Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 12, číslo 3/2010 **15. březen 2010**

3/2010

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1360 registrovaných odběratelů)

Obsah :

		str.
A.	**Analýza Blue Midnight Wish – útoky na stavební bloky (V.Klíma, D. Gligoroski)**	**2 - 13**
B.	**Přehled některých základních kritérií hodnocení bezpečnosti IT (P.Vondruška)**	**14 - 20**
C.	**Chcete si zaluštit? Díl 4. (M.Kolařík)**	**21**
D.	**Aktuální situace v oblasti uznávání zahraničních kvalifikovaných certifikátů (P.Vondruška)**	**22-24**
E.	**O čem jsme psali v březnu 1999-2009**	**25-26**
F.	**Závěrečné informace**	**27**

A. Analýza Blue Midnight Wish – útoky na stavební bloky

RNDr. Vlastimil Klíma, kryptolog konzultant, Praha
(http://cryptography.hyperlink.cz, v.klima@volny.cz)
Prof. Danilo Gligoroski, Norwegian University of Science and Technology, Norway (danilog@item.ntnu.no , http://www.item.ntnu.no/people/personalpages/fac/danilog/start)

Článek navazuje na příspěvky v číslech 1 a 2 Crypto-Worldu 2010, s nímž má společnou skoro celou úvodní stranu a několik obrázků. Volně také navazuje na články o BMW v 12/2009, 3/2009 a 7-8/2009. V čísle 1 jsme se zabývali hledáním vzoru (úloha první), v čísle 2 hledáním kolize (úloha druhá).

Nyní se na BMW podíváme z hlediska zkoumání vlastností stavebních bloků a s možností řešit (obě předchozí i jiné) úlohy a útoky v mnohem menší dimenzi než je 512 nebo 1024 bitů. V některém z dalších pokračování ukážeme definici BMW pro slova o malých šířkách. To umožní hledat řešení všech úloh na počítači a odhadovat jejich složitost i způsoby řešení. Nemusíte však na tuto definici čekat, protože pokud vás některá z těchto úloh zaujme, jistě si nadefinujete BMW pro slova o malé šířce sami.

Chceme stimulovat analýzy a útoky na BMW a prezentovat otevřené problémy. Ty by se mohly stát předmětem studentských prací. Proč? Velkou výhodou oproti jiným tématům je, že tyto rozbory jsou nyní velmi žádané, ať s negativním nebo pozitivním výsledkem. Když bude problém vyřešen nebo naopak bude ukázáno, že je složitý, je to v obou případech žádaný a velmi dobře publikovatelný výsledek.

Označení
Článek bude využívat označení zavedené v Crypto-Worldu 12/2009. Připomeňme jen šířku slova w = 32 nebo 64 bitů, délku bloku zprávy a průběžné haše n = 16*w (mají 16 slov) a výpočet haše:

1. Předzpracování
(a) Doplň zprávu M jednoznačným definovaným způsobem o délku zprávy v bitech a doplněk
(b) Rozděl zprávu na celistvý násobek (N) m-bitových bloků $M^{(1)}$, ..., $M^{(N)}$.
(c) Nastav počáteční hodnotu průběžné haše $H^{(0)}$ na konstantu ($CONST^0$).
2. Výpočet haše
For i = 1 to N: $H^{(i)} = f(M^{(i)}, H^{(i-1)})$.
3. Finalizace
$H^{final} = f(H^{(N)}, CONST^{final})$, kde $CONST^{final}$ je konstanta.
4. Závěr
H(M) = dolních n bitů z hodnoty H^{final}.

Rozbor po blocích
Při zkoumání složité funkce je vhodné začínat od jejích stavebních bloků. Základními stavebními bloky BMW jsou funkce f_0, f_1, f_2 a poté jejich kompozice $f_1 \bullet f_0$ a $f_2 \bullet f_1 \bullet f_0$. Už v předchozích úlohách jsme narazili na to, že první bod, kde lze očekávat nějaké zkratky, je proměnná $\mathbf{Q_a}$, tedy funkce $\mathbf{f_0}$. Dalším bodem je hodnota $\mathbf{Q_b}$ neboli funkce $\mathbf{f_1 \bullet f_0}$. Pokud je $\mathbf{Q_b}$ výsledným cílem zájmu, lze zkoumat jeho bijetivní předobraz, hodnotu **R**, která vznikne odebráním bijekce $\mathbf{T^L}$. Konečně finálním bodem zájmu je vlastní výstup **H** celé kompresní funkce $f_2 \bullet f_1 \bullet f_0$. Místo ní ovšem můžeme zkoumat také bijektivní předobraz H, proměnnou

G. Dále je možné se také odděleně zabývat čistě bloky f_2 a f_1 a jejich spojením $f_2 \bullet f_1$. Všechny stavební bloky f_0, f_1, f_2, $f_1 \bullet f_0$, $f_2 \bullet f_1 \bullet f_0$, $f_2 \bullet f_1$, nebo proměnné $\mathbf{Q_a}$, $\mathbf{Q_b}$, **R**, G, H můžeme potom uvažovat jako funkce vzhledem ke kolizím, vzorům nebo obecně z hlediska jakýchkoliv anomálií nebo prostě jen zjišťovat jejich vlastnosti.

Protože většina úloh, na které narazíme , bude velmi složitých pro rozměry n = 512/1024 (u BMW256/512), navrhujeme převést všechny tyto úlohy do menších dimenzí. To umožní řešit všechny tyto úlohy pro malý počet proměnných, získávat alespoň nějaké informace o problémech a eventuelně provádět extrapolace.

Důležité upozornění
V následujících formulacích problémů ponecháme označení f_0, f_1, f_2 pouze proto, aby bylo vidět systematické zkoumání BMW. Avšak u konkrétních úloh předpokládáme zkoumání zejména jednodušších variant, tj. **R** místo $f_1 \bullet f_0$ nebo G místo $f_2 \bullet f_1 \bullet f_0$ apod.

Systematické zkoumání úlohy kolize
Nyní formulujeme úlohy, vztažené k problému hledání kolize.
Máme
$f_0(M, H) = A_2A_1(M \oplus H) + ROTL^1(H)$

Úlohy (a) – (e)
První úloha je tato:
(a) najít co nejvíce řešení řešení H rovnice $f_0(0, H) = f_0(0, 0)$.

Tuto úlohu uvádíme zvlášť, protože má velmi jednoduchou formulaci i zápis. Jejím řešením je pochopitelně H = 0. Jde nám ovšem o netriviální řešení, stejně jako u všech ostatních úloh. Zápis této úlohy je na obr. 1. Myslíme, že vypadá velmi jednoduše a mohli byste se pokusit najít její řešení.

$$
\begin{aligned}
0 &= H_1 + s_0(H_5 - H_7 + H_{10} + H_{13} + H_{14}) \\
0 &= H_2 + s_1(H_6 - H_8 + H_{11} + H_{14} - H_{15}) \\
0 &= H_3 + s_2(H_0 + H_7 + H_9 - H_{12} + H_{15}) \\
0 &= H_4 + s_3(H_0 - H_1 + H_8 - H_{10} + H_{13}) \\
0 &= H_5 + s_4(H_1 + H_2 + H_9 - H_{11} - H_{14}) \\
0 &= H_6 + s_0(H_3 - H_2 + H_{10} - H_{12} + H_{15}) \\
0 &= H_7 + s_1(H_4 - H_0 - H_3 - H_{11} + H_{13}) \\
0 &= H_8 + s_2(H_1 - H_4 - H_5 - H_{12} - H_{14}) \\
0 &= H_9 + s_3(H_2 - H_5 - H_6 + H_{13} - H_{15}) \\
0 &= H_{10} + s_4(H_0 - H_3 + H_6 - H_7 + H_{14}) \\
0 &= H_{11} + s_0(H_8 - H_1 - H_4 - H_7 + H_{15}) \\
0 &= H_{12} + s_1(H_8 - H_0 - H_2 - H_5 + H_9) \\
0 &= H_{13} + s_2(H_1 + H_3 - H_6 - H_9 + H_{10}) \\
0 &= H_{14} + s_3(H_2 + H_4 + H_7 + H_{10} + H_{11}) \\
0 &= H_{15} + s_4(H_3 - H_5 + H_8 - H_{11} - H_{12}) \\
0 &= H_0 + s_0(H_{12} - H_4 - H_6 - H_9 + H_{13})
\end{aligned}
$$

Obr.1: Úloha (a)

Další úlohy už systematicky vyčerpávají všechny zajímavé možnosti vzhledem k hledání kolizí, pseudokolizí a jejich blízkých variant.

Najít netriviální řešení následujících úloh:

(b) $f_0(M_1, H_1) = f_0(M_2, H_2)$ pro $M_1 = M_2$ nějaké pevné, známé (nulové, nenulové)
(c) $f_0(M_1, H_1) = f_0(M_2, H_2)$ pro $M_1 \neq M_2$ nějaké pevné, známé (nulové, nenulové)
(d) $f_0(M_1, H_1) = f_0(M_2, H_2)$ pro $H_1 = H_2$ nějaké pevné, známé (nulové, nenulové)
(e) $f_0(M_1, H_1) = f_0(M_2, H_2)$ pro $H_1 \neq H_2$ nějaké pevné, známé (nulové, nenulové)

Nějaké znamená, že nás zajímá jakákoliv hodnota, čili je možné ji volit tak, aby rovnice byly lépe řešitelné. Pokud by se našlo obecnější řešení, tím lépe. Pro bezpečnost BMW má také velký význam odhad složitosti řešení těchto rovnic.

Úlohy (A) – (E)
Následující úlohy (A) – (E) odpovídají úlohám (a) – (e), ale týkají se blízkých řešení. Hledáme tedy proměnné, pro něž uvedené rovnice platí na co nejvíce bitech. Z hlediska složitosti nás zajímají zejména taková blízká řešení, která jsou dosažena rychleji než hrubou silou. Máme tedy tyto úlohy:
(A, B, C, D, E): nalezněte proměnné, které dávají blízkou rovnost v rovnicích (a, b, c, d , e). Čím bližší řešení je dosaženo, tím lépe.

Úlohy (AA) – (EE)
Následující úlohy (AA) – (EE) odpovídají úlohám (a) – (e), týkají se plných řešení, avšak pro blízké proměnné. Hledáme proměnné (M nebo H), pro něž uvedené rovnice platí na všech bitech, ale požadované podmínky pro proměnné M nebo H (jejich rovnost) mohou být splněny pouze na většině bitů. Například, pokud je požadováno $M_1 = M_2$, znamená to, že rovnost nemusí platit na všech bitech. Těmto proměnným říkáme blízké. Z hlediska složitosti nás zajímají zejména taková řešení pro blízké proměnné, která jsou dosažena rychleji než hrubou silou.
Máme tedy tyto úlohy:
(AA-EE): nalezněte blízké proměnné, které dávají plnou rovnost v rovnicích (a, b, c, d , e). Čím bližší proměnné nalezneme, tím lépe.

Úlohy (AAA) – (EEE)
Úlohy (AAA) – (EEE) odpovídají úlohám (a) – (e), ale týkají se blízkých řešení pro blízké proměnné. Hledáme tedy proměnné (M nebo H), pro něž uvedené rovnice platí na co nejvíce bitech, přičemž požadovaná rovnost proměnných M nebo H je také chápána jako blízká.
Z hlediska složitosti nás opět zajímají řešení, která jsou dosažena rychleji než hrubou silou.
Máme tedy tyto úlohy:
(AAA-EEE): nalezněte blízké proměnné, které dávají blízkou rovnost v rovnicích (a, b, c, d , e). Čím bližší proměnné a čím bližší řešení je dosaženo, tím lépe.

Poznámka: (d) je triviální, (D) není
Pokud se podíváte na úlohu (d), uvidíte, že je triviální. Je zde kvůli úplnosti a hned uvidíme proč. Například (D) už tak triviální není!
Úloha (d)
Úloha (d) znamená, že pro nějaké pevné známé $H_1 = H_2$ máme najít M_1, M_2 tak, aby platila rovnice
$f_0(M_1, H_1) = f_0(M_2, H_2)$.
Máme
$A_2A_1(M_1 \oplus H_1) + ROTL^1(H_1) = A_2A_1(M_2 \oplus H_2) + ROTL^1(H_2)$.
Protože $H_1 = H_2$, dostáváme

$A_2A_1(M_1 \oplus H_1) = A_2A_1(M_2 \oplus H_2)$,
a protože A_2 i A_1 jsou bijekce, máme $M_1 \oplus H_1 = M_2 \oplus H_2$, tj. řešením jsou libovolné bloky M_1, M_2, které jsou shodné.

Úloha (D)
Úloha (D) znamená, že pro nějaké pevné známé $H_1 = H_2$ máme najít M_1, M_2 tak, aby rovnice $f_0(M_1, H_1) = f_0(M_2, H_2)$
platila na co nejvíce bitech. Obdobně i zde rovnici upravíme na tvar
$A_2A_1(M_1 \oplus H_1) = A_2A_1(M_2 \oplus H_2)$. Protože $H_1 = H_2$, můžeme řešit rovnici
$A_2A_1(M_1) = A_2A_1(M_2)$ tak, že hledáme (netriviální řešení) M_1, M_2 aby tato rovnice platila na co nejvíce bitech. Označíme-li xor-diferenci M_1 a M_2 jako Δ, pak chceme najít M_1 a Δ tak, aby $A_2A_1(M_1 \oplus \Delta)$ bylo blízké hodnotě $A_2A_1(M_1)$. Jinými slovy, je to přesně výzkum diferenciálních vlastností zobrazení A_2A_1.
Zatím se ukazuje, že je velice netriviální definovat i obecné diferenciální vlastnosti dílčích zobrazení A_2 a A_1. Jejich složení A_2A_1 bude diferenciálně ještě složitější.

