A. Do druhéhokola soutěže SHA-3 postoupilo 14 kandidátů, mezi nimi i BMW

Vlastimil Klíma, nezávislý krypotolog, (v.klima@volny.cz)

Podle oficiální zprávy z 24. 7. 2009 NIST vybral do 2. kola soutěže o nový hašovací standard **SHA-3** 14 kandidátů. Překvapením je, že nepostoupil **EDON-R**, nejrychlejší z kandidátů. Zklamáním je jistě i to, že nepostoupil **MD6**, několik let vyvíjený a snad nejvíce teoreticky rozpracovaný algoritmus, za nímž stál největší vývojový akademický tým. NIST také vybral 14 místo 15 kandidátů a udělal to dokonce o měsíc dříve, než slíbil. Algoritmy, které postoupily, uvádíme v přiložené tabulce.

K tomu je velmi vhodné si nejprve přečíst, co NIST k výběru uvedl za komentář. Vybíráme a volně překládáme:

„… Byli jsme potěšeni velkým množstvím kryptoanalýzy, učiněné v prvním kole soutěže, a poněkud ohromeni vynalézavostí některých útoků. Byli jsme také potěšeni a vděčni (i když ne překvapeni) za graciézní a přímý způsob, s nímž několik předkladatelů přijalo špatné zprávy a potvrdilo útoky nebo slabiny svých návrhů.

Do výběru kandidátů druhého kola jsme se snažili zahrnout pouze algoritmy, o nichž si myslíme, že mají šanci být zvoleny jako **SHA-3**. Byli jsme ochotni extrapolovat rychlost u těch kandidátů, kteří měli přehnanou bezpečnostní rezervu, avšak neodpouštěli jsme prolomené algoritmy. Byli jsme více ochotni akceptovat určité slabosti (v originále zneklidňující vlastnosti) hašovací funkce, pokud je návrhář připustil, než když je nepřipustil, i když měly zřejmou nápravu. Byli jsme celkově znepokojeni útoky na kompresní funkce, které předkladatelé nepřipustili.

Krátce po této zprávě zveřejníme prohlášení, v němž u každého algoritmu druhého kola popíšeme to, co se nám na návrhu líbilo i veškeré přetrvávající obavy, které máme. Vyzýváme předkladatele, aby (pokud chtějí) vylepšili své návrhy pomocí drobných změn a odstranili všechny nekonzistence a nedostatky ve specifikaci nebo zdrojovém kódu, a to do 15. 9. 2009…“

