O kolizích hašovací funkce Turbo SHA-2

Vlastimil Klima

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

Abstrakt. Tento příspěvek se nezabývá bezpečností Turbo SHA-2 komplexně, pouze ukazuje nové kolizní útoky s menší složitostí, než předpokládali její autoři. V [1] se uvažuje Turbo SHA-224/256-*r* a Turbo SHA-384/512-*r* s proměnným počtem rund kompresní části *r* od 1 do 8. Při hledání kolizí autoři [1] ukazují kolizní útok na Turbo SHA-256-1 s jednou rundou se složitostí 2^{64}. Pro *r* od 2 do 8 nenalézají jiný útok, než se složitostí 2^{128}. Podobně pro Turbo SHA-512 nalézají pouze kolizní útok na Turbo SHA-512-1 s jednou rundou se složitostí 2^{128}. Pro *r* od 2 do 8 nenalézají jiný útok, než se složitostí 2^{256}. V tomto příspěvku ukazujeme útok na Turbo SHA-256-*r* pro *r* = 1, 2, ..., 8 se složitostí 2^{16r} a útok na Turbo SHA-512-*r* pro *r* = 1, 2, ..., 8 se složitostí 2^{32r}. Odtud vyplývá, že jediným kandidátem zůstává Turbo SHA-256 a Turbo SHA-512 s osmi rundami. Původní bezpečnostní rezerva 6 rund je však ztracena.

Klíčová slova: Turbo SHA-2, kolize.

Úvod

V dalším uvažujme pouze Turbo SHA-256-*r*. Tvrzení a důkazy pro Turbo SHA-512-*r* se liší pouze délkou slova 32 a 64 bitů. V následujícím textu nejprve uvedeme označení proměnných pro Turbo SHA-256-*r*. Potom následuje Lemma 1, hlavní tvrzení je obsaženo ve Větě 1. Závěr obsahuje důsledek Věty 1.

Označení

Původní definici Turbo SHA-2 ukazuje Obr. 1 [1]. Definici Turbo SHA-2-*r* ukazuje Obr. 2. Oproti originálnímu popisu očíslujeme proměnné a až h podle čísla rundy, dále uvažujme jen jeden blok hašování, a proto výslednou hašovací hodnotu uvažujme bez přičtení konstanty $H^{(0)}$ v kroku 5 originálního popisu. Dále v kroku 3 při úvodním načtení konstanty $H^{(0)}$ na proměnné $a[0] = W_{31} + H^{(0)}_0$, $b[0] = W_{30} + H^{(0)}_1$, ..., $h[0] = W_{24} + H^{(0)}_7$ označme toto přičtení pro jednoduchost jako $a[0] := W_{31}^{+}$, $b[0] := W_{30}^{+}$, ..., $h[0] := W_{24}^{+}$. Dále označme ještě

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

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 $H^{(i)}$:

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

}

Obr. 1: Turbo SHA-2 [1]

V definici Turbo SHA z Obr. 1 zapíšeme Kroky 3 a 4 následovně.

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

Krok 4:
For $t = 1$ to r
{
$T_1[t] = h[t-1] + \Sigma_1(e[t-1]) + Ch(e[t-1], f[t-1], g[t-1]) + W_{t-1}^{\sim}$
$T_2[t] = \Sigma_0(a[t-1]) + Maj(a[t-1], b[t-1], c[t-1])$
$h[t] = g[t-1]$
$g[t] = f[t-1]$
$f[t] = e[t-1]$
$e[t] = d[t-1] + T_1[t-1]$
$d[t] = c[t-1]$
$c[t] = b[t-1]$
$b[t] = a[t-1]$
$a[t] = T_1[t-1] + T_2[t-1]$
}

Hodnoty pracovních proměnných (*a, b, c, d, e, f, g, h*) vznikajících v jednotlivých rundách podle rovnic v Kroku 4 jsou uvedeny v tabulce 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: Hodnoty pracovních proměnných *a* - *h*

Lemma 1.
Nalezení kolize v Turbo SHA-*r* je ekvivalentní nalezení dvou různých zpráv, pro které jsou hodnoty proměnných z druhého a třetího sloupce Tab. 2 stejné.

