On Collisions of Hash Functions Turbo SHA-2

Vlastimil Klima

Prague, Czech Republic
http://cryptography.hyperlink.cz
v.klima@volny.cz

Abstract. In this paper we don't examine security of Turbo SHA-2 completely; we only show new collision attacks on it, with smaller complexity than it was considered by Turbo SHA-2 authors. In [1] they consider Turbo SHA-224/256-*r* and Turbo SHA-384/512-*r* with variable number of rounds *r* from 1 to 8. The authors of [1] show collision attack on Turbo SHA-256-1 with one round which has the complexity of 2^{64}. For other *r* from 2 to 8 they don't find better attack than with the complexity of 2^{128}. Similarly, for Turbo SHA-512 they find only collision attack on Turbo SHA-512-1 with one round which has the complexity of 2^{128}. For *r* from 2 to 8 they don't find better attack than with the complexity of 2^{256}. In this paper we show collision attack on SHA-256-*r* for $r = 1, 2, ..., 8$ with the complexity of 2^{16r}. We also show collision attack on Turbo SHA-512-*r* for $r = 1, 2, ..., 8$ with the complexity of 2^{32r}. It follows that the only one remaining candidate from the hash family Turbo SHA is Turbo SHA-256 (and Turbo SHA-512) with 8 rounds. The original security reserve of 6 round has been lost.

Keywords: Turbo SHA-2, collision attack.

1 Introduction

In the following we will deal with Turbo SHA-256-*r*, because all proofs for Turbo SHA-512-*r* differ only in the length of the word (32 or 64 bits). We start with notation, then present Lemma 1 and main Theorem 1. The conclusion contains consequence of the theorem.

2 Notation

We can see the original definition of Turbo SHA-2 on Fig. 1 [1]. The definition of Turbo SHA-2-*r* is on Fig. 2. We enumerate the variables *a, h* by the number of round. For the simplicity we assume only one message block. Thus we assume the final hash value without addition of the constant $H^{(0)}$ in Step 5 of the original description. In the Step 3 we denote the addition of the constant $H^{(0)}$ by variables

$W_{31}^{+} := a[0] = W_{31} + H^{(0)}_0$, $W_{30}^{+} := b[0] = W_{30} + H^{(0)}_1$, ..., $W_{24}^{+} := h[0] = W_{24} + H^{(0)}_7$.

Further, let us denote

$$W_t^{\sim} := (W_t \oplus W_{t+16}) + (W_{t+4} \oplus W_{t+24}) + (W_{t+8} \oplus W_{t+20}) + W_{t+12}, t = 0,...,7 .$$

For $i = 1$ to N:

{

1. Message expansion part for obtaining additional sixteen 32-bit (64-bit) words:

$$W_t = \begin{cases} M_t^{(i)}, & 0 \le t \le 15 \\ W_{t-16} + \sigma_0(W_{t-15}) + W_{t-14} + \sigma_1(W_{t-13}) + W_{t-12} + \sigma_0(W_{t-11}) + W_{t-10} + \sigma_1(W_{t-9}) + \\ +W_{t-8} + W_{t-7} + \sigma_0(W_{t-6}) + W_{t-5} + \sigma_1(W_{t-4}) + W_{t-3} + \sigma_1(W_{t-2}) + \sigma_0(W_{t-1}) + \\ +P_{t-16}^{(i-1)}, & 16 \le t \le 31 \end{cases}$$

2. Set the i^{th} intermediate double pipe value $P^{(i)}$: $P_t^{(i)} = W_t + W_{t+16}, \qquad 0 \le t \le 15$

3. Initialize eight working variables a, b, c, d, e, f, g and h with the $(i-1)^{\text{th}}$ hash value and the values of W_{31}, W_{30}, W_{29}, W_{28}, W_{27}, W_{26}, W_{25}, W_{24}:

$$a = H_0^{(i-1)} + W_{31}, \quad b = H_1^{(i-1)} + W_{30}, \quad c = H_2^{(i-1)} + W_{29}, \quad d = H_3^{(i-1)} + W_{28},$$
$$e = H_4^{(i-1)} + W_{27}, \quad f = H_5^{(i-1)} + W_{26}, \quad g = H_6^{(i-1)} + W_{25}, \quad h = H_7^{(i-1)} + W_{24}$$

4. For t=0 to 7

{

$T_1 = h + \sum_1(e) + Ch(e,f,g) + (W_t \oplus W_{t+16}) + (W_{t+4} \oplus W_{t+24}) + (W_{t+8} \oplus W_{t+20}) + W_{t+12}$

$T_2 = \sum_0(a) + Maj(a,b,c)$

$h = g$

$g = f$

$f = e$

$e = d + T_1$

$d = c$

$c = b$

$b = a$

$a = T_1 + T_2$

}

5. Compute the i^{th} intermediate hash value $H^{(i)}$:

$$H_0^{(i)} = a + H_0^{(i-1)}, \quad H_1^{(i)} = b + H_1^{(i-1)}, \quad H_2^{(i)} = c + H_2^{(i-1)}, \quad H_3^{(i)} = d + H_3^{(i-1)},$$
$$H_4^{(i)} = e + H_4^{(i-1)}, \quad H_5^{(i)} = f + H_5^{(i-1)}, \quad H_6^{(i)} = g + H_6^{(i-1)}, \quad H_7^{(i)} = h + H_7^{(i-1)}$$

}

Fig. 1: Turbo SHA-2 [1]

For Turbo SHA-r we have

Step 3:
$a[0] = W_{31}^+$, $b[0] = W_{30}^+$, $c[0] = W_{29}^+$, $d[0] = W_{28}^+$, $e[0] = W_{27}^+$, $f[0] = W_{26}^+$, $g[0] = W_{25}^+$, $h[0] = W_{24}^+$.

