Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 12, číslo 7-8/2010 **4.srpen 2010**

7-8/2010

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1362 registrovaných odběratelů)

Obsah: str.

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**

B. Generické kolizní útoky na úzké hašovací funkce rychlejší než narozeninový paradox, aplikovatelné na třídy funkcí MDx, SHA-1, SHA-2 a úzké kandidáty na SHA-3

Vlastimil Klíma, nezávislý kryptolog – konzultant a KNZ, s.r.o., Praha (http://cryptography.hyperlink.cz, vlastimil.klima@knzsro.cz)
Prof. Danilo Gligoroski, Norwegian University of Science and Technology, Norway (danilog@item.ntnu.no, http://www.item.ntnu.no/people/personalpages/fac/danilog/start)

Abstrakt
V tomto příspěvku ukazujeme na důsledek toho, že úzké hašovací funkce (narrow-pipe) se odlišují od ideálních náhodných funkcí. Odlišnosti od náhodných funkcí využíváme k návrhu metody pro nalezení kolizí, která vyžaduje mnohem nižší počet volání hašovacích funkcí, než narozeninový paradox. Tento výsledek platí pro všechny úzké hašovací funkce, včetně klasického Merkle-Damgardova schématu (a tedy i SHA-2) a je také použitelný na úzké kandidáty SHA-3 (BLAKE, Skein, SHAvite-3, Hamsi). Jedná se o generický útok, neboť nezávisí na konkrétní instanci kompresní funkce. Je to další z řady „ne ideálně-náhodných vlastností“, které úzké hašovací funkce vykazují ([1], [2]).

Úvod
Merkle-Damgardova (M-D) konstrukce byla navržena v roce 1989 ([3], [4]) a je nejpoužívanější konstrukcí hašovacích funkcí. Zajímavé je, že dokonce i před jejím formálním návrhem byly známy poznatky (v Merklově disertační práci z roku 1979 [5]), které říkají, že když má útočník k dispozici 2^k různých cílových haší, může nalézt (druhé) vzory těchto haší po provedení cca 2^{n-k} volání hašovací funkce, namísto očekávaných 2^n volání. Za první generický útok proti M-D konstrukci lze považovat známý *útok prodloužením zprávy*. Poté Joux v roce 2004 publikoval další generický útok [6]. Ukázal, že útočník může nalézt *multikolize* mnohem rychleji, než by bylo očekáváno: *r* zpráv se stejnou haší může být nalezeno po $\ln_2 r \times 2^{n/2}$ voláních hašovací funkce namísto očekávaných $2^{n(r-1)/r}$ volání. Krátce poté, v roce 2005, Kelsey a Schneier rozšířili tyto myšlenky v [7], a to k nalezení *druhých vzorů* zpráv (obsahujících 2^k bloků) se složitostí $k \times 2^{n/2+1} + 2^{n-k+1}$, což je také méně než generická hranice 2^n . V tomto příspěvku ukazujeme další generický útok na M-D konstrukci a na úzkou kompresní (hašovací) funkci. Náš *kolizní* útok, redukuje počet volání hašovací funkce z očekávané generické hranice $2^{n/2}$ na $2^{n/2-k/2}$ volání, přičemž kolidující zprávy mají délku 2^k bloků.

Označení
Definujme úzké a široké kompresní (hašovací) funkce. Označme

- *C(h, m)* – kompresní funkci *C* s průběžnou hašovací hodnotou *h* a hodnotou bloku zprávy *m*.
- *hlen* – délku průběžné hašovací hodnoty, tj. také délku výstupu kompresní funkce
- *mlen* – délku bloku zprávy
- *hashlen* – délku výstupu hašovací funkce
- Jestliže kompresní funkce má vlastnost, že pro každou hodnotu *m* je funkce $C(h, m) \equiv C_m(h)$ ideální náhodnou funkcí, pak tuto vlastnost označujeme jako *IRF (h)*.
- Jestliže kompresní funkce má vlastnost, že pro každou hodnotu *h* je funkce $C(h, m) \equiv C_h(m)$ ideální náhodnou funkcí, pak tuto vlastnost označujeme jako *IRF (m)*.

- Hašovací (kompresní) funkci označujeme jako úzkou (NPCF – Narrow-pipe compression function), právě když *hashlen = hlen = mlen/2* a kompresní funkce má vlastnosti *IRF(h)* a *IRF(m)*.
- Hašovací (kompresní) funkci označujeme jako širokou (WPCF – Wide-pipe compression function), právě když *hashlen = hlen/2 = mlen/2* a kompresní funkce má vlastnosti *IRF(h)* a *IRF(m)*.