	Kolize Turbo SHA-r		
r	***pevné hodnoty (zvolené náhodně)***	***kolize narozeninovým paradoxem na hodnotách***	***volné hodnoty (volené náhodně)***
1	$W_{31,\,30,\,29,\,28,\,27,\,26,\,25}$	$T_1[1]$	$W_{24,\,23,\,\ldots,\,16}$
2	$W_{31,\,30,\,29,\,28,\,27,\,26}$	$T_1[1]$, $T_1[2]$	$W_{25,\,24,\,\ldots,\,16}$
3	$W_{31,\,30,\,29,\,28,\,27}$	$T_1[1]$, $T_1[2]$, $T_1[3]$	$W_{26,\,25,\,\ldots,\,16}$
4	$W_{31,\,30,\,29,\,28}$	$T_1[1]$, $T_1[2]$, $T_1[3]$, $T_1[4]$	$W_{27,\,26,\,\ldots,\,16}$
5	$W_{31,\,30,\,29}$	$T_1[1]$, $T_1[2]$, $T_1[3]$, $T_1[4]$, $T_1[5]$	$W_{28,\,27,\,\ldots,\,16}$
6	$W_{31,\,30}$	$a[1]$,$T_1[2]$, $T_1[3]$, $T_1[4]$, $T_1[5]$, $T_1[6]$	$W_{29,\,28,\,\ldots,\,16}$
7	W_{31}	$a[1]$, $a[2]$,$T_1[3]$, $T_1[4]$, $T_1[5]$, $T_1[6]$, $T_1[7]$	$W_{30,\,29,\,\ldots,\,16}$
8	---	$a[1]$,$a[2]$,$a[3]$,$T_1[4]$,$T_1[5]$,$T_1[6]$,$T_1[7]$,$T_1[8]$	$W_{31,\,30,\,\ldots,\,16}$

Tab. 2: Kolize Turbo SHA-*r*

Důkaz

Případ *r* = 1

Po první rundě máme

$$T_1[1] = \mathrm{W}_{24}^{+} + \Sigma_1\left(\mathrm{W}_{27}^{+}\right) + Ch(\mathrm{W}_{27}^{+}, \mathrm{W}_{26}^{+}, \mathrm{W}_{25}^{+}) + W_0^{\sim}$$

$$T_2[1] = \Sigma_0\left(\mathrm{W}_{31}^{+}\right) + Maj(\mathrm{W}_{31}^{+}, \mathrm{W}_{30}^{+}, \mathrm{W}_{29}^{+})$$

$$e[1] = \mathrm{W}_{28}^{+} + T_1[1]$$

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

Hašovací hodnota je tvořena hodnotami v řádku $t = 1$ Tabulky 1. Kolize znamená, že dvě různé zprávy mají tyto stejné hodnoty:

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

Odtud plyne, že koliduje i $T_2[1]$, neboť používá kolidující hodnoty W_{31}, W_{30}, W_{29}.

Z kolize $a[1]$ a $T_2[1]$ vyplývá i kolize $\boldsymbol{T_1[1]}$.

Z kolize $e[1]$ a $T_1[1]$ vyplývá i kolize $\boldsymbol{W_{28}}$.

Z kolize hašovací hodnoty tak vyplývá celkově kolize hodnot W_{31}, W_{30}, W_{29}, W_{28}, W_{27}, W_{26}, W_{25} a $T_1[1]$. Snadno se přesvědčíme, že platí i obrácené tvrzení.

Případ *r* = 2

Po druhé rundě máme

$$T_1[1] = \mathrm{W}_{24}^{+} + \Sigma_1\left(\mathrm{W}_{27}^{+}\right) + Ch(\mathrm{W}_{27}^{+}, \mathrm{W}_{26}^{+}, \mathrm{W}_{25}^{+}) + W_0^{\sim}$$

$$T_2[1] = \Sigma_0\left(\mathrm{W}_{31}^{+}\right) + Maj(\mathrm{W}_{31}^{+}, \mathrm{W}_{30}^{+}, \mathrm{W}_{29}^{+})$$

$$e[1] = \mathrm{W}_{28}^{+} + T_1[1]$$

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

$$T_1[2] = \mathrm{W}_{25}^{+} + \Sigma_1\left(e[1]\right) + Ch(e[1], \mathrm{W}_{27}^{+}, \mathrm{W}_{26}^{+}) + W_1^{\sim}$$

$$T_2[2] = \Sigma_0(a[1]) + Maj(a[1], \mathrm{W}_{31}^{+}, \mathrm{W}_{30}^{+})$$
$$e[2] = \mathrm{W}_{29}^{+} + T_1[2]$$
$$a[2] = T_1[2] + T_2[2]$$

