Subject: OFFICIAL COMMENT:Blue Midnight Wish
From: "Danilo Gligoroski" <danilo.gligoroski@gmail.com>
Date: Mon, 15 Dec 2008 13:26:39 +0100
To: <hash-function@nist.gov>
CC: <hash-forum@nist.gov>

Hi,

A new optimized C version of Blue Midnight Wish hash function can be downloaded from:
http://people.item.ntnu.no/~danilog/Hash/Additional_Implementations_bmw_Dec2008.z

With Intel C++ v11.0.061 for Windows it achieves the following speeds:

32-bit environment
BlueMidnightWish performance in Cycles/Byte with different message lengths in BYTES

	1	10	100	1000	10000	100000
MD Size: 224	697.00	66.10	11.89	8.05	7.70	7.62
MD Size: 256	697.00	70.90	12.97	8.72	7.73	7.64
MD Size: 384	1801.00	181.30	18.13	16.90	13.00	12.61
MD Size: 512	1813.00	181.30	18.49	16.90	12.99	12.61

64-bit environment
BlueMidnightWish performance in Cycles/Byte with different message lengths in BYTES

	1	10	100	1000	10000	100000
MD Size: 224	2041.00	204.10	11.29	7.69	7.37	7.32
MD Size: 256	637.00	63.70	11.29	7.71	7.37	7.32
MD Size: 384	649.00	64.90	6.49	3.90	3.68	3.63
MD Size: 512	697.00	64.90	6.49	3.90	3.68	3.63

Regards,
Danilo Gligoroski

Subject: OFFICIAL COMMENT:Blue Midnight Wish
From: "Søren S. Thomsen" <ssth@win.dtu.dk>
Date: Thu, 16 Apr 2009 11:12:05 +0200
To: <hash-function@nist.gov>
CC: <hash-forum@nist.gov>

Dear all,

Blue Midnight Wish (BMW) allows pseudo-attacks---collisions and (2nd) preimages---below the expected security levels. These are attacks where the attacker is free to choose the IV. With respect to pseudo-attacks, the security level of BMW-256 is reduced by roughly 64 bits, and the security level of BMW-512 is reduced by roughly 128 bits. Memory requirements to obtain this security reduction are negligible.

For details, see http://www.mat.dtu.dk/people/S.Thomsen/bmw/bmw-pseudo.pdf.

Best regards,
/Søren

--
Søren Steffen Thomsen
Postdoctoral researcher
DTU Mathematics

Technical University of Denmark
Department of Mathematics
Matematiktorvet 303S
Building 303S
2800 Kgs. Lyngby
Direct +45 4525 3010
Mobile +45 2290 5443
S.Thomsen@mat.dtu.dk
www.mat.dtu.dk/