

A. Analýza Blue Midnight Wish – současné útoky na BMW-n

Vlastimil Klíma, kryptolog konzultant, Praha

(<http://cryptography.hyperlink.cz>, v.klima@volny.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>)



Dr. Vlastimil Klíma

Článek volně navazuje na články o BMW v 12/2009, 3/2009 a 7-8/2009 a na příspěvky v číslech 1 - 4 Crypto-Worldu 2010. V čísle 1 jsme se zabývali hledáním vzoru (úloha první), v čísle 2 hledáním kolize (úloha druhá), v čísle 3 různými bloky BMW a v čísle 4 aspektem složitosti.



Prof. Danilo Gligoroski

Dosud byly analýze BMW, kromě autorské analýzy (zde v Crypto-Worldu a v [6], [7]), věnovány tři příspěvky, viz [3], [4], [5]. Všechny tři jsou tzv. "rozlišovací" útoky (distinguishing attacks) na kompresní funkci BMW. V práci Aumassona [3] má útok složitost cca 2^{19} , v práci Nikolice [4] je to útok na modifikovanou variantu BMW512 se složitostí 2^{278} . Nejvýznamnějším a slibně znějícím je příspěvek Guo-Thomsena [5]. Má minimální složitost, proto se mu budeme věnovat jako prvnímu.

Guo-Thomsenův útok

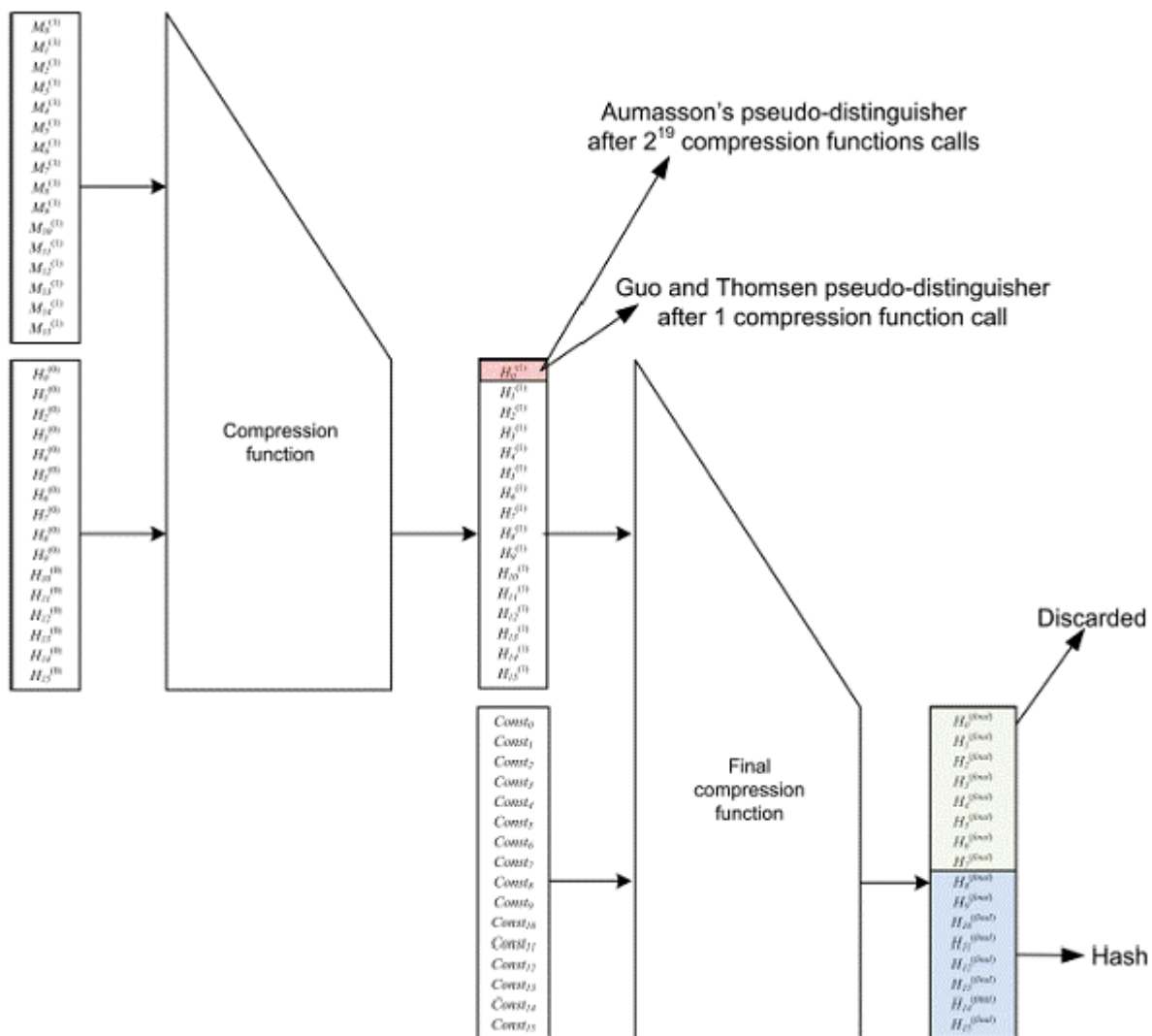
Nejprve poznamenejme, že se jedná o pseudoútok. Oč jde, uvidíme z následující ilustrace. Úvodní volání kompresní funkce na blok zprávy M lze našimi nástroji (z citovaných článků v Crypto-Worldu) jednoduše zapsat takto