Step 4:
For $t = 1$ to r
{

$$T_1[t] = h[t-1] + \Sigma_1(e[t-1]) + Ch(e[t-1], f[t-1], g[t-1]) + W_{t-1}^{\sim}$$
$$T_2[t] = \Sigma_0(a[t-1]) + Maj(a[t-1], b[t-1], c[t-1])$$
$$h[t] = g[t-1]$$
$$g[t] = f[t-1]$$
$$f[t] = e[t-1]$$
$$e[t] = d[t-1] + T_1[t-1]$$
$$d[t] = c[t-1]$$
$$c[t] = b[t-1]$$
$$b[t] = a[t-1]$$
$$a[t] = T_1[t-1] + T_2[t-1]$$

}

We can see the values of working variables (a, b, c, d, e, f, g, h) in appropriate rounds in Tab. 1.

t	***a***	***b***	***c***	***d***	***e***	***f***	***g***	***h***
0	W_{31}^+	W_{30}^+	W_{29}^+	W_{28}^+	W_{27}^+	W_{26}^+	W_{25}^+	W_{24}^+
1	$a[1]$	W_{31}^+	W_{30}^+	W_{29}^+	$e[1]$	W_{27}^+	W_{26}^+	W_{25}^+
2	$a[2]$	$a[1]$	W_{31}^+	W_{30}^+	$e[2]$	$e[1]$	W_{27}^+	W_{26}^+
3	$a[3]$	$a[2]$	$a[1]$	W_{31}^+	$e[3]$	$e[2]$	$e[1]$	W_{27}^+
4	$a[4]$	$a[3]$	$a[2]$	$a[1]$	$e[4]$	$e[3]$	$e[2]$	$e[1]$
5	$a[5]$	$a[4]$	$a[3]$	$a[2]$	$e[5]$	$e[4]$	$e[3]$	$e[2]$
6	$a[6]$	$a[5]$	$a[4]$	$a[3]$	$e[6]$	$e[5]$	$e[4]$	$e[3]$
7	$a[7]$	$a[6]$	$a[5]$	$a[4]$	$e[7]$	$e[6]$	$e[5]$	$e[4]$
8	$a[8]$	$a[7]$	$a[6]$	$a[5]$	$e[8]$	$e[7]$	$e[6]$	$e[5]$

Tab.1: Working variables (a, b, c, d, e, f, g, h) in appropriate rounds

Lemma 1

Finding a collision in Turbo SHA-256-r is equivalent to finding of 2 different messages for which the values of registers in the second and the third column in Tab. 2 are equal.

	Turbo SHA-r collision		
r	***fixed values (chosen randomly)***	***collision by birthday paradox***	***free values (chosen randomly)***
1	$W_{31, 30, 29, 28, 27, 26, 25}$	$T_1[1]$	$W_{24, 23, ..., 16}$
2	$W_{31, 30, 29, 28, 27, 26}$	$T_1[1]$, $T_1[2]$	$W_{25, 24, ..., 16}$
3	$W_{31, 30, 29, 28, 27}$	$T_1[1]$, $T_1[2]$, $T_1[3]$	$W_{26, 25, ..., 16}$
4	$W_{31, 30, 29, 28}$	$T_1[1]$, $T_1[2]$, $T_1[3]$, $T_1[4]$	$W_{27, 26, ..., 16}$
5	$W_{31, 30, 29}$	$T_1[1]$, $T_1[2]$, $T_1[3]$, $T_1[4]$, $T_1[5]$	$W_{28, 27, ..., 16}$
6	$W_{31, 30}$	$a[1]$, $T_1[2]$, $T_1[3]$, $T_1[4]$, $T_1[5]$, $T_1[6]$	$W_{29, 28, ..., 16}$
7	W_{31}	$a[1]$, $a[2]$, $T_1[3]$, $T_1[4]$, $T_1[5]$, $T_1[6]$, $T_1[7]$	$W_{30, 29, ..., 16}$
8	---	$a[1]$, $a[2]$, $a[3]$, $T_1[4]$, $T_1[5]$, $T_1[6]$, $T_1[7]$, $T_1[8]$	$W_{31, 30, ..., 16}$

Tab. 2: Collision of Turbo SHA-*r*

Proof

The case of *r* = 1

After the first round we have

$$T_1[1] = W_{24}^{+} + \Sigma_1(W_{27}^{+}) + Ch(W_{27}^{+}, W_{26}^{+}, W_{25}^{+}) + W_0^{\sim}$$

$$T_2[1] = \Sigma_0(W_{31}^{+}) + Maj(W_{31}^{+}, W_{30}^{+}, W_{29}^{+})$$

$$e[1] = W_{28}^{+} + T_1[1]$$

$$a[1] = T_1[1] + T_2[1]$$

Hash value consists of values in the row $t = 1$ of the Table 1. The collision means that two different messages have these values the same:

$a[1]$	W_{31}^{+}	W_{30}^{+}	W_{29}^{+}	$e[1]$	W_{27}^{+}	W_{26}^{+}	W_{25}^{+}

It means that the value $T_2[1]$ also collides, because it uses primarily colliding values

W_{31}, W_{30}, W_{29}.

