Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 10, číslo 1/2008 **15.leden 2008**

1/2008

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1227 registrovaných odběratelů)

Obsah :

Příloha: ---

A. O kolizích hašovací funkce Turbo SHA-2

Vlastimil Klíma, 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	$W_{31, 30, 29, 28, 27, 26, 25}$	$T_1[1]$	$W_{24, 23, ..., 16}$
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: Kolize Turbo SHA-*r*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$a[4] = T_1[4] + T_2[4]$

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

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

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

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

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

$e[3] = \mathrm{W}_{30}^{+} + T_1[3]$
$a[3] = T_1[3] + T_2[3]$

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

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

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

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

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

$$T_2[1] = \Sigma_0\left(W_{31}^+\right) + Maj(W_{31}^+, W_{30}^+, W_{29}^+)$$
$$e[1] = W_{28}^+ + T_1[1]$$
$$a[1] = T_1[1] + T_2[1]$$

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

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

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

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

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

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

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

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, 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

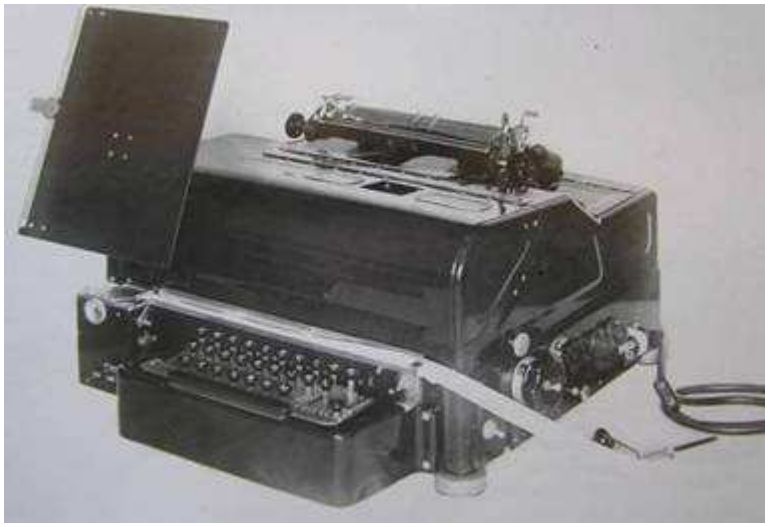
[1] Gligoroski D., Knapskog S. J.: Turbo SHA-2, IACR ePrint archive Report 2007/403, October 2007, http://eprint.iacr.org/2007/403.pdf

[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.

B. Z dějin československé kryptografie, část V., Československé šifrovací stroje z období 1955 – 1960. Šifrovací stroj ŠD – 2 (1. díl).

Mgr. Karel Šklíba (karel.skliba@cryptoworld.info)

Šifrovací stroj ŠD – 2 byl současníkem a v mnoha ohledech protikladem šifrátoru ŠD – 1 při záměrech vybavit československou šifrovou službu kvalitními kryptologicky bezpečnými šifrovacími stroji (zejména pro dálnopisné spojení) v letech 1955 až 1960. Stroj ŠD – 2 byl elektromechanický diskový šifrátor s vlastní tvorbou hesla určený pro práci off-line. Šifrovací stroj ŠD – 2 nebyl v Československu vyvinut ani vyvíjen. Jeho historie je svým způsobem zvláštní. V Československu se v té době jevila akutní potřeba šifrovacího stroje s vlastní tvorbou hesla. Koncem padesátých let 20. století existovaly ve světě dva hlavní modely pro konstrukci šifrovacích strojů s vlastní tvorbou hesla. Byl to jednak způsob tvorby náhodného (pro dlouhé texty bohužel periodického) hesla dle konstrukce Borise Hagelina, který byl použit při návrhu šifrátoru MAGDA a jejích modifikací. Po roce 1955 však již bylo známo, že jsou tyto stroje kryptoanalyticky slabé a pro utajené spojení nejsou bezpečné. Druhý způsob konstrukce představovaly diskové neboli komutátorové stroje, jejichž nejslavnějším představitelem je německý šifrátor ENIGMA. Koncem padesátých let panoval názor, že při dostatečně propracované konstrukci diskového stroje a přesném dodržování pravidel pro používání jsou tyto stroje kryptologicky bezpečné. V Československu na Zvláštní správě Ministerstva vnitra a na šifrovém úseku Ministerstva obrany bylo pouze několik jednotlivých kvalifikovaných konstruktérů, kteří svou pracovní kapacitou nebyli schopni zajistit vývoj kryptologicky bezpečného šifrátoru s vlastní tvorbou hesla. V roce 1957 byla proto vládou ČSR vyžádána pomoc v SSSR. Sovětská strana žádosti vyhověla a počátkem listopadu 1957 dodala do Československa 2 funkční kusy (vzory) šifrátoru CM – I (čti esem jedna) včetně podrobného popisu a projektové dokumentace, které měly představovat vzor pro výrobu československého šifrátoru s označením ŠD – 2.