Systematické zkoumání úlohy kolize
Výše uvedené úlohy systematicky vyčerpávaly možnosti jak vyšetřovat kolize, blízké kolize, pseudokolize a blízké pseudokolize u stavebního bloku f_0. Podobně můžeme definovat tytéž úlohy pro bloky f_1, f_2, $f_1 \bullet f_0$, $f_2 \bullet f_1$ a $f_2 \bullet f_1 \bullet f_0$. Definice bychom museli upravit tak, aby počítaly s tím, že bloky f_0, $f_1 \bullet f_0$, $f_2 \bullet f_1 \bullet f_0$ mají vstupy M a H, zatímco bloky f_2 a $f_2 \bullet f_1$ mají vstupy (M, Q_a, Q_b) a (M, Q_a, H). Formulace kolizních úloh bude proto trochu odlišná. Mohli bychom nyní definovat všechny možné úlohy blízkých/pseudo kolizí pro tyto bloky, ale to jistě laskavý čtenář udělá sám. Navíc je možné si v těchto úlohách zvolit vhodné podmínky nebo modifikace, které naopak přenecháváme na invenci čtenáře.

Systematické zkoumání úlohy vzoru
Podobným způsobem jako výše můžeme formulovat úlohy pro hledání vzoru. Začneme opět blokem f_0.

Blok f_0
Máme $f_0(M, H) = A_2A_1(M \oplus H) + ROTL^1(H)$. Pro pevné H je f_0 bijekce a vzor nalezneme velmi snadno. Naproti tomu pro pevné M a obraz $f_0(M, H)$ není snadné najít průběžnou hašovací hodnotu H. Máme totiž následující úlohu:
Pro dané pevné M = d (const) a hodnotu $f_0(M, H) = c$ (const), hledáme neznámou hodnotu H tak, aby $c = A_2A_1(d \oplus H) + ROTL^1(H)$. Soustava rovnic má pak tvar

$$
\begin{array}{rcccl}
c_0 = & H_1 & + & s_0 & ((d_5 \oplus H_5) - (d_7 \oplus H_7) + (d_{10} \oplus H_{10}) + (d_{13} \oplus H_{13}) + (d_{14} \oplus H_{14})) \\
c_1 = & H_2 & + & s_1 & ((d_6 \oplus H_6) - (d_8 \oplus H_8) + (d_{11} \oplus H_{11}) + (d_{14} \oplus H_{14}) - (d_{15} \oplus H_{15})) \\
c_2 = & H_3 & + & s_2 & ((d_0 \oplus H_0) + (d_7 \oplus H_7) + (d_9 \oplus H_9) - (d_{12} \oplus H_{12}) + (d_{15} \oplus H_{15})) \\
c_3 = & H_4 & + & s_3 & ((d_0 \oplus H_0) - (d_1 \oplus H_1) + (d_8 \oplus H_8) - (d_{10} \oplus H_{10}) + (d_{13} \oplus H_{13})) \\
c_4 = & H_5 & + & s_4 & ((d_1 \oplus H_1) + (d_2 \oplus H_2) + (d_9 \oplus H_9) - (d_{11} \oplus H_{11}) - (d_{14} \oplus H_{14})) \\
c_5 = & H_6 & + & s_0 & ((d_3 \oplus H_3) - (d_2 \oplus H_2) + (d_{10} \oplus H_{10}) - (d_{12} \oplus H_{12}) + (d_{15} \oplus H_{15})) \\
c_6 = & H_7 & + & s_1 & ((d_4 \oplus H_4) - (d_0 \oplus H_0) - (d_3 \oplus H_3) - (d_{11} \oplus H_{11}) + (d_{13} \oplus H_{13})) \\
c_7 = & H_8 & + & s_2 & ((d_1 \oplus H_1) - (d_4 \oplus H_4) - (d_5 \oplus H_5) - (d_{12} \oplus H_{12}) - (d_{14} \oplus H_{14})) \\
c_8 = & H_9 & + & s_3 & ((d_2 \oplus H_2) - (d_5 \oplus H_5) - (d_6 \oplus H_6) + (d_{13} \oplus H_{13}) - (d_{15} \oplus H_{15})) \\
c_9 = & H_{10} & + & s_4 & ((d_0 \oplus H_0) - (d_3 \oplus H_3) + (d_6 \oplus H_6) - (d_7 \oplus H_7) + (d_{14} \oplus H_{14})) \\
c_{10} = & H_{11} & + & s_0 & ((d_8 \oplus H_8) - (d_1 \oplus H_1) - (d_4 \oplus H_4) - (d_7 \oplus H_7) + (d_{15} \oplus H_{15})) \\
c_{11} = & H_{12} & + & s_1 & ((d_8 \oplus H_8) - (d_0 \oplus H_0) - (d_2 \oplus H_2) - (d_5 \oplus H_5) + (d_9 \oplus H_9)) \\
c_{12} = & H_{13} & + & s_2 & ((d_1 \oplus H_1) + (d_3 \oplus H_3) - (d_6 \oplus H_6) - (d_9 \oplus H_9) + (d_{10} \oplus H_{10})) \\
c_{13} = & H_{14} & + & s_3 & ((d_2 \oplus H_2) + (d_4 \oplus H_4) + (d_7 \oplus H_7) + (d_{10} \oplus H_{10}) + (d_{11} \oplus H_{11})) \\
c_{14} = & H_{15} & + & s_4 & ((d_3 \oplus H_3) - (d_5 \oplus H_5) + (d_8 \oplus H_8) - (d_{11} \oplus H_{11}) - (d_{12} \oplus H_{12})) \\
c_{15} = & H_0 & + & s_0 & ((d_{12} \oplus H_{12}) - (d_4 \oplus H_4) - (d_6 \oplus H_6) - (d_9 \oplus H_9) + (d_{13} \oplus H_{13}))
\end{array}
$$

kde c a d jsou známé konstanty a H neznámé proměnné. Ani u této soustavy rovnic neznáme snadné elegantní řešení. Zkuste to!!!

Blok f_1

Máme $f_1(Q_a, M, H) = T^L(T^U(Q_a) + ((B(rotM) + K) \oplus ROTL^7(H)))$. Protože všechna použitá zobrazení jsou bijekce, postačí znát dvě proměnné a obraz, a poslední neznámou dopočítáme prostým způsobem.

Blok f_2

Máme $f_2(Q_a, Q_b, M) = f_6((M \oplus L_a(Q_b)) + (Q_a \oplus L_b(Q_b)))$. Protože f_6 je bijekce, můžeme vzory funkce f_2 zkoumat jako vzory funkce $G(Q_a, Q_b, M) = (M \oplus L_a(Q_b)) + (Q_a \oplus L_b(Q_b))$. Pokud známe Q_b a jednu z proměnných (Q_a, M), pak ze znalosti obrazu G dopočítáme zbylou neznámou prostým způsobem.

Pokud neznáme Q_b, není její výpočet z hodnot G, Q_a a M triviální, ale může být jednoduchý. Dostáváme rovnici const = (const $\oplus$ $L_a(Q_b)$) + (const $\oplus$ $L_b(Q_b)$), což vede na úlohu nalezení Q_b (Q_{16}, ..., Q_{31}) jestliže známe konstanty c, d, e:

$$
\begin{aligned}
c_0 &= (d_0 \oplus SHR^5(Q_{16})) + (Q_{24} \oplus e_0)\\
c_1 &= (d_1 \oplus SHL^8(Q_{17})) + (Q_{25} \oplus e_1)\\
c_2 &= (d_2 \oplus SHL^5(Q_{18})) + (Q_{26} \oplus e_2)\\
c_3 &= (d_3 \oplus SHL^5(Q_{19})) + (Q_{27} \oplus e_3)\\
c_4 &= (d_4 \oplus Q_{20}) + (Q_{28} \oplus e_4)\\
c_5 &= (d_5 \oplus SHR^6(Q_{21})) + (Q_{29} \oplus e_5)\\
c_6 &= (d_6 \oplus SHL^6(Q_{22})) + (Q_{30} \oplus e_6)\\
c_7 &= (d_7 \oplus SHL^2(Q_{23})) + (Q_{31} \oplus e_7)\\
c_8 &= (d_8 \oplus Q_{24}) + (Q_{23} \oplus e_8)\\
c_9 &= (d_9 \oplus Q_{25}) + (Q_{16} \oplus e_9)\\
c_{10} &= (d_{10} \oplus Q_{26}) + (Q_{17} \oplus e_{10})\\
c_{11} &= (d_{11} \oplus Q_{27}) + (Q_{18} \oplus e_{11})\\
c_{12} &= (d_{12} \oplus Q_{28}) + (Q_{19} \oplus e_{12})\\
c_{13} &= (d_{13} \oplus Q_{29}) + (Q_{20} \oplus e_{13})\\
c_{14} &= (d_{14} \oplus Q_{30}) + (Q_{21} \oplus e_{14})\\
c_{15} &= (d_{15} \oplus Q_{31}) + (Q_{22} \oplus e_{15})
\end{aligned}
$$

Ani u této soustavy rovnic neznáme snadné elegantní řešení. Zkuste to!!!

Blok $f_1 \bullet f_0$

Výstupem bloku $f_1 \bullet f_0$ je hodnota Q_b. Máme

$Q_a = A_2(A_1(M \oplus H)) + ROTL^1(H)$,

$Q_b = T^L(T^U(Q_a) + ((B(rotM) + K) \oplus ROTL^7(H)))$, tedy

$Q_b(M, H) = T^L(T^U(A_2(A_1(M \oplus H)) + ROTL^1(H)) + ((B(rotM) + K) \oplus ROTL^7(H)))$.

Protože řešíme úlohu nalezení vzoru ke Qb, můžeme závěrečnou bijekci T^L vynechat a hledat pouze vzor k obrazu proměnné R, tedy funkce

$R(M, H) = T^U(A_2(A_1(M \oplus H)) + ROTL^1(H)) + ((B(rotM) + K) \oplus ROTL^7(H))$.

Pokud si napíšeme vznikající rovnice, musíme použít meziproměnné, jinak dostáváme dosti nepřehlednou změť funkcí a proměnných.

$$
\begin{array}{lllllllllllllllllll}
Q_0 = & H_1 & + & s_0 & (& (M_5 \oplus H_5) & - & (M_7 \oplus H_7) & + & (M_{10} \oplus H_{10}) & + & (M_{13} \oplus H_{13}) & + & (M_{14} \oplus H_{14}) &) \\
Q_1 = & H_2 & + & s_1 & (& (M_6 \oplus H_6) & - & (M_8 \oplus H_8) & + & (M_{11} \oplus H_{11}) & + & (M_{14} \oplus H_{14}) & - & (M_{15} \oplus H_{15}) &) \\
Q_2 = & H_3 & + & s_2 & (& (M_0 \oplus H_0) & + & (M_7 \oplus H_7) & + & (M_9 \oplus H_9) & - & (M_{12} \oplus H_{12}) & + & (M_{15} \oplus H_{15}) &) \\
Q_3 = & H_4 & + & s_3 & (& (M_0 \oplus H_0) & - & (M_1 \oplus H_1) & + & (M_8 \oplus H_8) & - & (M_{10} \oplus H_{10}) & + & (M_{13} \oplus H_{13}) &) \\
Q_4 = & H_5 & + & s_4 & (& (M_1 \oplus H_1) & + & (M_2 \oplus H_2) & + & (M_9 \oplus H_9) & - & (M_{11} \oplus H_{11}) & - & (M_{14} \oplus H_{14}) &) \\
Q_5 = & H_6 & + & s_0 & (& (M_3 \oplus H_3) & - & (M_2 \oplus H_2) & + & (M_{10} \oplus H_{10}) & - & (M_{12} \oplus H_{12}) & + & (M_{15} \oplus H_{15}) &) \\
Q_6 = & H_7 & + & s_1 & (& (M_4 \oplus H_4) & - & (M_0 \oplus H_0) & - & (M_3 \oplus H_3) & - & (M_{11} \oplus H_{11}) & + & (M_{13} \oplus H_{13}) &) \\
Q_7 = & H_8 & + & s_2 & (& (M_1 \oplus H_1) & - & (M_4 \oplus H_4) & - & (M_5 \oplus H_5) & - & (M_{12} \oplus H_{12}) & - & (M_{14} \oplus H_{14}) &) \\
Q_8 = & H_0 & + & s_3 & (& (M_2 \oplus H_2) & - & (M_5 \oplus H_5) & - & (M_6 \oplus H_6) & + & (M_{13} \oplus H_{13}) & - & (M_{15} \oplus H_{15}) &) \\
Q_9 = & H_{10} & + & s_4 & (& (M_0 \oplus H_0) & - & (M_3 \oplus H_3) & + & (M_6 \oplus H_6) & - & (M_7 \oplus H_7) & + & (M_{14} \oplus H_{14}) &) \\
Q_{10} = & H_{11} & + & s_0 & (& (M_8 \oplus H_8) & - & (M_1 \oplus H_1) & - & (M_4 \oplus H_4) & - & (M_7 \oplus H_7) & + & (M_{15} \oplus H_{15}) &) \\
Q_{11} = & H_{12} & + & s_1 & (& (M_8 \oplus H_8) & - & (M_0 \oplus H_0) & - & (M_2 \oplus H_2) & - & (M_5 \oplus H_5) & + & (M_9 \oplus H_9) &) \\
Q_{12} = & H_{13} & + & s_2 & (& (M_1 \oplus H_1) & + & (M_3 \oplus H_3) & - & (M_6 \oplus H_6) & - & (M_9 \oplus H_9) & + & (M_{10} \oplus H_{10}) &) \\
Q_{13} = & H_{14} & + & s_3 & (& (M_2 \oplus H_2) & + & (M_4 \oplus H_4) & + & (M_7 \oplus H_7) & + & (M_{10} \oplus H_{10}) & + & (M_{11} \oplus H_{11}) &) \\
Q_{14} = & H_{15} & + & s_4 & (& (M_3 \oplus H_3) & - & (M_5 \oplus H_5) & + & (M_8 \oplus H_8) & - & (M_{11} \oplus H_{11}) & - & (M_{12} \oplus H_{12}) &) \\
Q_{15} = & H_0 & + & s_0 & (& (M_{12} \oplus H_{12}) & - & (M_4 \oplus H_4) & - & (M_6 \oplus H_6) & - & (M_9 \oplus H_9) & + & (M_{13} \oplus H_{13}) &)
\end{array}
$$