From collision of $a[1]$ and $T_2[1]$ follows that $\mathbf{T_1[1]}$ collides too.

From collision of $e[1]$ and $T_1[1]$ follows that $\mathbf{W_{28}}$ collides too.

From collision of the hash value follows collision of the values W_{31}, W_{30}, W_{29}, W_{28}, W_{27}, W_{26}, W_{25} and $T_1[1]$. We can easily see that the reverse implication holds too.

The case of *r* = 2

After the second round we have

$$T_1[1] = W_{24}^{+} + \Sigma_1(W_{27}^{+}) + Ch(W_{27}^{+}, W_{26}^{+}, W_{25}^{+}) + W_0^{\sim}$$

$$T_2[1] = \Sigma_0(W_{31}^{+}) + Maj(W_{31}^{+}, W_{30}^{+}, W_{29}^{+})$$

$$e[1] = W_{28}^{+} + T_1[1]$$
$$a[1] = T_1[1] + T_2[1]$$

$$T_1[2] = W_{25}^{+} + \Sigma_1(e[1]) + Ch(e[1], W_{27}^{+}, W_{26}^{+}) + W_1^{\sim}$$
$$T_2[2] = \Sigma_0(a[1]) + Maj(a[1], W_{31}^{+}, W_{30}^{+})$$
$$e[2] = W_{29}^{+} + T_1[2]$$
$$a[2] = T_1[2] + T_2[2]$$

Hash value consist of values in the row t = 2 of the Table 1. The collision means that two different messages have these values the same:

$a[2]$	$a[1]$	W_{31}^{+}	W_{30}^{+}	$e[2]$	$e[1]$	W_{27}^{+}	W_{26}^{+}

It means that the value $T_2[2]$ also collides, because it uses primarily colliding values.

From collision of $a[2]$ and $T_2[2]$ follows that $\boldsymbol{T_1[2]}$ collides too.

From collision of $e[2]$ and $T_1[2]$ follows that $\boldsymbol{W_{29}}$ collides too.

From collision of W_{29} follows that $T_2[1]$ collides. From collision of $a[1]$ and $T_2[1]$ follows that $\boldsymbol{T_1[1]}$ collides.

From collision of $e[1]$ and $T_1[1]$ follows that $\boldsymbol{W_{28}}$ collides.

From collision of the hash value follows collision of the values W_{31}, W_{30}, W_{29}, W_{28}, W_{27}, W_{26} and $T_1[1]$, $T_1[2]$. We can easily see that the reverse implication holds too.

The case of r = 3

After the third round we have

$$T_1[1] = W_{24}^{+} + \Sigma_1(W_{27}^{+}) + Ch(W_{27}^{+}, W_{26}^{+}, W_{25}^{+}) + W_0^{\sim}$$
$$T_2[1] = \Sigma_0(W_{31}^{+}) + Maj(W_{31}^{+}, W_{30}^{+}, W_{29}^{+})$$
$$e[1] = W_{28}^{+} + T_1[1]$$
$$a[1] = T_1[1] + T_2[1]$$

$$T_1[2] = W_{25}^{+} + \Sigma_1(e[1]) + Ch(e[1], W_{27}^{+}, W_{26}^{+}) + W_1^{\sim}$$
$$T_2[2] = \Sigma_0(a[1]) + Maj(a[1], W_{31}^{+}, W_{30}^{+})$$
$$e[2] = W_{29}^{+} + T_1[2]$$
$$a[2] = T_1[2] + T_2[2]$$

$$T_1[3] = W_{26}^{+} + \Sigma_1(e[2]) + Ch(e[2], e[1], W_{27}^{+}) + W_2^{\sim}$$

$$T_2[3] = \Sigma_0(a[2]) + Maj(a[2], a[1], W_{31}^{+})$$
$$e[3] = W_{30}^{+} + T_1[3]$$
$$a[3] = T_1[3] + T_2[3]$$

Hash value consists of values in the row t = 3 of the Table 1. The collision means that two different messages have these values the same:

$a[3]$	$a[2]$	$a[1]$	W_{31}^{+}	$e[3]$	$e[2]$	$e[1]$	W_{27}^{+}

It means that the value $T_2[3]$ also collides, because it uses primarily colliding values.

From collision of $a[3]$ and $T_2[3]$ follows that $\boldsymbol{T_1[3]}$ collides too.

From collision of $e[3]$ follows that $\boldsymbol{W_{30}}$ collides too.

From collision of W_{30} follows that $T_2[2]$ collides. From collision of $a[2]$ and $T_2[2]$ follows that $\boldsymbol{T_1[2]}$ collides too.