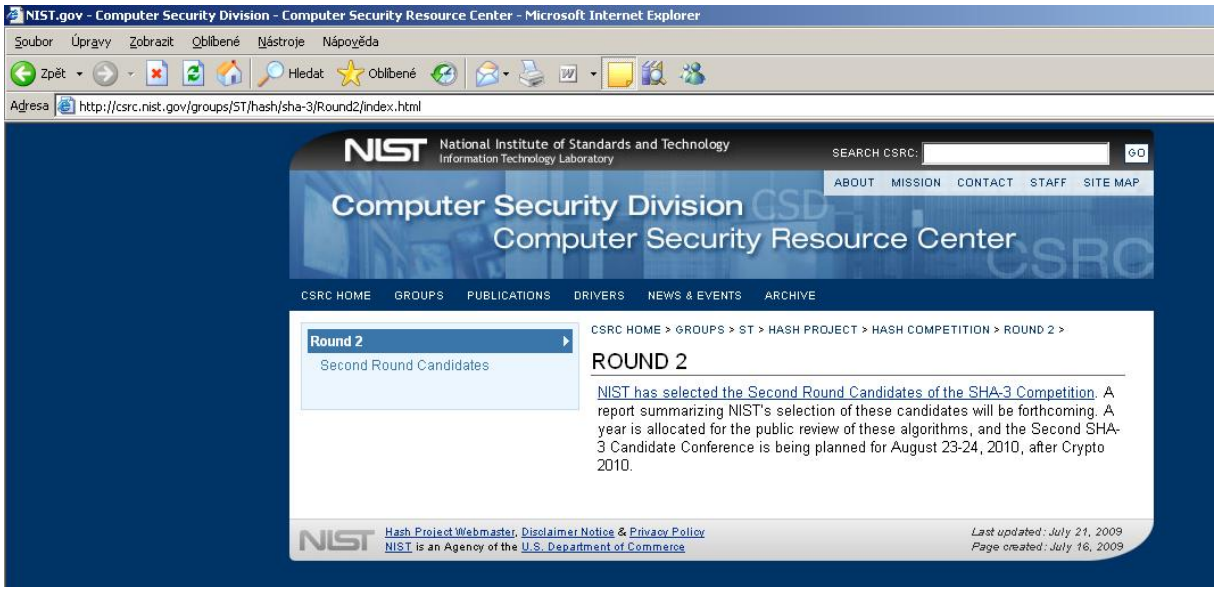
Doplňme, že *tweaks* neboli drobné změny, jsou nyní klíčovým bodem. Pomocí nich mohou předkladatelé mírně změnit své algoritmy tak, že se významně posílí nebo významně urychlí nebo obojí (🙂). Nesmí přitom zásadním způsobem změnit algoritmus! Diskuse i představy NISTu na téma, co jsou drobné změny, proběhla dosti obsáhle, takže všichni tuší, co si mohou dovolit, ale každý se toho bojí. Řada algoritmů bude ubírat na bezpečnosti a zvyšovat rychlost. Například prof. Bernstein zareagoval okamžitě a u svého **CubeHash** zvýšil rychlost o více než jeden řád! Nově se do popředí v rychlosti mohou dostat algoritmy, které nepřivábily tolik pozornosti dříve a nenápadně "postávaly opodál". Drobná změna je může vyhoupnout na špici rychlosti a současní favorité se mohou ztratit v pelotonu. Všechno, co platilo dosud, už neplatí, a bude nově nastoleno až 15.9. Po tomto datu už nelze očekávat, že by se v algoritmech dělaly drobné změny, ale pouze změny "miniaturně kosmetické". Jinými slovy, kostky jsou znovu vrženy, a to, že **Blue Midnight Wish (BMW)** je momentálně nejrychlejší, neznamená do 15. 9. vůbec nic navíc.

Jisté je jen to, že vítěz musí být rychlejší a bezpečnější než SHA-2.

Algoritmus	64bit	32bit	Autorský tým, poznámka
BMW	7/3	7/12	Mezinárodní tým 6 lidí, Gligoroski, Knapskog, El-Hadedy, Amundsen, Mjølsnes (Norw. Univ.), Klima
Shabal	8	10	Francouzský tým 14 lidí (DCSSI, EADS, Fr. Telecom, Gemalto, INRIA, Cryptolog, Sagem)
BLAKE	8/9	9/12	Mezinárodní tým 4 lidí, Aumasson, Henzen, Meier, Phan (Switzerland, UK)
SIMD	11/12	12/13	Francouzský tým 3 lidí, Leurent, Bouillaguet, Fouque
Skein	7/6	21/20	Mezinárodní tým 8 lidí, Schneier, Ferguson, Lucks, Whiting, Bellare, Kohno, Callas, Walker
CubeHash	160/160 13/13	200/200 13/13	Dan Bernstein, (Univ. of Illinois),v 2. řádku rychlost uvažovaného tweaku
SHA-2	20/13	20/40	NIST, stávající standard (nesoutěží, pouze pro srovnání)
JH	16	21	Hongjun Wu, Inst. for Inf. Res., Singapore
Luffa	13/23	13/25	Mezinárodní tým 3 lidí, Canniere (Kath. Univ. Leuven), Sato, Watanabe (Hitachi)
Hamsi	25	36	Özgül Kücük (Kath. Univ. Leuven)
Grøstl	22/30	23/36	Mezinárodní tým 7 lidí, Gauravaram, Mendel, Knudsen, Matusiewicz, Rechberger, Schlaeffer, Thomsen
SHAvite-3	26/38 18/28	35/55 26/35	Izraelský tým (Dunkelman, Biham), s Intel AES instrukcemi 8 cyklů/bajt, Bernsteinova měření viz 2. ř.
Keccak	10/20	31/62	Mezinárodní tým 4 lidí (Bertoni, Daemen, Peeters, Van Assche, STM, NXP)
Echo	28/53	32/61	Mezinárodní tým 7 lidí (Billet, Gilbert, Rat, Peyrin, Robshaw, Seurin), Intel AES instr. ho urychlí
Fugue	28/56	36/72	Americký tým 3 lidí Halevi, Hall, Jutla (IBM)

