A. Blížící se konference k SHA-3 a rušno mezi kandidáty

Vlastimil Klíma, kryptolog konzultant, KNZ, s.r.o., Praha
(http://cryptography.hyperlink.cz, vlastimil.klima@knzsro.cz)

Přesně před rokem jsme v čísle 7-8/2009 uvedli základní informace o kandidátech na SHA-3, kteří postoupili do druhého kola, v prosinci jsme pak v Crypto-Worldu 12/2009 predikovali, kdo má největší šanci dostat se do finále, tj. mezi pět nejlepších. Připomeneme si publikované údaje, a to tabulkou 1 z prvního článku a tabulkou 2 z druhého článku.

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)

Tab. 1: Původní údaje z Crypto-World 7-8/2009

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

Tab.2: Původní údaje z Crypto-World 12/2009

Na základě toho jsme také predikovali, že první 4 kandidáti z tabulky 2 určitě postoupí do třetího kola.

S blížícím se datem druhé konference o SHA-3, která se bude konat už za týden (23. - 24. 8. 2010) v Santa Barbaře, se začal zvyšovat počet příspěvků k jednotlivým kandidátům. Některé byly zveřejněny, některé z nich mají dosud neznámý obsah a budou prezentovány až na konferenci (program konference viz dále). Také tým BMW i členové týmu přihlásili několik příspěvků. Byli jsme docela zklamáni, že námi považované závažné výsledky nejsou tak závažné pro NIST, aby je zařadil do konference, ale pak jsme (zdá se) trochu pochopili, proč tomu tak je a jak NIST mohl uvažovat. Krátce řečeno se domníváme, že to, co NIST ví nebo co ho už tolik nezajímá, nedává na konferenci, zatímco to, co potřebuje prodiskutovat nebo to, co ho eminentně zajímá, to na konferenci dá. Navíc, aby byli všichni spokojeni, každý ze 14 kandidátů má prostor na krátké vystoupení dle své libosti. Pokud se podíváme na program

konference, jsou to poslední dva bloky. Překvapilo nás také, že příspěvek k BMW, který se týká (drobného) urychlení softwarové realizace, byl přijat, zatímco více teoretický příspěvek o tom, jak je BMW bezpečný, přijat nebyl. Teď omluvte zaslepenost autorů BMW, ale podle nás to může podle předchozí úvahy znamenat, že BMW již bylo víceméně vybráno do dalšího kola. V třetím kole se totiž předpokládá, že všichni kandidáti už budou z hlediska bezpečnosti (prakticky, téměř) bez chyb a bude se mezi nimi rozhodovat z hlediska praktické realizace na různých platformách, prostředích a procesorech. Tomu by nahrávalo i to, že v programu konference je BMW vlastně zastoupeno pouze z hlediska praktické realizace. Omlouváme se za tyto spekulace, ale asi si dovedete představit jaké je napětí je mezi účastníky a co se jim honí v hlavě, když slyší nějaký nový drb.

Nejsilnější útok na BMW

Výjimku v příspěvcích k BMW tvoří jediný teoretický příspěvek, který prezentuje nejsilnější útok na BMW, a který je zahajovacím příspěvkem konference (to může být doopravdy náhoda). Jeho autoři, Guo a Thomsen, ho přihlásili a publikovali s názvem "Distinguishers for the Compression Function of Blue Midnight Wish with Probability 1. Název je dosti hrozivý, takže jsme se připravili na obhajobu, avšak v těchto dnech byl příspěvek změněn, a to jak název (nově "Deterministic Differential Properties of the BMW Compression Function"), tak i obsah. Téměř detektivní zápletka vrcholí, neboť se ukázalo, že původní tvrzení příspěvku neplatí. Autoři volili příliš odvážné tvrzení (a tím zřejmě zmátli i NIST), že nalezli odlišovač kompresní funkce BMW od náhodné funkce. Pravda, i v původním příspěvku to byl odlišovač pouze v jednom bitu z 512, který se notabene ještě vypouštěl v závěrečném krácení výstupu, ale i tak by to byl výsledek s velkým V. Nicméně se ukázalo, že žádný odlišovač (a to ani jednoho bitu) zkonstruovat na bázi jejich pozorování nelze, což by si jistě museli od nás na konferenci vyslechnout. Naštěstí pro ostatní účastníky konference na to přišli sami a změnili jak název, tak obsah příspěvku.