From collision of $e[2]$ and $T_1[2]$ follows that $\boldsymbol{W_{29}}$ collides too.

From collision of W_{29} follows that $T_2[1]$ collides. From collision of $a[1]$ and $T_2[1]$ follows that $\boldsymbol{T_1[1]}$ collides.

From collision of $e[1]$ and $T_1[1]$ follows that $\boldsymbol{W_{28}}$ collides too.

From collision of the hash value also follows collision of the values W_{31}, W_{30}, W_{29}, W_{28}, W_{27} and $T_1[1]$, $T_1[2]$ and $T_1[3]$. We can easily see that the reverse implication holds too.

The case of *r* = 4

After the fourth round we have

$$T_1[1] = W_{24}^{+} + \Sigma_1(W_{27}^{+}) + Ch(W_{27}^{+}, W_{26}^{+}, W_{25}^{+}) + W_0^{\sim}$$
$$T_2[1] = \Sigma_0(W_{31}^{+}) + Maj(W_{31}^{+}, W_{30}^{+}, W_{29}^{+})$$
$$e[1] = W_{28}^{+} + T_1[1]$$
$$a[1] = T_1[1] + T_2[1]$$

$$T_1[2] = W_{25}^{+} + \Sigma_1(e[1]) + Ch(e[1], W_{27}^{+}, W_{26}^{+}) + W_1^{\sim}$$
$$T_2[2] = \Sigma_0(a[1]) + Maj(a[1], W_{31}^{+}, W_{30}^{+})$$
$$e[2] = W_{29}^{+} + T_1[2]$$
$$a[2] = T_1[2] + T_2[2]$$

$$T_1[3] = W_{26}^{+} + \Sigma_1(e[2]) + Ch(e[2], e[1], W_{27}^{+}) + W_2^{\sim}$$
$$T_2[3] = \Sigma_0(a[2]) + Maj(a[2], a[1], W_{31}^{+})$$

$$e[3] = W_{30}^{+} + T_1[3]$$
$$a[3] = T_1[3] + T_2[3]$$

$$T_1[4] = W_{27}^{+} + \Sigma_1(e[3]) + Ch(e[3], e[2], e[1]) + W_3^{\sim}$$
$$T_2[4] = \Sigma_0(a[3]) + Maj(a[3], a[2], a[1])$$
$$e[4] = W_{31}^{+} + T_1[4]$$
$$a[4] = T_1[4] + T_2[4]$$

Hash value consists of values in the row $t = 4$ of the Table 1. The collision means that two different messages have these values the same:

$a[4]$	$a[3]$	$a[2]$	$a[1]$	$e[4]$	$e[3]$	$e[2]$	$e[1]$

It means that the value $T_2[4]$ also collides, because it uses primarily colliding values.
From collision of $a[4]$ and $T_2[4]$ follows that $\boldsymbol{T_1[4]}$ collides.
From collision of $e[4]$ follows that $\boldsymbol{W_{31}}$ collides.
From collision of W_{31} follows that $T_2[3]$ collides. From collision of $a[3]$ and $T_2[3]$ follows that $\boldsymbol{T_1[3]}$ collides.
From collision of $e[3]$ and $T_1[3]$ follows that $\boldsymbol{W_{30}}$ collides.
From collision of W_{30} follows that $T_2[2]$ collides. From collision of $a[2]$ and $T_2[2]$ follows that $\boldsymbol{T_1[2]}$ collides.
From collision of $e[2]$ and $T_1[2]$ follows that $\boldsymbol{W_{29}}$ collides.
From collision of W_{29} follows that $T_2[1]$ collides. From collision of $a[1]$ and $T_2[1]$ follows that $\boldsymbol{T_1[1]}$ collides.
From collision of $e[1]$ and $T_1[1]$, follows that $\boldsymbol{W_{28}}$ collides.

From collision of the hash value also follows collision of the values W_{31}, W_{30}, W_{29}, W_{28} and $T_1[1]$, $T_1[2]$, $T_1[3]$ and $T_1[4]$. We can easily see that the reverse implication holds too.

The case of *r* = 5

After the fifth round we have

$$T_1[1] = W_{24}^{+} + \Sigma_1(W_{27}^{+}) + Ch(W_{27}^{+}, W_{26}^{+}, W_{25}^{+}) + W_0^{\sim}$$
$$T_2[1] = \Sigma_0(W_{31}^{+}) + Maj(W_{31}^{+}, W_{30}^{+}, W_{29}^{+})$$
$$e[1] = W_{28}^{+} + T_1[1]$$
$$a[1] = T_1[1] + T_2[1]$$

$$T_1[2] = W_{25}^{+} + \Sigma_1(e[1]) + Ch(e[1], W_{27}^{+}, W_{26}^{+}) + W_1^{\sim}$$
$$T_2[2] = \Sigma_0(a[1]) + Maj(a[1], W_{31}^{+}, W_{30}^{+})$$
$$e[2] = W_{29}^{+} + T_1[2]$$