$$
\begin{aligned}
P_0 &= s1(Q_0) + s2(Q_1) + s3(Q_2) + s0(Q_3) + s1(Q_4) + s2(Q_5) + s3(Q_6) + s0(Q_7) + s1(Q_8) + s2(Q_9) + s3(Q_{10}) + s0(Q_{11}) + s1(Q_{12}) + s2(Q_{13}) + \\
&\quad + s3(Q_{14}) + s0(Q_{15}) \\
P_1 &= s1(Q_1) + s2(Q_2) + s3(Q_3) + s0(Q_4) + s1(Q_5) + s2(Q_6) + s3(Q_7) + s0(Q_8) + s1(Q_9) + s2(Q_{10}) + s3(Q_{11}) + s0(Q_{12}) + s1(Q_{13}) + \\
&\quad + s2(Q_{14}) + s3(Q_{15}) \\
P_2 &= Q_2 + r1(Q_3) + Q_4 + r2(Q_5) + Q_6 + r3(Q_7) + Q_8 + r4(Q_9) + Q_{10} + r5(Q_{11}) + Q_{12} + r6(Q_{13}) + Q_{14} + r7(Q_{15}) \\
P_3 &= Q_3 + r1(Q_4) + Q_5 + r2(Q_6) + Q_7 + r3(Q_8) + Q_9 + r4(Q_{10}) + Q_{11} + r5(Q_{12}) + Q_{13} + r6(Q_{14}) + Q_{15} \\
P_4 &= Q_4 + r1(Q_5) + Q_6 + r2(Q_7) + Q_8 + r3(Q_9) + Q_{10} + r4(Q_{11}) + Q_{12} + r5(Q_{13}) + Q_{14} + r6(Q_{15}) \\
P_5 &= Q_5 + r1(Q_6) + Q_7 + r2(Q_8) + Q_9 + r3(Q_{10}) + Q_{11} + r4(Q_{12}) + Q_{13} + r5(Q_{14}) + Q_{15} \\
P_6 &= Q_6 + r1(Q_7) + Q_8 + r2(Q_9) + Q_{10} + r3(Q_{11}) + Q_{12} + r4(Q_{13}) + Q_{14} + r5(Q_{15}) \\
P_7 &= Q_7 + r1(Q_8) + Q_9 + r2(Q_{10}) + Q_{11} + r3(Q_{12}) + Q_{13} + r4(Q_{14}) + Q_{15} \\
P_8 &= Q_8 + r1(Q_9) + Q_{10} + r2(Q_{11}) + Q_{12} + r3(Q_{13}) + Q_{14} + r4(Q_{15}) \\
P_9 &= Q_9 + r1(Q_{10}) + Q_{11} + r2(Q_{12}) + Q_{13} + r3(Q_{14}) + Q_{15} \\
P_{10} &= Q_{10} + r1(Q_{11}) + Q_{12} + r2(Q_{13}) + Q_{14} + r3(Q_{15}) \\
P_{11} &= Q_{11} + r1(Q_{12}) + Q_{13} + r2(Q_{14}) + Q_{15} \\
P_{12} &= Q_{12} + r1(Q_{13}) + Q_{14} + r2(Q_{15}) \\
P_{13} &= Q_{13} + r1(Q_{14}) + Q_{15} \\
P_{14} &= Q_{14} + r1(Q_{15}) \\
P_{15} &= Q_{15}
\end{aligned}
$$

$$
\begin{array}{lllllllllllllllll}
R_0 = & P_0 + A_0 & = & P_0 & + & (& H_6 & \oplus (& ROTL^1(M_0) & + & ROTL^4(M_3) & - & ROTL^{11}(M_{10}) & + & K_0 &)) \\
R_1 = & P_1 + A_1 & = & P_1 & + & (& H_7 & \oplus (& ROTL^2(M_1) & + & ROTL^5(M_4) & - & ROTL^{12}(M_{11}) & + & K_1 &)) \\
R_2 = & P_2 + A_2 & = & P_2 & + & (& H_8 & \oplus (& ROTL^3(M_2) & + & ROTL^6(M_5) & - & ROTL^{13}(M_{12}) & + & K_2 &)) \\
R_3 = & P_3 + A_3 & = & P_3 & + & (& H_9 & \oplus (& ROTL^4(M_3) & + & ROTL^7(M_6) & - & ROTL^{14}(M_{13}) & + & K_3 &)) \\
R_4 = & P_4 + A_4 & = & P_4 & + & (& H_{10} & \oplus (& ROTL^5(M_4) & + & ROTL^8(M_7) & - & ROTL^{15}(M_{14}) & + & K_4 &)) \\
R_5 = & P_5 + A_5 & = & P_5 & + & (& H_{11} & \oplus (& ROTL^6(M_5) & + & ROTL^9(M_8) & - & ROTL^{16}(M_{15}) & + & K_5 &)) \\
R_6 = & P_6 + A_6 & = & P_6 & + & (& H_{12} & \oplus (& ROTL^7(M_6) & + & ROTL^{10}(M_9) & - & ROTL^1(M_0) & + & K_6 &)) \\
R_7 = & P_7 + A_7 & = & P_7 & + & (& H_{13} & \oplus (& ROTL^8(M_7) & + & ROTL^{11}(M_{10}) & - & ROTL^2(M_1) & + & K_7 &)) \\
R_8 = & P_8 + A_8 & = & P_8 & + & (& H_{14} & \oplus (& ROTL^9(M_8) & + & ROTL^{12}(M_{11}) & - & ROTL^3(M_2) & + & K_8 &)) \\
R_9 = & P_9 + A_8 & = & P_9 & + & (& H_{15} & \oplus (& ROTL^{10}(M_9) & + & ROTL^{13}(M_{12}) & - & ROTL^4(M_3) & + & K_9 &)) \\
R_{10} = & P_{10} + A_{10} & = & P_{10} & + & (& H_0 & \oplus (& ROTL^{11}(M_{10}) & + & ROTL^{14}(M_{13}) & - & ROTL^5(M_4) & + & K_{10} &)) \\
R_{11} = & P_{11} + A_{11} & = & P_{11} & + & (& H_1 & \oplus (& ROTL^{12}(M_{11}) & + & ROTL^{15}(M_{14}) & - & ROTL^6(M_5) & + & K_{11} &)) \\
R_{12} = & P_{12} + A_{12} & = & P_{12} & + & (& H_2 & \oplus (& ROTL^{13}(M_{12}) & + & ROTL^{16}(M_{15}) & - & ROTL^7(M_6) & + & K_{12} &)) \\
R_{13} = & P_{13} + A_{13} & = & P_{13} & + & (& H_3 & \oplus (& ROTL^{14}(M_{13}) & + & ROTL^1(M_0) & - & ROTL^8(M_7) & + & K_{13} &)) \\
R_{14} = & P_{14} + A_{14} & = & P_{14} & + & (& H_4 & \oplus (& ROTL^{15}(M_{14}) & + & ROTL^2(M_1) & - & ROTL^9(M_8) & + & K_{14} &)) \\
R_{15} = & P_{15} + A_{15} & = & P_{15} & + & (& H_5 & \oplus (& ROTL^{16}(M_{15}) & + & ROTL^3(M_2) & - & ROTL^{10}(M_9) & + & K_{15} &))
\end{array}
$$

Z této soustavy je vidět, že pokud jedna z hodnot M nebo H bude konstantní, zatímco druhá se bude měnit, bude se měnit proměnná Q_a, která vtáhne složité výrazy pro Q_0, ..., Q_{15} do rovnic pro proměnnou P. Takový systém opět nezapíšeme jednoduše. Jako vhodná cesta se jeví hledání takových pseudovzorů, u nichž bude M ⊕ H konstantní. Je to vidět i z rovnice R(M, H) = $T^U(A_2(A_1(M \oplus H)) + ROTL^1(H)) + ((B(rotM) + K) \oplus ROTL^7(H))$, která nyní bude mít přijatelný tvar const = $T^U(const + ROTL^1(H)) + ((B(rotM) + K) \oplus ROTL^7(H))$. Soustava by tedy vypadala následovně:

$$
\begin{aligned}
Q_0 &= H_1 + d_1 \\
Q_1 &= H_2 + d_2 \\
Q_2 &= H_3 + d_3 \\
Q_3 &= H_4 + d_4 \\
Q_4 &= H_5 + d_5 \\
Q_5 &= H_6 + d_6 \\
Q_6 &= H_7 + d_7 \\
Q_7 &= H_8 + d_8 \\
Q_8 &= H_0 + d_0 \\
Q_9 &= H_{10} + d_{10} \\
Q_{10} &= H_{11} + d_{11} \\
Q_{11} &= H_{12} + d_{12} \\
Q_{12} &= H_{13} + d_{13} \\
Q_{13} &= H_{14} + d_{14} \\
Q_{14} &= H_{15} + d_{15} \\
Q_{15} &= H_0 + d_0
\end{aligned}
$$

$$
\begin{aligned}
P_0 &= s1(Q_0) + s2(Q_1) + s3(Q_2) + s0(Q_3) + s1(Q_4) + s2(Q_5) + s3(Q_6) + s0(Q_7) + s1(Q_8) + s2(Q_9) + s3(Q_{10}) + s0(Q_{11}) + s1(Q_{12}) + s2(Q_{13}) + \\
&\quad + s3(Q_{14}) + s0(Q_{15}) \\
P_1 &= s1(Q_1) + s2(Q_2) + s3(Q_3) + s0(Q_4) + s1(Q_5) + s2(Q_6) + s3(Q_7) + s0(Q_8) + s1(Q_9) + s2(Q_{10}) + s3(Q_{11}) + s0(Q_{12}) + s1(Q_{13}) + \\
&\quad + s2(Q_{14}) + s3(Q_{15}) \\
P_2 &= Q_2 + r1(Q_3) + Q_4 + r2(Q_5) + Q_6 + r3(Q_7) + Q_8 + r4(Q_9) + Q_{10} + r5(Q_{11}) + Q_{12} + r6(Q_{13}) + Q_{14} + r7(Q_{15}) \\
P_3 &= Q_3 + r1(Q_4) + Q_5 + r2(Q_6) + Q_7 + r3(Q_8) + Q_9 + r4(Q_{10}) + Q_{11} + r5(Q_{12}) + Q_{13} + r6(Q_{14}) + Q_{15} \\
P_4 &= Q_4 + r1(Q_5) + Q_6 + r2(Q_7) + Q_8 + r3(Q_9) + Q_{10} + r4(Q_{11}) + Q_{12} + r5(Q_{13}) + Q_{14} + r6(Q_{15}) \\
P_5 &= Q_5 + r1(Q_6) + Q_7 + r2(Q_8) + Q_9 + r3(Q_{10}) + Q_{11} + r4(Q_{12}) + Q_{13} + r5(Q_{14}) + Q_{15} \\
P_6 &= Q_6 + r1(Q_7) + Q_8 + r2(Q_9) + Q_{10} + r3(Q_{11}) + Q_{12} + r4(Q_{13}) + Q_{14} + r5(Q_{15}) \\
P_7 &= Q_7 + r1(Q_8) + Q_9 + r2(Q_{10}) + Q_{11} + r3(Q_{12}) + Q_{13} + r4(Q_{14}) + Q_{15} \\
P_8 &= Q_8 + r1(Q_9) + Q_{10} + r2(Q_{11}) + Q_{12} + r3(Q_{13}) + Q_{14} + r4(Q_{15}) \\
P_9 &= Q_9 + r1(Q_{10}) + Q_{11} + r2(Q_{12}) + Q_{13} + r3(Q_{14}) + Q_{15} \\
P_{10} &= Q_{10} + r1(Q_{11}) + Q_{12} + r2(Q_{13}) + Q_{14} + r3(Q_{15}) \\
P_{11} &= Q_{11} + r1(Q_{12}) + Q_{13} + r2(Q_{14}) + Q_{15} \\
P_{12} &= Q_{12} + r1(Q_{13}) + Q_{14} + r2(Q_{15}) \\
P_{13} &= Q_{13} + r1(Q_{14}) + Q_{15} \\
P_{14} &= Q_{14} + r1(Q_{15}) \\
P_{15} &= Q_{15}
\end{aligned}
$$