Z dalších "drbů" je jistě zajímavé sledovat, jak se dělají různé nezávislé statistiky a porovnávání výkonnosti a vhodnosti různých kandidátů v SW i HW tak, aby někteří kandidáti vypadali lépe než ostatní. Připisujeme to jednoznačně spíše nadšení pro vlastního kandidáta, které mírně zaslepuje některé autory (stejně jako nás), než zlému úmyslu. Nicméně nezaujatý pozorovatel se musí dobře bavit, jak lze vytvářet různé "nezávislé platformy" a "stejné podmínky" pro všechny kandidáty, kteří jsou naprosto nesourodí.

Výkonnost kandidátů

Chtěli bychom přinést skutečné rychlostní charakteristiky jednotlivých kandidátů na různých platformách (hradlová pole, 8 bitové až 64 bitové procesory, omezená prostředí s malou pamětí apod.), ale to v tuto dobu není možné. Právě těmito otázkami se má zabývat většina příspěvků na konferenci, a uveřejnit objektivní čísla teď ještě nelze. Dozvíme se je bohužel až po konferenci, po vyhodnocení diskuse k jednotlivým objektivním hodnocením a po stanovisku NIST k těmto srovnávacím analýzám.

Fair play a praktičnost

Také jsou snahy uprostřed soutěže poněkud měnit její podmínky, což se ukázalo u diskuse kolem Cubehash. Často může člověk podlehnout argumentům, které vypadají velmi rozumně. Například prof. Bernstein, autor Cubehash, navrhl tzv. „normální a formální“ definici Cubehash, které se pochopitelně dost liší v rychlosti a bezpečnosti:

```
CubeHash16/32-224 for SHA-3-224,
CubeHash16/32-256 for SHA-3-256,
CubeHash16/32-384 for SHA-3-384-normal,
CubeHash16/32-512 for SHA-3-512-normal,
CubeHash16/1-384 for SHA-3-384-formal, and
CubeHash16/1-512 for SHA-3-512-formal.
```

Někteří diskutující v poštovní konferenci, zřízené na začátku soutěže, se přimlouvali za to, aby NIST zmírnil podmínky na bezpečnost, že není potřeba odolnost 2^512 proti útoku nalezením vzoru, ale že postačí 2^384 nebo méně. A že „… není možné kvůli tomu, že některý kandidát to nesplňuje, jej vyřadit ze hry, i když jinak je velmi rychlý a užitečný…“. Že "...NIST by měl vybrat nejvhodnějšího a nejlepšího kandidáta pro praxi, než se ohlížet jen na "fair-play", což konkrétně znamená vyžadovat nesmyslnou odolnost 2^512 oproti prakticky zcela vyhovující 2^384 nebo méně, atd. ..." Copak to nevypadá rozumně? Avšak dotčení ostatní účastníci se bouřili, že to nelze, protože kdyby věděli o mírnějších požadavcích na počátku, mohli by navrhnout zcela jiné kandidáty, než ty, co navrhli. Ono čertovo kopýtko je v tvrzení "vybrat nejvhodnějšího a nejlepšího kandidáta pro praxi". To znamená dát stejné šance všem ho navrhnout a potom teprve vybírat. Pokud se změní pohled hodnocení uprostřed soutěže, už se nejedná o "výběr nejlepšího", protože není z čeho vybírat. „Vybrat nejlepšího“ proto indukuje „fair-play“ podmínku.