$$a[2] = T_1[2] + T_2[2]$$

$$T_1[3] = W_{26}^{+} + \Sigma_1(e[2]) + Ch(e[2], e[1], W_{27}^{+}) + W_2^{\sim}$$
$$T_2[3] = \Sigma_0(a[2]) + Maj(a[2], a[1], W_{31}^{+})$$
$$e[3] = W_{30}^{+} + T_1[3]$$
$$a[3] = T_1[3] + T_2[3]$$

$$T_1[4] = W_{27}^{+} + \Sigma_1(e[3]) + Ch(e[3], e[2], e[1]) + W_3^{\sim}$$
$$T_2[4] = \Sigma_0(a[3]) + Maj(a[3], a[2], a[1])$$
$$e[4] = W_{31}^{+} + T_1[4]$$
$$a[4] = T_1[4] + T_2[4]$$

$$T_1[5] = e[1] + \Sigma_1(e[4]) + Ch(e[4], e[3], e[2]) + W_4^{\sim}$$
$$T_2[5] = \Sigma_0(a[4]) + Maj(a[4], a[3], a[2])$$
$$e[5] = a[1] + T_1[5]$$
$$a[5] = T_1[5] + T_2[5]$$

Hash value consists of values in the row $t = 5$ of the Table 1. The collision means that two different messages have these values the same:

$a[5]$	$a[4]$	$a[3]$	$a[2]$	$e[5]$	$e[4]$	$e[3]$	$e[2]$

It means that the value $T_2[5]$ also collides, because it uses primarily colliding values.

From collision of $T_2[5]$ and $a[5]$ follows that $\boldsymbol{T_1[5]}$ collides.

From collision of $T_1[5]$ and $e[5]$ follows that $\boldsymbol{a[1]}$ collides.

From collision of $a[1]$ follows that $T_2[4]$ collides. From collision of $T_2[4]$ and $a[4]$ and follows that $\boldsymbol{T_1[4]}$ collides.

From collision of $T_1[4]$ and $e[4]$ follows that $\boldsymbol{W_{31}}$ collides.

From collision of W_{31} follows that $T_2[3]$ collides. From collision of $a[3]$ and $T_2[3]$ follows that $\boldsymbol{T_1[3]}$ collides.

From collision of $e[3]$ and $T_1[3]$ follows that $\boldsymbol{W_{30}}$ collides.

From collision of W_{30} follows that $T_2[2]$ collides. From collision of $a[2]$ and $T_2[2]$ follows that $\boldsymbol{T_1[2]}$ collides.

From collision of $e[2]$ and $T_1[2]$ follows that $\boldsymbol{W_{29}}$ collides.

From collision of the hash value follows collision of the values W_{31}, W_{30}, W_{29} and $a[1]$, $T_1[2]$, $T_1[3]$, $T_1[4]$ and $T_1[5]$. We can easily see that the reverse implication holds too.

The case of *r* = 6

After the sixth round we have

$$T_1[1] = W_{24}^{+} + \Sigma_1\left(W_{27}^{+}\right) + Ch(W_{27}^{+}, W_{26}^{+}, W_{25}^{+}) + W_0^{\sim}$$
$$T_2[1] = \Sigma_0\left(W_{31}^{+}\right) + Maj(W_{31}^{+}, W_{30}^{+}, W_{29}^{+})$$
$$e[1] = W_{28}^{+} + T_1[1]$$
$$a[1] = T_1[1] + T_2[1]$$

$$T_1[2] = W_{25}^{+} + \Sigma_1(e[1]) + Ch(e[1], W_{27}^{+}, W_{26}^{+}) + W_1^{\sim}$$
$$T_2[2] = \Sigma_0(a[1]) + Maj(a[1], W_{31}^{+}, W_{30}^{+})$$
$$e[2] = W_{29}^{+} + T_1[2]$$
$$a[2] = T_1[2] + T_2[2]$$

$$T_1[3] = W_{26}^{+} + \Sigma_1(e[2]) + Ch(e[2], e[1], W_{27}^{+}) + W_2^{\sim}$$
$$T_2[3] = \Sigma_0(a[2]) + Maj(a[2], a[1], W_{31}^{+})$$
$$e[3] = W_{30}^{+} + T_1[3]$$
$$a[3] = T_1[3] + T_2[3]$$

$$T_1[4] = W_{27}^{+} + \Sigma_1(e[3]) + Ch(e[3], e[2], e[1]) + W_3^{\sim}$$
$$T_2[4] = \Sigma_0(a[3]) + Maj(a[3], a[2], a[1])$$
$$e[4] = W_{31}^{+} + T_1[4]$$
$$a[4] = T_1[4] + T_2[4]$$

$$T_1[5] = e[1] + \Sigma_1(e[4]) + Ch(e[4], e[3], e[2]) + W_4^{\sim}$$
$$T_2[5] = \Sigma_0(a[4]) + Maj(a[4], a[3], a[2])$$
$$e[5] = a[1] + T_1[5]$$
$$a[5] = T_1[5] + T_2[5]$$

$$T_1[6] = e[2] + \Sigma_1(e[5]) + Ch(e[5], e[4], e[3]) + W_5^{\sim}$$
$$T_2[6] = \Sigma_0(a[5]) + Maj(a[5], a[4], a[3])$$
$$e[6] = a[2] + T_1[6]$$
$$a[6] = T_1[6] + T_2[6]$$

Hash value consists of values in the row t = 6 of the Table 1. The collision means that two different messages have these values the same:

$a[6]$	$a[5]$	$a[4]$	$A[3]$	$e[6]$	$e[5]$	$e[4]$	$e[3]$

It means that the value $T_2[6]$ also collides, because it uses primarily colliding values.

