

# Soutěž o flexibilnější a rychlejší digitální otisk

Ve světě existují stovky kryptografických norem a nástrojů, které jsou standardizovány. A přesto se neustále vyvíjejí nové. Místo toho, aby toto úsilí skončilo a byla konečně vynalezena rychlá a kvalitní šifra, hašovací funkce, podpisové schéma, atd. tak tisíce výzkumníků máří čas přípravou nových kryptografických technik. Velké elektronické a SW firmy staví své profesionální kryptologické týmy, které jim mohou závidět mnohé státní služby, a vyvíjejí nové a nové věci. Chtít po někom, aby vyvinul konečně už kvalitní šifru, je stejné jako chtít, aby se už konečně vyvinul kvalitní rychlý počítač nebo paměť.

## Kryptografie prorůstá elektronikou

A pro nové mikroprocesory, paměti (právě teď například populární flash disky), ale hlavně komunikace je potřeba nové šifry. Protože ty staré jsou pomalé. Zkrátka je to nekončící proces nejen co do hloubky problému, ale i do šířky. Kryptografie nachází použití stále v nových oblastech. Jeden z autorů se například účastnil zajištění ochrany komunikace domácích elektroměrů s centrem jejich řízení. A tohle tempo se zrychluje – proto jsou staré šifry, haše a podpisy zapomenuty a požadují se nové. Jenže tak jako má elektrotechnika svoje meze, věda také. Kromě toho se zapomnělo na fakt, že dnešní prakticky využitelná kryptografie je postavena na nedokazatelných principech. Existují výjimky, ale jsou drahé a nepraktické. Ostatní „masová“ kryptografie používá nástroje, které mohou být prolomeny. Vezměte prosím v úvahu to, že prakticky všechny dnešní kryptografické nástroje mohou být prolomeny. To, že se to neděje ze dne na den, je zásluha kryptologů, kteří je navrhovali. Že předvídali nepředvídatelné a maximálně tento proces zpomalili a znesnadnili. Nicméně čas od času se stane a může stát, že nějaká technika je doporučena ke stažení. To se například stalo se standardy MD4, MD5, SHA-0, SHA-1 (platí jen do konce příštího roku). Místo nich je k dispozici třída hašovacích funkcí SHA-2, ale už nyní se připravuje nový standard SHA-3.

## Mezinárodní soutěž o standard

Aby mohl obstát v nových zařízeních a komunikacích, jsou na něj kladena nesmyslná kritéria. Musí být bezpečnější než předchozí dosud neprolomené a silné SHA-2, flexibilnější na různých platfor-

mách a rychlejší. Mezi bezpečností a rychlostí je však odvěký rozpor – čím bezpečnější algoritmus, tím je pomalejší. Teď tomu má být naopak. Co se stane? Teoretici

**Tabulka 1 Nejrychlejší kandidáti, jejich rychlost v cyklech CPU na bajt pro 256/512 bitový výstup a požadovaná paměť pro 256/512 bitový výstup**

Algoritmus	CPU 64b	CPU 32b	Paměť [B]
Edon-R	4.30/2.29	6.46/10.0	256/512
Blue Midnight Wish	7.85/4.06	8.63/13.4	264/528
Skein	7.6/6.1	32.8/32.5	100/200
TIB3	7.68/6.24	13/17.7	
SHAMATA	8/11	15/22	
Sarmal	9.4/10.9	19.2/23.3	

kové musí přijít s novými myšlenkami, novou „kryptografickou technologií“, která umožní podobně jako nové technologie u disků a pamětí, aby byly „větší“, ale na menší ploše. Proto byla vypsána celosvětová veřejná soutěž SHA-3, a to s uvedenými požadavky. Je to monstrózní akce, která začala v roce 2006 a skončí 31. 12. 2012, vše je pod veřejnou mezinárodní kontrolou. Detaily naleznete na [1].