Hlavní výsledek tohoto příspěvku

Věta 1.

Předpokládejme, že hašovací funkce H : {0, 1}∗ →{0, 1}n používá úzkou kompresní funkci $C: \{0,1\}^n \times \{0,1\}^{mlen} \rightarrow \{0,1\}^n$. Potom můžeme nalézt kolizi *(M, M´)* pro hašovací funkci H s použitím mnohem méně než $2^{n/2}$ volání hašovací funkce (počet volání při útoku s využitím narozeninového paradoxu).

Důkaz.

Pro jednoduchost uvažujme *n = hashlen = 256* (obecný případ je zcela analogický). V tomto případě je hašovaná zpráva doplněna a rozdělena na 512-bitové bloky. Uvažujme, že zpráva *M* (například obsah pevného disku nebo paměti RAM) je rozdělena na dvě části, *A* a *B*, tj. *M = A||B*, kde část *A* se skládá právě z jednoho bloku 512 bitů a část *B* se skládá z $N = 2^{35}$ bloků (to je případ běžného 2TByte HDD). Označme h_A hodnotu průběžné haše po zpracování části *A* zprávy *M* a předpokládejme, že část *B* se nikdy nemění , tj. obsahuje konstantní bloky $const_1$, $const_2$, ... $const_N$ (pokud je padding součástí definice, je to také konstantní blok). Výslednou hodnotu haše vypočítáme následující iterativní procedurou:

$$h_1 = C(h_A, const_1)$$
$$h_2 = C(h_1, const_2)$$
$$h_3 = C(h_2, const_3)$$
$$\ldots$$
$$h_N = C(h_{N-1}, const_N)$$
$$H(M) = h_N$$

Jestliže kompresní funkce *C* je *IRF (h)*, pak průběžná hodnota haše ztrácí entropii v každém z N předchozích kroků. Z Důsledku 3 v [2] obdržíme, že entropie výsledné haše h_N je rovna

$$E(hash) = hashlen + 1 - log_2(N),$$

což pro $N = 2^{35}$ dává *E(hash)* = 222. Jestliže vypočítáme hašovací hodnoty pro 2^{111} různých částí A (zatímco B zůstává stejné), obdržíme 2^{111} hašovacích hodnot h_N. Protože entropie výsledných haší je pouze 222 bitů, podle narozeninového paradoxu je 2^{111} hašovacích hodnot dostačující pro nalezení kolize v množině těchto hodnot (s pravděpodobností blízkou 1/2).

Důsledek 1.

Pro hašovací funkce *H()* konstruované podle Věty 1, nalezení dvojice kolidujících zpráv *(M, M´)*, které mají délku $N = 2^k$ bloků, může být uděláno se složitostí $O(2^{n/2-k/2})$ volání hašovací funkce *H()*.

Poznámka 1.
Jestliže počítáme počet volání *kompresní funkce* $C(H_i, M_i)$, pak naším postupem voláme kompresní funkci $2^{111} \times 2^{35} = 2^{145}$ krát, což je více než 2^{128}. Uvedeným postupem tedy nesnížíme *počet operací* pod hranici 2^{128}, avšak je prokázáno, že počet volání hašovací funkce je nižší než by u narozeninového paradoxu mělo být tedy, že úzké hašovací funkce se nechovají tak, jak bychom si přáli.

Poznámka 2.
Tato technika není použitelná u širokých kompresních funkcí, protože redukce entropie začíná od hodnoty $E(hash) = hlen = 2 * hashlen$, tedy dvakrát vyšší! Konkrétně pro 256-bitovou hašovací funkci máme pro náš postup $E(hash) = hashlen + 1 - log_2(N) = 512 + 1 - log_2(N)$. Abychom byli rychlejší než narozeninový paradox, museli bychom docílit $E(hash) < 2^{256}$, což můžeme, ale zprávy, které k tomu využijeme, budou mít délku $N > 2^{256}$ bloků. Jinými slovy, ztráta entropie nastává i u širokých kompresních funkcí, ale je nevyužitelná.

Literatura

[1] D. Gligoroski: "Narrow-pipe SHA-3 candidates differ significantly from ideal random-functions defined over big domains", NIST hash-forum mailing list, 7 May 2010.

[2] D. Gligoroski, V. Klima: "Practical consequences of the abberation of narrow-pipe hash designs form ideal random functions", IACR eprint archive Report 384/2010, http://eprint.iacr.org/2010/384.pdf (2010/08/08) .

