

## B. Predikce finalistů SHA-3, Vlastimil Klíma, kryptolog konzultant, Praha (<http://cryptography.hyperlink.cz>, [v.klima@volny.cz](mailto:v.klima@volny.cz))

V tomto kratičkém článku uvedeme poznámku, kterou jsme prezentovali v rámci vystoupení na MKB 2009 nad rámec základní reference o BMW.

Jedná se o to, že definicí tzv. tweaků pro druhé kolo soutěže SHA-3 skončily veškeré kryptograficky významné změny algoritmů. Mezi kandidáty je tak zcela jistě nový standard. Máme proto k dispozici vše, abychom mohli testovat výkonnost potenciálního vítěze v SW i HW a vyjadřovat se k realizaci jeho protivníků v ultraomezených prostředích (třeba bezkontaktní čipy, osmibitové procesory) nebo na ultravýkonných strojích s 64-bitovou architekturou a mnoha jádry.

Na základě následující tabulky si dovoluujeme predikovat, že čtyři z pěti finalistů budou čtyři nejrychlejší algoritmy, které jsou uvedeny v tabulce na počátku. Tato predikce vychází z jednoduchého faktu, že průmysl by nepřijal žádný standard, který by nebyl výrazněji rychlejší než v současné době platné SHA-2. Protože převládající architekturou bude 64-bitová, zvolili jsme měření rychlosti pro 64-bitové procesory a to pro variantu SHA-3 s 512bitovým kódem. Měření na různých strojích, architekturách apod. jsou důležitá a budou předmětem velmi podrobného vážení mezi kandidáty, včetně dalších vlastností (kromě bezpečnosti na prvním místě) jako jsou nároky na paměť kódu nebo paměť na výpočet apod. Výhodou je, že v následující tabulce ta čísla velmi zhruba odpovídají „všeobecnému vzájemnému poměru“ mezi kandidáty. Velmi zhruba znamená, že pořadí se může lišit, ale důležité je, že první čtyři kandidáti jsou prakticky vždy v první čtveřici ve všemožných srovnáních.

64 bitový procesor, 256 bitový hašový kód, rychlost v cyklech/byte			64 bitový procesor, 512 bitový hašový kód, rychlost v cyklech/byte		
1	Blue Midnight Wish	7.55	1	Blue Midnight Wish	3.88
2	Skein	7.6	2	Skein	6.1
3	Shabal	8.03	3	Shabal	8.03
4	BLAKE	8.19	4	BLAKE	9.29
5	Keccak	10	5	CubeHash	11
6	CubeHash	11	6	SIMD	12
7	SIMD	11	7	SHA-512	12.59
8	Luffa	13.4	8	JH	16.8
9	SHA-256	15.34	9	Keccak	20
10	JH	16.8	10	Luffa	23.2
11	Grøstl	22.2	11	Hamsi	25
12	Hamsi	25	12	Grøstl	30.5
13	SHAvite-3	26.7	13	SHAvite-3	38.2
14	Fugue	28	14	ECHO	53.5
15	ECHO	28.5	15	Fugue	56

V tabulce je uvedena rychlost v cyklech na bajt, a to na počítači a v prostředí, které NIST definoval jako testovací. To znamená, že na běžném 2GHz PC máme za vteřinu k dispozici 2 miliardy cyklů, v rámci nichž můžeme například pomocí BMW512 podle tabulky zhašovat cca 4 Mbyte dat za vteřinu.

Do finalistů se může dostat i některý další algoritmus, pokud budou nalezeny závažné slabiny u některého z prvních čtyř algoritmů. Samozřejmě je zde místo i na pátého finalistu, kterého je těžké predikovat. Myslíme si však, že ve skutečnosti bude v pěti pouze do počtu, vítěz může být pouze z první čtveřice, i když si uvědomujeme, že je to trochu troufalá předpověď.

A pokud bychom měli tipovat vítěze, tady nemůžeme hádat a raději vsadíme na nezpochybnitelné tvrzení, že vítěz je vždycky první 😊😐😐😐😐😐😐😐😐😐😐😐😐.