Vlastimil Klíma: EDON-R, popis a principy,
Crypto-World 4/2009, ISSN 1801-2140, 15. duben 2009, str. 3 - 8

B. Popis a principy EDON-R

Vlastimil Klíma, nezávislý konzultant - kryptolog, Praha,
(http://cryptography.hyperlink.cz, v.klima@volny.cz)

Úvod

O SHA-3 se v Crypto-Worldu píše přímo i nepřímo už od začátku tohoto roku, nicméně podrobné informace může čtenář nalézt na spoustě míst na internetu, například na [1 - 11]. EDON-R je velmi zajímavým kandidátem na nový hašovací standard v rámci soutěže SHA-3, protože je ze všech nejrychlejší. V současné době jsem spoluautorem návrhu EDON-R, i když můj vztah k algoritmu prodělal různé změny. Nejprve jsem byl o algoritmu kolegiálně zpraven jeho duchovním otcem Danilem Gligoroskim v době, kdy jsme společně pracovali na Blue Midnight Wish (BMW), ale až do okamžiku jeho publikace jsem ve skutečnosti o něm nic nevěděl. Seznámil jsem se s ním jako s největším konkurentem BMW po zveřejnění všech kandidátů. Nejprve jsem byl jeho kritikem, což vyústilo v kryptoanalýzu [15], poukazující na jednu nevýhodnou vlastnost. Poté jsme s Danilem přirozeně začali diskutovat o možnostech zlepšení. Bylo to náročné a trvalo to velmi dlouho a dosud trvá, protože to vyžaduje novou kryptoanalýzu. To pak vyústilo v Danilovo rozhodnutí, že jsem se de facto stal spoluautorem, proto mě zařadil při první oficiální příležitosti do týmu. To nastalo v lednu 2009 před první konferencí kandidátů, kdy předkladatelé mohli zaslat drobné opravy dokumentace (překlepy, oprava nepřesností v SW, apod.) [12]. Na první konferenci kandidátů SHA-3 [13] byli pak představeni všichni spoluautoři EDON-R a jejich úloha v týmu ([13]). Velice mě to potěšilo, na druhé straně je to velká zodpovědnost a ohromná dobrovolná pracovní zátěž. Mít v takové soutěži dva nejrychlejší kandidáty znamená nejen čest, ale občas i vražedné pracovní nasazení. Nevěřili byste jaké ohromné množství práce se za jednotlivými návrhy skrývá a co práce a prostředků NIST ušetří, když si nechá zdarma vytvořit standard v mezinárodní soutěži. Člověk si myslí, že se nic neděje a mezitím na analýze a prolamování kandidátů velmi tvrdě pracuje mnoho desítek špičkových kryptologů, které by NIST jen tak nezaplatil. Samozřejmě, že je pro autory bolestné, když někdo najde v jejich funkci chybu. Jejich odhalování je ale přímo náplní soutěže a povinností všech účastníků, i vzhledem ke svým algoritmům! S velmi klidným svědomím můžu prohlásit, že kdybych našel nějakou chybu v BMW nebo EDON-R, tak bych ji publikoval. A předpokládám, že drtivá většina ostatních účastníků by to u svých algoritmů udělala také.

Vznik EDON-R

Vznik EDON-R je poměrně dlouhý, první návrh této funkce pochází z roku 2006 na konferenci [17], kde byla představena jen teoretická východiska, ale nikoli konkrétní náplň. Základním stavebním prvkem jsou kvazigrupy. Právě možnost jejich rychlé implementace posunula EDON-R na první místo v rychlosti. Jsou kritikové, kteří by rádi EDON-R diskvalifikovali a odsunuli do prolomených algoritmů (viz například stránka Nielse Fergusona z Microsoftu, spoluautora algoritmu Skein [11]) nebo poukázali na jeho nevýhody (kvazigrupy se jim zdají neprobádanou oblastí). Nebudeme rozvíjet diskuse na tato témata, i když je to moc zajímavé, jenom si řekněme, že podobných výtek bude přibývat a přitvrdí se. V současné době je jisté, že EDON-R tak jak je, je prakticky odolný proti kryptoanalýze podle představy NIST o bezpečnosti, prezentované na první konferenci SHA-3 (přednáška M. Nandiho z NIST, [7]). Zároveň jsme s Danilem oznámili, že pracujeme na drobné změně (tzv. tweak), která bude NISTem povolena u všech kandidátů, kteří postoupí do druhého kola. Tento tweak je nutný pro to, aby EDON-R mohl být vítězným kandidátem. Vítěz by měl odolat i teoretickým útokům, které byly prezentovány v [18 - 21]. Takovou opravu není jednoduché navrhnout, protože by neměla narušit (změnit) existující kryptoanalýzu a

