Nový standard digitálního otisku SHA-3

Vlastimil Klíma

Americký úřad pro standardy a technologie NIST oznámil 2. října 2012, že ukončil pětiletou soutěž na federální standard digitálního otisku (hašovací funkce).

Kryptografické hašovací funkce jsou nejzákladnější nástroje informační bezpečnosti, protože zajišťují autentičnost a integritu digitálních dokumentů a souborů a dat, přenášených v nejrůznějších komunikačních protokolech. Proto jsou široce používány v praxi IT/IS. Kryptologové pomocí hašovací funkce realizovali v digitálním světě to, co

```
10001100111010001001001110101001001010110
10100101010110101000101010101011011101011
01010110101010101010101010110010100010000
10011100100101011100101010010101110100101
011101001110011.....0111001110110100
01101001010101001101010101011100110101010
10101101101011110011001100001110110101101O
11110101001010110110010110110100110111001
10011010111010111010101100010110011010011
```

Obr. 1 Digitální otisk

v lidském světě znamená otisk prstu. Vynález hašovacích funkcí přinesl do té doby úžasnou a mnohdy stále ještě nepředstavitelnou věc: každý digitální dokument, soubor, program nebo kousek přenesených dat má svůj digitální otisk, stejně jedinečný a stejně fungující jako otisk prstu u lidí. To umožňuje se přesvědčit o neporušenosti

přenesených dat i o tom (ve spojení s kryptografickými klíči), kdo je jejich původce. Dnes se jako super bezpečné používají 256bitové otisky, ale jsou i 512bitové, ale zcela běžně postačí 128bitové. Pomocí takového řetězce jako vidíte na obrázku, lze binárními číslicemi identifikovat jakýkoli digitální soubor na světě. NIST garantuje, že není možné, aby někdo nalezl dva jakékoliv (krátké nebo dlouhé, smysluplné nebo nesmyslné) soubory, které by měly stejný digitální otisk. NIST dokonce garantuje, že když se změní byť jedno písmeno v knize, tak její nový digitální otisk bude naprosto náhodně odlišný od původního. To je síla kryptografie a její revoluční myšlenka digitálního otisku.

Vítězem výše uvedené mezinárodní soutěže (které se zúčastnili i dva Češi) se stala hašovací funkce KECCAK. Tato hašovací funkce byla navržena týmem kryptografů z Belgie a Itálie, konkrétně těmito výzkumníky:

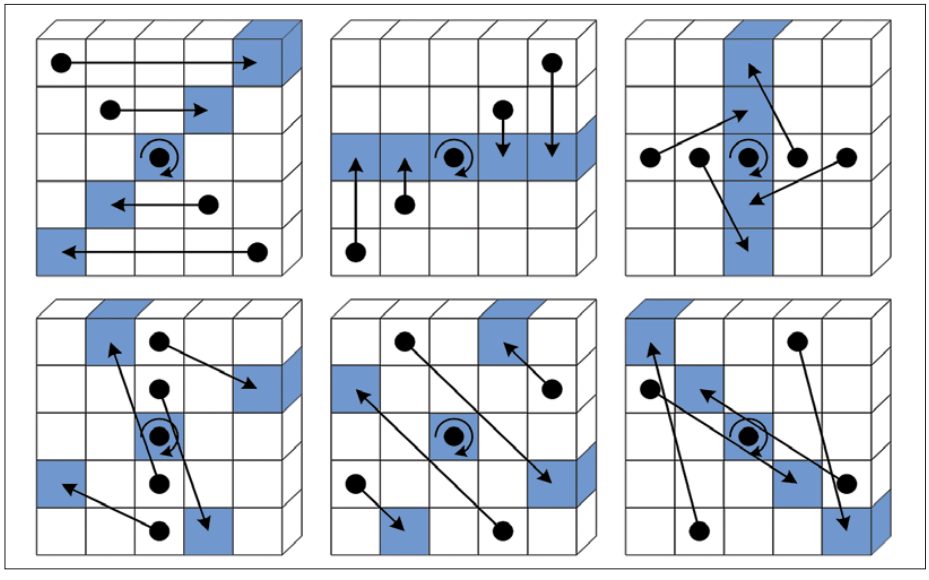
- Guido Bertoni (Itálie) z firmy STMicroelectronics,
- Joan Daemen (Belgie) z firmy STMicroelectronics,
- Michaël Peeters (Belgie) z firmy NXP Semiconductors,
- Gilles Van Assche (Belgie) z firmy STMicroelectronics.

