A framework for Measuring and Evaluating the Progress of the Cryptanalysis of the Hash Function Blue Midnight Wish

The Blue Midnight Wish team

October 6, 2010

Attacker	Hash size	Type of attack	Compression function		Whole function	
			Attacked variables (rounds)	Complexity	Attacked variables (rounds)	Complexity
Aumasson[1]	All	pseudo-distinguisher	1 out of 16	2^{19}	0 out of 32	N/A
Nikolic et.al.[2]	512	pseudo-distinguisher on modified function	1 out of 16	$2^{278.2}$	0 out of 32	N/A
Guo &Thomsen[3]	All	pseudo-distinguisher	1 out of 16	2^{1}	0 out of 32	N/A
Leurent[4]	256	pseudo-collision	3 out of 16	2^{32}	0 out of 32	N/A

Table 1: Evaluating the progress of the cryptanalysis of Blue Midnight Wish

This note is in a direct compliance with the discussions that took over at the last SHA-3 conference in Santa Barbara on 23-24 August 2010, that there should be better classification on the growing number of attacks on all hash functions that do not follow the well established definition in cryptology for a distinguisher of a pseudo-random function (see for example Bellare and Rogaway [5], Ch. 3.4, or Goldreich [6], Ch. 3.3) and how these attacks can be observed from a global perspective of the security margins in the attacked functions. Thus, as a response to the growing cryptanalytic work on Blue Midnight Wish hash function we define a framework for classification of all those and future attacks both on the compression function and on the whole hash function.

Blue Midnight Wish [7] hash function has no explicit rounds in its design. However, the compression function is producing 16 variables of the double-pipe chain with increased complexity beginning from the variable H_0 that has the lowest computational complexity, up

to the variable H_{15} that has the highest computational complexity. That is a very strong analogy with the designs that have rounds in their design and where the complexity of computed components in those designs is increasing in every round.

By setting the output variables $H_i,\ i = 0, \ldots, 15$ of the compression function of Blue Midnight Wish to denote an equivalent notion to the "rounds" in classical designs, we will enable independent cryptographers to evaluate and measure the success of their attack and the strength of the function in accordance of the cryptanalytic progress. Since the whole hash function has additional blank final invocation of the compression function this implies that in this framework the number of rounds that will correspond for the whole hash function is at least by 16 more than in the compression function.

Thus from cryptanalytic point of view we can talk about two values that are determining the security margins in Blue Midnight Wish:

1. Number of variables (rounds) with ever-increasing computational complexity as security margin on the compression function.

The security margin in the compression function has a value 16 as an analogy with the designs that have 16 rounds in their compression functions.

2. Number of variables (rounds) with ever-increasing computational complexity as security margins for the whole hash function.

The security margin for the whole hash function has a value 32 as an analogy with the designs that have 32 rounds in their compression functions. The rationale for setting the security margin as 32 is that for the whole hash function, the minimal number of produced variables out of the compression function calls in Blue Midnight Wish is 32 (one call to the compression function and one finalization call). Thus any successful attack on the compression function, in order to be transferred to the whole function will have at least 32 produced variables out of the compression function with each of them produced in a series of ever increasing computational complexity.

All independent cryptanalysis for Blue Midnight Wish that has happened so far (and the new one that has been recently announced in the Rump session of CRYPTO 2010) are naturally fitting in this framework for measuring and evaluating the progress of the cryptanalysis of the hash function. They are presented in Table 1.

Additionally, so far all attacks have gone in the direction of taking the control over both H and M variable. According to the taxonomy of the attacks on hash functions developed in the PhD thesis of Preneel (see [8] Ch. 2.5), all these attacks are "pseudo-attacks"[1]. This fact is automatically making these attack techniques non-applicable and non-effective against the whole function because the final invocation of the compression function is such that it excludes attack techniques that assume control over both H and M.

The actual situation that all attacks so far are pseudo-attacks is a direct confirmation of the soundness of the design rationale to incorporate big number of entangled bijections that will force the attacks to be only pseudo-attacks. Additionally, from the described framework and Table 1 it is clear that Blue Midnight Wish is not just the best performer, but also a candidate with the biggest security margin among Second Round SHA-3 candidates.

[1] According to Miriam-Webster online dictionary (`http://www.merriam-webster.com/dictionary/pseudo` - accessed Aug 27 2010) the meaning of the word "pseudo" is: being apparently rather than actually as stated.

References

[1] J.-P. Aumasson: "Practical distinguisher for the compression function of Blue Midnight Wish", Feburary 2010. Available: `http://131002.net/data/papers/Aum10.pdf` (2009/08/27).

[2] I. Nikolić, J. Pieprzyk, P. Sokołowski, and R. Steinfeld: "Rotational Cryptanalysis of (Modified) Versions of BMW and SIMD", March 2010. Available: `https://cryptolux.org/mediawiki/uploads/0/07/Rotational\_distinguishers\_(Nikolic,\_Pieprzyk,\_Sokolowski,\_Steinfeld).pdf` (2010/08/27).

[3] J. Guo and S. S. Thomsen: "Distinguishers for the Compression Function of Blue Midnight Wish with Probability 1", March 2010. Available: `http://www2.mat.dtu.dk/people/S.Thomsen/bmw/bmw-distinguishers.pdf` (2010/08/27).

[4] G. Leurent, "Self-Defence Against Fresh Fruit", CRYPTO 2010 Rump Session. Available: `http://rump2010.cr.yp.to/c659ebaf681758e01ccf824fd58f3c42.pdf` (2010/08/27). The details of the attack are not yet fully disclosed but according to the author, more details will be posted soon.

[5] Mihir Bellare and Phillip Rogaway, "Introduction to Modern Cryptography," Department of Computer Science and Engineering, University of California, September 2005

[6] Oded Goldreich, "Foundations of cryptography: a primer," New Publishers Inc., USA, 2005

[7] D. Gligoroski, V. Klima, S. J. Knapskog, M. El-Hadedy, J. Amundsen, and S. F. Mjølsnes: "Cryptographic hash function BLUE MIDNIGHT WISH. Submission to NIST (Round 2)". Available: `http://people.item.ntnu.no/~danilog/Hash/BMW-SecondRound/Supporting_Documentation/BlueMidnightWishDocumentation.pdf` (2010/08/27), September 2009.

[8] B. Preneel, "Analysis and Design of Cryptographic Hash Functions," PhD thesis, Katholieke Universiteit Leuven, January 1993.