Po prostudování předané dokumentace a po provedení funkčních zkoušek předaných šifrovacích strojů včetně jejich předvedení zodpovědným funkcionářům Ministerstva vnitra a armády byly koncem listopadu 1957 přijaty zvláštní správou Ministerstva vnitra následující závěry:

1. Šifrovací stroj ŠD – 2 slouží k předběžnému (tj. off-line) šifrování zpráv, to znamená, že se na něm elektromechanickým způsobem provádí přeměna otevřeného textu na text šifrový a naopak. Takto připravenou zprávu je potom nutno předat adresátovi za pomocí známých druhů pojítek (rádio, dálnopis, telefon, telegraf). Se šifrovým strojem ŠD – 2 je možno uskutečňovat tři druhy šifrového spojení – osobní, oběžníkové, vzájemné. Pro provádění těchto druhů spojení je nutno vyrábět 3 druhy klíčových materiálů, sloužících k nastavení prvků ve stroji a k určení počáteční polohy heslových disků. Výroba těchto materiálů se musí provádět přesně dle předem stanovených pravidel. Potom při správném dodržování provozních pravidel garantuje stroj bezpečné utajení zpráv o délce až 500 znaků při jednom nastavení heslových disků.

2. Výhody šifrovacího stroje ŠD – 2 spočívají v tom, že oproti dnešnímu ručnímu způsobu šifrování zaručuje použití šifrového stroje ŠD – 2 při poměrně stejné bezpečnosti mnohem rychlejší a kvalitnější provoz. Jeho použití snižuje duševní námahu a tím i možnost chyb u obsluhy. Schopnost stroje pracovat na osobním, oběžníkovém i vzájemné spojení určuje stroj pro široké použití zejména v armádě a u Ministerstva vnitra. Možnost reprodukce textu na perforační pásku umožňuje za použití dálnopisného vysílače a přijímače rychlé předávání zpráv. Nezávislost na určitém druhu pojítka umožňuje jeho libovolnou volbu pro předání předem zašifrované zprávy. To je obzvláště výhodné pro oběžníkové spojení.

3. Nevýhody šifrového stroje ŠD – 2 spočívají v tom, že stroj je určen pro předběžné šifrování a není jej proto možno využívat pro vedení přímých utajených rozhovorů. Šifrový stroj ŠD – 2 je složen z několika přesných mechanických a elektrických bloků, které vyžadují velkou péči po provozní a servisní stránce. Šifrový stroj ŠD – 2 si vytváří vlastní heslo pro zašifrování. Z tohoto důvodu je nutno dbát na přísné dodržování všech bezpečnostních a provozních pravidel. Šifrový stroj ŠD – 2 vyžaduje pečlivou přípravu ke svému provozu, tj. nastavení jednotlivých klíčů, jakož i pečlivou manipulaci při šifrování a dešifrování. Vzhledem k tomu bude nutno zvýšit odbornou kvalifikaci obsluhujícího personálu. Maximální délka zprávy pro použití jednoho nastavení heslových disků nesmí překročit 100 skupin, tj. 500 znaků. Při zašifrování delší zprávy je nutno tuto zprávu dělit. Při vynechání některého znaku šifrového textu chybou při předávání po pojítkách se stane zbylý šifrový text těžko dešifrovatelný.

Na základě provedených rozborů stručně popsaných výše byly předloženy dvě varianty sériové výroby stroje ŠD – 2. Obě varianty domácí i zahraniční měly řadu úskalí a problémů a nakonec nedošlo k realizaci ani jedné z nich. Šifrový stroj ŠD – 2 nebyl pro použití v československé šifrové službě nikdy vyráběn doma ani v zahraničí a zůstal jen jedním z historických mezníků. V Československu byly v pozdějších letech až do let devadesátých používány jiné diskové stroje sovětské provenience, což je samostatná kapitola, která by mohla být zpracována možná někdy v budoucnu.