$$
\begin{aligned}
R_0 &= P_0 + A_0 = P_0 + (H_6 \oplus (ROTL^1(M_0) + ROTL^4(M_3) - ROTL^{11}(M_{10}) + K_0)) \\
R_1 &= P_1 + A_1 = P_1 + (H_7 \oplus (ROTL^2(M_1) + ROTL^5(M_4) - ROTL^{12}(M_{11}) + K_1)) \\
R_2 &= P_2 + A_2 = P_2 + (H_8 \oplus (ROTL^3(M_2) + ROTL^6(M_5) - ROTL^{13}(M_{12}) + K_2)) \\
R_3 &= P_3 + A_3 = P_3 + (H_9 \oplus (ROTL^4(M_3) + ROTL^7(M_6) - ROTL^{14}(M_{13}) + K_3)) \\
R_4 &= P_4 + A_4 = P_4 + (H_{10} \oplus (ROTL^5(M_4) + ROTL^8(M_7) - ROTL^{15}(M_{14}) + K_4)) \\
R_5 &= P_5 + A_5 = P_5 + (H_{11} \oplus (ROTL^6(M_5) + ROTL^9(M_8) - ROTL^{16}(M_{15}) + K_5)) \\
R_6 &= P_6 + A_6 = P_6 + (H_{12} \oplus (ROTL^7(M_6) + ROTL^{10}(M_9) - ROTL^1(M_0) + K_6)) \\
R_7 &= P_7 + A_7 = P_7 + (H_{13} \oplus (ROTL^8(M_7) + ROTL^{11}(M_{10}) - ROTL^2(M_1) + K_7)) \\
R_8 &= P_8 + A_8 = P_8 + (H_{14} \oplus (ROTL^9(M_8) + ROTL^{12}(M_{11}) - ROTL^3(M_2) + K_8)) \\
R_9 &= P_0 + A_8 = P_0 + (H_{15} \oplus (ROTL^{10}(M_9) + ROTL^{13}(M_{12}) - ROTL^4(M_3) + K_9)) \\
R_{10} &= P_{10} + A_{10} = P_{10} + (H_0 \oplus (ROTL^{11}(M_{10}) + ROTL^{14}(M_{13}) - ROTL^5(M_4) + K_{10})) \\
R_{11} &= P_{11} + A_{11} = P_{11} + (H_1 \oplus (ROTL^{12}(M_{11}) + ROTL^{15}(M_{14}) - ROTL^6(M_5) + K_{11})) \\
R_{12} &= P_{12} + A_{12} = P_{12} + (H_2 \oplus (ROTL^{13}(M_{12}) + ROTL^{16}(M_{15}) - ROTL^7(M_6) + K_{12})) \\
R_{13} &= P_{13} + A_{13} = P_{13} + (H_3 \oplus (ROTL^{14}(M_{13}) + ROTL^1(M_0) - ROTL^8(M_7) + K_{13})) \\
R_{14} &= P_{14} + A_{14} = P_{14} + (H_4 \oplus (ROTL^{15}(M_{14}) + ROTL^2(M_1) - ROTL^9(M_8) + K_{14})) \\
R_{15} &= P_{15} + A_{15} = P_{15} + (H_5 \oplus (ROTL^{16}(M_{15}) + ROTL^3(M_2) - ROTL^{10}(M_9) + K_{15}))
\end{aligned}
$$

Po vyloučení proměnné H = M ⊕ const ze soustavy dostaneme
const = T^U(const + $ROTL^1$(M ⊕ const)) + ((B(rotM) + const) ⊕ $ROTL^7$(M ⊕ const)).
Tato soustava není jednoduchá, ale snad by se dala řešit. Konkrétně vypadá takto:

$$
\begin{aligned}
&R_0\\
&= s1((M_1 \oplus c_1) + d_1) + s2((M_2 \oplus c_2) + d_2) + s3((M_3 \oplus c_3) + d_3) + s0((M_4 \oplus c_4) + d_4) +\\
&+s1((M_5 \oplus c_5) + d_5) + s2((M_6 \oplus c_6) + d_6) + s3((M_7 \oplus c_7) + d_7) + s0((M_8 \oplus c_8) + d_8) +\\
&+s1((M_9 \oplus c_9) + d_9) + s2((M_{10} \oplus c_{10}) + d_{10}) + s3((M_{11} \oplus c_{11}) + d_{11}) + s0((M_{12} \oplus c_{12}) + d_{12}) +\\
&+s1((M_{13} \oplus c_{13}) + d_{13}) + s2((M_{14} \oplus c_{14}) + d_{14}) + s3((M_{15} \oplus c_{15}) + d_{15}) + s0((M_0 \oplus c_0) + d_0) +\\
&+((M_6 \oplus c_6) \oplus (ROTL^1(M_0) + ROTL^4(M_3) - ROTL^{11}(M_{10}) + K_0))
\end{aligned}
$$

$$
\begin{aligned}
&R_1\\
&= s1((M_2 \oplus c_2) + d_2) + s2((M_3 \oplus c_3) + d_3) + s3((M_4 \oplus c_4) + d_4) + s0((M_5 \oplus c_5) + d_5) +\\
&+s1((M_6 \oplus c_6) + d_6) + s2((M_7 \oplus c_7) + d_7) + s3((M_8 \oplus c_8) + d_8) + s0((M_9 \oplus c_9) + d_9) +\\
&+s1((M_{10} \oplus c_{10}) + d_{10}) + s2((M_{11} \oplus c_{11}) + d_{11}) + s3((M_{12} \oplus c_{12}) + d_{12}) + s0((M_{13} \oplus c_{13}) + d_{13}) +\\
&+s1((M_{14} \oplus c_{14}) + d_{14}) + s2((M_{15} \oplus c_{15}) + d_{15}) + s3((M_0 \oplus c_0) + d_0)\\
&+((M_7 \oplus c_7) \oplus (ROTL^2(M_1) + ROTL^5(M_4) - ROTL^{12}(M_{11}) + K_1))
\end{aligned}
$$

$$
\begin{aligned}
&R_2\\
&= (M_3 \oplus c_3) + d_3 + r1((M_4 \oplus c_4) + d_4) + (M_5 \oplus c_5) + d_5 + r2((M_6 \oplus c_6) + d_6) +\\
&+(M_7 \oplus c_7) + d_7 + r3((M_8 \oplus c_8) + d_8) + (M_9 \oplus c_9) + d_9 + r4((M_{10} \oplus c_{10}) + d_{10}) +\\
&+(M_{11} \oplus c_{11}) + d_{11} + r5((M_{12} \oplus c_{12}) + d_{12}) + (M_{13} \oplus c_{13}) + d_{13} + r6((M_{14} \oplus c_{14}) + d_{14}) +\\
&+(M_{15} \oplus c_{15}) + d_{15} + r7((M_0 \oplus c_0) + d_0) +\\
&+((M_8 \oplus c_8) \oplus (ROTL^3(M_2) + ROTL^6(M_5) - ROTL^{13}(M_{12}) + K_2))
\end{aligned}
$$

$$
\begin{aligned}
&R_3\\
&= (M_4 \oplus c_4) + d_4 + r1((M_5 \oplus c_5) + d_5) + (M_6 \oplus c_6) + d_6 + r2((M_7 \oplus c_7) + d_7) +\\
&+(M_8 \oplus c_8) + d_8 + r3((M_9 \oplus c_9) + d_9) + (M_{10} \oplus c_{10}) + d_{10} + r4((M_{11} \oplus c_{11}) + d_{11}) +\\
&+(M_{12} \oplus c_{12}) + d_{12} + r5((M_{13} \oplus c_{13}) + d_{13}) + (M_{14} \oplus c_{14}) + d_{14} + r6((M_{15} \oplus c_{15}) + d_{15}) +\\
&+(M_0 \oplus c_0) + d_0 + ((M_9 \oplus c_9) \oplus (ROTL^4(M_3) + ROTL^7(M_6) - ROTL^{14}(M_{13}) + K_3))
\end{aligned}
$$

$$
\begin{aligned}
&R_4\\
&= (M_5 \oplus c_5) + d_5 + r1((M_6 \oplus c_6) + d_6) + (M_7 \oplus c_7) + d_7 + r2((M_8 \oplus c_8) + d_8) +\\
&+(M_9 \oplus c_9) + d_9 + r3((M_{10} \oplus c_{10}) + d_{10}) + (M_{11} \oplus c_{11}) + d_{11} + r4((M_{12} \oplus c_{12}) + d_{12}) +\\
&+(M_{13} \oplus c_{13}) + d_{13} + r5((M_{14} \oplus c_{14}) + d_{14}) + (M_{15} \oplus c_{15}) + d_{15} + r6((M_0 \oplus c_0) + d_0) +\\
&+((M_{10} \oplus c_{10}) \oplus (ROTL^5(M_4) + ROTL^8(M_7) - ROTL^{15}(M_{14}) + K_4))
\end{aligned}
$$

$$
\begin{aligned}
&R_5\\
&= (M_6 \oplus c_6) + d_6 + r1((M_7 \oplus c_7) + d_7) + (M_8 \oplus c_8) + d_8 + r2((M_9 \oplus c_9) + d_9) +\\
&+(M_{10} \oplus c_{10}) + d_{10} + r3((M_{11} \oplus c_{11}) + d_{11}) + (M_{12} \oplus c_{12}) + d_{12} + r4((M_{13} \oplus c_{13}) + d_{13}) +\\
&+(M_{14} \oplus c_{14}) + d_{14} + r5((M_{15} \oplus c_{15}) + d_{15}) + (M_0 \oplus c_0) + d_0 +\\
&+((M_{11} \oplus c_{11}) \oplus (ROTL^6(M_5) + ROTL^9(M_8) - ROTL^{16}(M_{15}) + K_5))
\end{aligned}
$$

$$
\begin{aligned}
&R_6\\
&= (M_7 \oplus c_7) + d_7 + r1((M_8 \oplus c_8) + d_8) + (M_9 \oplus c_9) + d_9 + r2((M_{10} \oplus c_{10}) + d_{10}) +\\
&+(M_{11} \oplus c_{11}) + d_{11} + r3((M_{12} \oplus c_{12}) + d_{12}) + (M_{13} \oplus c_{13}) + d_{13} + r4((M_{14} \oplus c_{14}) + d_{14}) +\\
&+(M_{15} \oplus c_{15}) + d_{15} + r5((M_0 \oplus c_0) + d_0) +\\
&+((M_{12} \oplus c_{12}) \oplus (ROTL^7(M_6) + ROTL^{10}(M_9) - ROTL^1(M_0) + K_6))
\end{aligned}
$$

$$
\begin{aligned}
&R_7\\
&= (M_8 \oplus c_8) + d_8 + r1((M_9 \oplus c_9) + d_9) + (M_{10} \oplus c_{10}) + d_{10} + r2((M_{11} \oplus c_{11}) + d_{11}) +\\
&+(M_{12} \oplus c_{12}) + d_{12} + r3((M_{13} \oplus c_{13}) + d_{13}) + (M_{14} \oplus c_{14}) + d_{14} + r4((M_{15} \oplus c_{15}) + d_{15}) +\\
&+(M_0 \oplus c_0) + d_0 +\\
&+((M_{13} \oplus c_{13}) \oplus (ROTL^8(M_7) + ROTL^{11}(M_{10}) - ROTL^2(M_1) + K_7))
\end{aligned}
$$

$$
\begin{aligned}
&R_8\\
&= (M_9 \oplus c_9) + d_9 + r1((M_{10} \oplus c_{10}) + d_{10}) + (M_{11} \oplus c_{11}) + d_{11} + r2((M_{12} \oplus c_{12}) + d_{12}) +\\
&+(M_{13} \oplus c_{13}) + d_{13} + r3((M_{14} \oplus c_{14}) + d_{14}) + (M_{15} \oplus c_{15}) + d_{15} + r4((M_0 \oplus c_0) + d_0) +\\
&+((M_{14} \oplus c_{14}) \oplus (ROTL^9(M_8) + ROTL^{12}(M_{11}) - ROTL^3(M_2) + K_8))
\end{aligned}
$$

$$
\begin{aligned}
&R_9\\
&= (M_{10} \oplus c_{10}) + d_{10} + r1((M_{11} \oplus c_{11}) + d_{11}) + (M_{12} \oplus c_{12}) + d_{12} + r2((M_{13} \oplus c_{13}) + d_{13}) +\\
&+(M_{14} \oplus c_{14}) + d_{14} + r3((M_{15} \oplus c_{15}) + d_{15}) + (M_0 \oplus c_0) + d_0 +\\
&+((M_{15} \oplus c_{15}) \oplus (ROTL^{10}(M_9) + ROTL^{13}(M_{12}) - ROTL^4(M_3) + K_9))
\end{aligned}
$$

$$
\begin{aligned}
&R_{10}\\
&= (M_{11} \oplus c_{11}) + d_{11} + r1((M_{12} \oplus c_{12}) + d_{12}) + (M_{13} \oplus c_{13}) + d_{13} + r2((M_{14} \oplus c_{14}) + d_{14}) +\\
&+(M_{15} \oplus c_{15}) + d_{15} + r3((M_0 \oplus c_0) + d_0) +\\
&+((M_0 \oplus c_0) \oplus (ROTL^{11}(M_{10}) + ROTL^{14}(M_{13}) - ROTL^5(M_4) + K_{10}))
\end{aligned}
$$