Hašovací hodnota je tvořena hodnotami v řádku $t = 2$ Tabulky 1. Kolize znamená, že dvě různé zprávy mají tyto stejné hodnoty:

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

Odtud plyne, že koliduje i $T_2[2]$, neboť používá primární kolidující hodnoty.
Z kolize $a[2]$ a $T_2[2]$ vyplývá i kolize $\boldsymbol{T_1[2]}$.
Z kolize $e[2]$ a $T_1[2]$ vyplývá i kolize $\boldsymbol{W_{29}}$.
Z kolize W_{29} plyne kolize $T_2[1]$. Z kolize $a[1]$ a $T_2[1]$ vyplývá kolize $\boldsymbol{T_1[1]}$.
Z kolize $e[1]$ a $T_1[1]$ vyplývá i kolize $\boldsymbol{W_{28}}$.

Z kolize hašovací hodnoty tak vyplývá i kolize hodnot W_{31}, W_{30}, W_{29}, W_{28}, W_{27}, W_{26} a $T_1[1]$, $T_1[2]$. Snadno se přesvědčíme, že platí i obrácené tvrzení.

Případ $r = 3$
Po třetí rundě máme
$$T_1[1] = \mathrm{W}_{24}^{+} + \Sigma_1(\mathrm{W}_{27}^{+}) + Ch(\mathrm{W}_{27}^{+}, \mathrm{W}_{26}^{+}, \mathrm{W}_{25}^{+}) + W_0^{\sim}$$
$$T_2[1] = \Sigma_0(\mathrm{W}_{31}^{+}) + Maj(\mathrm{W}_{31}^{+}, \mathrm{W}_{30}^{+}, \mathrm{W}_{29}^{+})$$
$$e[1] = \mathrm{W}_{28}^{+} + T_1[1]$$
$$a[1] = T_1[1] + T_2[1]$$

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

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

Hašovací hodnota je tvořena hodnotami v řádku $t = 3$ Tabulky 1. Kolize znamená, že dvě různé zprávy mají tyto stejné hodnoty:

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

Odtud plyne, že koliduje i $T_2[3]$, neboť používá primární kolidující hodnoty.
Z kolize $a[3]$ a $T_2[3]$ vyplývá i kolize $\boldsymbol{T_1[3]}$.
Z kolize $e[3]$ vyplývá i kolize $\boldsymbol{W_{30}}$.
Z kolize W_{30} plyne kolize $T_2[2]$. Z kolize $a[2]$ a $T_2[2]$ vyplývá kolize $\boldsymbol{T_1[2]}$.
Z kolize $e[2]$ a $T_1[2]$ vyplývá i kolize $\boldsymbol{W_{29}}$.
Z kolize W_{29} plyne kolize $T_2[1]$. Z kolize $a[1]$ a $T_2[1]$ vyplývá kolize $\boldsymbol{T_1[1]}$.
Z kolize $e[1]$ a $T_1[1]$ vyplývá i kolize $\boldsymbol{W_{28}}$.

Z kolize hašovací hodnoty tak vyplývá i kolize hodnot W_{31}, W_{30}, W_{29}, W_{28}, W_{27} a $T_1[1]$, $T_1[2]$ a $T_1[3]$. Snadno se přesvědčíme, že platí i obrácené tvrzení.

Případ $r = 4$
Po čtvrté rundě máme

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

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

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

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

Hašovací hodnota je tvořena hodnotami v řádku $t = 4$ Tabulky 1. Kolize znamená, že dvě různé zprávy mají tyto stejné hodnoty:

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

Odtud plyne, že koliduje i $T_2[4]$, neboť používá primární kolidující hodnoty.
Z kolize $a[4]$ a $T_2[4]$ vyplývá i kolize $\boldsymbol{T_1[4]}$.
Z kolize $e[4]$ vyplývá i kolize $\boldsymbol{W_{31}}$.
Z kolize W_{31} plyne kolize $T_2[3]$. Z kolize $a[3]$ a $T_2[3]$ vyplývá kolize $\boldsymbol{T_1[3]}$.
Z kolize $e[3]$ a $T_1[3]$ vyplývá i kolize $\boldsymbol{W_{30}}$.
Z kolize W_{30} plyne kolize $T_2[2]$. Z kolize $a[2]$ a $T_2[2]$ vyplývá kolize $\boldsymbol{T_1[2]}$.
Z kolize $e[2]$ a $T_1[2]$ vyplývá i kolize $\boldsymbol{W_{29}}$.
Z kolize W_{29} plyne kolize $T_2[1]$. Z kolize $a[1]$ a $T_2[1]$ vyplývá kolize $\boldsymbol{T_1[1]}$.
Z kolize $e[1]$ a $T_1[1]$ vyplývá i kolize $\boldsymbol{W_{28}}$.