Čtenáři ST by mohli být překvapeni, že firmy, které velmi dobře znají jako čistě hardwarové, zaměstnávají kryptology. Je to tak, nejlepší kryptologové jsou rozebráni do tří oblastí – špičkové technologické firmy, tajné služby a akademický výzkum. Dokonce poprvé v historii tajné služby přímo přihlásily do této veřejné soutěže své kandidáty. Během pěti let se původních 64 návrhů zužovalo v druhém kole na 14, ve třetím na 5 a pak už zbyl jen vítěz. V každém kole se konala jedna mezinárodní konference a bylo odvedeno enormní množství kryptologické práce. Vše veřejně.

NIST vybral KECCAK jak oficiálně praví [1], z důvodu jeho elegantního návrhu, velké bezpečnostní rezervy, přizpůsobivosti, dobrého výkonu obecně a výborného výkonu v hardwaru.

KECCAK používá poměrně mladou „konstrukci houby" s řetězením (viz ST č. 11/2011). Jádrem funkce je pevná permutace, přitom výstup může být zkracován podle potřeby a bezpečnostních požadavků na velikost výstupu. Výhodu je také vedlejší modus funkce KECCAK, který poskytuje autentizované šifrování.

Keccak má jinou konstrukci, než nejpoužívanější hašovací funkce MD5, SHA-1 a platná rodina funkcí SHA-2. S odstupem času je stále zřejmější, že to je jeho největší výhoda, na níž se během pěti let soutěžení pozapomnělo. NIST měl obavy, že by se útoky na funkce MD5 (dokonaný) a na SHA-1 (teoretický, nedokonaný) mohly přelít i do rodiny SHA-2, což byla prapůvodní příčina vyhlášení soutěže. Teď je tedy splněn záměr, aby nový standard byl jakousi pojistkou pro tento krizový scénář. Co se nepovedlo, je rychlost, neboť všeobecná rychlost Keccaku je pouze „dobrá" jak konstatuje NIST. Takže Keccak bude zřejmě nasazován tam, kde bude rychlejší než stávající funkce z rodiny SHA-2, a to v softwaru asi vždy nebude.



Obr. 2 Jádrem Keccaku je funkce f, která připomíná operace na Rubikově kostce

Připomeňme, že NIST se „odklonil“ od vyhlášených platných požadavků soutěže a uprostřed soutěže je změnil, což také veřejně konstatoval. Ustoupil z požadavku, že nový standard musí být podstatně rychlejší, než SHA-2. To NISTu jako jeden ze soutěžících (a spoluautor nejrychlejšího kandidáta v druhém kole) nikdy neodpustím. Trochu se u tohoto bodu zastavíme, protože je obecně zajímavý. Soutěž na hašovací funkci se dá přirovnat k soutěži na tanky. NIST požadoval, aby nový tank byl rychlejší i bezpečnější než stávající. Kdo by se odvážil přihlásit nový tank do soutěže, který nesplňuje tyto podmínky? Kupodivu takových týmů, včetně mocných průmyslových formací a včetně vítěze, bylo více. Důvod je prostý, tyto podmínky byly téměř nesplnitelné. Pouze několik týmů to dokázalo! Jak? Kde ušetřit, když pancíř musí být silnější, ale těžší tank nemůže být rychlejší? Motory (současné procesory) totiž měly všechny tanky dané a stejné! Pár týmů, které splnily zadání, použilo obrazně řečeno nový materiál, takže ochranný plášť mohl být přece jen odolnější a hmotnost se také snížila! Nový tank byl nakonec i rychlejší i bezpečnější! Jenže NIST (snad někde ve skrytu duše úřadu) chtěl použít osvědčený materiál, kterému věřil (což deklarováno nikde nebylo), a tím se zamotal do neřešitelné situace. Proto se vrátil k původnímu smyslu soutěže, tj. navrhnout nějakou alternativu pro případ kdyby byl současný standard SHA-2 prolomen a ustoupil z požadavku podstatně vyšší rychlosti. Je jasné, že kdyby ostatní týmy věděly, co vlastně NIST chce, a že má rád nějaký materiál nebo že bude ve skutečnosti preferovat bezpečnost oproti rychlosti, tak by mohli navrhnout třeba lepší konstrukci než vítěz.