nesnižovat rychlost. Navíc by měla být malá, aby neměnila zásadní konstrukci algoritmu, ale zároveň velká silou obrany.

Společné rysy EDON-R, BMW a SHA-2

Připomeňme si v krátkosti, co mají EDON-R, BMW a SHA-2 společné. Jsou založeny na iterativním principu a kompresní funkci. Zpráva, která se má hašovat, se doplní definovaným způsobem tzv. paddingem a počtem zpracovávaných bitů původní zprávy a zarovná se na nejbližší násobek délky bloku buď 512/1024 bitů podle toho, zda se jedná o EDON-R256/512 nebo SHA256/SHA512. Potom se tyto funkce shodují v tom, že používají iterativní výpočet s použitím tzv. kompresní funkce (budeme používat označení R z dokumentace EDON-R) a průběžné hašovací hodnoty. Průběžná hašovací hodnota se nastaví na počátku na hodnotu tzv. inicializačního vektoru. Potom se v N krocích vždy ze staré průběžné hašovací hodnoty a daného bloku zprávy pomocí kompresní funkce vytvoří nová hodnota průběžné haše. Poslední průběžná hodnota haše (nebo její část) je pak prohlášena za skutečnou hodnotu haše. Hašování tedy probíhá u EDON-R i SHA-2 podle stejného následujícího scénáře. Poznamenejme, že SHA-2 používá klasické označení H pro průběžnou hašovací hodnotu, zatímco u EDON-R je to označení P (pumpa).

Algorithm: EDON-$\mathcal{R}$

Input: Message M of length l bits, and the message digest size n.

Output: A message digest *Hash*, that is long n bits.

1. Preprocessing
   (a) Pad the message M.
   (b) Parse the padded message into N, m-bit message blocks, $M^{(1)}, M^{(2)}, \ldots, M^{(N)}$.
   (c) Set the initial value of the double pipe $P^{(0)}$.
2. Hash computation
   For $i = 1$ to N
   $P^{(i)} = \mathcal{R}(P^{(i-1)}, M^{(i)})$;
3. $Hash$ =Take_n_Least_Significant_Bits($P^{(N)}$).

1. Předzpracování

(a) Doplň zprávu M jednoznačným definovaným způsobem o délku zprávy v bitech a doplněk
(b) Rozděl zprávu na celistvý násobek (N) m-bitových bloků $M^{(1)}$, ..., $M^{(N)}$.
(c) Nastav počáteční hodnotu průběžné haše $P^{(0)}$ = IV.

