = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, e_{31}, 0). \end{aligned}$$

Since the key schedule of HAS-160 offers a high degree of linearity we can easily determine all the 80 round key differences derived from the master key differences

ΔK^* and $\Delta K'$ respectively. We observe that if we choose $\Delta x_0 = \Delta x_{10}$ and the remaining word differences as zero, i.e., $\Delta x_i = 0, i = 1, 2, \dots, 8, 9, 11, 12, \dots, 15$, then a zero difference can be obtained starting from round 14 up to round 37. We use this observation for the related-key differential for $E0$. Moreover, we can observe that if $\Delta x_{12} = \Delta x_{14}$ holds and the remaining word differences in $\Delta K'$ are all zero, then a zero difference can be obtained from round 44 to round 65. This observation is used in our related-key differential for $E1$.

Considering Property 1 and Theorem 1 we have found a 39-round related-key differential from round 0 to 39 for $E0$ ($\alpha \rightarrow \beta$) using the master key difference ΔK^* . The related-key differential is:

$$(e_7, e_1, 0, e_{5,19,31}, e_{12,26,31}) \rightarrow (e_{4,31}, e_{31}, 0, 0, 0).$$

The related-key differential $E0$ is shown in Table 4.³

Table 4. The Related-Key Differential $E0$

i	ΔA_i	ΔB_i	ΔC_i	ΔD_i	ΔE_i	Δk_i	Prob.
0	e_7	e_1	0	$e_{5,19,31}$	$e_{12,26,31}$	–	2^{-7}
1	e_{26}	e_7	e_{11}	0	$e_{5,19,31}$	e_{31}	2^{-5}
2	e_{19}	e_{26}	e_{17}	e_{11}	0	e_{31}	2^{-6}
3	0	e_{19}	e_4	e_{17}	e_{11}	0	2^{-5}
4	e_{11}	0	e_{29}	e_4	e_{17}	0	2^{-3}
5	e_{23}	e_{11}	0	e_{29}	e_4	0	2^{-4}
6	e_{21}	e_{23}	e_{21}	0	e_{29}	0	2^{-4}
7	0	e_{21}	e_1	e_{21}	0	0	2^{-3}
8	0	0	e_{31}	e_1	e_{21}	0	2^{-3}
9	e_{21}	0	0	e_{31}	e_1	0	2^{-3}
10	0	e_{21}	0	0	e_{31}	0	2^{-2}
11	0	0	e_{31}	0	0	e_{31}	2^{-1}
12	0	0	0	e_{31}	0	0	2^{-1}
13	0	0	0	0	e_{31}	0	1
14	0	0	0	0	0	e_{31}	1
15	0	0	0	0	0	0	1
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
37	0	0	0	0	0	0	1
38	e_{31}	0	0	0	0	e_{31}	2^{-1}
39	$e_{4,31}$	e_{31}	0	0	0	0	

³ Note that $\Pr[(\Delta c_i, \Delta k_i) \stackrel{\boxplus}{\rightarrow} \Delta k_i] = 1$ always holds due to Property 1. This is true since Δc_i is equal to zero for all i and Δk_i is either zero or e_{31} .

We exploit a 32-round related-key differential for $E1$ ($\gamma \rightarrow \delta$) that covers rounds 39 to 71 using the key difference $\Delta K'$. The related-key differential is:

$$(e_6, 0, 0, 0, e_{19}) \rightarrow (e_{5,6,7,14,17,18,19,28,29,30}, e_{5,8,9,19,21,29}, e_{5,26,27}, e_{19}, e_5)$$

The 160-bit difference δ can be written as a concatenation of five 32-bit word differences

$$\delta = (\delta_A, \delta_B, \delta_C, \delta_D, \delta_E) = (\Delta A_{71}, \Delta B_{71}, \Delta C_{71}, \Delta D_{71}, \Delta E_{71}). \quad (2)$$