Nicméně důležité je, že NIST nové SHA-3 věří. Také obavy o bezpečnost SHA-2, panující před soutěží, se nenaplnily. Dokonce se ještě nepodařilo prakticky prolomit SHA-1! To je dobrá zpráva pro nás všechny, neboť průmysl IT se bez kvalitní kryptografie neobejde. Přínosem soutěže bezesporu je, že dnes může průmysl IT na poli hašovacích funkcí být v klidu, neboť máme ve skutečnosti dva standardy SHA-2 a SHA-3 a není pravděpodobné, že by se někomu podařilo prolomit jak SHA-2, tak SHA-3. Vývojáři si dnes mohou vybrat ten algoritmus z rodin SHA-2 a SHA-3, který bude pro ně rychlejší, bezpečnější, méně náročný na paměť, výkon, apod. Nemusí přitom pospíchat, protože SHA-2 by mohla být v platnosti ještě cca 10 let a možná i déle.

Vítěz soutěže je vybrán, teď už se jen čeká na publikaci zdůvodnění finálního výběru na [1] a na administrativní vydání nového standardu v příštím roce. Podrobné výkonnostní výsledky Keccaku v SW a HW je možné studovat na [2] a [3]. Zde pro přehlednost uvedeme zjednodušené výsledky. V první tabulce vidíme výsledky na 64bitových procesorech, a to ve spotřebě hašovací funkce v cyklech na bajt. Takže pokud známe taktovací frekvenci daného čipu nebo procesoru, můžeme si snadno vypočítat rychlost hašování v bajtech. Uvádíme spotřebu cyklů na bajt jen pro dlouhé zprávy, pro krátké zprávy je toto číslo zavádějící, protože tato funkce musí v každém případě udělat jakýsi stejně náročný “rozjezd”, nezávisle na tom, jestli má zpráva jeden bajt nebo jeden terabajt. Čas tohoto konstantního “rozjezdu” se u dlouhých zpráv rozpustí, ale u krátkých nikoli. Pro krátké zprávy jsou měření rychlosti např. v [4]. V *tabulce 1* vidíme, že u více než poloviny 64bitových procesorů není Keccak-256 rychlejší než SHA-256 a současně Keccak-512 rychlejší než SHA-512. Pro 32bitové procesory (viz *tabulka 2*) to teprve není žádná sláva, ale na druhé straně to není

Tabulka 1 Průchodnost Keccaku na různých 64bitových procesorech

Procesor	Keccak-256 (c/b)	SHA-256 (c/b)	Keccak-512 (c/b)	SHA-512 (c/b)
AMD Athlon 64 X2	9,94	14.88	12,28	9.93
AMD Phenom 9550	9,90	15.06	12,23	9.92
AMD Phenom II X4 955	9,96	15.04	12,30	11.83
AMD Phenom II X6 1090T	9,89	15.05	12,22	11.51
HP Itanium II	4,78	20.47	5,91	9.30
IBM POWER4	15,94	25.34	19,69	15.37
IBM POWER5	12,88	22.19	15,92	13.52
IBM PowerPC G5 970	14,83	22.28	18,32	13.32
ICT Loongson-2 V0.3	18,83	35.03	23,27	24.27
Intel Core 2 Duo	9,63	15.34	11,90	11.73
Intel Core 2 Duo E4600	9,62	15.55	11,89	10.27
Intel Core 2 Duo E8400	9,65	15.28	11,92	10.22
Intel Core 2 Quad Q9550	9,63	15.26	11,90	10.26
Intel Core i5 750	8,37	14.08	10,33	10.61
Intel Core i5 M 520	8,28	13.90	10,23	10.48
Intel Core i7 920	9,97	16.94	12,32	11.45
Intel Xeon E5420	9,63	15.16	11,90	11.79
Intel Xeon E5530	10,00	16.92	12,35	11.82
Sun UltraSPARC IIIi	28,87	27.71	35,66	20.50
Sun UltraSPARC T1	62,45	75.00	77,14	131.26

Tabulka 2 Průchodnost Keccaku na různých 32bitových procesorech

Procesor	Keccak-256 (c/b)	SHA-256 (c/b)	Keccak-512 (c/b)	SHA-512 (c/b)
AMD Athlon	28,93	19,53	35,74	70,65
Atmel AT91RM9200	87,62	47,37	108,24	122,51
Freescale i.MX515	47,91	22,31	59,18	89,50
Intel Pentium 3	31,13	24,80	38,46	67,47
Intel Pentium 4	37,25	35,88	46,01	37,44
Intel Pentium M	25,77	21,62	31,83	29,96
Luminary Micro LM3S811	78,62	40,64	97,12	172,77
Motorola PowerPC 750CXe	35,67	21,08	44,07	54,38
Motorola PowerPC G4 7410	35,60	21,17	43,97	54,10
Motorola PowerPC G4 7447a	40,07	16,59	49,50	44,99
TI OMAP 2420	74,19	47,11	91,64	117,95
TI AR7 (4KEc)	113,01	84,00	139,60	140,48

