From: hash -forum@nist.gov on behalf of Thomas PEYRIN [Thomas.PEYRIN@ingenico.com]
Sent: Tuesday, August 17, 2010 10:25 AM
To: Multiple recipients of list
Subject: OFFICIAL COMMENT: ECHO (Round 2)

Dear all,

According to NIST's request, the website of the ECHO hash function available at

http://crypto.rd.francetelecom.com/ECHO

has been updated and augmented.

The changes include:

1) A new section providing details about all security analyses we are aware of, including the latest results that will be presented at the upcoming SHA-3 conference.

2) Our proof for the number of active S-boxes for ECHO has now a better bound: instead of the 125 active S-boxes for 4 rounds, we are able to prove that there are at least 200 active S-boxes for 4 rounds. This sheds light on the differential paths currently used against ECHO as it shows that they are actually very close to being optimal. The proof can be read from our updated specification document: http://crypto.rd.francetelecom.com/echo/doc/echo_description_2-0.pdf

3) We report new benchmarks on AES-NI processors run on a Core i5. ECHO is running at 6.8 c/B, which makes it one of the fastest semi-finalists on today's platforms.

4) We provide new benchmarks comparing the performances on legacy processors Pentiums 2, 3 , and 4 based on the eBASH framework and implementations available in the latest version of eBASH for all semi-finals candidates.

5) We provide a hardware section listing the implementations we are aware of. We also report a high-throughput FPGA implementation of ECHO running at 29.5 Gbit/sec, which makes it one of the fastest semi-finalists on FPGA.

See you in Santa Barbara !

The ECHO designers.

From: hash-forum@nist.gov on behalf of Thomas Peyrin [thomas.peyrin@gmail.com]
Sent: Tuesday, November 09, 2010 9:48 PM
To: Multiple recipients of list
Subject: OFFICIAL COMMENT: ECHO (Round 2) - clarifying analysis results

Dear all,

Recently J. Jean and P-A. Fouque posted an article on eprint (http://eprint.iacr.org/2010/569). This article indicates that there are some errors in attacks on reduced-round ECHO that were presented at SAC 2010 and the SHA-3 conference (http://eprint.iacr.org/2010/321). More precisely, there are issues in the analysis of "the final merging phase" of the attack (which makes it work only with probability 2^-128) and this impacts all the results from the SAC 2010 article. It is not clear yet how many rounds have to be removed from the previous attack claims. J. Jean and P-A. Fouque provide in their article a collision attack on 4 rounds of the compression function with the same method, but without this issue (whereas the SAC 2010 paper claimed a collision attack on 4 rounds of the hash function).

We have therefore updated our ECHO security webpage to take account of this news and, to summarize, the current best attacks on *the ECHO compression function* are as follows. We emphasize that both ECHO compression function and hash function offer a very large security margin for collision or distinguishing attacks.

- 256-bit version (simple pipe):
collision attack on 4 rounds over 8
distingu. attack on 4 rounds over 8

- 512-bit version (simple pipe):
collision attack on 4 rounds over 10
distingu. attack on 4.5 rounds over 10

- 256-bit version (double pipe):
collision attack on 4 rounds over 8
distingu. attack on 4.5 rounds over 8

- 512-bit version (double pipe):
collision attack on 4 rounds over 10
distingu. attack on 6.5 rounds over 10

Concerning the hash function, please note that the only analysis conducted so far was in the SAC 2010 paper, thus subject to the final merging phase problem.

Please see http://crypto.rd.francetelecom.com/ECHO/security/ for more details.

The ECHO team.

From: hash-forum@nist.gov on behalf of Martin Schläffer [martin.schlaeffer@iaik.tugraz.at]
Sent: Monday, November 22, 2010 12:20 PM
To: Multiple recipients of list
Subject: Re: OFFICIAL COMMENT: ECHO (Round 2) - clarifying analysis results

Dear all,

thanks to J. Jean and P.-A. Fouque for their analysis of ECHO. Indeed,
there is an additional 128-bit condition due to the low rank of the
combined MixColumns/BigMixColumns transformation.

Since there is still lots of freedom available in the attacks on ECHO,
this condition can be solved efficiently using a meet-in-the-middle
approach. Moreover, exactly the low rank of the combined
MixColumns/BigMixColumns transformation allows to extend the collision
attack by one round to (5 out of 8) rounds of the ECHO-256 *hash function*.

The corrected and improved attacks on the ECHO-256 hash function and on
the ECHO-256 compression function (for up to 7 out of 8 rounds with
chosen salt) are now available at http://eprint.iacr.org/2010/588.

Kind regards,
Martin

Thomas Peyrin wrote:
> Dear all,
>
> Recently J. Jean and P-A. Fouque posted an article on eprint
> (http://eprint.iacr.org/2010/569). This article indicates that there are
> some errors in attacks on reduced-round ECHO that were presented at SAC
> 2010 and the SHA-3 conference (http://eprint.iacr.org/2010/321). More
> precisely, there are issues in the analysis of "the final merging phase"
> of the attack (which makes it work only with probability 2^-128) and
> this impacts all the results from the SAC 2010 article. It is not clear
> yet how many rounds have to be removed from the previous attack claims.
> J. Jean and P-A. Fouque provide in their article a collision attack on 4
> rounds of the compression function with the same method, but without
> this issue (whereas the SAC 2010 paper claimed a collision attack on 4
> rounds of the hash function).
>
> We have therefore updated our ECHO security webpage to take account of
> this news and, to summarize, the current best attacks on *the ECHO
> compression function* are as follows. We emphasize that both ECHO
> compression function and hash function offer a very large security
> margin for collision or distinguishing attacks.
>
> - 256-bit version (simple pipe):
> collision attack on 4 rounds over 8
> distingu. attack on 4 rounds over 8
>
> - 512-bit version (simple pipe):
> collision attack on 4 rounds over 10
> distingu. attack on 4.5 rounds over 10
>
> - 256-bit version (double pipe):
> collision attack on 4 rounds over 8
> distingu. attack on 4.5 rounds over 8

>
> - 512-bit version (double pipe):
> collision attack on 4 rounds over 10
> distingu. attack on 6.5 rounds over 10
>
>
> Concerning the hash function, please note that the only analysis
> conducted so far was in the SAC 2010 paper, thus subject to the final
> merging phase problem.
>
> Please see http://crypto.rd.francetelecom.com/ECHO/security/ for more
> details.
>
> The ECHO team.