$$\begin{aligned} Q_a &= A_2(A_1(M \oplus \text{CONST}^{(0)})) + \text{ROTL}^1(\text{CONST}^{(0)}), \\ Q_b &= T^L(T^U(Q_a) + ((B(\text{rot}M) + K) \oplus \text{ROTL}^7(\text{CONST}^{(0)}))) \\ G &= (M \oplus L_a(Q_b)) + (Q_a \oplus L_b(Q_b)), \\ X &= (f_6(G)). \end{aligned}$$

Guo a Thomsen uvažují, že mohou měnit současně blok zprávy M a hodnotu průběžné haše, což u prvního bloku je konstanta $\text{CONST}^{(0)}$. Protože takový útok právě neřeší co s prvním voláním kompresní funkce (a u BMW speciálně navíc i s posledním voláním), říká se mu pseudoútok. Tak tedy, zkoumají kompresní funkci

$$\begin{aligned} Q_a &= A_2(A_1(M \oplus H)) + \text{ROTL}^1(H), \\ Q_b &= T^L(T^U(Q_a) + ((B(\text{rot}M) + K) \oplus \text{ROTL}^7(H))) \\ G &= (M \oplus L_a(Q_b)) + (Q_a \oplus L_b(Q_b)), \\ \text{new}H &= (f_6(G)), \end{aligned}$$

kde mohou měnit jak M, tak H. Konkrétně je mění současně tak, aby $M \oplus H$ bylo konstantní. Tím vyblokují změnu v dosti nepříjemné difúzní funkci $A_2(A_1(M \oplus H))$ a nastane jen v $ROTL^1(H)$. Konkrétně mění jen slovo M_1 a H_1 , takže změna v $Q_a = A_2(A_1(M \oplus H)) + ROTL^1(H)$ nastane jen v jeho nejnižším slově (Q_0). Z Q_a pak tato změna postupuje dále do Q_b , kde se podařilo zjistit, co způsobí, a dojít přes Q_b zatím nejdále k nejnižším bitům nultého slova proměnné G, viz obrázek.



Obr. 1: Výsledky současných útoků na BMW256/512

V těchto místech jsou schopni říci, jak se tyto bity změní nebo je odlišit od náhodných. Konkrétní počty dotčených bitů jsou uvedeny na následujících dvou obrázcích. Jsou zde uvedeny i varianty BMW 0/16, 1/15 a 2/14, z nichž ta poslední je definitorická BMW s dvěma rundami číslo jedna a 14 rundami číslo 2, ostatní jsou pouze nestandardní varianty. V nejlepším případě se jedná o 11 bitů u nestandardních verzí a o 1 bit u standardních verzí. O změnách ostatních z 512 nebo 1024 bitů (pro BMW256/512) proměnné G nejsou schopni prohlásit už nic. Nová proměnná newH má tak určeno několik nejnižších bitů, které přebírá z G. Jakmile však newH vstoupí do posledního volání kompresní funkce, je zde jednak chování tohoto vstupu už dosti omezeno (právě jsme si řekli, že víme jak se chová pár jeho bitů z 512 nebo 1024) a jednak zbývající vstup už nemůžeme měnit, neboť je to konstanta $CONST^{(final)}$:

$$Q_a = A_2(A_1(newH \oplus CONST^{(final)})) + ROTL^1(CONST^{(final)}),$$

$$\begin{aligned}
Q_b &= T^L(T^U(Q_a) + ((B(\text{rotnewH}) + K) \oplus \text{ROTL}^7(\text{CONST}^{\text{(final)}}))) \\
G &= (M \oplus L_a(Q_b)) + (Q_a \oplus L_b(Q_b)), \\
\text{Hash} &= 8_l\text{swords_of}(f_6(G)).
\end{aligned}$$

