Subject: OFFICIAL COMMENT:NaSHA
From: Aleksandra Mileva <aleksandra.mileva@ugd.edu.mk>
Date: Sat, 17 Jan 2009 22:07:25 +0100
To: <hash-function@nist.gov>
CC: <hash-forum@nist.gov>

We have proved that the collision attack on NaSHA-512, suggested by Li Ji, Xu Liangyu and Guan Xu in "Collision attack on NaSHA-512" (http://eprint.iacr.org/2008/519) is in fact a conditional attack with unknown probability. You can find our answer in "On a Conditional Collision Attack on NaSHA-512" (http://eprint.iacr.org/2009/034).

Smile Markovski and Aleksandra Mileva

Subject: OFFICIAL COMMENT:NaSHA
From: Aleksandra Mileva <aleksandra.mileva@ugd.edu.mk>
Date: Mon, 23 Feb 2009 09:12:06 +0100
To: <hash-function@nist.gov>
CC: <hash-forum@nist.gov>

Dear all,
First and most important, we have response to the second collision attack on NaSHA-384/512, on http://inf.ugd.edu.mk/images/stories/file/Mileva/response.pdf.
We confirmed that the attack of Zhimin Li and Daofeng Li (http://eprint.iacr.org/2009/026), is a variation of the previous one (http://eprint.iacr.org/2008/519). The attackers claiming about probability of the attack will be true if a system of two quasigroup equations with five variables always has a solution. This is not generally true, so the probability of the attack is unknown, and attackers need to find it, and then to speak about succesufful attack on NaSHA-384/512. It is easy to find systems of quasigroup equations with more variables and without solutions for quasigroup of different order.

Secondly, we have new official web page for NaSHA
http://inf.ugd.edu.mk/images/stories/file/Mileva/nasha_hf.html

From: hash-forum@nist.gov on behalf of Aleksandra Mileva [aleksandra.mileva@ugd.edu.mk]
Sent: Friday, July 03, 2009 6:35 AM
To: Multiple recipients of list
Subject: OFFICIAL COMMENT:NaSHA

Dear NIST and all,
http://inf.ugd.edu.mk/images/stories/file/Mileva/CD_NIST3.rar is the link to the our latest version of NaSHA with the tweak on 384/512 version, mansioned in presentation in Leuven. We have corrected KAT_MCT values for 384/512 version. The speed of the optimized 32-bit version on defined reference platform is 34.56 cycles/byte for 224/256 version and 35.58/37.16 cycles/byte for 384/512 version. The speed of the optimized 64-bit version on defined reference platform is 23.06 cycles/byte for 224/256 version and 24.52 cycles/byte for 384/512 version.
Best regards,
Aleksandra Mileva