2. Výpočet haše

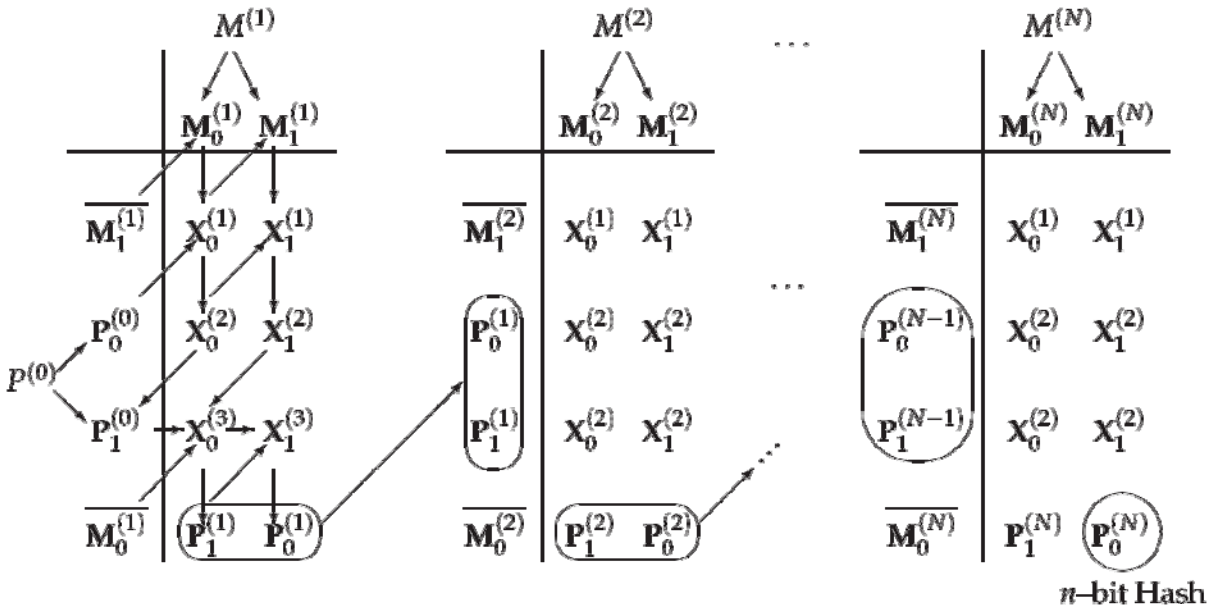
For i = 1 to N
{ $P^{(i)} = R(M^{(i)}, P^{(i-1)})$ }

3. Závěr

H(M) = definovaných n bitů z hodnoty $P^{(N)}$.

Dvojnásobná pumpa

EDON-R používá stejně jako BMW dvojnásobnou pumpu, tedy průběžnou hašovací hodnotu P o délce 2n bitů, kde n je délka haše [16]. To zabraňuje útoku prodloužením zprávy a posouvá složitost Jouxova útoku [14] do nereálna. Kompresní funkce zpracovává také bloky 2n bitů najednou. Obě základní verze EDON-R256/512 používají bloky (P i M) o délce 16 slov, ale liší se délkou použitého slova (w = 32/64 = n/8 bitů), jinak všechny funkce a transformace vypadají až na konstanty stejně. Zpracování zprávy pak probíhá podle následujícího schématu, kde je také vidět závěrečná n-bitová hash.



V jednoduchosti je krása

Celé hašování lze právě zobrazit jen tímto obrázkem. K tomu malý komentář. Na obrázku je vždy dolním indexem 0 nebo 1 označena dolní nebo horní polovina proměnné (tj. 8 w-bitových slov). Proměnné $X^{1,2,3}$ uvnitř mají také dvě poloviny (s dolním indexem 0, 1) a označují průběžné meziproměnné - výsledky kvazigrupové operace Q. Kvazigupová operace Q má dva operandy o 8 slovech (A a B) a výsledkem je také 8 slov C = Q(A, B). Na obrázku je první operand (A) vždy ten odkud vychází *šikmá* šipka, která směřuje do operandu B, a z operandu B jde *vodorovná* nebo *svislá* šipka do výsledku C. Poznamenejme, že rozdělení pumpy P a zprávy M na dvě poloviny $P_{0,1}$ a $M_{0,1}$ je značeno také šikmou šipkou, ale tentokrát to neznamená kvazigrupovou operaci, nýbrž prosté rozdělení na dvě poloviny. Čára nad proměnnou (například nad M_0) znamená obrácení pořadí osmi slov této proměnné. Například první operace, která proběhne je $X_0^1 = Q(M_1^{(1)}$ s čarou, $M_0^{(1)})$.

Kvazigrupová operace

Operace je definována pomocí rychlých a dostupných operací ve všech procesorech: sčítání, xor a bitové rotace.

Quasigroup operation of order 2^{256}

Input: $\mathbf{X} = (X_0, X_1, \ldots, X_7)$ and $\mathbf{Y} = (Y_0, Y_1, \ldots, Y_7)$

where X_i and Y_i are 32–bit variables.