Tedy do tohoto posledního bloku vstupuje mnoho neznámým způsobem změněných bitů zcela na počátku v proměnné newH a několik známých změn. Autoři sami potvrzují, že o výsledku (Hash) nejsou schopni nic říci, a že jejich přístup ukazuje pouze vlastnost kompresní funkce, ale neohrožuje bezpečnost celé hašovací funkce.

Book Chapter



large version

On the Computational Asymmetry of the S-Boxes Present in BLUE MIDNIGHT WISH Cryptographic Hash Function

Book	ICT Innovations 2009
Publisher	Springer Berlin Heidelberg
DOI	10.1007/978-3-642-10781-8
Copyright	2010
ISBN	978-3-642-10780-1 (Print) 978-3-642-10781-8 (Online)
Part	Part 2
DOI	10.1007/978-3-642-10781-8_40
Pages	391-400
Subject Collection	Engineering
SpringerLink Date	Wednesday, January 06, 2010



 PDF (236.5 KB)  Free Preview

ICT Innovations 2009

10.1007/978-3-642-10781-8_40

Danco Davcev and Jorge Marx Gómez

Daniilo Gligoroski¹  **and Vlastimil Klima²** 

(1) Department of Telematics, Norwegian University of Science and Technology, O.S.Bragstads plass 2B, N-7491 Trondheim, Norway

(2) Independent cryptologist - consultant, Czech Republic

Abstract

BLUE MIDNIGHT WISH hash function is one of 14 candidate functions that are continuing in the Second Round of the SHA-3 competition. In its design it has several S-boxes (bijective components) that transform 32-bit or 64-bit values. Although they look similar to the S-boxes in SHA-2, they are also different. It is well known fact that the design principles of SHA-2 family of hash functions are still kept as a classified NSA information. However, in the open literature there have been several attempts to analyze those design principles. In this paper first we give an observation on the properties of SHA-2 S-boxes and then we investigate the same properties in BLUE MIDNIGHT WISH.

Aumassonův útok

V práci Aumassona [3] má útok složitost cca 2^{19} , ale na BMW-512 má srovnatelné výsledky jako Guo-Thomsen [5]. Postup je téměř stejný, i když vznikl nezávisle. Opět se jedná o pseudoútok a opět mění současně M a H tak, aby $M \oplus H$ bylo konstantní. Zde však mění dvě slova, a to M_1 a H_1 a M_5 a H_5 současně. Výsledkem je znalost nikoli přesné difference v dolních 4 bitech nultého slova proměnné G, ale možnost difference odlišit od náhodných diferencí pomocí 2^{19} párů M_1 a H_1 a M_5 a H_5 .

	Distinguisher of Aumasson		Distinguisher of Guo and Thomsen			
	Compression function 2/14	Full BMW-256	Compression function 0/16	Compression function 1/15	Compression function 2/14	Full BMW-256
BMW-256						
Distinguished bits	4	0	9	1	1	0
Distinguished Variables	H_{new0}	/	H_{new0}, H_{new5}	H_{new0}	H_{new0}	/

Obr.2: Počet odlišitelných bitů kompresní a hašovací funkce BMW256

	Distinguisher of Aumasson		Distinguisher of Guo and Thomsen			
	Compression function 2/14	Full BMW-512	Compression function 0/16	Compression function 1/15	Compression function 2/14	Full BMW-512
BMW-512						
Distinguished bits	4	0	11	1	1	0
Distinguished Variables	H_{new0}	/	H_{new0}, H_{new5}	H_{new0}	H_{new0}	/