The related-key differential $E1$ is shown in Table 5. The probability for the

Table 5. The Related-Key Differential $E1$

i	ΔA_i	ΔB_i	ΔC_i	ΔD_i	ΔE_i	Δk_i	Prob.
39	e_6	0	0	0	e_{19}	–	2^{-1}
40	0	e_6	0	0	0	0	2^{-1}
41	0	0	e_{31}	0	0	0	1
42	0	0	0	e_{31}	0	e_{31}	2^{-1}
43	0	0	0	0	e_{31}	0	1
44	0	0	0	0	0	e_{31}	1
45	0	0	0	0	0	0	1
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
65	0	0	0	0	0	0	1
66	e_{31}	0	0	0	0	e_{31}	2^{-1}
67	e_7	e_{31}	0	0	0	0	2^{-1}
68	e_{21}	e_7	e_{29}	0	0	e_{31}	2^{-3}
69	$e_{7,28,29}$	e_{21}	e_5	e_{29}	0	0	2^{-6}
70	$e_{5,8,9,19,21,29}$	$e_{7,28,29}$	e_{19}	e_5	e_{29}	0	2^{-10}
71	$e_{5,6,7,14,17,18,19,28,29,30}$	$e_{5,8,9,19,21,29}$	$e_{5,26,27}$	e_{19}	e_5	0	

differential $E0$ is 2^{-48} due to Table 4, while the probability for $E1$ is 2^{-24} from Table 5. Thus, the probability of our related-key rectangle distinguisher for round 1–71 is:

$$(2^{-48} \cdot 2^{-24})^2 \cdot 2^{-160} = 2^{-304}$$

However, the correct difference δ occurs in two ciphertext pairs of a quartet for a random cipher with probability $(2^{-160})^2 = 2^{-320}$.

5.2 The Attack on the full HAS-160 in Encryption Mode

Our attack uses four related keys K^a, K^b, K^c and K^d where each two of the four master keys are related as stated in (2). It is assumed that an attacker chooses the

two master key differences ΔK^* and $\Delta K'$, but not the maser keys themselves. In the first step we apply the 71-round related-key rectangle distinguisher to obtain a small amount of subkey candidates in rounds 72, 73, 74, 76, 77, 78, 80. In the second step we find the remaining subkey candidates by an exhaustive search for the obtained subkey candidates and the remaining subkeys to recover the four 512-bit master keys K^a, K^b, K^c and K^d .

The attack works as follows:

1. Choose 2^{155} plaintexts $P_i^a = (A_i, B_i, C_i, D_i, E_i)$, $i = 1, 2, \dots, 2^{155}$. Compute 2^{155} plaintexts P_i^b , i.e., $P_i^b = P_i^a \oplus \alpha$, where α is a fixed 160-bit word as stated above. Set $P_i^c = P_i^a$ and $P_i^d = P_i^b$. In a chosen plaintext attack scenario ask for the encryption of the plaintexts $P_i^a, P_i^b, P_i^c, P_i^d$ under K^a, K^b, K^c and K^d , respectively, and obtain the ciphertexts C_i^a, C_i^b, C_i^c and C_i^d .
2. Guess seven 32-bit round keys $k_{80}^a, k_{79}^a, k_{78}^a, k_{77}^a, k_{76}^a, k_{75}^a, k_{74}^a$ and compute $k_{80}^l, k_{79}^l, k_{78}^l, k_{77}^l, k_{76}^l, k_{75}^l, k_{74}^l$, $l \in \{b, c, d\}$ using the known round key differences.
 - 2.1. Decrypt each of the ciphertexts $C_i^a, C_i^b, C_i^c, C_i^d$ under $k_{80}^l, k_{79}^l, k_{78}^l, k_{77}^l, k_{76}^l, k_{75}^l, k_{74}^l$, $l \in \{a, b, c, d\}$ respectively and obtain the intermediate encryption values $C_{73,i}^a, C_{73,i}^b, C_{73,i}^c$ and $C_{73,i}^d$, respectively. From Property 2 we know the value of the 96-bit difference $\delta_{A \lll 30}$, $\delta_{B \lll 30}$ and δ_C , see (2).
 - 2.2. Check whether the following conditions are fulfilled for any quartet $(C_{73,j}^a, C_{73,j}^b, C_{73,j}^c, C_{73,j}^d)$:

$$\begin{aligned} C_{73,j}^a \oplus C_{73,j}^c &= \delta_{A \lll 30} = C_{73,j}^b \oplus C_{73,j}^d, \\ D_{73,j}^a \oplus D_{73,j}^c &= \delta_{B \lll 30} = D_{73,j}^b \oplus D_{73,j}^d, \\ E_{73,j}^a \oplus E_{73,j}^c &= \delta_C = E_{73,j}^b \oplus E_{73,j}^d \end{aligned}$$

Discard all the quartets that do not satisfy the above conditions and discard the quartets that do not satisfy this condition.

3. Guess a 32-bit round key k_{73}^a and compute k_{73}^l , $l \in \{b, c, d\}$ using the known round key differences.
 - 3.1. Decrypt each remaining quartet $(C_{73,j}^a, C_{73,j}^b, C_{73,j}^c, C_{73,j}^d)$ under k_{73}^l , $l \in \{a, b, c, d\}$, respectively and obtain the quartets $(C_{72,j}^a, C_{72,j}^b, C_{72,j}^c, C_{72,j}^d)$.
 - 3.2. Check whether $E_{72,j}^a \oplus E_{72,j}^c = \delta_D = E_{72,j}^b \oplus E_{72,j}^d$ holds. From Property 2 we know the value of the 32-bit difference δ_D . Discard all the quartets that do not satisfy the above condition.
4. Guess one 32-bit round keys k_{72}^a and compute k_{72}^l , $l \in \{b, c, d\}$ using the known round key differences.
 - 4.1. Decrypt each remaining quartet $(C_{72,j}^a, C_{72,j}^b, C_{72,j}^c, C_{72,j}^d)$ under k_{72}^l , $l \in \{a, b, c, d\}$ respectively and obtain the quartets $(C_{71,j}^a, C_{71,j}^b, C_{71,j}^c, C_{71,j}^d)$.
 - 4.2. Check whether $E_{71,j}^a \oplus E_{71,j}^c = \delta_E = E_{71,j}^b \oplus E_{71,j}^d$ holds. From Property 2 we know the value of the 32-bit difference δ_E . If there exist at least 21 quartets passing the above condition, record $k_{80}^l, k_{79}^l, k_{78}^l, k_{77}^l, k_{76}^l, k_{75}^l, k_{74}^l, k_{73}^l, k_{72}^l$, $l \in \{a, b, c, d\}$ and go to Step 5. Otherwise go to Step 4 with another guessed round key. If all the possible round keys for k_{72}^a are tested, then repeat Step

- 3 with another guessed round key k_{73}^a . If all the possible round keys for k_{73}^a are tested, then go to Step 2 with another guess for the round keys $k_{80}^a, k_{79}^a, k_{78}^a, k_{77}^a, k_{76}^a, k_{75}^a, k_{74}^a$.
5. For a suggested $(k_{80}^l, k_{79}^l, k_{78}^l, k_{77}^l, k_{76}^l, k_{75}^l, k_{74}^l, k_{73}^l, k_{72}^l)$, do an exhaustive key search for the remaining $512 - 9 \cdot 32 = 224$ key bits by trial encryptions. If a 512-bit key is suggested, output it as the master key of the full HAS-160 encryption mode. Otherwise, restart the algorithm.