Output: $\mathbf{Z} = (Z_0, Z_1, \ldots, Z_7)$ where Z_i are 32–bit variables.

Temporary 32–bit variables: $T_0, \ldots, T_{15}$.

1.
$$
\begin{aligned}
T_0 &\leftarrow ROTL^0(\texttt{0xAAAAAAAA} + X_0 + X_1 + X_2 + X_4 + X_7);\\
T_1 &\leftarrow ROTL^4(X_0 + X_1 + X_3 + X_4 + X_7);\\
T_2 &\leftarrow ROTL^8(X_0 + X_1 + X_4 + X_6 + X_7);\\
T_3 &\leftarrow ROTL^{13}(X_2 + X_3 + X_5 + X_6 + X_7);\\
T_4 &\leftarrow ROTL^{17}(X_1 + X_2 + X_3 + X_5 + X_6);\\
T_5 &\leftarrow ROTL^{22}(X_0 + X_2 + X_3 + X_4 + X_5);\\
T_6 &\leftarrow ROTL^{24}(X_0 + X_1 + X_5 + X_6 + X_7);\\
T_7 &\leftarrow ROTL^{29}(X_2 + X_3 + X_4 + X_5 + X_6);
\end{aligned}
$$

2.
$$
\begin{aligned}
T_8 &\leftarrow T_3 \oplus T_5 \oplus T_6;\\
T_9 &\leftarrow T_2 \oplus T_5 \oplus T_6;\\
T_{10} &\leftarrow T_2 \oplus T_3 \oplus T_5;\\
T_{11} &\leftarrow T_0 \oplus T_1 \oplus T_4;\\
T_{12} &\leftarrow T_0 \oplus T_4 \oplus T_7;\\
T_{13} &\leftarrow T_1 \oplus T_6 \oplus T_7;\\
T_{14} &\leftarrow T_2 \oplus T_3 \oplus T_4;\\
T_{15} &\leftarrow T_0 \oplus T_1 \oplus T_7;
\end{aligned}
$$

3.
$$
\begin{aligned}
T_0 &\leftarrow ROTL^0(\texttt{0x55555555} + Y_0 + Y_1 + Y_2 + Y_5 + Y_7);\\
T_1 &\leftarrow ROTL^5(Y_0 + Y_1 + Y_3 + Y_4 + Y_6);\\
T_2 &\leftarrow ROTL^9(Y_0 + Y_1 + Y_2 + Y_3 + Y_5);\\
T_3 &\leftarrow ROTL^{11}(Y_2 + Y_3 + Y_4 + Y_6 + Y_7);\\
T_4 &\leftarrow ROTL^{15}(Y_0 + Y_1 + Y_3 + Y_4 + Y_5);\\
T_5 &\leftarrow ROTL^{20}(Y_2 + Y_4 + Y_5 + Y_6 + Y_7);\\
T_6 &\leftarrow ROTL^{25}(Y_1 + Y_2 + Y_5 + Y_6 + Y_7);\\
T_7 &\leftarrow ROTL^{27}(Y_0 + Y_3 + Y_4 + Y_6 + Y_7);
\end{aligned}
$$

4.
$$
\begin{aligned}
Z_5 &\leftarrow T_8 + (T_3 \oplus T_4 \oplus T_6);\\
Z_6 &\leftarrow T_9 + (T_2 \oplus T_5 \oplus T_7);\\
Z_7 &\leftarrow T_{10} + (T_4 \oplus T_6 \oplus T_7);\\
Z_0 &\leftarrow T_{11} + (T_0 \oplus T_1 \oplus T_5);\\
Z_1 &\leftarrow T_{12} + (T_2 \oplus T_6 \oplus T_7);\\
Z_2 &\leftarrow T_{13} + (T_0 \oplus T_1 \oplus T_3);\\
Z_3 &\leftarrow T_{14} + (T_0 \oplus T_3 \oplus T_4);\\
Z_4 &\leftarrow T_{15} + (T_1 \oplus T_2 \oplus T_5);
\end{aligned}
$$