From collision of $T_2[6]$ and $a[6]$ follows that $\boldsymbol{T_1[6]}$ collides.

From collision of $T_1[6]$ and $e[6]$ follows that $\boldsymbol{a[2]}$ collides.

From collision of $a[2]$ follows that $T_2[5]$ collides. From collision of $T_2[5]$ and $a[5]$ follows that $\boldsymbol{T_1[5]}$ collides.

From collision of $T_1[5]$ and $e[5]$ follows that $\boldsymbol{a[1]}$ collides.

From collision of $a[1]$ follows that $T_2[4]$ collides. From collision of $T_2[4]$ and $a[4]$ follows that $\boldsymbol{T_1[4]}$ collides.

From collision of $e[4]$ and $T_1[4]$ follows that $\boldsymbol{W_{31}}$ collides.

From collision of W_{31} follows that $T_2[3]$ collides. From collision of $T_2[3]$ and $a[3]$ follows that $\boldsymbol{T_1[3]}$ collides.

From collision of $e[3]$ and $T_1[3]$ follows that $\boldsymbol{W_{30}}$ collides.

From collision of the hash value also follows collision of the values W_{31}, W_{30} and $a[1]$, $a[2]$, $T_1[3]$, $T_1[4]$, $T_1[5]$ and $T_1[6]$. We can easily see that the reverse implication holds too.

The case of *r* = 7

After the seventh round we have

$$T_1[1] = \mathrm{W}_{24}^{+} + \Sigma_1(\mathrm{W}_{27}^{+}) + Ch(\mathrm{W}_{27}^{+}, \mathrm{W}_{26}^{+}, \mathrm{W}_{25}^{+}) + W_0^{\sim}$$
$$T_2[1] = \Sigma_0(\mathrm{W}_{31}^{+}) + Maj(\mathrm{W}_{31}^{+}, \mathrm{W}_{30}^{+}, \mathrm{W}_{29}^{+})$$
$$e[1] = \mathrm{W}_{28}^{+} + T_1[1]$$
$$a[1] = T_1[1] + T_2[1]$$

$$T_1[2] = \mathrm{W}_{25}^{+} + \Sigma_1(e[1]) + Ch(e[1], \mathrm{W}_{27}^{+}, \mathrm{W}_{26}^{+}) + W_1^{\sim}$$
$$T_2[2] = \Sigma_0(a[1]) + Maj(a[1], \mathrm{W}_{31}^{+}, \mathrm{W}_{30}^{+})$$
$$e[2] = \mathrm{W}_{29}^{+} + T_1[2]$$
$$a[2] = T_1[2] + T_2[2]$$

$$T_1[3] = \mathrm{W}_{26}^{+} + \Sigma_1(e[2]) + Ch(e[2], e[1], \mathrm{W}_{27}^{+}) + W_2^{\sim}$$
$$T_2[3] = \Sigma_0(a[2]) + Maj(a[2], a[1], \mathrm{W}_{31}^{+})$$
$$e[3] = \mathrm{W}_{30}^{+} + T_1[3]$$
$$a[3] = T_1[3] + T_2[3]$$

$$T_1[4] = W_{27}^{+} + \Sigma_1(e[3]) + Ch(e[3], e[2], e[1]) + W_3^{\sim}$$
$$T_2[4] = \Sigma_0(a[3]) + Maj(a[3], a[2], a[1])$$
$$e[4] = W_{31}^{+} + T_1[4]$$
$$a[4] = T_1[4] + T_2[4]$$

$$T_1[5] = e[1] + \Sigma_1(e[4]) + Ch(e[4], e[3], e[2]) + W_4^{\sim}$$
$$T_2[5] = \Sigma_0(a[4]) + Maj(a[4], a[3], a[2])$$
$$e[5] = a[1] + T_1[5]$$
$$a[5] = T_1[5] + T_2[5]$$

$$T_1[6] = e[2] + \Sigma_1(e[5]) + Ch(e[5], e[4], e[3]) + W_5^{\sim}$$
$$T_2[6] = \Sigma_0(a[5]) + Maj(a[5], a[4], a[3])$$
$$e[6] = a[2] + T_1[6]$$
$$a[6] = T_1[6] + T_2[6]$$

$$T_1[7] = e[3] + \Sigma_1(e[6]) + Ch(e[6], e[5], e[4]) + W_6^{\sim}$$
$$T_2[7] = \Sigma_0(a[6]) + Maj(a[6], a[5], a[4])$$
$$e[7] = a[3] + T_1[7]$$
$$a[7] = T_1[7] + T_2[7]$$

Hash value consists of values in the row t = 7 of the Table 1. The collision means that two different messages have these values the same:

$a[7]$	$a[6]$	$a[5]$	$a[4]$	$e[7]$	$e[6]$	$e[5]$	$e[4]$

It means that the value $T_2[7]$ also collides, because it uses primarily colliding values.