Nový generický útok

Crypto-World vyjde ještě před vlastní konferencí, kdy všechny týmy ještě "vaří" svoji strategii jak prezentovat svého kandidáta co nejlépe nebo naopak jak najít chyby na ostatních nebo jak rozporovat jejich srovnávací analýzy. V rámci přípravy na konferenci vznikla i u našeho týmu práce, která možná ještě do soutěže zasáhne (opět omluvte zaslepenost autorů). Jedná se o teoretickou práci ukazující nový generický útok na hašovací funkce, které mají tzv. „narrow-pipe“ konstrukci. V zářijovém čísle Crypto-Worldu bude už jasno. Pokud NIST vezme v úvahu zmiňovanou práci, mohlo by to vyloučit některé favority ze hry (Skein, Blake, Hamsi, SHAvite-3) a tím by se do první pětice dostali i ti kandidáti, kteří dříve neměli šanci. Proto výběr a konečné pořadí finalistů je nyní dosti nejisté a původní predikci to může výrazně ovlivnit. Vzhledem k tomu, že je to čistě teoretický útok, může ho NIST ignorovat, ale může si také říci, že má dost kandidátů, kteří uvedenou slabinu nemají. Poznamenejme, že útok se týká tříd MDx, SHA-1 i SHA-2.

Literatura

- Kandidáti druhého kola SHA-3: http://csrc.nist.gov/groups/ST/hash/sha-3/Round2/index.html
- Druhá konference SHA-3: http://csrc.nist.gov/groups/ST/hash/sha-3/Round2/Aug2010/index.html

Doplněno po uzávěrce (5.8, 19.00 hod.):

- Drtivá kritika srovnávací studie HW výkonnosti kandidátů SHA-3 http://crypto-world.info/news/index.php?prispevek=12775&sekce=c

The Second SHA-3 Candidate Conference

August 23-24, 2010

University of California, Santa Barbara [Corwin Pavilion] ***First Day*** ***Monday, August 23, 2010***	
9:00 – 9:10 (10 minutes)	**Opening Remarks** William Burr, *Manager, Security Technology Group, Computer Security Division, National Institute of Standards and Technology*
9:10 – 10:30 (80 minutes)	**Session I: Security Analysis (Part A)** (15 minutes each) **Session Chair:** Lily Chen, NIST 1. **Deterministic Differential Properties of the BMW Compression Function** 2. *Presented by:* Søren S. Thomsen, *Technical University of Denmark* 3. **Distinguisher for Full Final Round of Fugue-256** 4. *Presented by:* Jean-Philippe Aumasson, Nagravision SA 5. **New Non-Ideal Properties of AES-Based Permutations Applications to ECHO and Grøstl** 6. *Presented by:* Yu Sasaki, NTT Corporation 7. **Subspace Distinguisher for 58 Rounds of the ECHO-256 Hash Function** 8. *Presented by:* Martin Schlaeffer, IAIK, TU Graz 9. **Rotational Rebound Attacks on Reduced Skein** 10. *Presented by:* Christian Rechberger, KU Leuven and IBBT
10:30 – 10:55 (25 minutes)	**Coffee Break**

10:55 – 12:15 (80 minutes)	**Session II: Security Analysis (Part B)** (15 minutes each) **Session Chair:** John Kelsey, NIST 1. **Cryptanalysis of the Compression Function of SIMD** 2. *Presented by:* Hongbo Yu, Institute for Advanced Study, Tsinghua University Beijing 3. **Message Recovery and Pseudo-Preimage Attacks on the Compression Function of Hamsi-256** 4. *Presented by:* Cagdas Calik, Institute of Applied Mathematics, Middle East Technical University 5. **Symmetric States and their Structure – Improved Analysis of CubeHash** 6. *Presented by:* Kerry McKay, George Washington University 7. **Building power analysis resistant implementations of Keccak** 8. *Presented by:* Guido Bertoni, STMicroelectronics 9. **Duplexing the sponge – authenticated encryption and other applications** 10. *Presented by:* Joan Daemen, STMicroelectronics
12:15 – 13: 45 (90 minutes)	**Lunch** ***De La Guerra Dining Commons***