Jak je vidět, na 8 slov prvního operandu Q(X, Y) je v prvním kroku aplikována nejprve aritmetická bijektivní transformace, a to převod dílčích slov na jejich součty po pěticích. Dále je vždy každé výsledné slovo rotováno a v druhém kroku je na výsledek aplikována tentokrát lineární transformace, a to vždy tři binární součty (xor) dílčích slov. V druhém kroku vzniká operace, kterou označujeme také π_2 a výsledkem je $\pi_2(X)$, bijektivní obraz X. Podobně druhý argument Y je pomocí podobné ale odlišné transformace π_3 převeden na obraz $\pi_3(Y)$. Oba dva obrazy jsou sečteny a slova výsledku mírně permutována permutací označovanou π_1 (permutaci vidíte v kroku 4, kde pořadí slov proměnné Z je posunuto oproti 0,.., 7). Máme tak alternativní zápis pro $Q(X, Y) = \pi_1(\pi_2(X) + \pi_3(Y))$.Jak je vidět, není tady nic neobvyklého, avšak za návrhem stojí velmi hezká teorie Latinských čtverců. Dále tato volba kvazigrupové operace umožňuje odhadnout diferenciální charakteristiky celé kompresní funkce R a tím kvantitativně dokázat odolnost proti diferenciální kryptoanalýze. Pochopitelně složitost kryptoanalýzy je založena podobně jako u BMW na neschopnosti řešit složité nelineární

soustavy booleovských rovnic o mnoha neznámých, což je známý NP-úplný problém. Navíc je zde problém řešení soustavy kvazigrupových rovnic.

Výkonové charakteristiky

Rychlostní charakteristiky jsou nejlepší ze všech algoritmů, měří se v počtech cyklů procesoru, nutných na zpracování jednoho bajtu (vypočítaný poměrně z počtu cyklů nutných pro zpracování dlouhých zpráv). Spotřeba paměti je trochu vyšší než u některých konkurentů, ale rozdíl ani absolutní hodnoty nejsou velké. Charakteristiky ukazuje slajd z přednášky [13].

Software performances of the optimized C implementation on the NIST reference platform

Intel C++ v11.0.66, in 64-bit mode
EDON-R 224/256 achieves **4.54 cycles/byte**

Intel C++ v11.0.66, in 64-bit mode
EDON-R 384/512 achieves **2.29 cycles/byte**

Memory requirements

EDON-R 224/256 needs **256 bytes**

EDON-R 384/512 needs **512 bytes**

HW – gate count

EDON-R 224/256, ~13,000 gates

EDON-R 384/512, ~25,000 gates

8-bit MCU (ATmega16, ATmega406)

EDON-R 224/256, compiled C code produces ~6KB of machine instructions, speed 616 cycles/bytes

EDON-R 384/512, compiled C code produces ~38KB of machine instructions, speed 1857 cycles/bytes

Kritika

Samotná kvazigrupová operace není jednocestná, ale R jako celek je jednocestná v případě, že neznáme zprávu M. Tedy ze znalosti nové i staré hodnoty pumpy nelze určit M. Avšak při znalosti nové hodnoty pumpy a M lze dojít k předchozí hodnotě pumpy. Tato vlastnost se nezdála být na počátku nebezpečná, ale ukázalo se, že je nevhodná, i když nepřinesla žádný *přímý* útok. Proto bude vhodné navrhnout opravu tak, aby funkce R byla jednocestná i v tomto druhém případě. Podrobnější popis, analýzu a průběžné novinky je možné sledovat na internetu (např. [2]).

Závěr

V tomto článku jsme uvedli základní popis a některé vlastnosti hašovací funkce EDON-R, nejrychlejšího kandidáta na SHA-3. Čtenářům se omlouváme za tak drastické zkrácení popisu a vlastností. Skutečně šlo jen o základní seznámení a poukaz na to, jak je tato funkce elegantní. Podrobnější popis, analýzu a průběžné novinky je možné sledovat na internetu (např. [2]).