$$
\begin{aligned}
&R_{11}\\
&= (M_{12} \oplus c_{12}) + d_{12} + r1((M_{13} \oplus c_{13}) + d_{13}) + (M_{14} \oplus c_{14}) + d_{14} + r2((M_{15} \oplus c_{15}) + d_{15}) +\\
&+(M_0 \oplus c_0) + d_0 +\\
&+((M_1 \oplus c_1) \oplus (ROTL^{12}(M_{11}) + ROTL^{15}(M_{14}) - ROTL^6(M_5) + K_{11}))
\end{aligned}
$$

$$
\begin{aligned}
&R_{12}\\
&= (M_{13} \oplus c_{13}) + d_{13} + r1((M_{14} \oplus c_{14}) + d_{14}) + (M_{15} \oplus c_{15}) + d_{15} + r2((M_0 \oplus c_0) + d_0) +\\
&+((M_2 \oplus c_2) \oplus (ROTL^{13}(M_{12}) + ROTL^{16}(M_{15}) - ROTL^7(M_6) + K_{12}))
\end{aligned}
$$

$$
\begin{aligned}
&R_{13}\\
&= (M_{14} \oplus c_{14}) + d_{14} + r1((M_{15} \oplus c_{15}) + d_{15}) + (M_0 \oplus c_0) + d_0 +\\
&+((M_3 \oplus c_3) \oplus (ROTL^{14}(M_{13}) + ROTL^1(M_0) - ROTL^8(M_7) + K_{13}))
\end{aligned}
$$

$$
\begin{aligned}
&R_{14}\\
&= (M_{15} \oplus c_{15}) + d_{15} + r1((M_0 \oplus c_0) + d_0) +\\
&+((M_4 \oplus c_4) \oplus (ROTL^{15}(M_{14}) + ROTL^2(M_1) - ROTL^9(M_8) + K_{14}))
\end{aligned}
$$

$$
\begin{aligned}
&R_{15}\\
&= (M_0 \oplus c_0) + d_0 +\\
&+((M_5 \oplus c_5) \oplus (ROTL^{16}(M_{15}) + ROTL^3(M_2) - ROTL^{10}(M_9) + K_{15}))
\end{aligned}
$$

kde R, c, d, K jsou známé konstanty a M je neznámá proměnná. Rozhodně stojí za to zkusit najít nějaké řešení.

Stavební bloky $f_2 \bullet f_1$ a $f_2 \bullet f_1 \bullet f_0$
Pokud se podíváme na schéma těchto bloků vidíme, že žádné rozumné zjednodušení se zde nerýsuje. Do rovnic vstupují M, H i M ⊕ H a prostřednictvím funkce AddElement další kombinace M a H.

Měnící se proměnné
Při zkoumání kompresní funkce vždy zkoumáme některou ze situací, že se M nebo H mění, neboť oba dva vstupy nemohou být konstantní (v tom případě by kompresní funkce byla sama konstantní). Důležité je, zda se také mění M ⊕ H nebo ne. Máme tedy tyto možnosti:
M se mění, H se mění, M ⊕ H se nemění
M se mění, H se mění, M ⊕ H se mění
M se mění, H se nemění (⇒ M ⊕ H se mění)
M se nemění, H se mění (⇒ M ⊕ H se mění)

Při zkoumání bloku f_1 a f_2 , pokud chceme dostávat jednodušší rovnice, můžeme uvažovat o některých dalších meziproměnných jako o konstantách, jsou to Q_a, Q_b nebo R. Celkově tak má smysl uvažovat o konstantách M, H, M ⊕ H, Q_a, Q_b a R. To platí pro všechny typy útoků.

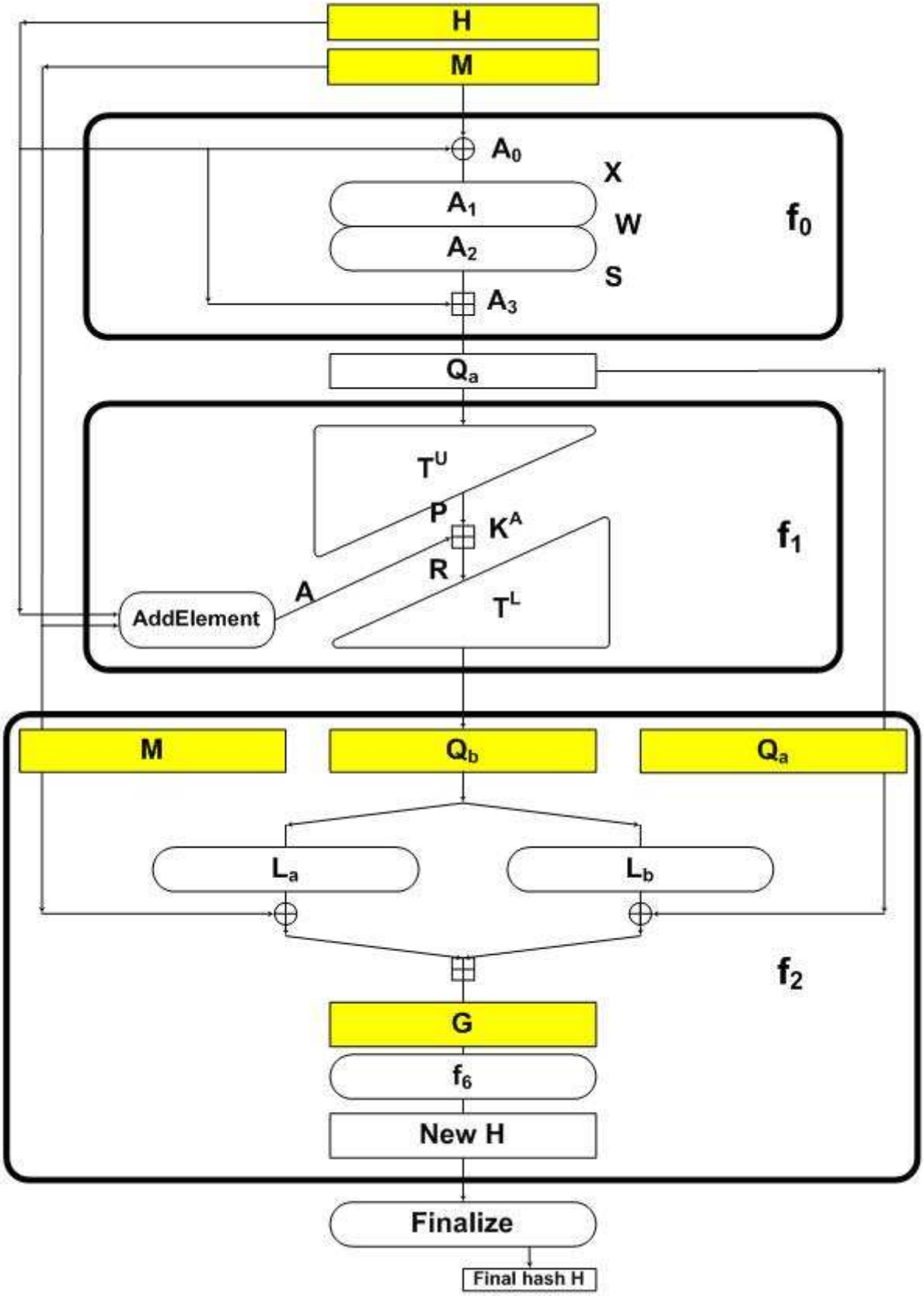
Další poznámka k substituci
Kompresní funkci lze přepsat tak, že místo proměnných (M, H) uvažujeme proměnné (M, X) nebo (H, X), kde X = M ⊕ H.

Řešení všech úloh od malé dimenze k větší
Všechny výše uvedené úlohy mohou být pro skutečné rozměry používané u BMW (n = 512 /1024) velmi složité. Proto je vhodné tyto úlohy řešit pro malá n (w), hledat anomálie a pokusit se tyto postupy přenést do vyšších dimenzí n (w). Jedna z možností je definovat BMW pro šířku slova w = 2, 3, 4, ... Pokud nalezneme příslušná řešení a jejich složitosti, mohli bychom možná extrapolovat složitost pro vyšší hodnoty w = 32 a 64.

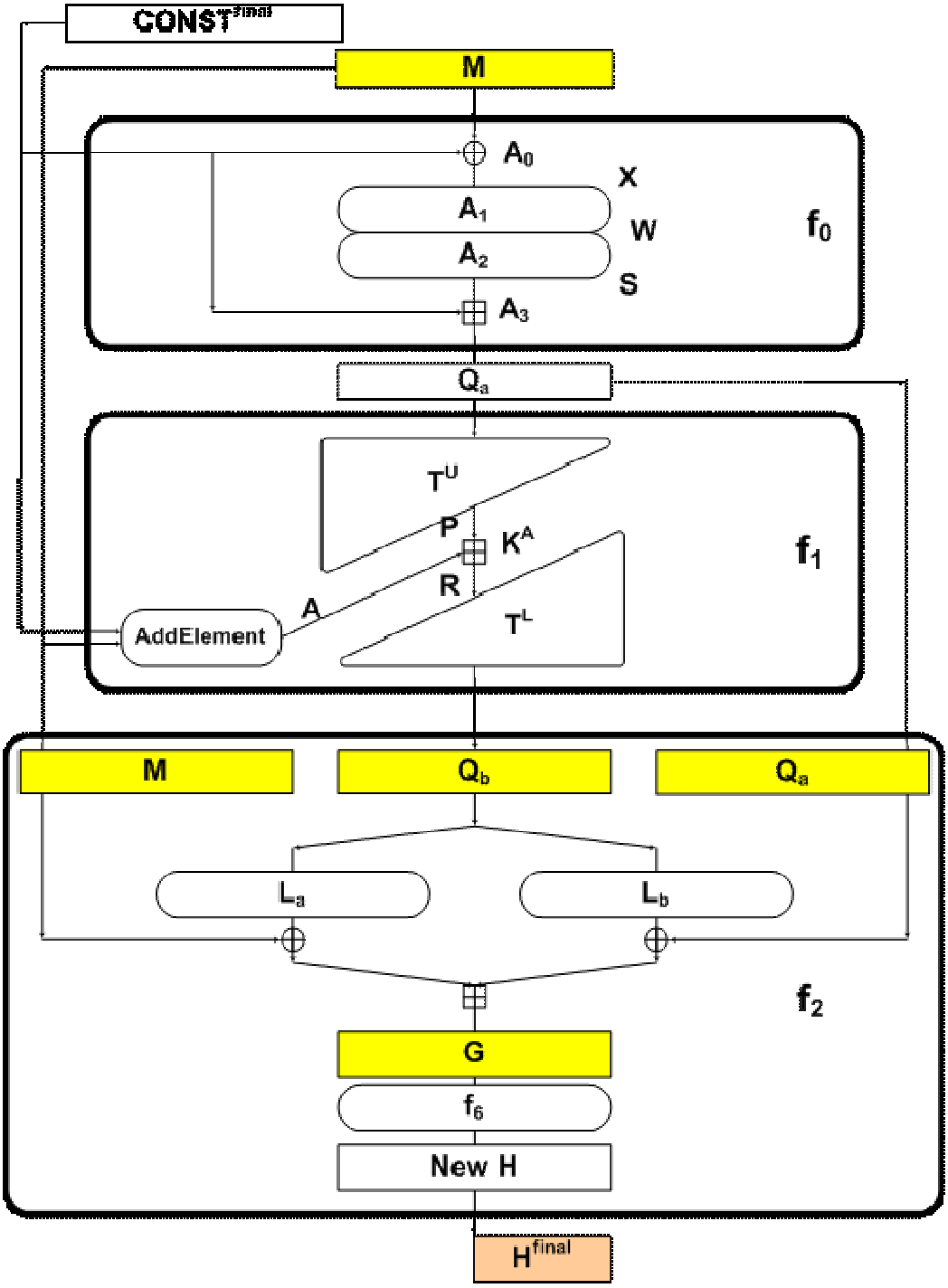
Závěr
V tomto článku jsme uvedli řadu dílčích úloh, které se objevují při hledání kolize a vzoru ke stavebním blokům a celé hašovací funkci BMW. Řešení všech těchto úloh je otevřené a velmi žádané.