[3] R. C. Merkle: "One Way Hash Functions and DES", Proceedings of CRYPTO '89, Santa Barbara, California, USA, Lecture Notes in Computer Science, Vol. 435, Springer, 1990, pp. 428 - 446.

[4] I. Damgard: "A Design Principle for Hash Functions", Proceedings of CRYPTO '89, Santa Barbara, California, USA, Lecture Notes in Computer Science, Vol. 435, Springer, 1990, pp. 416 - 427.

[5] R. C. Merkle: „Secrecy, authentication, and public key systems", Ph.D. thesis, Stanford University, 1979, pp. 12 -13, http://www.merkle.com/papers/Thesis1979.pdf (2010/08/08).

[6] A. Joux: "Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions", Proceedings of CRYPTO'04, Lecture Notes in Computer Science, Vol. 3152, Springer, 2004, pp. 306 - 316.

[7] J. Kelsey, B. Schneier: "Second Preimages on n-Bit Hash Functions for Much Less than 2^n Work", Proceedings of EUROCRYPT'05, Lecture Notes in Computer Science, Vol. 3494, Springer, 2005, pp. 474 - 490.

C. Podzimní *Soutěž v luštění 2010*, úvodní informace

Pavel Vondruška (pavel.vondruska@crypto-world.info)

Vážení čtenáři, **15. 9. 2010** bude zahájena tradiční **podzimní soutěž v luštění jednoduchých šifrových textů o ceny – *Soutěž v luštění 2010***. Pro nově registrované čtenáře uvádím, že obdobné soutěže pořádal náš e-zin již od roku 2000 a doporučuji se s minulými příklady a jejich řešením seznámit (http://crypto-world.info/souteze.php).

V prvních letech (2000-2004) byly úlohy zaměřeny na klasické šifrové systémy. Od roku 2005 jsou úlohy doprovázeny komentáři a nápovědami v NEWS na naší domovské stránce.

V roce 2006 úlohy spojoval vymyšlený doprovodný příběh. Jednalo se o drobné epizody ze života detektiva kapitána Cardy. Příběh vyústil v lov na chameleóna rasy Cryptomelon Pragensis.

V roce 2007 byl použit rozsáhlý doprovodný fiktivní příběh historické osoby matematika Štěpána Schmidta, který se odehrával v době Marie Terezie. Příběh z 18.století byl zkombinován s fikcí, která popisovala jeho údajné působení v Černé komnatě – luštitelském pracovišti na tehdejším císařském dvoře ve Vídni.
http://soutez2007.crypto-world.info/index.php?crypto=pribeh

V roce 2008 soutěž provázel fiktivní příběh z druhé světové války. Odehrával se kolem snahy vyluštit důležitou depeši odvysílanou 15. října 1941. Společně s britským důstojníkem Johnem Wellingtonem jste tak mohli postupně odhalovat záhadu nového neznámého německého šifrovacího zařízení - šifrátoru SZ 40. Simulátor tohoto zařízení je dostupný na stránce našeho e-zinu. http://soutez2008.crypto-world.info/index.php?crypto=pribeh

V loňském roce 2009 se pak doprovodný příběh k soutěži odehrával v Československé republice koncem padesátých let. Jednalo se o příběh se špionážní zápletkou. Hlavní postavou byl kryptolog Václav Prokopec. V soutěži sehrál důležitou úlohu šifrátor ŠD-2. Simulátor je pro zájemce opět k dispozici na stránce e-zinu.
http://soutez2009.crypto-world.info/index.php?crypto=pribeh

Letošní doprovodný příběh k soutěži je inspirován životními osudy známého dobrodruha a svůdníka Giacoma Casanovy (1725-1798). Své pověsti svůdníka se těší pravděpodobně zásluhou svého nejvýznamnějšího autobiografického díla, „Dějiny mého života (Storia della mia vita)“, v němž autor bez skrupulí popisuje svá četná milostná dobrodružství. Dílo sepsal na sklonku svého života na zámku Duchcov v Čechách, kde byl jako knihovník ve službách hraběte Valdštejna.