První variantou výroby šifrovacího stroje ŠD – 2 byla výroba doma v Československu. Vzhledem k tomu, že stroj ŠD – 2 byl konstrukčně navržen a ve dvou prototypech vyroben v SSSR a s ohledem na skutečnost, že předané stroje svou koncepcí naznačovaly směr vývoje šifrových strojů v zemi svého vzniku, byla československá strana požádána, aby přijala všechna nezbytná opatření k tomu, aby nebylo možno určit opravdový původ těchto strojů. V případě výroby v ČSR bylo proto nutno přepracovat veškerou technickou a výrobní dokumentaci podle tuzemských norem a zvyklostí. Bylo by proto nutné provést tyto práce:

- Vyhotovit převodové tabulky GOST – ČSN a to materiálové, toleranční, opracování, povrchové úpravy a tepelného zpracování.
- Přeložit a upravit veškerou výkresovou dokumentaci dle ČSN a přečíslovat výkresy.
- Sepsat materiálové rozpisy a kusovníky.
- Překreslit všechny výkresy v počtu 3000 kusů, což by si vyžádalo 8 kresličů po dobu šesti měsíců. Zajištění tohoto počtu kvalifikovaných a prověřených pracovníků by si vyžádalo mimořádné opatření.
- Výše uvedené práce za předpokladu personálního zajištění by trvaly 7 až 9 měsíců.
- Takto připravenou technickou dokumentaci by bylo nutno zadat do sériové výroby mimořádným způsobem, protože výrobní plány jednotlivých závodů na roky 1958 – 1960 byly již schváleny. Sériová výroba v rámci Ministerstva vnitra vzhledem k jeho malé kapacitě nebyla možná. Vzhledem k charakteru výroby mohl tento výrobní program převzít jen závod Aritma Praha nebo závody Jana Švermy Brno. Přesto i v těchto závodech by muselo dojít ke kooperaci s jinými podniky. Otázka zajištění dostatečné konspirace výroby stroje by byla velmi obtížná.
- Příprava výroby na závodě by si vyžádala zhotovení velkého množství cca 2500 kusů přípravků, což by představovalo vzhledem k výrobní vytíženosti nástrojáren časovou prodlevu nejméně 12 měsíců.
- Vlastní výroba součástek a montáž bloků za předpokladu série 500 kusů stroje ŠD – 2 by s ohledem na kapacitu výrobních středisek v uvedených závodech trvala dalších cca 12 měsíců.
- Dle názoru sovětské strany by konečná montáž a seřízení jednoho stroje trvala jednomu pracovníku asi 3 až 4 týdny.
- Odhadovaná cena jednoho stroje při předpokládané sérii 500 kusů by byla 50 až 60 tisíc Kčs.
- V případě hladkého a bezproblémového průběhu všech výše uvedených prací by bylo možné očekávat dodání prvních kusů hotových strojů ŠD – 2 v druhé polovině roku 1960.

Problémy domácí výroby, zejména její konspirace a časová zdlouhavost byly projednávány v Moskvě se sovětskou stranou, která posléze nabídla možnost sériové výroby těchto strojů v SSSR. V tomto případě by odpadla veškerá práce s přepracováním technické a výrobní dokumentace a rovněž by se řádově zkrátila příprava výroby (odpadlo by zhotovování přípravků, vývoj elektromotorů apod.). Bylo možné předpokládat značné zkrácení výrobního procesu asi o rok a půl. Tato varianta představovala rovněž vyřešení jedné z nejpodstatnějších otázek produkce domácí a to zajištění dokonalé konspirace výroby. Studium dějin kryptoanalýzy však ukazuje, jaká jiná úskalí by tato varianta mohla mít. V případě zahraniční výroby by první stroje mohly být dodány začátkem roku 1959, což byl skvělý závěr. Cena jednoho stroje by však byla 35000 až 40000 rublů. Bylo navrhováno, že

v případě schválení této varianty budou k výrobě přizváni 2 československí technici, kteří tak získají potřebné zkušenosti v organizování takovéto výroby, v provádění výrobních procesů, seznámí se s používanými technologiemi, s montáží a seřizováním.