Obr.3: Počet odlišitelných bitů kompresní a hašovací funkce BMW512

Porovnání s naším seriálem

V předchozích 4 dílech jsme otázku rozlišovače na úrovni průběžné hašovací hodnoty neuvažovali, protože jsme se zabývali možnostmi skutečných útoků. I když představené útoky nevedou k použitelným výsledkům na prolomení BMW, jsou to samozřejmě cenné analýzy, neboť ukazují hranice, kam se dá s diferenciální kryptoanalýzou u BMW dostat. Současné útoky mají cenný význam pro analýzu vlastností konstrukce BMW, nikoli jako útoky, což uvádí ostatně i autoři těchto prací

[3]:

“Conclusion. The compression functions of BMW-256 and BMW-512 do not behave ideally, as they admits strong differential biases. However, these seem difficult to exploit to build a distinguisher (or any other attack) for the hash function, because

- 1. the IV is fixed, hence an adversary cannot choose differences in the chaining values entering the compression function;*
- 2. even if differences in the IV could be controlled, the additional “blank” invocation to the compression function would prevent an adversary from observing the output differences of the first compression function.”*

a [5]:

final note present in the work of Guo and Thomsen: *“Another interesting problem to consider is to devise distinguishers on other output words than merely H_0^* . In particular, a bias on one of the output words $H_8^* \dots H_{15}^*$ would be interesting.”*

Ten, kdo se hlouběji ponoří do studia BMW, uvidí mnohem více podobných přístupů i to, proč musí skončit a na co vlastně „umřou“. Pro zájemce dáváme malý „hint“: příčina je v trojúhelníkových transformacích, které následují po sobě – horní a dolní trojúhelníkové transformace rozprostírají změny proti sobě. Chceme-li co nejmenší změnu v T^U , zapříčiníme největší změnu v T^L , použijeme-li co nejmenší změnu v T^L , způsobilíme změnu všech slov v T^U . A navíc, T^L a T^U jsou bijekce, takže změna nastat musí (!), a to v obou (!) transformacích. Toto se nedá obejít jinak než anulováním změn uprostřed – tj. pomocí AddElement. Útok je pak zcela určen tím, jak se výzkumník vypořádá s touto anulací nebo, je-li odvážný, s řízenou změnou ve všech transformacích AddElement, T^L a T^U . Držíme Vám palce, ať jste úspěšnější, než dosavadní útočníci, hodně štěstí!

Literatura

- [1] domácí stránka týmu BMW: http://www.q2s.ntnu.no/sha3_nist_competition/start
- [2] stránka NIST k projektu SHA-3: <http://csrc.nist.gov/groups/ST/hash/index.html>
- [3] J. P. Aumasson: Practical distinguisher for the compression function of Blue Midnight Wish, February 2010, <http://131002.net/data/papers/Aum10.pdf>
- [4] I. Nikolic, J. Pieprzyk, P. Sokolowski, R. Steinfeld: Rotational Cryptanalysis of (Modified) Versions of BMW and SIMD, March 2010, tento link vypadá podivně, ale funguje, pokud ho vložíte celý do adresy prohlížeče:
https://cryptolux.org/mediawiki/uploads/0/07/Rotational_distinguishers_%28Nikolic%2C_Pieprzyk%2C_Sokolowski%2C_Steinfeld%29.pdf
- [5] J. Guo and S. S. Thomsen: Distinguishers for the Compression Function of Blue Midnight Wish with Probability 1, March 2010, <http://www2.mat.dtu.dk/people/S.Thomsen/bmw/bmw-distinguishers.pdf>
- [6] Danilo Gligoroski, Vlastimil Klima: On the Computational Asymmetry of the S-boxes Present in Blue Midnight Wish Cryptographic Hash Function, Information on ICT Innovations 2009, Sept. 28 - 30, Ohrid, R. Macedonia, in Danco Davcev and Jorge Marx Gómez (eds): ICT Innovations 2009, Springer, Berlin, Heidelberg, 2010, pp. 391 - 400, <http://cryptography.hyperlink.cz/BMW/BijectionsInBMW03-plain.pdf>
- [7] Danilo Gligoroski, Vlastimil Klima: On Blue Midnight Wish Decomposition, SantaCrypt 2009, Dec. 3-4, 2009, Prague, Czech Republic, Proceedings of SantaCrypt 2009, ISBN 978-80-904257-0-5, pp. 41-51, available on line: <http://cryptography.hyperlink.cz/2009/BMWDecomposition04.pdf>