From collision of $T_2[7]$ and $a[7]$ follows that $\boldsymbol{T_1[7]}$ collides.

From collision of $T_1[7]$ and $e[7]$ follows that $\boldsymbol{a[3]}$ collides.

From collision of $a[3]$ follows that $T_2[6]$ collides. From collision of $T_2[6]$ and $a[6]$ follows that $\boldsymbol{T_1[6]}$ collides.

From collision of $T_1[6]$ and $e[6]$ follows that $\boldsymbol{a[2]}$ collides.

From collision of $a[2]$ follows that $T_2[5]$ collides. From collision of $T_2[5]$ and $a[5]$ follows that $\boldsymbol{T_1[5]}$ collides.

From collision of $e[5]$ and $T_1[5]$ follows that $\boldsymbol{a[1]}$ collides.

From collision of $a[1]$ follows that $T_2[4]$ collides. From collision of $T_2[4]$ and $a[4]$ follows that $\boldsymbol{T_1[4]}$ collides.

From collision of $T_1[4]$ and $e[4]$ follows that $\boldsymbol{W_{31}}$ collides.

From collision of the hash value follows collision of the values W_{31} and $a[1]$, $a[2]$, $a[3]$, $T_1[4]$, $T_1[5]$, $T_1[6]$ and $T_1[7]$. We can easily see that the reverse implication holds too.

The case of *r* = 8

After the 8th round we have

$$T_1[1] = \mathrm{W}_{24}^{+} + \Sigma_1(\mathrm{W}_{27}^{+}) + Ch(\mathrm{W}_{27}^{+}, \mathrm{W}_{26}^{+}, \mathrm{W}_{25}^{+}) + W_0^{\sim}$$
$$T_2[1] = \Sigma_0(\mathrm{W}_{31}^{+}) + Maj(\mathrm{W}_{31}^{+}, \mathrm{W}_{30}^{+}, \mathrm{W}_{29}^{+})$$
$$e[1] = \mathrm{W}_{28}^{+} + T_1[1]$$
$$a[1] = T_1[1] + T_2[1]$$

$$T_1[2] = \mathrm{W}_{25}^{+} + \Sigma_1(e[1]) + Ch(e[1], \mathrm{W}_{27}^{+}, \mathrm{W}_{26}^{+}) + W_1^{\sim}$$
$$T_2[2] = \Sigma_0(a[1]) + Maj(a[1], \mathrm{W}_{31}^{+}, \mathrm{W}_{30}^{+})$$
$$e[2] = \mathrm{W}_{29}^{+} + T_1[2]$$
$$a[2] = T_1[2] + T_2[2]$$

$$T_1[3] = \mathrm{W}_{26}^{+} + \Sigma_1(e[2]) + Ch(e[2], e[1], \mathrm{W}_{27}^{+}) + W_2^{\sim}$$
$$T_2[3] = \Sigma_0(a[2]) + Maj(a[2], a[1], \mathrm{W}_{31}^{+})$$
$$e[3] = \mathrm{W}_{30}^{+} + T_1[3]$$
$$a[3] = T_1[3] + T_2[3]$$

$$T_1[4] = \mathrm{W}_{27}^{+} + \Sigma_1(e[3]) + Ch(e[3], e[2], e[1]) + W_3^{\sim}$$
$$T_2[4] = \Sigma_0(a[3]) + Maj(a[3], a[2], a[1])$$
$$e[4] = \mathrm{W}_{31}^{+} + T_1[4]$$
$$a[4] = T_1[4] + T_2[4]$$

$$T_1[5] = e[1] + \Sigma_1(e[4]) + Ch(e[4], e[3], e[2]) + W_4^{\sim}$$
$$T_2[5] = \Sigma_0(a[4]) + Maj(a[4], a[3], a[2])$$
$$e[5] = a[1] + T_1[5]$$
$$a[5] = T_1[5] + T_2[5]$$

$$T_1[6] = e[2] + \Sigma_1(e[5]) + Ch(e[5], e[4], e[3]) + W_5^{\sim}$$
$$T_2[6] = \Sigma_0(a[5]) + Maj(a[5], a[4], a[3])$$

$$e[6] = a[2] + T_1[6]$$
$$a[6] = T_1[6] + T_2[6]$$

$$T_1[7] = e[3] + \Sigma_1(e[6]) + Ch(e[6], e[5], e[4]) + W_6^{\sim}$$
$$T_2[7] = \Sigma_0(a[6]) + Maj(a[6], a[5], a[4])$$
$$e[7] = a[3] + T_1[7]$$
$$a[7] = T_1[7] + T_2[7]$$

$$T_1[8] = e[4] + \Sigma_1(e[7]) + Ch(e[7], e[6], e[5]) + W_7^{\sim}$$
$$T_2[8] = \Sigma_0(a[7]) + Maj(a[7], a[6], a[5])$$
$$e[8] = a[4] + T_1[8]$$
$$a[8] = T_1[8] + T_2[8]$$

Hash value consists of values in the row $t = 8$ of the Table 1. The collision means that two different messages have these values the same:

$a[8]$	$a[7]$	$a[6]$	$a[5]$	$e[8]$	$e[7]$	$e[6]$	$e[5]$

It means that the value $T_2[8]$ also collides, because it uses primarily colliding values.