Koncem roku 1957 byla Zvláštní správou navrhována vedení Ministerstva vnitra a vládě varianta druhá. K její realizaci však nedošlo. Později byly v Československu používány jiné diskové šifrátory s vlastní tvorbou hesla, zejména pak stroje s označením M-125M, M–125MR a M–125–3MR3.

S podrobnějším technickým popisem šifrovacího stroje ŠD – 2 se seznámíme ve druhém díle. Pro zajímavost lze ještě dodat, že podle pamětníků byly oba původní stroje dodány do Československa asi v deseti velkých bednách. Bedny kromě vlastních dvou strojů obsahovaly další dvě sady komutátorů v dřevěných bedničkách, dvě sady pečlivě zabalených a do přepravních dřevěných krabic (spíše kufříků) uložených náhradních dílů a speciálního nářadí (například utahovací klíče neobvykle malých a zvláštních rozměrů, pravoúhle zahnuté šroubováky a speciální utahovací přípravky). Vše bylo v dřevěných kufřících ne svém určeném místě drženo speciální úchytkou. Proto byly tyto „kufříky“ uvnitř vybaveny různými přepážkami a výčnělky a každá věc měla své přesné místo v některém z „kufříků“. Všechno příslušenství i náhradní díly musely být kontrolovány podle seznamů a případné použité náhradní díly musely být zničeny dle přísných pravidel ochrany utajovaných skutečností. V bednách byla dále obsáhlá technická a výrobní dokumentace o váze pravděpodobně několika desítek kilogramů.

C. První česká kryptografická příručka

Pavel Vondruška (pavel.vondruska@crypto-world.info)

Historie díla

Nejstarší česká kryptografická rukopisná příručka nazvaná ***Constructio sive Strues Trithemiana*** pochází z roku 1628 a napsal ji právník a vysoký císařský úředník ***Rafael Soběhrd Mnišovský ze Sebuzína a Horštejna***.

Mnišovského rukopis byl v Čechách ovšem pouze krátkou dobu. Ke konci třicetileté války byl jako válečná kořist odvezen do Švédska. Rukopis Mnišovského je v současnosti uložen v univerzitní knihovně v Uppsale ve Švédsku pod sign. MS Slav. 60. Obsahuje 208 papírových listů oktávového formátu, vlastní text příručky je na fol. 5r - 187r.

Jako první na příručku upozornil ***Josef Dobrovský*** v roce 1796 ve svém spisu nazvaném ***Literarische Nachrichten von einer Reise nach Schweden und Russland.*** Konstatuje v něm, že se jedná o česko-latinskou gramatickou příručku sestavenou podle Trithemiovy metody. Jako autora označil Rafaela Mnišovského. O půl století později se seznámil s rukopisem B. Dudík, který nesouhlasil s Dobrovského určením autora, ale rukopis také označil za pomůcku k výuce češtiny (viz ***B. Dudík, Forschungen in Schweden für Mährens Geschichte, Brünn 1852, s. 326-328***). Správnost Dobrovského identifikace autora rukopisu potvrdil ***V. Flajšhans*** (***Knihy české v knihovnách švédských a ruských, Praha 1897, s. 52-53***) a upozornil také na Jirečkovu domněnku, že Rafael Mnišovský ze Sebuzína sepsal tento česko-latinský spis původně pro svého svěřence arciknížete Ferdinanda, pozdějšího císaře Ferdinanda III.

Díky těmto pracím se v literatuře po celá další desetiletí uváděla mylná domněnka, že Mnišovský sestavil rukopis jako učebnici češtiny pro svého svěřence arciknížete Ferdinanda. Jedná se však o omyl, nejedná se o učebnici česko-latinskou a pravděpodobně nebyla ani psána pro Ferdinanda.

Mnišovský sice Ferdinanda skutečně učil, ale již roku 1619. Příručka však vznikla později a to roku 1628, kdy byl Mnišovský sekretářem dvorské kanceláře. Navíc je charakter rukopisu takový, že by se z něho Ferdinand jistě česky naučit nemohl a navíc je dokladováno, že roku 1627, tedy rok před dohotovením rukopisu, Ferdinand hovořil česky. Kdyby práce byla skutečně psána pro následníka trůnu, jistě by to Mnišovský v úvodu či v dedikaci, jak tehdy bylo zvykem, uvedl.