Literatura
[1] domácí stránka týmu BMW: http://www.q2s.ntnu.no/sha3_nist_competition/start
[2] stránka NIST k projektu SHA-3: http://csrc.nist.gov/groups/ST/hash/index.html
[3] dokumenty a analýzy BMW a průběžné novinky k projektu SHA-3: http://cryptography.hyperlink.cz/BMW/BMW_CZ.html
[4] Danilo Gligoroski, Vlastimil Klima, On Blue Midnight Wish Decomposition, SantaCrypt 2009, Dec. 3-4, 2009, Prague, Czech Republic, Proceedings of SantaCrypt 2009, ISBN 978-80-904257-0-5, pp. 41-51

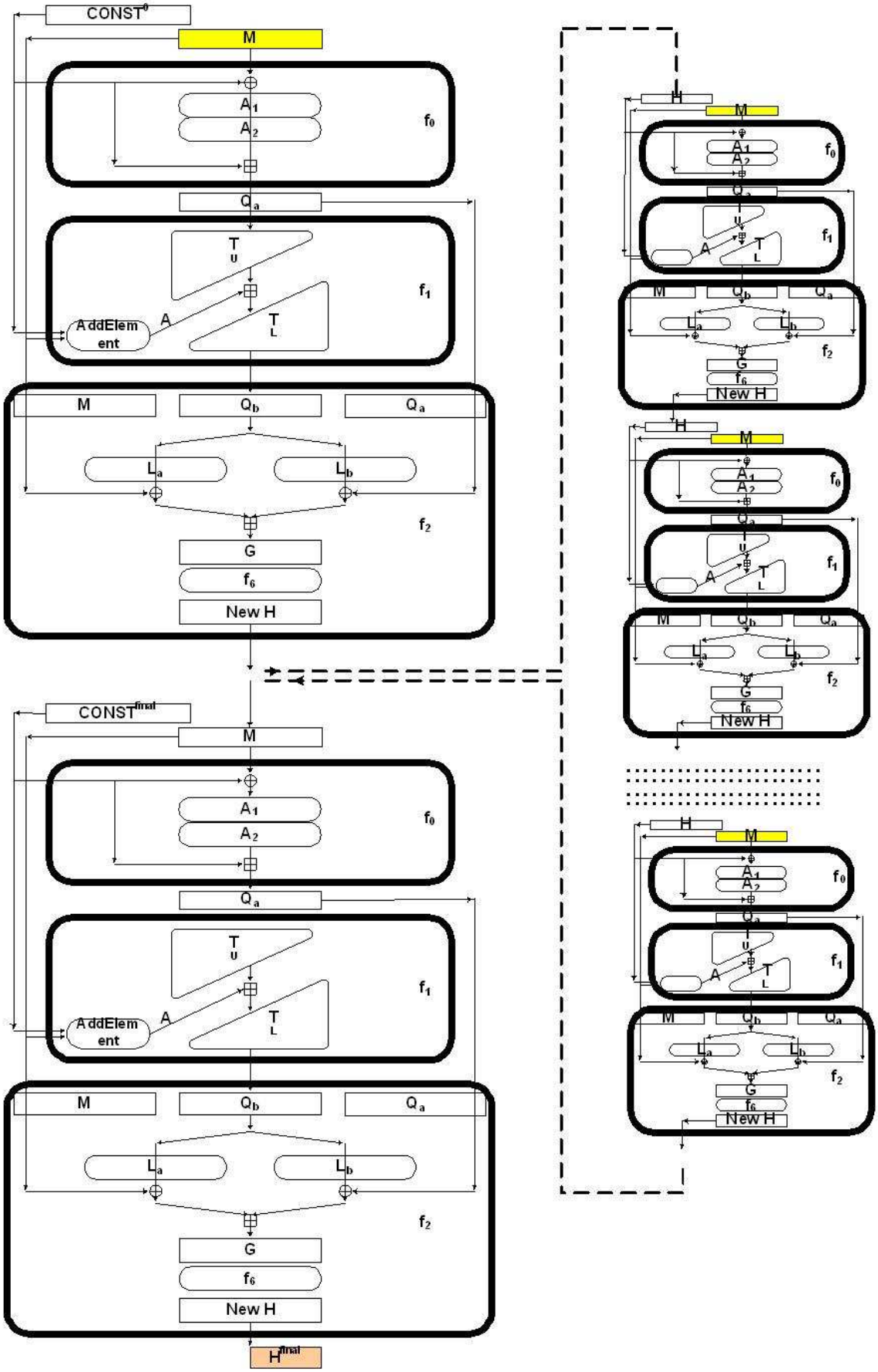
Příloha – Obrázky



Obr.2: Kompresní funkce BMW



Obr. 3: Finální iterace



Obr. 4: Počáteční, vnitřní a závěrečná iterace

B. Přehled některých základních kritérií hodnocení bezpečnosti IT

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

Úvod

Kritéria pro hodnocení bezpečnosti informačních technologií (dále jen "kritéria") slouží především jako **měřítko používané k hodnocení informačních technologií s ohledem na jejich bezpečnost, na konkrétní aplikace služeb a na opatření k zajištění bezpečnosti**. Vládní kritéria většinou určují hlavní směr vývoje i pro kritéria bankovní, komerční atd., obvykle však jsou vládní kritéria používána i nevládními organizacemi. Na rozdíl od těchto kritérií se obdobná vlastní vládní kritéria používaná pro hodnocení kryptografických zařízení zpravidla v řadě zemí nezveřejňují.

Hodnocené objekty se často dělí na *produkty* (nemají specifikováno provozní prostředí a tedy ani některé související hrozby) a na *systémy* (větší spojité celky, při hodnocení se bere v úvahu i konkrétní konfigurace a provozní prostředí).

Při hodnocení *je* od výrobce (žadatele o hodnocení) *vyžadována podrobná specifikace, dokumentace a popis postupu při vývoji*, které by u jiné než komerčně nezávislé agentury byly vystaveny většímu riziku ohrožení úniku informací, jež jsou pro výrobce často životně důležité. Hodnocení je prováděno hodnotitelem na základě žádosti (a za prostředky) výrobce, který také specifikuje, na jaké úrovni má být produkt či systém hodnocen. Podle specifikace požadavků v kritériích musí výrobce hodnotiteli poskytnout potřebnou dokumentaci, podporu odborníků atd.

Hodnocení probíhá v určitém prostředí a konfiguraci, proto je také nutno tyto údaje uvádět při prezentování výsledků hodnocení a dosaženého stupně certifikace (např. u databázových systémů uvést platformu a operační systém, se kterými bylo hodnocení prováděno, verze všech produktů atd.).

I. Trusted Computer System Evaluation Criteria (TCSEC)

"Oranžová kniha"

Koncem 60. let si odpovědní činitelé amerických vládních agentur začali uvědomovat potřebu jednotného měřítka pro hodnocení produktů s ohledem na jejich služby při ochraně informací. Hodnocení produktů pro jednotlivé úřady bylo jak časově, tak i finančně náročné a perspektiva jednoho zhodnocení a akreditace, která by byla platná pro daný produkt na celém území USA, byla snad nejjednodušším řešením**. Daná certifikace (výsledek hodnocení) šetří čas a vládní prostředky**, protože bez ní by bylo nutno provádět hodnocení vždy znovu při každém nákupu. **Druhým pozitivním aspektem je pak možnost srovnání a snazší specifikace potřeb jednotlivých úřadů.**

Výsledek dlouholeté práce ministerstva obrany, standardizačních orgánů a také vládě blízkých firem se dostavil v podobě kritérií pro hodnocení důvěryhodných výpočetních systémů. Tato kritéria byla vydána v roce 1985 jako standard ministerstva obrany. Oranžový přebal charakterizoval tuto publikaci, která je dodnes pod názvem "Orange Book" známa po celém světě.

Trusted Computer System Evaluation Criteria (TCSEC) jsou ovlivněna dobou vzniku a slouží především pro potřeby víceuživatelských monolitických počítačů. Databázové systémy, sítě, menší části systémů atd. byly pak s postupem času zohledněny "interpretacemi" TCSEC -- jako např. Trusted Database Interpretation, Trusted Network Interpretation atd. Barvy přebalů těchto publikací daly podnět k názvům jako "Red Book" atd. Souhrnně se pak pro celou sérii vžilo označení Duhová série (Rainbow series).

TCSEC hodnotí míru splnění požadavků ve třech oblastech informační bezpečnosti

- *Zásady* (Policy) - metody řízení přístupu, označení stupně utajení
- *Odpovědnost* (Accountability) - zjištění identity uživatele, monitoring činnosti uživatele
- *Záruky* (Assurance) - požadavky na nezávislé hodnocení a průběžné provádění bezpečnostních funkcí.

TCSEC zavádí čtyři skupiny hodnocení (A, B, C, D), které odpovídají vždy jednomu kvalitativně odlišnému stupni bezpečnosti a jsou dále děleny do tříd (D, C1, C2, B1, B2, B3, A1). Každá ze tříd pokrývá a popisuje požadované aspekty hodnocení (bezpečnostní směrnice, odpovědnost, zabezpečení a dokumentaci).

Tím jsou zavedeny stupně míry splnění požadavků

- minimální ochrana - třída D
- výběrová ochrana - třída C
- povinná ochrana - třída B
- verifikovaná ochrana - třída A

Jednotlivé požadavky pro dané třídy se postupně zpodrobňují a tvoří hierarchii s třídou D jako prvkem nejnižším a s třídou A1 jako prvkem nejvyšším. Praktického užití se dostává především skupinám B a hlavně C, neboť třída D zahrnuje prostě produkty, které byly podrobeny hodnocení s užitím TCSEC, ale které nedosáhly žádné z vyšších tříd, a třída A1 stanovuje požadavky, které jsou pro většinu produktů z finančních důvodů nerealizovatelné.

TCSEC a „duhová série“: http://csrc.nist.gov/publications/secpubs/rainbow/
Department Of Defense Trusted Computer System Evaluation Criteria" ("Orange Book")
http://csrc.nist.gov/publications/secpubs/rainbow/std001.txt

II. Information Technology Security Evaluation Criteria (ITSEC)

Hodnocení bezpečnosti podle IT ITSEC (Information Technology Security Evaluation Criteria) bylo vytvořeno v roce 1990. Harmonizovaná verze národních kritérií přijatých ve Francii, Německu, Anglii a Nizozemí, byla předložena v září 1990 v Bruselu k připomínkám a diskuzi, které se zúčastnily i USA. Po úpravách byla vydána Úřadem pro oficiální publikace Evropského společenství v červnu 1991 (materiál byl označen jako prozatímní materiál k dvouletému ověření). Schválena jako doporučení byla v dubnu 1995.

Na rozdíl od standardu TCSEC, který vznikal pro vojenské prostředí a orientoval se zejména na důvěrnost informace, je ITSEC koncipován mnohem obecněji a pokrývá částečně i požadavky integrity a dostupnosti informace. Oproti TCSEC definuje ITSEC navíc způsob

dokumentace hodnoceného předmětu, způsob definování bezpečnostního cíle a způsob provádění hodnocení.

Třídy funkčnosti ITSEC

Kritéria ITSEC specifikují sedm tříd **míry zaručitelnosti bezpečnosti** E0 až E6 reprezentujících vzrůstající úrovně důvěry a dále ve své příloze definují dalších deset tříd bezpečnostní funkčnosti F-xx.

Dosažená úroveň bezpečnosti se hodnotí dosaženou důvěryhodností ve 4 pohledech
- proces vývoje IS (forma specifikace požadavků, návrh architektury, detailní návrh, implementace)
- prostředí vývoje IS (jak probíhalo řízení projektu, použité programovací jazyky, použité kompilátory, aplikovaná bezpečnost při vývoji)
- provozní dokumentace IS (dokumentace správce, dokumentace uživatele)
- provozní prostředí IS (dodávka, distribuce, konfigurace, spuštění, provoz.

V kritériích ITSEC je definováno sedm tříd zaručitelnosti bezpečnosti E0 až E6 a nepředpokládá se, že by uživatelé kritérií definice těchto tříd měnili nebo si definovali své vlastní třídy.

V příloze definovaných pět tříd funkčnosti F-C1, F-C2, F-B1, F-B2 a F-B3 odpovídá stejnojmenným třídám kritérií TCSEC. Zbylých definovaných pět tříd funkčnosti je orientováno aplikačně, jsou to třídy se zvýšenými bezpečnostními požadavky v některé oblasti bezpečnosti, nemají hierarchickou strukturu. Jsou to F-IN (vysoké nároky na integritu), F-AV (vysoké nároky na dostupnost), F-DI (vysoké nároky na integritu při přenosu), F-DC (vysoké nároky na důvěrnost při přenosu), F-DX (vysoké nároky na důvěrnost a integritu při přenosu)

Výše uvedené třídy funkčnosti jsou, na rozdíl od tříd míry zaručitelnosti bezpečnosti, pouze příklady. Nejsou závazné a mají sloužit pro usnadnění práce uživatelům kritérií ITSEC.

První možností využití je, že uživatel si přímo vybere některou ze tříd funkčnosti uvedenou v kritériích ITSEC. V tomto případě si zpravidla vybere některou ze tříd, které jsou hierarchické a odpovídají třídám kritérií TCSEC.

Druhou možností je, že uživatel kritérií použije vhodné kombinace některých ze tříd funkčnosti, uvedených v kritériích ITSEC. Tato možnost dává uživateli kritérií větší možnosti a dovoluje mu vytvořit zodolněnou třídu funkčnosti, která lépe odpovídá jeho požadavkům.

Třetí možností je, že uživatel kritérií použije některou, již vytvořenou třídu funkčnosti, která není součástí kritérií ITSEC, ale je vytvořena v souladu s těmito kritérii a vyhovuje požadavkům uživatele.

Konečně poslední, čtvrtou, možností je případ, kdy si uživatel kritérií vytvoří sám vlastní třídu funkčnosti, která je v souladu s požadavky kritérií ITSEC. Tento případ nastane zejména v okamžiku, kdy je hodnocený předmět natolik specifický, že jsou všechny výše uvedené cesty neschůdné. Vzhledem k pracnosti tohoto způsobu stojí však vždy za úvahu, zda skutečně nelze využít některý ze tří výše uvedených případů.