Postava Giacoma Casanovy se velmi hodí pro náš příběh. Nebyl totiž jen známý svůdce, ale byl také členem lóže Svobodných zednářů, špión a diplomat. S šiframi se ve svém životě tedy skutečně běžně setkával a zabýval. Dokonce je známo, že rozluštil dopis markýzy Jeanne d'Urfé (1705-1775), velmi bohaté a extravagantní šlechtičny, s níž udržoval dlouhý milostný vztah. Dopis byl psán periodickou šifrou (Beaufortova varianta) a markýza byla velmi překvapena jeho uměním. Nemohla pochopit, jak to jen mohl dokázat. Pro ni to bylo něco nadpřirozeného. Heslo si totiž nikdy nikam nepoznamenala a tak jí nebylo jasné, jak to mohl dokázat. Tento příběh, který uvádí i David Kahn ve své knize *The Codebreakes: The Story OF Sekret Writing*, je zajímavý mimo jiné i tím, že šifru Casanova rozluštil skoro o sto let

dříve, než byla obecná metoda řešení periodických šifer publikovaná pruským důstojníkem Friedrichem Wilhelmem Kasiskim (1805–1881). Přišel snad sám na tuto metodu luštění?

Jaké další šifry lze v příběhu očekávat?

V době, v níž se příběh odehrává, byly za zcela bezpečné a nerozluštitelné považovány již zmíněné různé verze periodických šifer, a pak to byly poměrné rozsáhlé a dokonalé nomenklátory, ale také osobní velmi jednoduché nomenklátory. Oblíbené byly stále různé steganografické metody typu Cardanovy či Fleissnerovy mřížky a nejrůznější tajné inkousty. Dochovány jsou záznamy o tom, že špióni této doby používali také tzv. knižní šifru. Kvalita používaných šifer však byla velmi rozličná. I přesto, že v 18. století byla již jednoduchá substituce považována za lehce luštitelnou, stala se v jedné zajímavé variantě šifrou Svobodných zednářů. Ale nebyla používána jen Svobodnými zednáři, např. v roce 1775 vedlo vyluštění zachyceného dopisu napsaného jednoduchou substitucí k odhalení špiona v hlavním stanu George Washingtona.

Přesná pravidla, ceny sponzorů a prvé úlohy soutěže najdete již v příštím čísle našeho e-zinu Crypto-World 9/2010, který by měl vyjít 15. 9. 2010. Všechny informace budou současně dostupné i na našem webu v sekci věnované soutěžím http://crypto-world.info/souteze.php .

Soutěž bude opět určena pouze registrovaným čtenářům našeho e-zinu, do soutěže bude nutné (tak jako v minulých ročnících) se zaregistrovat. Heslo k registraci bude rozesláno čtenářům Crypto-Worldu společně s adresou k jeho stažení.

Soutěžícím již teď přeji pěknou zábavu a úspěšné vyřešení všech úloh!

D. Chcete si zaluštit? Díl 8.

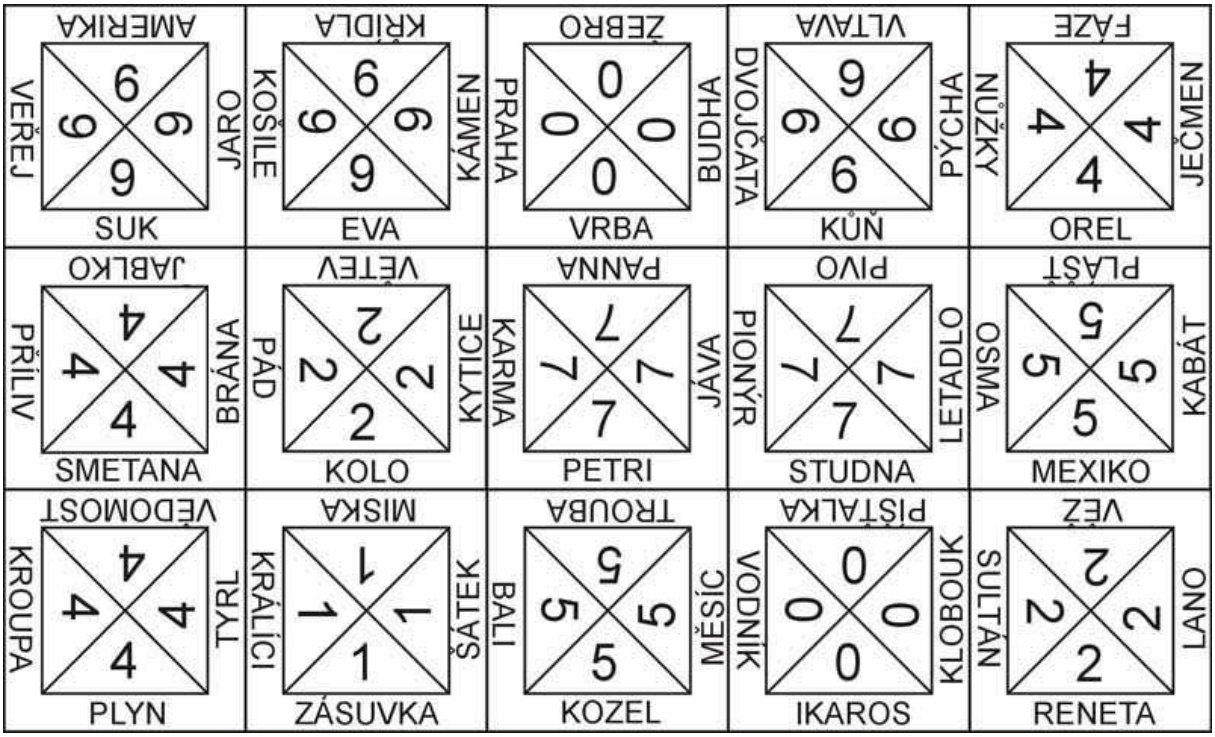
Martin Kolařík (marram.mail@gmail.com)