5.3 Analysis of the Attack

There are 2^{155} pairs (P_i^a, P_i^b) and 2^{155} pairs (P_i^c, P_i^d) of plaintexts, thus we have $(2^{155})^2 = 2^{310}$ quartets. The data complexity of Step 1 is $2^2 \cdot 2^{155} = 2^{157}$ chosen plaintexts. The time complexity of Step 1 is about $2^2 \cdot 2^{155} = 2^{157}$ encryptions. Step 2.1 requires time about $2^{224} \cdot 2^2 \cdot 2^{155} \cdot (7/80) \approx 2^{377.5}$ eighty round encryptions. The number of remaining quartets after Step 2.2 is $2^{310} \cdot (2^{-96})^2 = 2^{118}$, since we have a 96-bit filtering condition on both pairs of a quartet. The time complexity of Step 3.1 is about $2^{256} \cdot 2^2 \cdot 2^{118} \cdot (1/80) \approx 2^{370}$ encryptions. After Step 3.2 about $2^{118} \cdot (2^{-32})^2 = 2^{54}$ quartets remain, since we have a 32-bit filtering condition on both pairs of a quartet. The time complexity of Step 4.1 is $2^{288} \cdot 2^2 \cdot 2^{54} \cdot (1/80) \approx 2^{337.5}$ encryptions. After Step 4.2 the number of remaining quartets is about $2^{54} \cdot (2^{-32})^2 = 2^{-10}$ for each subkey guess, since we have a 32-bit filtering condition on both pairs of a quartet. The expected number of quartets that remain for the correct round keys are about $2^{310} \cdot 2^{-304} = 2^6$.

Using the Poisson distribution we can compute the success rate of our attack. The probability that the number of remaining quartets for each false key bit combination is larger than 21 is $Y_i \sim \text{Poisson}(\mu = 2^{-10})$, $\Pr(Y_i \geq 22) \approx e^{-2^{-10}} \cdot \frac{(2^{-10})^{22}}{22!}$, where i indicates a wrong key. Thus, for all the $2^{288} - 1$ wrong keys we expect that about $2^{188} \cdot 2^{-189} = 2^{-1}$ quartets are counted. The probability that the number of quartets counted for the correct key bits is at least 21 is $Z \sim \text{Poisson}(\mu = 2^6)$, $\Pr(Z \geq 22) \approx 1$. The data complexity of our attack is $2^{155} \cdot 2^2 = 2^{157}$ chosen plaintexts, while the time complexity is about $2^{377.5}$ full HAS-160 encryptions. Our attack has a success rate of 1.

6 Conclusion

In this paper we present the first cryptanalytic result on the inner block cipher of the Korean hash algorithm standard HAS-160. Our related-key rectangle attack can break the full block cipher. A more complex and non-linear key schedule would have defended our attack. Moreover, to strengthen the cipher against differential attacks, we propose to use the f -function more often in each round and so the f -function may influence more than one word in each round. Note that this analysis does not seem to say anything about the collision, preimage, or 2nd-preimage resistance of HAS-160, but it shows some interesting properties that occur if HAS-160 is used as a block cipher.

