Subject: OFFICIAL COMMENT: ESSENCE
From: Søren Steffen Thomsen <S.Thomsen@mat.dtu.dk>
Date: Sat, 24 Jan 2009 11:30:25 +0100
To: "hash-function@nist.gov" <hash-function@nist.gov>
CC: "hash-forum@nist.gov" <hash-forum@nist.gov>

Hi,

we (Nicky Mouha, Meltem Sönmez Turan, and myself) made some observations of non-randomness in the ESSENCE compression function. These include an input leading to the zero output, as well as slid pairs.
The observations are presented in a note available at
http://www.mat.dtu.dk/people/S.Thomsen/essence/Essence-obs.pdf.

Best regards,
Søren.

--
Søren Steffen Thomsen
PH.D.-student
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/

From: hash-forum@nist.gov on behalf of Maria Naya [maria.naya.plasencia@gmail.com]
Sent: Tuesday, June 16, 2009 9:40 AM
To: Multiple recipients of list
Subject: OFFICIAL COMMENT: ESSENCE

Dear all,

We have found shortcut collision attacks on ESSENCE, reported in the following note:
http://www.131002.net/data/papers/NRALMP09.pdf

Our attacks find collisions on the full ESSENCE-256 in about 2^109 trials, and on the full ESSENCE-512 in about 2^198, and they use negligible memory. The designer, Jason Worth Martin, has been informed of our results.

This work is parallel to but not independent of that of Mouha et al. Our results are complementary, and do not overlap. In particular, we use distinct differential characteristics, and we developed distinct techniques to search efficiently for conforming messages.

Best regards,

Andrea Röck
Jean-Philippe Aumasson
Gaëtan Leurent
Willi Meier
Thomas Peyrin
and
María Naya-Plasencia

From: hash-forum@nist.gov on behalf of Jean-Philippe Aumasson [jeanphilippe.aumasson@gmail.com]
Sent: Tuesday, June 23, 2009 4:05 AM
To: Multiple recipients of list
Subject: Re: OFFICIAL COMMENT: ESSENCE

We have revised the note cited below with improved attack complexities: a collision can now be found within fewer than 2^91 compression-equivalent computations for ESSENCE-256, and fewer than 2^168 for ESSENCE-512, with negligible memory requirements.

On Tue, Jun 16, 2009 at 3:39 PM, Maria Naya<maria.naya.plasencia@gmail.com> wrote:

> Dear all,
>
> We have found shortcut collision attacks on ESSENCE, reported in the
> following note:
> http://www.131002.net/data/papers/NRALMP09.pdf
>
> Our attacks find collisions on the full ESSENCE-256 in about 2^109
> trials, and on the full ESSENCE-512 in about 2^198, and they use
> negligible memory. The designer, Jason Worth Martin, has been informed of our results.
>
> This work is parallel to but not independent of that of Mouha et al.
> Our results are complementary, and do not overlap. In particular, we
> use distinct differential characteristics, and we developed distinct
> techniques to search efficiently for conforming messages.
>
> Best regards,
>
> Andrea Röck
> Jean-Philippe Aumasson
> Gaëtan Leurent
> Willi Meier
> Thomas Peyrin
> and
> María Naya-Plasencia
>