Specifikace funkcí prosazujících bezpečnost podle ITSEC

Popis těchto funkcí využívá následující povinná ***generická záhlaví:***

- Identifikace a autentizace
- Řízení přístupu
- Účtovatelnost
- Audit
- Opakované užití
- Přesnost
- Spolehlivost a dostupnost služeb
- Výměna dat

Zařazení do třídy zaručitelnosti bezpečnosti

Zařazení do třídy zaručitelnosti bezpečnosti se děje v závislosti na:
1) způsobu specifikace vlastností (formálně, polo-formálně, neformálně)
2) způsobu prokazování bezpečnostních vlastností (testování jen funkcí, testování funkcí i mechanismů)
3) Dosažení předepsaných vlastnosti pro danou třídu zaručitelnosti bezpečnosti

Jednotlivé třídy zaručitelnosti bezpečnosti

E0 (požadavky ITSEC nesplněny)
- nedostatečná zaručitelnost bezpečnosti, hodnocení nelze provést

E1 (požadavek na neformální zadání bezpečnosti a popis návrhu a důkazní testy)
- musí být dodán bezpečnostní cíl a neformální popis hodnoceného předmětu a testování bezpečnostních funkcí musí indikovat, že hodnocený předmět splňuje bezpečnostní cíl

E2 (požadavek na neformální popis detailního návrhu, nezávislé testy)
- navíc proti E1 se požaduje dostupnost neformálního popisu detailního návrhu hodnoceného předmětu a hodnotiteli se musí dodat důkazy testování; musí se provádět správa konfigurace a musí být zaveden proces dodávky hodnoceného předmětu

E3 (jako třída E2 + hodnocení zdrojového kódu (SW) nebo obvodových schémat (HW))
- navíc proti E2 se požaduje dostupnost detailního návrhu a zdrojové texty programů bezpečnostních funkcí

E4 - bezpečnostní politika hodnoceného předmětu musí být vyjádřena formálním modelem, požaduje se semi-formální popis architektury a detailního návrhu hodnoceného předmětu a provedení analýzy zranitelnosti na této úrovni

E5 (požadavek na specifikaci návaznosti detailního návrhu a zdrojových kódů a schémat)
- musí se prokázat úzká souvislost mezi detailním návrhem a implementací na úrovni zdrojových textů programů a provedení analýzy zranitelnosti na této úrovni

E6 (jako třída E5 a dále formální popis návrhu a doložení jeho konzistence s matematickým modelem)
- požaduje se formální popis bezpečnostní architektury hodnoceného předmětu konzistentní s formálním modelem bezpečnostní politiky; musí být jednoznačně prokazatelná souvislost výkonných (binárních) programů s jejich zdrojovými formami.

<table>
<tr><th colspan="2"></th><th>E0</th><th>E1</th><th>E2</th><th>E3</th><th>E4</th><th>E5</th><th>E6</th></tr>
<tr><td rowspan="3">Vývojový proces</td><td colspan="2">Stanovení požadavků
návrh architektury</td><td colspan="2">Neformální</td><td colspan="3">Semi-formální</td><td>Formální</td></tr>
<tr><td colspan="2">Detailní návrh</td><td colspan="2">Neformální</td><td colspan="3">Semi-formální</td><td>formální</td></tr>
<tr><td colspan="2">Důkaz implementace</td><td>xxx</td><td>Bezp. fce</td><td colspan="2">+ mechanismů</td><td colspan="2">+ návaznost na návrh</td></tr>
<tr><td rowspan="3">Vývojové prostředí</td><td colspan="2">Programovací jazyky</td><td>xxx</td><td>xxx</td><td>normované</td><td>definované volby kompilátorů</td><td colspan="2">+ hodnocení knihoven</td></tr>
<tr><td colspan="2">Bezpečnostní politika</td><td>xxx</td><td colspan="6">Definovaná a hodnotitelná</td></tr>
<tr><td colspan="2">Správa konfigurace</td><td>identifikace</td><td>Systém správy</td><td colspan="5">Vývojové prostředí (stupňující se nároky)</td></tr>
<tr><td rowspan="2">Provozní prostředí</td><td colspan="2">Dodávka, konfigurace</td><td>Generační postupy</td><td colspan="4">Auditovatelný generační postup</td><td>Form. definovaná konfigurace</td></tr>
<tr><td colspan="2">Oživení a provoz</td><td>Postupy pro oživení</td><td colspan="3">diagnostika</td><td colspan="3">Postupy důvěryhodné obnovy</td></tr>
</table>

ITSEC: http://www.cesg.gov.uk/publications/com-crit-itsec.shtml
ITSEC (June 1991). *Information Technology Security Evaluation Criteria (ITSEC): Preliminary Harmonised Criteria*.

III. Canadian Trusted Computer Product Evaluation Criteria (CTPEC)

Kanadská kritéria pro hodnocení bezpečnosti informačních systémů CTCPEC (Canadian Trusted Computer Product Evaluation Criteria) se pokusila vytvořit prakticky použitelnější kategorizaci bezpečnostních funkcí. Bezpečnostní funkce jsou v CTCPEC nazývány bezpečnostními službami. Tyto bezpečnostní služby jsou rozděleny do čtyř kategorií, na bezpečnostní funkce zajišťující **důvěrnost, integritu, dostupnost a účtovatelnost (odpovědnost)**. V rámci každé bezpečnostní služby je definováno několik úrovní. Úroveň bezpečnostní služby je definovaný a měřitelný požadavek na granularitu nebo sílu bezpečnostní funkce vzhledem k určité množině hrozeb. Bezpečnostní služby s vyšší úrovní poskytují účinnější ochranu proti hrozbám. To však neznamená, že následující úroveň musí nutně zahrnovat vše, co bylo požadováno v předcházejících úrovních. Úrovně jsou vzestupně číslovány číselně počínaje od nuly, která představuje nejnižší úroveň ochrany. Například bezpečnostní funkce identifikace a autentizace, která má zkratku WA, obsahuje úrovně WA-0, WA-1, WA-2 a WA-3.

Bezpečnostní služby zajišťující důvěrnost (4 funkce)
Bezpečnostní služby v této kategorii jsou určeny proti hrozbám, které mohou zapříčinit odhalení informace neoprávněným subjektům (neoprávněné prozrazení informace). Jedná se o následující bezpečnostní služby:

- *Skryté kanály* (obsahuje čtyři úrovně CC-0 až CC-3)
- *Nepovinné řízení důvěrnosti* (CD-0 až CD-4)
- *Povinné řízení důvěrnosti* (CM-0 až CM-4)
- *Opětné použití objektů* (CR-0 až CR-1)

Bezpečnostní služby zajišťující integritu – konsistenci dat a systému (7 funkcí)
Bezpečnostní služby zajišťující dostupnost/dosažitelnost (4 funkce)
Bezpečnostní služby zajišťující účtovatelnost (3 funkce)

Záruky jsou dány kvalitou návrhu, vývojovým prostředím, provozním prostředím, dokumentací a rozsahem testování - úrovně záruk jsou označeny vzestupně T-1 až T-6

Terminologie
- prvky systému jsou „předměty“
- předmět zahrnuje „uživatele“, „procesy“ a „objekty“
- spojení uživatele a procesu vytváří „subjekt“
„funkční profily“ - registrovaná seskupení bezpečnostních služeb pro určitý účel - buď pro určenou třídu bezpečnosti (C2 - B3) nebo pro uzavřené produkty (např. čipové karty).

V současné době se již standard prakticky nepoužívá. Zpravidla byl nahrazen standardem CC (Common Criteria) .

http://www.javvin.com/networksecurity/CTCPEC.html

III. Federal Criteria (FC)

Práce na tomto standardu probíhaly začátkem devadesátých let (1992). Připravoval je National Institute of Standards and Technology (NIST) a byly iniciovány National Security Agency (NSA).

Standard je rozdělen na dva oddíly:

První oddíl – vlastní kritéria, obsahuje:
Požadavky na funkční složky - členěno podle bezpečnostních funkcí
Požadavky na vývoj systému - vývojový proces, provozní podpora, vývojové prostředí a dokumentace
Požadavky na hodnotitelské záruky - testování systému, hodnotitelské posudky, hodnotitelské analýzy

Druhý oddíl - bezpečnostní profily (BP)
obsahuje vysvětlení vlastností a rysů připravených profilů bezpečnosti

Seskupení požadavků ve FC
Míra záruk se označuje vzestupně od T1 až do T7.
Profil bezpečnosti (formální komplexní vyjádření obecných bezpečnostních vlastností – účel, podmínky použití, stanovení požadavků na bezpečnostní funkce, vývojové a hodnotitelské záruky.)
Dále jsou zde stanoveny tyto základní profily:
Profily pro komerční použití (odpovídají třídě C2 podle TCSEC)
Profily pro systémy víceúrovňové bezpečnosti (odpovídají třídám B3, B2 a B1 podle TCSEC)

ftp://ftp.su.se/pub/security/csir/nist/nistgen/fcscope.txt

V. Srovnání kritérií a jejich přínosy

TCSEC

- nízká přizpůsobivost novým podmínkám
- míra bezpečnosti je vyjádřena pouze jednou hodnotou
- dosud se používá např. pro hodnocení bezpečnosti OS

ITSEC

- výsledek hodnocení ve více rozměrech (funkčnost, míra záruk)

CTPEC

- nezávislé vyjádření kvality jednotlivých bezpečnostních služeb
- velká schopnost přizpůsobení se novým podmínkám

FC

- bezpečnostní profil
- komplexní seskupení
- předkládá ucelený pohled na bezpečnost, jehož součástí je upřesnění podmínek pro použití

Mapování hodnocení mezi jednotlivými standardy:

TCSEC	ITSEC		CTCPEC	FC	CC/ISO15408
-	E0		-	-	-
D minimální ochrana	-		-	-	EAL 1 funkčně testovaný HP
C1 výběrový přístup	E1	F-C1	-	-	EAL 2 strukturálně testovaný HP
C2 řízený přístup	E2	F-C2	T-1	T1	EAL 3 metodicky testovaný a kontrolovaný HP
B1 ochrana návěštím	E3	F-B1	T-2	T2	EAL 4 metodicky navržený, testovaný a přezkoumaný HP
-	-	-	T-3	T3	-
-	-	-	-	T4	-
B2 strukturální ochrana	E4	F-B2	T-4	T5	EAL 5 semiformálně navržený a testovaný HP
B3 bezpečnostní domény	E5	F-B3	T-5	T6	EAL 6 semiformálně navržený se semiformálně ověřeným návrhem a testovaný HP
A1 verifikovaný návrh	E6	-	T-6	T7	EAL 7 formálně navržený s formálně ověřeným návrhem a testovaný HP

C. Chcete si zaluštit? Díl 4.

Martin Kolařík (marram.mail@gmail.com)

Březnová dávka luštění

Dnes jsem vybral mystery keše, které mě svým provedením zaujaly, první má i velmi povedené umístění finále, vřele doporučuji.

Základy geocachingu jsme si již vysvětlili, další informace již nejsou potřeba. Zbývá jen vyrazit do terénu a zkusit na vlastní kůži najít nějaký ten poklad. Doplním tedy jen jednu novinku ze světa geocachingu, 7. března 2010 bylo na celém světě již 1 000 000 aktivních keší.

A teď již slíbené **únorové GeoŠifry**:

James Bond - For Your Eyes Only (http://coord.info/GC1C563)

nanomania 4 - Pristaviste (http://coord.info/GC1NNHQ)

Batuv Mrakodrap - Bata Building No. 21 (http://coord.info/GC10NR6)

Přeji úspěšné luštění a šťastný lov.

Martin

D. Aktuální situace v oblasti uznávání zahraničních kvalifikovaných certifikátů

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

(volně sestaveno z informací ***Odboru koncepce a koordinace informačních a komunikačních technologií ve veřejné správě***, které jsou publikovány na webu MV ČR)

1. Úvod

Potřebujete si ověřit, že certifikát, který používá váš partner, byl vydán jako kvalifikovaný certifikát v některém státu EU (např. při ověření elektronické faktury)? Pokud ano, pak právě pro vás mohou být následující informace velmi cenné.
Tyto informace jsou dostupné na stránce Odboru koncepce a koordinace informačních a komunikačních technologií ve veřejné správě MV ČR a zde je pouze výtah podstatných sdělení.

Dne 16. 10. 2009 bylo přijato rozhodnutí Komise 2009/767/ES, kterým se stanovují opatření pro usnadnění užití postupů s využitím elektronických prostředků prostřednictvím „jednotných kontaktních míst" podle směrnice EP a Rady 2006/123/ES o službách na vnitřním trhu, které nabylo účinnosti dne 28. 12. 2009.

Tímto dnem nastala povinnost uznávat kvalifikované certifikáty vydané poskytovateli certifikačních služeb usazenými v jiných státech EU i pro orgány veřejné moci, viz následující oznámení Ministerstva vnitra.

2. Uznávání kvalifikovaných certifikátů vydaných poskytovateli certifikačních služeb usazenými v ostatních členských státech EU

Povinnost uznávat kvalifikované certifikáty vydané poskytovateli certifikačních služeb usazenými v jiných státech EU nastává dne 28. 12. 2009 nejen pro jednotná kontaktní místa, ale i pro jiné orgány veřejné moci, a to z důvodu existence ustanovení čl. 3 odst. 7 směrnice č. 1999/93/ES, zejména jeho poslední věty.

Rozhodnutí Rady 2006/123/ES o službách na vnitřním trhu (dále jen „Rozhodnutí") ukládá členským státům povinnost uvést do provozu nástroj umožňující vzájemné uznávání kvalifikovaných certifikátů, na kterých jsou založeny zaručené elektronické podpisy. Tímto nástrojem budou „důvěryhodné seznamy" (dále jen TSL - Trusted Services Lists) které budou obsahovat údaje o poskytovatelích certifikačních služeb, kteří vydávají kvalifikované certifikáty pro veřejnost v daném státu a kteří jsou zároveň akreditováni, resp. jsou pod dohledem (dozorem) orgánu, který je v daném státu k tomu určen. Každý stát vytvoří vlastní TSL, který bude k dispozici uživatelům ze všech členských států. Pomocí tohoto TSL bude možné ověřit, zda je certifikát kvalifikovaný ve smyslu směrnice.