From collision of $T_2[8]$ and $a[8]$ follows that $\boldsymbol{T_1[8]}$ collides.

From collision of $T_1[8]$ and $e[8]$ follows that $\boldsymbol{a[4]}$ collides.

From collision of $a[4]$ and $a[7]$ follows that $\boldsymbol{T_1[7]}$ collides.

From collision of $T_1[7]$ and $e[7]$ follows that $\boldsymbol{a[3]}$ collides.

From collision of $a[3]$ follows that $T_2[6]$ collides. From collision of $T_2[6]$ and $a[6]$ follows that $\boldsymbol{T_1[6]}$ collides.

From collision of $T_1[6]$ and $e[6]$ follows that $\boldsymbol{a[2]}$ collides.

From collision of $a[2]$ follows that $T_2[5]$ collides. From collision of $T_2[5]$ and $a[5]$ follows that $\boldsymbol{T_1[5]}$ collides.

From collision of $e[5]$ and $T_1[5]$ follows that $\boldsymbol{a[1]}$ collides.

From collision of $a[1]$ follows that $T_2[4]$ collides. From collision of $T_2[4]$ and $a[4]$ follows that $\boldsymbol{T_1[4]}$ collides.

From collision of the hash value follows collision of the values $a[1]$, $a[2]$, $a[3]$, $a[4]$, $T_1[4]$, $T_1[5]$, $T_1[6]$, $T_1[7]$ and $T_1[8]$. We can easily see that the reverse implication holds too. QED.

Theorem 1

(i) The complexity of finding a collision of Turbo SHA-256-r is maximally of the order 2^{16r} for $r = 1, ..., 8$.

(ii) The complexity of finding a collision of Turbo SHA-512-r is maximally of the order 2^{32r} for $r = 1, ..., 8$.

Furthermore, we can partially choose the colliding hash value for $r = 1$, 2 and 3.

Proof. The proof of Theorem 1 is very similar for all values of r. We find Turbo SHA-r collision using the row r of Tab.2, Lemma 1 and the following algorithm:

1. Set randomly values of variables in the second column of Tab.2 (for instance for $r = 2$ we randomly set values of $W_{31}, ..., W_{26}$)
2. For i = 1 to 2^{16r} do

   {

   a) choose randomly set of values of variables in the forth column (for instance for $r = 2$ randomly set values of $W_{25}, ..., W_{16}$)
   b) from $W_{31}, ..., W_{16}$ compute $W_{15},..., W_0$ (it is bijective transformation, [1])
   c) from $W_{31}, ..., W_{16}$ and $W_{15},..., W_0$ compute the values of variables in the third column and store them in the set S (for instance for $r = 2$ we compute and store set of values ($T_1[1]$, $T_1[2]$) in S)

   }
3. Using birthday paradox find a collision in the set S

Because we have r (32-bit) variables in the third column, we need to choose approximately $2^{32*r/2}$ values in the Step 2 to have a good chance to find a collision in the set S[1]. We always have at minimum r words in the fourth column, so the attack is possible.

Conclusion

In this paper we don't examine security of Turbo SHA-2 completely, we only show new collision attacks on it, with smaller complexity than it was considered by Turbo SHA-2 authors [1]. From Theorem 1 follows that the only remaining candidates from the hash family Turbo SHA-2 are Turbo SHA-256 and Turbo SHA-512 with full 8

[1] Let us note that we can assume that variables in the third column in Tab. 2 are statistically independent random variables. For instance in case of $r = 8$ we can express $a[1]$, $a[2]$ and $a[3]$ in terms of $T_1[1]$, $T_1[2]$ and $T_1[3]$. Furthermore, $T_1[1]$, $T_1[2]$, $T_1[3]$, $T_1[4]$, $T_1[5]$, $T_1[6]$, $T_1[7]$, $T_1[8]$ depend on different variables $W_t^{\sim} = (W_t \oplus W_{t+16}) + (W_{t+4} \oplus W_{t+24}) + (W_{t+8} \oplus W_{t+20}) + W_{t+12}, t = 0,...,7$, what means dependence on different variables from the set $\{W_{31}, ..., W_{16}\}$ and different variables from the set $\{W_{15},..., W_0\}$. Because we choose variables in the fourth column randomly and independently, we can also expect that $a[1]$, $a[2]$, $a[3]$, $T_1[4]$, $T_1[5]$, $T_1[6]$, $T_1[7]$, $T_1[8]$ behave as independent random variables.

rounds. The original security reserve of 6 round has been lost. There is an open question how to increase security of the proposal.

Acknowledgement

We would like to thank Daniel Joščák for insightful comments on a preliminary draft of the paper. It helped us to improve the clarity of the paper.

References

[1] Gligoroski D., Knapskog S. J.: Turbo SHA-2, IACR ePrint archive Report 2007/403, October 2007, http://eprint.iacr.org/2007/403.pdf.