Jako první si všimla, že se nejedná o učebnici češtiny, ale kryptografickou příručku ***Carin Davidssonová*** a publikovala svůj zajímavý objev v článku ***Johannes Trithemius' Polygraphia als tschechisches Lehrbuch, Cod. Slav. 60 der Universitätsbibliothek in Uppsala, Scando-Slavica 5, 1959, s. 148-164.***

V Čechách pak byla tato informace pravděpodobně poprvé publikována v roce 1993 v díle ***J. Kašpara Soubor statí o novověkém písmu.*** Protože se však jednalo o odborné paleografické dílo, tak tato informace poněkud zapadla a v kryptografických kruzích není všeobecně známa. Děkuji proto touto cestou Dr. Jozefu Krajčovičovi, který mne na tuto knihu upozornil a poskytl výše uvedené informace.

Obsah díla

nás všech. L.

hříchy	a	scelera
provinění	b	dulicta
dopuštění	c	culpae
vejstupení	d	transgressiones
zlosti	e	iniquitates
nepravosti	f	facinora
nečistoty	g	immunditiae
zahálení	h	negligentiae
zanedbání	i	omissiones
nedbanlivosti	k	incuriae
opouštění	l	ignaviae
nespravedlnosti	m	iniustitiae
činy	n	facta
skutky	o	opera
zlá myšlení	p	cogitationes
praktiky	q	practicae
omyly	r	errores
šibalství	s	nequitiae
fortele	t	dolus
zlé zachování	u	noxae
zlé chování	w	excessus
poskvrny	x	nauae(?)
zlé živobytí	y	victum malum
přestoupení	z	reatus

omnium nostrum. L.

Ukázka a přepis jedné ze stránek rukopisu (fol. 61v) .

Práce vychází z ***Trithemiova*** díla ***Polygraphia.*** Práce Mnišovského se však liší od Trithemiovy tím, že je dvojjazyčná, česko-latinská a měla podle úvodních autorových slov

sloužit nejen jako kryptografická příručka, ale i jako pomůcka k překladům z latiny do češtiny a naopak a k opakování latinsko-českých slovíček. Proto snad došlo k rozšíření omylu, že se jedná o česko-latinskou učebnici. Latinská ani česká slova však v ní nejsou abecedně ani jinak logicky utříděna, a proto není možno příručky použít jako latinsko-českého nebo česko-latinského slovníku. Struktura celé práce naopak zcela jednoznačně ukazuje, že mohla být užitečná pouze jako kryptografická příručka a jako taková byla také sestavena. Její dvojjazyčnost snad mohla dokonce zvyšovat možnosti utajení existence šifrového textu. O jejím použití jako kryptografické pomůcky není žádných zpráv, není znám ani druhý exemplář příručky, který by musel mít příjemce šifrovaných zpráv.

Šifrování, s největší pravděpodobností, podle ní probíhalo tak, že se místo písmen vyhledávala vhodná česká (resp. latinská) slova, která se následně uspořádala do textu, který měl vyhlížet jako nezávadný český resp. latinský text. Šifra tak (až na uvedenou dvojjazyčnost) připomíná Trithemiovu šifru AVE MARIA uvedená v knize Polygraphia.

Příklad **(viz přepis fol. 61v)**

Otevřený text: CRYPTO

Šifrový text s využitím latinské části:
Culpae errores victum malum cogitationes dolus opera

Šifrový text s využitím české části:
Dopuštění omyly zlé živobytí zlá myšlení fortele skutky

Litertaura

[1] http://friedo.szm.sk/

[2] Kašpar, J.: Soubor statí o novověkém písmu. Praha, Karolinum 1993. ISBN 80-7066-679-X. str. 188-190

[3] Davidsson, C.: Johannes Trithemius' Polygraphia als tschechisches Lehrbuch, Cod. Slav. 60 der Universitätsbibliothek in Uppsala, Scando-Slavica 5, 1959, s. 148-164.

[4] Vondruška, P.: Doba nomenklátorů, Sborník příspěvků MKB, Praha 2007, ISBN 80-903083-8-4 , str.77-90

D. Pozvánka
Konference EOIF GigaCon 2008 – Elektronický oběh informací ve firmě

Dne 12. února 2008 se v hotelu Diplomat v Praze uskuteční **konference EOIF**, která bude věnována správě oběhu dokumentů a informací v českých a světových institucích a podnicích.