Letní, závěrečná dávka luštění.

Tímto dílem zakončím sérii pěkných šifer použitých ve světě geocachingu. Cílem bylo nabídnout zajímavé šifry. Smysl geocachingu mi bohužel neumožňoval poskytnout návod jak tyto šifry řešit, protože by pak takové keše ztratily svůj smysl a vy byste přišli o radost z nalezení řešení. Ale i já jsem někdy potřeboval s některou šifrou poradit, takže můj e-mail je vám stále k dispozici. Z posledních tří šifer jsou dvě grafické, obě je dobré vytisknout a pak hledat řešení. Zašifrovaný dub mě hodně potrápil a přitom to jako obvykle nebyla žádná věda.

Uvidíme, zda najdeme způsob jak v této sérii pokračovat a zároveň nabídnout nějaké rady a návody na luštění.

Vetrak v Jalubi (http://coord.info/GC1DB1G)
HalbPneu (http://coord.info/GC16ZWX)
Zasifrovany dub (http://coord.info/GC26EFD)



Přeji úspěšné luštění a šťastný lov.

Martin

E. O čem jsme psali v létě 2000 – 2009

Crypto-World 78/2000

Příloha : 10000.txt , soubor obsahuje prvních 10 000 prvočísel (další informace viz závěr článku "Fermatův test primality, Carmichaelova čísla, bezčtvercová čísla" , str.9) .

Crypto-World 78/2001

Příloha : priloha78.zip (dopis pana Sůvy - detailní informace k horké sazbě, viz. článek Záhadná páska z Prahy, Crypto-World 6/2001)

Crypto-World 78/2002

Crypto-World 78/2003

Crypto-World 78/2004

Crypto-World 78/2005

Crypto-World 78/2006

Crypto-World 7/2007 (mimořádné vydání)

Crypto-World 78/2007

Crypto-World 78/2008

Crypto-World 78/2009

Přílohy: Simulátor šifrátoru ŠD-2 http://crypto-world.info/soutez2009/sd2/cti.txt
(viz článek Rekonstrukce šifrovacího stroje ŠD-2)
Program RSAM.EXE (viz článek Malá soutěž v luštění RSA – řešení).

F. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.
Adresa URL, na níž můžete najít tento sešit (zpravidla 3 týdny po jeho rozeslání) a předchozí e-ziny, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály: http://crypto-world.info

2. Registrace / zrušení registrace

Zájemci o e-zin se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci elektronický formulář na http://crypto-world.info. Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání kódů ke stažení sešitu.
Ke zrušení registrace stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info. Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byly kódy zasílány.

3. Redakce

E-zin Crypto-World

Redakční práce:	Pavel Vondruška
Stálí přispěvatelé:	Vlastimil Klíma
	Pavel Vondruška
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS (výběr příspěvků, komentáře a vkládání na web)	Jaroslav Pinkava Vlastimil Klíma Pavel Vondruška Tomáš Rosa
Webmaster	Pavel Vondruška, jr.

4. Spojení (abecedně)

redakce e-zinu	ezin@crypto-world.info ,	http://crypto-world.info
Vlastimil Klíma	v.klima@volny.cz ,	http://cryptography.hyperlink.cz/
Jaroslav Pinkava	jaroslav.pinkava@gmail.com ,	http://crypto-world.info/pinkava/
Tomáš Rosa	tomas.rosa@rb.cz ,	http://crypto.hyperlink.cz/
Pavel Vondruška	pavel.vondruska@crypto-world.info	http://crypto-world.info/vondruska/index.php
Pavel Vondruška,jr.	pavel@crypto-world.info ,	http://webdesign.crypto-world.info