Z kolize hašovací hodnoty tak vyplývá i kolize hodnot W_{31}, W_{30}, W_{29}, W_{28} a $T_1[1]$, $T_1[2]$, $T_1[3]$ a $T_1[4]$. Snadno se přesvědčíme, že platí i obrácené tvrzení.

Případ $r = 5$
Po páté rundě máme

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

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

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

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

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

Hašovací hodnota je tvořena hodnotami v řádku $t = 5$ Tabulky 1. Kolize znamená, že dvě různé zprávy mají tyto stejné hodnoty:

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

Odtud plyne, že koliduje i $T_2[5]$, neboť používá primární kolidující hodnoty.
Z kolize $T_2[5]$ a $a[5]$ a vyplývá i kolize $\boldsymbol{T_1[5]}$.
Z kolize $T_1[5]$ a $e[5]$ vyplývá kolize $\boldsymbol{a[1]}$.
Z kolize $a[1]$ vyplývá i kolize $T_2[4]$. Z kolize $T_2[4]$ a $a[4]$ a vyplývá i kolize $\boldsymbol{T_1[4]}$.
Z kolize $T_1[4]$ a $e[4]$ vyplývá i kolize $\boldsymbol{W_{31}}$.
Z kolize W_{31} plyne kolize $T_2[3]$. Z kolize $a[3]$ a $T_2[3]$ vyplývá kolize $\boldsymbol{T_1[3]}$.
Z kolize $e[3]$ a $T_1[3]$ vyplývá i kolize $\boldsymbol{W_{30}}$.
Z kolize W_{30} plyne kolize $T_2[2]$. Z kolize $a[2]$ a $T_2[2]$ vyplývá kolize $\boldsymbol{T_1[2]}$.
Z kolize $e[2]$ a $T_1[2]$ vyplývá i kolize $\boldsymbol{W_{29}}$.

Z kolize hašovací hodnoty tak vyplývá i kolize hodnot W_{31}, W_{30}, W_{29} a $a[1]$, $T_1[2]$, $T_1[3]$, $T_1[4]$ a $T_1[5]$. Snadno se přesvědčíme, že platí i obrácené tvrzení.

Případ $r = 6$
Po šesté rundě máme
$$T_1[1] = W_{24}^{+} + \Sigma_1(W_{27}^{+}) + Ch(W_{27}^{+}, W_{26}^{+}, W_{25}^{+}) + W_0^{\sim}$$
$$T_2[1] = \Sigma_0(W_{31}^{+}) + Maj(W_{31}^{+}, W_{30}^{+}, W_{29}^{+})$$
$$e[1] = W_{28}^{+} + T_1[1]$$
$$a[1] = T_1[1] + T_2[1]$$

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

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

$$a[3] = T_1[3] + T_2[3]$$

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

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

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

Hašovací hodnota je tvořena hodnotami v řádku $t = 6$ Tabulky 1. Kolize znamená, že dvě různé zprávy mají tyto stejné hodnoty:

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

Odtud plyne, že koliduje i $T_2[6]$, neboť používá primární kolidující hodnoty.
Z kolize $T_2[6]$ a $a[6]$ a vyplývá i kolize $\boldsymbol{T_1[6]}$.
Z kolize $T_1[6]$ a $e[6]$ vyplývá kolize $\boldsymbol{a[2]}$.
Z kolize $a[2]$ vyplývá kolize $T_2[5]$. Z kolize $T_2[5]$ a $a[5]$ vyplývá kolize $\boldsymbol{T_1[5]}$.
Z kolize $T_1[5]$ a $e[5]$ vyplývá kolize $\boldsymbol{a[1]}$.
Z kolize $a[1]$ vyplývá kolize $T_2[4]$. Z kolize $T_2[4]$ a $a[4]$ vyplývá kolize $\boldsymbol{T_1[4]}$.
Z kolize $e[4]$ a $T_1[4]$ vyplývá kolize $\boldsymbol{W_{31}}$.
Z kolize W_{31} vyplývá kolize $T_2[3]$. Z kolize $T_2[3]$ a $a[3]$ vyplývá kolize $\boldsymbol{T_1[3]}$.
Z kolize $e[3]$ a $T_1[3]$ vyplývá kolize $\boldsymbol{W_{30}}$.