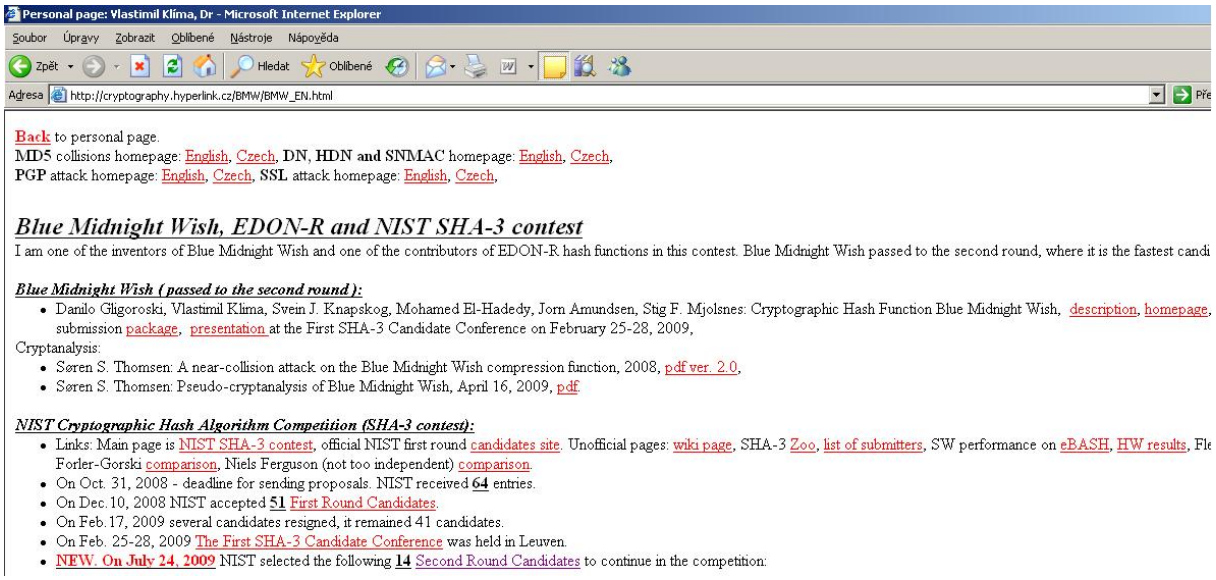
Tabulka: Rychlost kandidátů v cyklech na bajt pro 64/32bitové procesory (1./2. sloupec) a pro 256/512 bitové varianty hašovacích funkcí (v buňce tabulky)

Odkazy



[1] Informace o 2. kole:

http://csrc.nist.gov/groups/ST/hash/sha-3/Round2/index.html



[2] Stránka autora s novinkami o soutěži a algoritmu BMW:

http://cryptography.hyperlink.cz/BMW/BMW_EN.html

[3] V.Klíma: Blue Midnight Wish, kandidát na SHA-3 aneb poněkud privátně o tom, jak jsem k BMW přišel, Crypto-World 2/2009, str. 2-12