Varování ministra fair-play: *jediné nezávislé stránky v následujícím seznamu jsou stránky NIST. Ostatní internetové stránky produkují skupiny a lidé, kteří mají své zájmy v soutěži. Většina těchto stránek to skrývá, nelze je považovat za nezávislé, i když se o to všemožně snaží, a často to tak působí.*

Literatura

[1] (nezávislá) oficiální domácí stránka NIST k projektu SHA-3: http://csrc.nist.gov/groups/ST/hash/index.html
[2] stránka autora s novinkami k projektu SHA-3 a algoritmům BMW a EDON-R: http://cryptography.hyperlink.cz/BMW/BMW_CZ.html (naleznete tam rozcestník a všechny zde uvedené linky)
[3] Stránka kandidátů, kteří postoupili do prvního kola (NIST): http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/submissions_rnd1.html
[4] Stránka SHA-3 na wiki: http://en.wikipedia.org/wiki/SHA-3
[5] Stránka SHA-3 projektu ECRYPT: http://ehash.iaik.tugraz.at/index.php/The_SHA-3_Zoo
[6] Seznam všech autorů všech kandidátů: http://ehash.iaik.tugraz.at/wiki/SHA-3_submitters
[7] Stránka NIST, věnovaná první konferenci kandidátů SHA-3: http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/Feb2009/program.html
[8] Stránka o SW výkonnosti algoritmů eBash: http://bench.cr.yp.to/results-hash.html
[9] Stránka (ECRYPT) o HW výkonnosti algoritmů : http://ehash.iaik.tugraz.at/wiki/SHA-3_Hardware_Implementations
[10] Srovnávací stránka Fleischmann-Forler-Gorski: http://www.uni-weimar.de/cms/fileadmin/medien/medsicherheit/Research/SHA3/Classification_of_the_SHA-3_Candidates.pdf
[11] Srovnávací stránka (Niels Ferguson): http://www.skein-hash.info/sha3-engineering
[12] Danilo Gligoroski, Rune Steinsmo Odegard, Marija Mihova, Svein Johan Knapskog, Ljupco Kocarev, Aleš Drápal, Vlastimil Klima: Cryptographic Hash Function EDON-R, homepage of EDON-R (http://www.item.ntnu.no/people/personalpages/fac/danilog/edon-r), the whole submission package (Accepted by NIST, Jan 12, 2009, http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/documents/Edon-RUpdate.zip)
[13] EDON-R presentation at the First SHA-3 Candidate Conference on February 25-28, 2009, http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/Feb2009/documents/Edon-R-Presentation-04-pdf-friendly.pdf
[14] A. Joux: Multicollisions in iterated hash functions. Application to cascaded constructions. Proceedings of Crypto 2004, LNCS 3152, pages 306-316.
[15] Vlastimil Klima: Multicollisions of EDON-R hash function and other observations, November 2008, preliminary analysis, http://cryptography.hyperlink.cz/BMW/EDONR_analysis_vk.pdf
[16] Stefan Lucks. Design principles for iterated hash functions. Cryptology ePrint Archive, Report 2004/253, 2004, http://eprint.iacr.org/2004/253.pdf
[17] SECOND CRYPTOGRAPHIC HASH WORKSHOP, USA, August 24-25, 2006, http://csrc.nist.gov/groups/ST/hash/second_workshop.html
[18] Gaëtan Leurent: Key Recovery Attack against Secret-prefix Edon-R, Cryptology ePrint Archive: Report 2009/135, http://eprint.iacr.org/2009/135.pdf,
[19] Dmitry Khovratovich, Ivica Nikolić, Ralf-Philipp Weinmann: Cryptanalysis of Edon-R, 2008, http://ehash.iaik.tugraz.at/uploads/7/74/Edon.pdf,
[20] Danilo Gligoroski, Rune Steinsmo Ødegård - On the Complexity of Khovratovich et. al's Preimage Attack on EDON-R, http://eprint.iacr.org/2009/120.pdf,
[21] Vlastimil Klima: Multicollisions of EDON-R hash function and other observations, November 2008, http://cryptography.hyperlink.cz/BMW/EDONR_analysis_vk.pdf .