Z kolize hašovací hodnoty tak vyplývá i kolize hodnot W_{31}, W_{30} a $a[1]$, $a[2]$, $T_1[3]$, $T_1[4]$, $T_1[5]$ a $T_1[6]$. Snadno se přesvědčíme, že platí i obrácené tvrzení.

Případ $r = 7$
Po sedmé rundě máme

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

$$e[1] = \mathrm{W}_{28}^{+} + T_1[1]$$
$$a[1] = T_1[1] + T_2[1]$$

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

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

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

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

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

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

Hašovací hodnota je tvořena hodnotami v řádku $t = 7$ Tabulky 1. Kolize znamená, že dvě různé zprávy mají tyto stejné hodnoty:

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

Odtud plyne, že koliduje i $T_2[7]$, neboť používá primární kolidující hodnoty.
Z kolize $T_2[7]$ a $a[7]$ a vyplývá i kolize $\boldsymbol{T_1[7]}$.
Z kolize $T_1[7]$ a $e[7]$ vyplývá kolize $\boldsymbol{a[3]}$.
Z kolize vyplývá kolize $T_2[6]$. Z kolize $T_2[6]$ a $a[6]$ vyplývá kolize $\boldsymbol{T_1[6]}$.
Z kolize $T_1[6]$ a $e[6]$ vyplývá kolize $\boldsymbol{a[2]}$.
Z kolize $a[2]$ vyplývá kolize $T_2[5]$. Z kolize $T_2[5]$ a $a[5]$ vyplývá kolize $\boldsymbol{T_1[5]}$.
Z kolize $e[5]$ a $T_1[5]$ vyplývá kolize $\boldsymbol{a[1]}$.
Z kolize $a[1]$ vyplývá kolize $T_2[4]$. Z kolize $T_2[4]$ a $a[4]$ vyplývá kolize $\boldsymbol{T_1[4]}$.
Z kolize $T_1[4]$ a $e[4]$ vyplývá kolize $\boldsymbol{W_{31}}$.

Z kolize hašovací hodnoty tak vyplývá i kolize hodnot W_{31} a $a[1]$, $a[2]$, $a[3]$, $T_1[4]$, $T_1[5]$, $T_1[6]$ a $T_1[7]$. Snadno se přesvědčíme, že platí i obrácené tvrzení.

Případ $r = 8$
Po osmé rundě máme

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

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

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

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

$$e[4] = \mathrm{W}_{31}^{+} + T_1[4]$$
$$a[4] = T_1[4] + T_2[4]$$

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

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

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

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

Hašovací hodnota je tvořena hodnotami v řádku $t = 8$ Tabulky 1. Kolize znamená, že dvě různé zprávy mají tyto stejné hodnoty:

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

Odtud plyne, že koliduje i $T_2[8]$, neboť používá primární kolidující hodnoty.
Z kolize $T_2[8]$ a $a[8]$ a vyplývá i kolize $\boldsymbol{T_1[8]}$.
Z kolize $T_1[8]$ a $e[8]$ vyplývá kolize $\boldsymbol{a[4]}$.
Z kolize $a[4]$ a $a[7]$ a vyplývá i kolize $\boldsymbol{T_1[7]}$.
Z kolize $T_1[7]$ a $e[7]$ vyplývá kolize $\boldsymbol{a[3]}$.
Z kolize $a[3]$ vyplývá kolize $T_2[6]$. Z kolize $T_2[6]$ a $a[6]$ vyplývá kolize $\boldsymbol{T_1[6]}$.
Z kolize $T_1[6]$ a $e[6]$ vyplývá kolize $\boldsymbol{a[2]}$.
Z kolize $a[2]$ vyplývá kolize $T_2[5]$. Z kolize $T_2[5]$ a $a[5]$ vyplývá kolize $\boldsymbol{T_1[5]}$.
Z kolize $e[5]$ a $T_1[5]$ vyplývá kolize $\boldsymbol{a[1]}$.
Z kolize $a[1]$ vyplývá kolize $T_2[4]$. Z kolize $T_2[4]$ a $a[4]$ vyplývá kolize $\boldsymbol{T_1[4]}$.