Na konferenci **Elektronický oběh informací ve firmě** věnujeme nejnovějším technologiím pro elektronické zpracování, ukladání a sdílení informací ve firmě. Pro účastnické firmy je místem kontaktu s potenciálním zákazníkem, příležitostí ukázání předností a možností promovaných řešení. Účastníci budou moci srovnat a hodnotit nabízené produkty, setkat se a diskutovat s odborníky.

Vstup na konferenci je **zcela zdarma**, podmínkou je pouze registrace na http://eoif.swmedia.cz/prt/view/eoif-gigacon-praha.html

Další podrobnosti na stránce www.eoif.swmedia.cz

Přednášky a prezentace:

- **Edvard Kožušník** z občanského sdružení Michala Tošovského eStat.cz – Efektivní stát
- **Zbyněk Loebl** a **Pavel Vondruška** - **Dlouhodobá archivace digitálních dokumentů se zachováním původu.** Přednáška vychází z grantu Ministerstva informatiky ČR **Dlouhodobé uchovávání elektronických dokumentů se zaručeným elektronickým podpisem** http://digiarchiv.eu/
- **Ing. Jiří Kohout** z Univerzity Hradec Králové – **Identita management, zejména v ramci banky**
- **Zbyněk Šonka** z DICOM Data Management CZ – **Přeměňte nákladová střediska v centra tvorby zisku pomocí IC&E (Intelligent Capture & Exchange)**

Mediální partneři: Ben – technická literatura, Boston, BAR, Ccmag, CryptoWorld, Devítka, E-mag – technologický, e-stat.cz, finance.cz, Hakin9, It Point, Lex – a Wolters Klower business, Linux+, PracaIT.com, Press Forum, SBK – bankovní karty, Security Revue

Mezi účastníky slosujeme atraktivní dárky od **Ben – technická literatura**, **DS Software**, **Hakin9**
a **Linux+**! Neváhejte, přihlášte se raději již dnes!

Kontakt:

Weronika Buszko
weronika.buszko@swmedia.cz
tel.+420 246 019 138
fax.+420 227 203 610

Anna Uścińska
anna.uscinska@swmedia.cz

E. O čem jsme psali v lednu 2000 – 2007

Crypto-World 1/2000

Crypto-World 1/2001

Příloha:
trustcert.pdf (upoutávka na služby Certifikační Autority TrustCert)

Crypto-World 1/2002

Crypto-World 1/2003

Příloha : Crypto_p1.pdf
CEN Workshop Agreements (dokumenty vztahující se k elektronickému podpisu)

Crypto-World 1/2004

Crypto-World 1/2005

Příloha :
Speciál 2004 - přehled článků a prezentací členů redakce Crypto-World za rok 2004
(http://crypto-world.info/casop6/prehled_2004.pdf)

Crypto-World 1/2006

Crypto-World 1/2007

F. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.
Adresa URL, na níž můžete najít tento sešit (zpravidla 3 týdny po jeho rozeslání) a předchozí sešity GCUCMP, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály:
http://crypto-world.info

2. Registrace / zrušení registrace

Zájemci o e-zin se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci elektronický formulář na http://crypto-world.info. Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání kódů ke stažení sešitu.
Ke zrušení registrace stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info. Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byly kódy zasílány.

3. Redakce

E-zin Crypto-World

Redakční práce:	Pavel Vondruška
Stálí přispěvatelé:	Pavel Vondruška
	Jaroslav Pinkava
Jazyková úprava:	Jakub Vrána
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS	Vlastimil Klíma
(výběr příspěvků,	Jaroslav Pinkava
komentáře a	Tomáš Rosa
vkládání na web)	Pavel Vondruška
Webmaster	Pavel Vondruška, jr.

4. Spojení (abecedně)

redakce e-zinu	ezin@crypto-world.info ,	http://crypto-world.info
Vlastimil Klíma	v.klima@volny.cz ,	http://cryptography.hyperlink.cz/
Jaroslav Pinkava	Jaroslav.Pinkava@zoner.cz ,	http://crypto-world.info/pinkava/
Tomáš Rosa	t_rosa@volny.cz ,	http://crypto.hyperlink.cz/
Pavel Vondruška	pavel.vondruska@crypto-world.info ,	http://crypto-world.info/vondruska/index.php
Pavel Vondruška,jr.	pavel@crypto-world.info ,	http://webdesign.crypto-world.info
Jakub Vrána	jakub@vrana.cz ,	http://www.vrana.cz/