13:45 – 15:05 (80 minutes)	**Session III: Hardware Implementations – Surveys** (15 minutes each) **Session Chair:** Lawrence Bassham, NIST 1. **Uniform Evaluation of Hardware Implementations of the Round-Two SHA-3 Candidates** 2. *Presented by:* Stefan Tillich, University of Bristol 3. **Fair and Comprehensive Performance Evaluation of 14 Second Round SHA-3 ASIC Implementations** 4. *Presented by:* Patrick Schaumont, Virginia Tech 5. **FPGA Implementations of the Round Two SHA-3 Candidates** 6. *Presented by:* Brian Baldwin, Claude Shannon Institute for Discrete Mathematics, Coding and Cryptography 7. **How Can We Conduct Fair and Consistent Hardware Evaluation for SHA-3 Candidate** 8. *Presented by:* Shin'ichiro Matsuo, National Institute of Information and Communications Technology 9. **Comprehensive Comparison of Hardware Performance of Fourteen Round 2 SHA-3 Candidates with 512-bit Outputs Using Field Programmable Gate Arrays** 10. *Presented by:* Kris Gaj, George Mason University 11. **ATHENa – Automated Tool for Hardware EvaluatioN – Toward Fair and Comprehensive Benchmarking of Cryptographic Algorithms using FPGAs** 12. *Presented by:* Kris Gaj, George Mason University
15:05 – 15:30 (25 minutes)	**Coffee Break**

15:30 – 16:35 (65 minutes)	**Session IV: Hardware Implementations – Selected Algorithms** (12 minutes each) **Session Chair:** Andrew Regenscheid, NIST 1. **Sharing Resources Between AES and the SHA-3 Second Round Candidates Fugue and Grøstl** 2. *Presented by:* Kimmo Järvinen, Aalto University, School of Science and Technology 3. **Efficient Hardware Implementations of High Throughput SHA-3 Candidates Keccak, Luffa and Blue Midnight Wish for Single- and Multi-Message Hashing** 4. *Presented by:* Erkay Savas, Sabanci University 5. **Resource-Efficient Implementation of Blue Midnight Wish-256 Hash Function on Xilinx FPGA Platform** 6. *Presented by:* Mohamed Hadedy, Norwegian University of Science and Technology 7. **Unfolding Method for Shabal on Virtex-5 FPGAs – Concrete Results** 8. *Presented by:* Julien Francq, EADS Defence & Security, France 9. **A Skein-512 Hardware Implementation** 10. *Presented by:* Jesse Walker, Intel Corporation
16:35 – 16:40 (5 minutes)	**Short Break**
16:40 – 17:30 (50 minutes)	**Session V: Open Discussion – SHA-3 Competition Strategies and Timeline** **Session Chair:** William Burr**,** *Manager, Security Technology Group, Computer Security Division, National Institute of Standards and Technology*
17:30	**Adjourn for Day**