Z kolize hašovací hodnoty tak vyplývá i kolize hodnot $a[1]$, $a[2]$, $a[3]$, $a[4]$, $T_1[4]$, $T_1[5]$, $T_1[6]$, $T_1[7]$ a $T_1[8]$. Snadno se přesvědčíme, že platí i obrácené tvrzení. QED.

Věta 1

(i) Složitost nalezení kolize Turbo SHA-256-r je nejvýše řádu 2^{16r}, $r = 1, ..., 8$.

(ii) Složitost nalezení kolize Turbo SHA-512-r je nejvýše řádu 2^{32r} pro $r = 1, ..., 8$.

Pro $r = 1$, 2 a 3 můžeme dokonce část hašovací hodnoty volit.

Důkaz

Důkaz Věty 1 je velmi podobný pro všechny hodnoty r. Kolizi Turbo SHA-r konstruujeme s využitím řádku r tab. 2, Lemmatu 1 a následujícího algoritmu:

1. Zvol náhodně hodnoty proměnných ve druhém sloupci tab. 2 (například pro $r = 2$ zvolíme náhodně $W_{31}, ..., W_{26}$).
2. Pro i = 1 do 2^{16r} opakuj
   {
   a. Zvol náhodně množinu hodnot proměnných ve čtvrtém sloupci (například pro $r = 2$ zvolíme náhodně $W_{25}, ..., W_{16}$),
   b. z hodnot $W_{31}, ..., W_{16}$ vypočítáme $W_{15},..., W_0$ (toto zobrazení je bijekce, viz [1]),
   c. z hodnot $W_{31}, ..., W_{16}$ a $W_{15},..., W_0$ vypočítáme hodnoty proměnných ve třetím sloupci a uložíme je do množiny S (například pro $r = 2$ vypočítáme a uložíme dvojici hodnot $(T_1[1], T_1[2])$ v S).
   }
3. V množině S nalezneme kolizi narozeninovým paradoxem.

Protože ve třetím sloupci je vždy r (32 bitových) hodnot, potřebujeme volit přibližně $2^{32r/2}$ hodnot v Kroku 2, abychom docílili dobré pravděpodobnosti nalezení kolize v množině S[1]. Ve čtvrtém sloupci však máme k dispozici minimálně r slov, takže útok je proveditelný.

Závěr

Tento příspěvek se nezabývá bezpečností Turbo SHA-2 komplexně, pouze ukazuje nové kolizní útoky s menší složitostí, než předpokládali její autoři. Z Věty 1 vyplývá,

[1] Poznamenejme, že můžeme uvažovat, že proměnné ve třetím sloupci tabulky 2 jsou statisticky nezávislé náhodné veličiny. Například pro $r = 8$ můžeme vyjádřit $a[1]$, $a[2]$ a $a[3]$ pomocí $T_1[1]$, $T_1[2]$ a $T_1[3]$. Dále, $T_1[1]$, $T_1[2]$, $T_1[3]$, $T_1[4]$, $T_1[5]$, $T_1[6]$, $T_1[7]$, $T_1[8]$ závisí na různých proměnných $W_t^{\sim} = (W_t \oplus W_{t+16}) + (W_{t+4} \oplus W_{t+24}) + (W_{t+8} \oplus W_{t+20}) + W_{t+12}, t = 0,...,7$, což znamená závislost na různých proměnných z množiny $\{W_{31}, ..., W_{16}\}$ a různých proměnných z množiny $\{W_{15},..., W_0\}$. Protože proměnné ze čtvrtého sloupce volíme náhodně a nezávisle, můžeme také očekávat, že $a[1]$, $a[2]$, $a[3]$, $T_1[4]$, $T_1[5]$, $T_1[6]$, $T_1[7]$, $T_1[8]$ se chovají jako nezávislé náhodné veličiny.

že jediným kandidátem zůstává Turbo SHA-2 s osmi rundami. Původní bezpečnostní rezerva 6 rund je však ztracena. Zůstává otevřena otázka, jak bezpečnost Turbo SHA-2 posílit.

Poděkování
Chtěl bych poděkovat Danielu Joščákovi za cenné připomínky k textu příspěvku.

Literatura

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