References

- [1] Telecommunications Technology Association. Hash Function Standard Part 2: Hash Function Algorithm Standard (HAS-160). TTAS.KO-12.0011/R1, December 2000.
- [2] Eli Biham. New Types of Cryptanalytic Attacks Using Related Keys. *J. Cryptology*, 7(4):pages 229–246, 1994.
- [3] Eli Biham, Orr Dunkelman, and Nathan Keller. The Rectangle Attack - Rectangling the Serpent. In Birgit Pfitzmann, editor, *EUROCRYPT*, volume 2045 of *Lecture Notes in Computer Science*, pages 340–357. Springer, 2001.
- [4] Eli Biham, Orr Dunkelman, and Nathan Keller. Related-Key Boomerang and Rectangle Attacks. In Cramer [8], pages 507–525.
- [5] Eli Biham and Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystems. In Menezes and Vanstone [16], pages 2–21.
- [6] Gilles Brassard, editor. *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*, volume 435 of *Lecture Notes in Computer Science*. Springer, 1990.
- [7] Hong-Su Cho, Sangwoo Park, Soo Hak Sung, and Aaram Yun. Collision Search Attack for 53-Step HAS-160. In Min Surp Rhee and Byoungcheon Lee, editors, *ICISC*, volume 4296 of *Lecture Notes in Computer Science*, pages 286–295. Springer, 2006.
- [8] Ronald Cramer, editor. *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*, volume 3494 of *Lecture Notes in Computer Science*. Springer, 2005.
- [9] Ivan Damgård. A Design Principle for Hash Functions. In Brassard [6], pages 416–427.
- [10] Seokhie Hong, Jongsung Kim, Guil Kim, Jaechul Sung, Changhoon Lee, and Sangjin Lee. Impossible Differential Attack on 30-Round SHACAL-2. In Thomas Johansson and Subhamoy Maitra, editors, *INDOCRYPT*, volume 2904 of *Lecture Notes in Computer Science*, pages 97–106. Springer, 2003.
- [11] Seokhie Hong, Jongsung Kim, Sangjin Lee, and Bart Preneel. Related-Key Rectangle Attacks on Reduced Versions of SHACAL-1 and AES-192. In Henri Gilbert and Helena Handschuh, editors, *FSE*, volume 3557 of *Lecture Notes in Computer Science*, pages 368–383. Springer, 2005.
- [12] John Kelsey, Tadayoshi Kohno, and Bruce Schneier. Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent. In Bruce Schneier, editor, *FSE*, volume 1978 of *Lecture Notes in Computer Science*, pages 75–93. Springer, 2000.
- [13] Jongsung Kim, Guil Kim, Seokhie Hong, Sangjin Lee, and Dowon Hong. The Related-Key Rectangle Attack - Application to SHACAL-1. In Wang et al. [22], pages 123–136.
- [14] Jiqiang Lu, Jongsung Kim, Nathan Keller, and Orr Dunkelman. Related-Key Rectangle Attack on 42-Round SHACAL-2. In Sokratis K. Katsikas, Javier Lopez, Michael Backes, Stefanos Gritzalis, and Bart Preneel, editors, *ISC*, volume 4176 of *Lecture Notes in Computer Science*, pages 85–100. Springer, 2006.
- [15] Florian Mendel and Vincent Rijmen. Colliding Message Pair for 53-Step HAS-160. In Kil-Hyun Nam and Gwangsoo Rhee, editors, *ICISC*, volume 4817 of *Lecture Notes in Computer Science*, pages 324–334. Springer, 2007.

- [16] Alfred Menezes and Scott A. Vanstone, editors. *Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings*, volume 537 of *Lecture Notes in Computer Science*. Springer, 1991.
- [17] Ralph C. Merkle. One Way Hash Functions and DES. In Brassard [6], pages 428–446.
- [18] National Institute of Standards and Technology. FIPS 180-1: Secure Hash Standard. April 1995. See <http://csrc.nist.gov>.
- [19] Ron Rivest. The MD5 Message-Digest Algorithm. Request for Comments: 1321, <http://tools.ietf.org/html/rfc1321>, April 1992.
- [20] Ronald L. Rivest. The MD4 Message Digest Algorithm. In Menezes and Vanstone [16], pages 303–311.
- [21] David Wagner. The Boomerang Attack. In Lars R. Knudsen, editor, *Fast Software Encryption*, volume 1636 of *Lecture Notes in Computer Science*, pages 156–170. Springer, 1999.
- [22] Huaxiong Wang, Josef Pieprzyk, and Vijay Varadharajan, editors. *Information Security and Privacy: 9th Australasian Conference, ACISP 2004, Sydney, Australia, July 13-15, 2004. Proceedings*, volume 3108 of *Lecture Notes in Computer Science*. Springer, 2004.
- [23] Xiaoyun Wang, Xuejia Lai, Dengguo Feng, Hui Chen, and Xiuyuan Yu. Cryptanalysis of the Hash Functions MD4 and RIPEMD. In Cramer [8], pages 1–18.
- [24] Aaram Yun, Soo Hak Sung, Sangwoo Park, Donghoon Chang, Seokhie Hong, and Hong-Su Cho. Finding Collision on 45-Step HAS-160. In Dongho Won and Seungjoo Kim, editors, *ICISC*, volume 3935 of *Lecture Notes in Computer Science*, pages 146–155. Springer, 2005.