19:00 – 21:00 (2 hours)	**Reception** ***The Faculty Club***

Second Day ***Tuesday, August 24, 2010***	
9:00 – 9:50 (50 minutes)	**Session VI: Software Implementations – Surveys** (15 minutes each) **Session Chair:** Rene Peralta, NIST 1. **Comparative Performance Review of the SHA-3 Second-Round Candidates** 2. *Presented by:* Thomas Pornin, Cryptolog International 3. **Software speed of SHA-3 candidates** 4. *Presented by:* Daniel J. Bernstein, University of Illinois at Chicago 5. **Benchmarking SHA-3 Candidates on Embedded Platforms** 6. *Presented by:* Christian Wenzel-Benner, ITK Engineering AG
9:50 – 10:20 (30 minutes)	**Session VII: Software Implementations – Embedded/Lightweight** (15 minutes each) **Session Chair:** Rene Peralta, NIST 1. **Evaluation of SHA-3 Candidates for 8-bit Embedded Processors** 2. *Presented by:* Stefan Heyse, Ruhr-University Bochum 3. **Serialized Keccak Architecture for Lightweight Applications** 4. *Presented by:* Tolga Yalcin, Department of Cryptography, Institute of Applied Mathematics, Middle East Technical University
10:20 – 10:45 (25 minutes)	**Coffee Break**
10:45 – 11:10 (25 minutes)	**Session VIII: Software Implementations – Selected Algorithms** (12 minutes each) **Session Chair:** John Kelsey, NIST 1. **Optimizing Blue Midnight Wish for size** 2. *Presented by:* Daniel Otte 3. **An Efficient Software Implementation of Fugue** 4. *Presented by:* Cagdas Calik, Institute of Applied Mathematics, Middle East Technical University

11:10 – 12:15 (65 minutes)	**Session IX: Security Analysis (Part C)** (15 minutes each) **Session Chair:** John Kelsey, NIST 1. **Practical Near-Collisions for Reduced Round Blake, Fugue, Hamsi and JH** 2. *Presented by:* Meltem Turan, NIST 3. **A SAT-based preimage analysis of reduced KECCAK hash functions** 4. *Presented by:* Pawel Morawiecki, University of Commerce, Poland 5. **Pseudo-Linear Approximations for ARX Ciphers With Application to Threefish** 6. *Presented by:* Kerry McKay, George Washington University 7. **Security Reductions of the SHA-3 Candidates; On the Indifferentiability of the Grøstl Hash Function** 8. *Presented by:* Bart Mennink, KULeuven, Belgium
12:15 – 13: 45 (90 minutes)	**Lunch** ***De La Guerra Dining Commons***

13:45 – 15:15 (90 minutes)	**Session X: Round 2 Candidates Update (Part A)** (12 minutes each) **Session Chair:** Ray Perlner, NIST 1. **Blake** 2. *Presented by:* Jean-Philippe Aumasson, Nagravision SA 3. **BMW** 4. *Presented by:* Svein Johan Knapskog, Norwegian University of Science and Technology 5. **CubeHash** 6. *Presented by:* D.J. Bernstein, University of Illinois at Chicago 7. **ECHO** 8. *Presented by:* Thomas Peyrin, Ingenico 9. **Fugue** 10. *Presented by:* Charanjit S. Jutla, IBM Watson Research Center 11. **Groestl** 12. *Presented by:* Christian Rechberger, KU Leuven and IBBT 13. **Hamsi** 14. *Presented by:* Ozgul Kucuk, KULeuven, Belgium
15:15 – 15:40 (25 minutes)	**Coffee Break**

15:40 – 17:10 (90 minutes)	**Session XI: Round 2 Candidates Update (Part B)** (12 minutes each) **Session Chair:** Lily Chen, NIST 1. **JH** 2. *Presented by:* Honjun Wu, Institute for Infocomm Research 3. **Keccak Update and (Optional) Presentation** 4. On the security of the keyed sponge construction 5. *Presented by:* Gilles Van Assche, STMicroelectronics 6. **Luffa** 7. *Presented by:* Dai Watanabe, Hitachi, Ltd. 8. **Shabal Update and (Optional) Presentation** 9. Internal Distinguishers in Indifferentiable Hashing - The Shabal Case 10. *Presented by:* Anne Canteaut, *INRIA Paris-Rocquencourt* 11. **Shavite-3** 12. *Presented by:* Orr Dunkelman, ENS 13. **SIMD Update and (Optional) Presentation** 14. Security Analysis of SIMD 15. *Presented by:* Charles Bouillaguet, ENS 16. **Skein** 17. *Presented by:* Jon Callas, PGP Corporation
17:10 – 17:30 (20 minutes)	**Closing Remarks** William Burr, *Manager, Security Technology Group, Computer Security Division, National Institute of Standards and Technology*
17:30	**Adjourn**