Tabulka 3 Průchodnost Keccaku v různých realizacích ASIC

Hlavní autor realizace	Technologie	Syntéza	Plocha [kGE]	Kmitočet [MHz]	Rychlost [Gb/s]
Sugawara	STM 90nm	Gate level	55,9	1030	44
Sugawara	STM 90nm	Gate level	26,5	553	24
Henzen	UMC 90nm	Place and route	50,0	949	40
Henzen	UMC 90nm	Place and route	27,5	149	6
AIST	STM 90nm	Gate level	50,6	781	33
AIST	STM 90nm	Gate level	33,6	541	23
AIST	STM 90nm	Gate level	29,5	355	15
Tillich	UMC 0.18µm	Gate level	56,3	488	20
Tillich	UMC 0.18µm	Place and route	56,7	267	11
Guo	UMC 130nm	Place and route	47,4	377	15
Guo	UMC 130nm	Place and route	34,9	161	7
Tým Keccaku	STM 130nm	Gate level	48,0	526	22
Tým Keccaku	STM 130nm	Gate level	9,3	200	39 Mb/s
Kavun	130nm	Gate level	20,0	0,1	85 kb/s

zase nějak devastující. U HW realizací se porovnání s SHA-256 nebo SHA-512 v tabulce neuvádí, ale NIST tvrdí, že Keccak je tam výhodnější (přesnější číselná vyjádření snad budou v důvodové zprávě). V *tabulce 3* je pak průchodnost Keccaku v různých realizacích ASIC a v *tabulce 4* v různých realizacích FPGA.

Tabulka 4 Průchodnost Keccaku v různých realizacích FPGA

Hlavní autor realizace	Typ	Plocha	Kmitočet [MHz]	Rychlost [Gb/s]
Strömbergson	Cyclone III	2670 reg., 5842 LE	123	7,000
Strömbergson	Cyclone III	242 reg., 1769 LE	85	0,022
Tým Keccaku	Cyclone III	2670 reg., 5770 LE	145	6,100
Tým Keccaku	Cyclone III	242 reg., 1570 LE	183	0,039
Strömbergson	Spartan 3A	2780 reg., 3393 slices	85	4,800
Gai	Spartan III	3339 CLB	83	3,161
Gai	Stratix III	4458 ALUT	296	13,000
Strömbergson	Stratix III	2670 reg., 4550 ALUT	176	10,000
Tým Keccaku	Stratix III	2641 reg., 4684 ALUT	206	8,700
Tým Keccaku	Stratix III	242 reg., 855 ALUT	359	0,070
Strömbergson	Stratix III	242 reg., 1026 ALUT	133	0,035
Gai et al.	Virtex V	1229 CLB	238	10,000
AIST	Virtex V	2666 reg., 1433 slices	205	8,397
Gai et al.	Virtex V	1412 CLB	195	7,840
Strömbergson	Virtex V	2669 reg., 1483 slices	118	6,700
Guo et al.	Virtex V	1556 slices	154	6,570
Baldwin	Virtex V	1117 slices	189	5,895
Tým Keccaku	Virtex V	2640 reg., 1330 slices	122	5,200
Tým Keccaku	Virtex V	244 reg., 448 slices	265	0,005

Technické detaily, kompletní popis, celou dokumentaci, testovací příklady a množství realizací v různých jazycích a spoustu dalších informací naleznete na webu Keccaku [5]. Vše je veřejně dostupné, bez poplatků a často jako freeware nebo s podobnou licencí. Na závěr připomeňme ještě pěknou vlastnost přizpůsobivosti Keccaku. Jeho varianty (mimo standard) lze totiž s úspěchem využít v embedded systémech, také o tom jsou další informace v [5].

LITERATURA

[1] Domácí stránka soutěže. Dostupné z: www.nist.gov/hash-competition.

[2] Výkon v SW. Dostupné z: http://keccak.noekeon.org/sw_performance.html.

[3] Výkon v HW. Dostupné z: http://keccak.noekeon.org/hw_performance.html.

[4] Obsáhlá měření. Dostupné z: http://ehash.iaik.tugraz.at/wiki/SHA-3_Hardware_Implementations a http://bench.cr.yp.to/results-sha3.html.

[5] Domácí stránka Keccaku. Dostupné z: http://keccak.noekeon.org/.