## Česká účast na špičce pelotonu

Do soutěže se přihlásilo 64 algoritmů a do prvního kola jich bylo propuštěno 51. Vítěz musí projít několika koly, a než bude vybrán, bude vše kontrolováno, kritizováno a přemýšláno na několika speciálních mezinárodních konferencích. Soutěž prostřednictvím svých kryptologů obslaly firmy jako STMicroelectronics, Microsoft, Sony, IBM, RSA, MIT, PGP, Gemalto, Intel, Hitachi, Hifn a známá jména jako Rivest, Schneier a další. Češi jsou podepsáni pod dvěma kandidáty. Pod algoritmem EDON-R jsou jako dva přispěvatelé uvedeni Vlastimil Klíma a prof. Aleš Drápal z MFF UK, jeho vlastníkem a vynálezcem je Makedonec prof. Danilo Gligoroski, působící nyní na technické univerzitě v Norsku. Norský tým Gligoroského je také přispěvatelem druhého algoritmu s poetickým názvem Blue Midnight Wish (BMW). Jeho vynálezcem a vlastníkem je Vlastimil Klíma společně s Danilem Gligoroskim. Shodou okolností (nebo spíše výsledkem trpělivé práce Gligoroského) jsou oba zmíněné algoritmy v čele rychlostního pelotonu. S určitým odstupem za nimi následuje skupina algoritmů Skein, TIB3, SHAMATA a Sarmal.

## Rychlost

Jak je rychlost důležitá, ukazují měření, provedená pro různé délky zpráv na více než

50 platformách, celkem se jedná o stovky srovnávacích grafů [2]. Proto je také těžké uvádět nějaká čísla. Dalšími faktory jsou délka zprávy, paměť, jazyk, ve kterém je algoritmus napsán a další. Nicméně velmi orientačně lze srovnání vidět z *tabulky 1*, kde je uveden počet cyklů procesoru, který je potřeba na zpracování jednoho bajtu zprávy. Hašovací funkce nabízí navíc 4 velikosti výstupního kódu (224, 256, 384, 512), v *tabulce 1* je v řádku uveden počet cyklů pro 256/512bitový výstup a ve sloupci je 32- a 64bitová architektura CPU a v posledním sloupci požadavky algoritmu na paměť v bajtech.

Některí, včetně BMW a EDON-R, publikovali přihlášené kandidáty dříve. Týmy kryptologů se pak bavily tím, jak rychle vyřadí své konkurenty. Byla to napínavá podívaná a soutěž, kde podražení konkurenta je přímo součástí pravidel hry. Za uplynulých dva měsíce tak bylo „prolomeno“ 17 kandidátů! Některé zcela (například přímo nalezené kolizí), jiné byly jen „škrábnuty“. Neoficiálně, nicméně fakticky, zbylo 34 algoritmů.

Některé týmy nerespektovaly nesmyslné požadavky na současné zvýšení rychlosti i bezpečnosti, a přidržely se klasických postupů. Zákonitě se tak ocitly na konci pelotonu, i když mohou nabídnout solidnější návrh. Pochopitelně nikdo neviděl do karet konkurenci, takže si musel sám vybrat cestu jak překonat uvedený rozpor. Kdo neriskoval a nepřišel s něčím novým, je na konci a musí čekat až se „vystřelí“ všichni před ním. Kdo riskoval, je v čele, ale první na ráně a může být snadněji „sestřelen“. A o tom ta soutěž je.

## Závěr

Vítězem soutěže a novým hašovacím standardem bude silný algoritmus. Slabý nemůže přestát soustředěně několikaleté zkoumání jeho kvalit mezinárodní komunitou kryptologů, které ho čeká do konce roku 2012 (i v letech následujících). Zájemci mohou najít další informace na speciální stránce k soutěži na [3].

Vlastimil Klíma, Tomáš Rosa,  
v.klima@volny.cz, tomas.rosa@rb.cz

## LITERATURA

- [1] <http://csrc.nist.gov/groups/ST/hash/index.html>
- [2] <http://bench.cr.yt.to/results-hash.html>
- [3] [http://cryptography.hyperlink.cz/BMW/BMW\\_CZ.html](http://cryptography.hyperlink.cz/BMW/BMW_CZ.html)
- [4] E-archivy <http://cryptography.hyperlink.cz>, <http://crypto.hyperlink.cz>