Rozhodnutí 2009/767/ES lze považovat za akt, kterým Komise Evropských společenství odstranila překážky pro faktickou realizaci vzájemného uznávání kvalifikovaných certifikátů.

V ojedinělých případech orgány veřejné moci (především Rejstřík trestů) využívají identifikátor klienta MPSV k ověření totožnosti fyzické osoby (například žadatel o výpis či

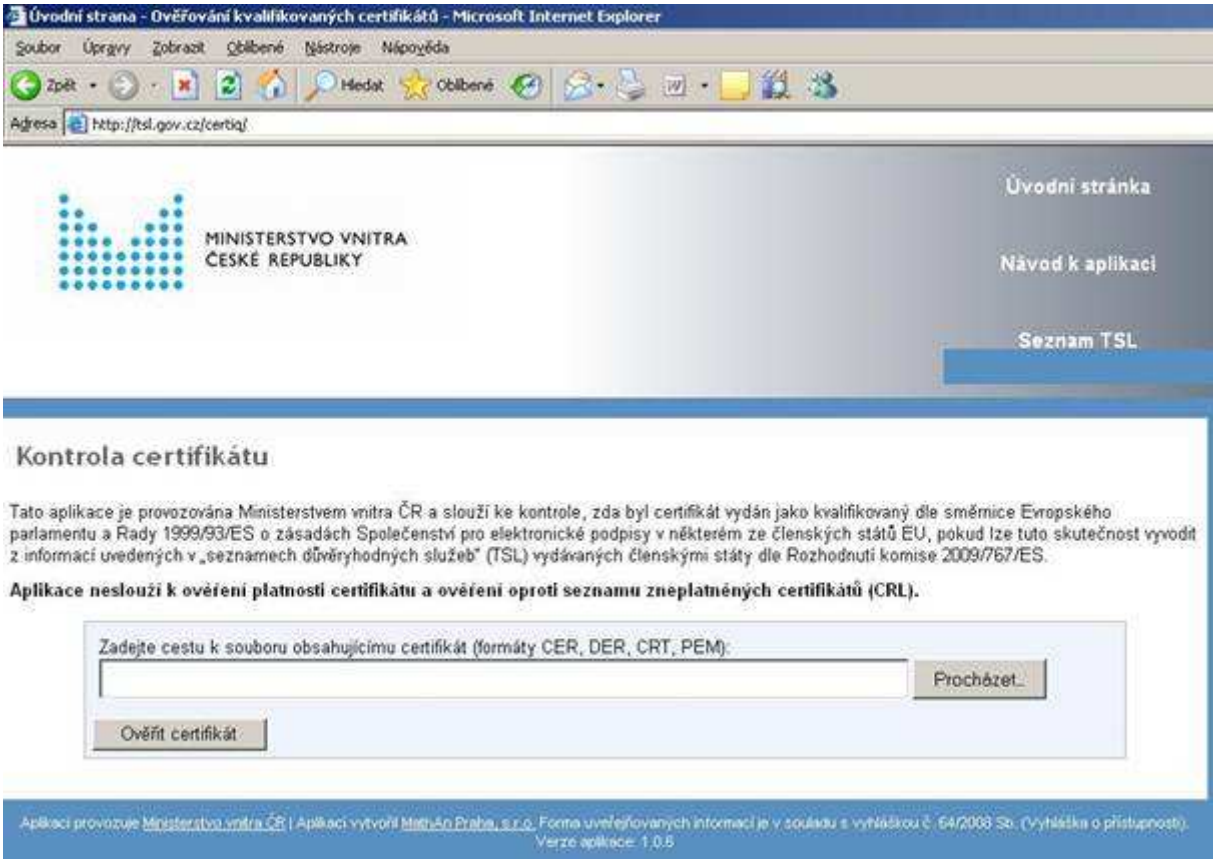
opis z Rejstříku trestů), neboť jim povinnost ověření totožnosti stanoví zvláštní právní předpis. V těchto případech sice musí být kvalifikovaný certifikát vydaný v jiném členském státu akceptován, ovšem žadatel musí prokázat totožnost jiným způsobem.

Za Českou republiku vytváří TSL Ministerstvo vnitra. Zároveň připravuje novelu zákona o elektronickém podpisu tak, aby bylo dosaženo plné kompatibility. Povinnost uvádět identifikátor klienta MPSV v kvalifikovaném certifikátu bude omezena na kvalifikované certifikáty vydané poskytovateli certifikačních služeb vydávajícími kvalifikované certifikáty v České republice. Akceptovány tak budou při komunikaci s orgány veřejné moci rovněž kvalifikované certifikáty vydané v jiných členských státech, pokud bude možné ověřit jejich statut kvalifikovaného certifikátu v TSL.

Tato informace byla publikována ve stavu ke dni 16. 12. 2009.

3. „Čertík“, nástroj umožňující vzájemné uznávání kvalifikovaných certifikátů

Předpokladem funkčnosti je, že stát, ve kterém byl certifikát vydán, zveřejní TSL. Seznam adres všech publikovaných TSL členských států by měl být zveřejněn Evropskou komisí v „seznamu TSL“ (LOTL - List of the Lists). Ten je dostupný v lidsky čitelné podobě (human readable form) na adrese https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-hr.pdf a ve strojově zpracovatelné formě (machine processable form) na adrese https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml.



Pro usnadnění ověřování certifikátů z jiných členských států nechalo Ministerstvo vnitra připravit webovou aplikaci, která po nahrání souboru s certifikátem vyhodnotí na základě informací publikovaných v TSL jednotlivých členských států, zda byl tento certifikát vydán jako kvalifikovaný. Aplikace je volně dostupná na adrese http://tsl.gov.cz/certiq/.

Vzhledem k velmi krátkému času pro implementaci rozhodnutí však ostatní členské státy nestihly svá TSL publikovat v požadovaném termínu. K naplnění seznamu TSL (LOTL) adresami TSL jednotlivých členských států tedy bude docházet průběžně. Jelikož funkčnost výše zmíněné aplikace je na TSL jednotlivých států závislá, doporučujeme při každém použití aplikace zkontrolovat, se kterými TSL aplikace v daném okamžiku pracuje. Tato informace se nachází pod záložkou Seznam TSL. Pokud bude chybět větší množství TSL nebo pokud bude chybět TSL konkrétního státu, ze kterého ověřovaný certifikát pravděpodobně pochází, je možné se obrátit s žádostí o pomoc při ověření, zda je certifikát kvalifikovaný, na Ministerstvo vnitra a to konkrétně na emailovou adresu okkisvs@mvcr.cz.

Ukázka výstupu z ověření kvalifikovaného certifikátu v aplikaci certiq (Čertík), konkrétně kořenového certifikátu I. CA.
V době tohoto ověření (12. 3. 2010) byl k dispozici seznam TSL těchto států: Česká republika, Estonsko, Lucembursko, Maďarsko, Norsko, Polsko, Portugalsko, Rakousko, Řecko, Slovinsko. Ostatní státy EU dosud nesplnily svoji povinnost a nedodaly příslušný vstupní seznam.

E. O čem jsme psali v březnu 2000 – 2009

Crypto-World 3/2000

A. Nehledá Vás FBI ? (P.Vondruška) 2-3
B. Aktuality z problematiky eliptických křivek v kryptografii (J. Pinkava) 3-4
C. Hrajeme si s mobilním telefonem Nokia (anonym) 5
D. Tiskové prohlášení - Pozměňovací návrhy k zákonu o elektronickém podpisu bude projednávat hospodářský výbor Parlamentu 6
E. Digital Signature Standard (DSS) 7-8
F. Matematické principy informační bezpečnosti 9
G. Letem šifrovým světem 9-10
H. Závěrečné informace 11

Crypto-World 3/2001

A. Typy elektronických podpisů (P.Vondruška) 2 - 9
B. Tiskové prohlášení č.14, Microsoft, 15.2.2001 10
C. Kryptografický modul MicroCzech I. (P. Vondruška) 11-16
D. Názor na článek J.Hrubý, I.Mokoš z 2/2001 (P. Vondruška) 17-18
E. Názor na článek J.Hrubý, I.Mokoš z 2/2001 (J. Pinkava) 19-20
F. Letem šifrovým světem 21-22
G. Závěrečné informace 23

Crypto-World 3/2002

A. Vysvětlení základních pojmů zákona o elektronickém podpisu (D.Bosáková, P.Vondruška) 2-17
B. Digitální certifikáty. IETF-PKIX část 1. (J.Pinkava) 17-20
C. Bezpečnost RSA – význačný posun? (J.Pinkava) 21
D. Terminologie II. (V.Klíma) 22
E. Letem šifrovým světem 23-26
   1. O čem jsme psali v březnu roku 2000 a 2001
   2. Encryption in corporate networks can be 'pried open'
   3. ISO-registr kryptografických algoritmů byl zpřístupněn On-Line!
   4. Velikonoční kryptobesídka , 3. - 4. dubna 2002 v Brno
   5. Uľahčí elektronický podpis podnikanie? Zámery a prvé praktické skúsenosti, 20.2.2002, Bratislava
   6. Seminář GnuPG, 5. 4. 2002 v Praze
   7. DATAKON 2002, 19. - 22. 10. 2002, Brno
F. Závěrečné informace

Crypto-World 3/2003

A. České technické normy a svět, III.část (Národní normalizační proces) (P.Vondruška) 2 – 6
B. Přehled norem v oblasti bezpečnosti informačních technologií (normy vyvíjené ISO/IEC JTC1 SC27 a ISO TC 68) zavedených do soustavy českých norem (P. Wallenfels) 7-10
C. Digitální certifikáty. IETF-PKIX část 10. CVP(J.Pinkava) 11-13
D. Obecnost neznamená nejednoznačnost, aneb ještě malá poznámka k některým nedostatkům zákona o elektronickém podpisu před jeho novelizací (J.Matejka) 14-19
E. Letem šifrovým světem 20-23
F. Závěrečné informace 24
Příloha : crypto_p3.pdf Mezinárodní a zahraniční normalizační instituce 3 strany

Crypto-World 3/2004

A. Nastavení prohlížeče IE pro používání kontroly CRL (P.Vondruška) 2-4
B. Jak jsem pochopil ochranu informace, část 2. (T.Beneš) 5-9
C. Požadavky na politiku poskytovatele, který vydává atributové certifikáty, které lze používat spolu s kvalifikovanými certifikáty (Technical report ETSI 102 158), část 3. (J.Pinkava) 10-12
D. Archivace elektronických dokumentů, část 4. (J.Pinkava) 13-16
E. Letem šifrovým světem (TR,JP,PV) 17-19
F. Závěrečné informace 20

Crypto-World 3/2005

A. Nalézání kolizí MD5 - hračka pro notebook (V.Klíma) 2-7
B. Co se stalo s hašovacími funkcemi?, část 1 (V.Klíma) 8-10
C. Popis šifry PlayFair (P. Vondruška) 11-14
D. První rotorové šifrovací stroje (P. Vondruška) 15-16
E. Recenze knihy: Guide to Elliptic Curve Cryptography 17-18
F. O čem jsme psali v březnu 2000 - 2004 19
G. Závěrečné informace 20

Crypto-World 3/2006

A. Klíče a hesla (doporučení pro začátečníky) (P.Vondruška) 2-6
B. Poznámky k internetovému podvodu zaměřenému na klienty české Citibank (O. Suchý) 7-12
C. NIST (National Institute of Standards and Technology - USA) a kryptografie, část 2. (J.Pinkava) 13-15
D. Elektronické volby v ČR ? (J.Hrubý) 16-20
E. O čem jsme psali v březnu 2000 - 2005 21
F. Závěrečné informace 22

Crypto-World 3/2007

A. O speciální blokové šifře DN a hašovací funkci HDN (T.Rosa) 2-3
B. Rodina speciálních blokových šifer DN a hašovacích funkcí nové generace HDN typu SNMAC (V.Klíma) 4-26
C. Najväčšia tma je pod lampou – STEGANOGRAFIA, část II. (R.Cinkais) 27-33
D. Šifrování v MS Office (P.Tesař) 34
E. O čem jsme psali v březnu 2000 – 2006 35-36
F. Závěrečné informace 37

Crypto-World 3/2008

A. E-zin 3/2008 + Voynichův rukopis (P.Vondruška) 2-3
B. Voynichův rukopis (Wikipedia) 4-7
C. Záhadný Dr. Rafael (J.Hurych) 8-12
D. Z dějin československé kryptografie, část VI., Československé šifrovací stroje z období 1955 – 1960. Šifrovací stroj ŠD – 2 (2. díl) (K.Šklíba) 13-22
E. O čem jsme psali v březnu 2000 - 2007 23-24
F. Závěrečné informace

Crypto-World 3/2009

A. Prvá konferencia SHA-3 kandidátov (M.Hojsík) 2-6
B. Blue Midnight Wish, popis a principy (V. Klíma) 7-21
C. Pozvánka na konferenci SmartCard Forum 2009 22
D. O čem jsme psali v březnu 1999-2008 23-24
E. Závěrečné informace 25

G. 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 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 e-ziny, 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:	Vlastimil Klíma
	Pavel Vondruška
Jazyková úprava:	Jakub Vrána
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS (výběr příspěvků, komentáře a vkládání na web)	Jaroslav Pinkava Vlastimil Klíma Pavel Vondruška Tomáš Rosa
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@gmail.com ,	http://crypto-world.info/pinkava/
Tomáš Rosa	tomas.rosa@rb.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/