Subject: OFFICIAL COMMENT: AURORA-512 and AUROA-384
From: Stefan.Lucks@uni-weimar.de
Date: Wed, 11 Mar 2009 04:47:22 -0400
To: Multiple recipients of list <hash-forum@nist.gov>

Dear NIST, dear all,

we (Niels Ferguson and myself) have written a paper on attacking the wide-state versions of AURORA. The paper has been submitted to the IACR ePrint server as ePrint 2009/113:

  Attacks on AURORA-512 and the Double-Mix Merkle-Damgaard Transform

  http://eprint.iacr.org/2009/113

Abstract: We analyse the Double-Mix Merkle-Damgaard construction (DMMD) used in the AURORA family of hash functions. We show that DMMD falls short of providing the expected level of security. Specifically, we are able to find 2nd pre-images for AURORA-512 in time 2^{291}, and collisions in time 2^{234.4}. A limited-memory variant finds collisions in time 2^{249}.

This is a write-up of the concerns we raised during the conference in Leuven, at February 27, after Tetsu Iwata's presentation of AURORA.

Stefan Lucks

```
--
------ Stefan Lucks   --  Bauhaus-University Weimar  --   Germany  ------
               Stefan dot Lucks at uni minus weimar dot de
------  I  love  the  taste  of  Cryptanalysis  in  the  morning!  ------
```

Subject: OFFICIAL COMMENT: AURORA
From: Tetsu Iwata <iwata@cse.nagoya-u.ac.jp>
Date: Sun, 22 Mar 2009 17:47:25 +0900
To: hash-function@nist.gov
CC: hash-forum@nist.gov

Dear NIST, dear all,

Three papers, by Sasaki, and Ferguson and Lucks, have been uploaded on the IACR ePrint archive (2009/106,112,113).
We, the AURORA team, confirmed that the claimed time and memory of these attacks on AURORA-384/512 are correct, and they work as claimed.
It turns out that AURORA-384/512 do not achieve the expected strength, and these hash functions are wounded (rather than broken, according to the definition of NIST).

To mitigate the security threats, one option may be to insert the mix function after every message block (instead of every eight message blocks), but this is still wounded.
Another option may be to use other domain extension (e.g., Lucks, Asiacrypt'05 or Hirose, FSE'06). We will continue to explore the possible tweaks, and we will update our website when we have a better solution.

We would like to emphasize that these attacks do not have any impact on AURORA-224/256, and these hash functions remain one of the smallest hash functions in hardware. We therefore would like NIST and the community to continue to evaluate AURORA.

Best regards,
Tetsu Iwata

From: hash-forum@nist.gov on behalf of Tetsu Iwata [iwata@cse.nagoya-u.ac.jp]
Sent: Thursday, May 28, 2009 2:41 AM
To: Multiple recipients of list
Subject: OFFICIAL COMMENT: AURORA

Dear NIST, dear all,

We'd like to notice additional information of the hash family AURORA.
One is a report on hardware implementation of AURORA-224/256, and the other is about a possible tweak of AURORA-384/512.

In the first candidate conference, we mentioned smaller hardware implementation of AURORA-224/256. A technical report of the small hardware architecture which processes an F-function per 1 clock cycle is now available. Using the architecture, AURORA-256 can be implemented with only 8,870 gates where the throughput is more than 1Gpbs.

Also, informatively, we propose a possible tweak of AURORA-384/512.
The updated AURORA-512 employs Hirose's DBL construction in place of the DMMD (Double-Mix Merkle-Damgaard) transform which has been reported vulnerable to certain classes of attacks.

Consequently, the tweak prevents the attacks which were applied on the DMMD. Also, the impacts on performance are limited. On the NIST reference platform (64-bit), the updated AURORA-512 achieves 37.8 cycles/byte. In hardware implementation using 0.13um CMOS ASIC library, the smallest size is 12.4K gates and the highest throughput is 6.9 Gbps.

More details on the small hardware implementation of AURORA-256 and the updated AURORA-512 are available from:
 http://www.sony.net/aurora
The reference codes and test vectors of the updated AURORA-512 will be uploaded soon.

Best regards,
Tetsu Iwata