Subject: OFFICIAL COMMENT: TIB3
From: Miguel Montes <miguel.montes@gmail.com>
Date: Sat, 17 Jan 2009 17:17:27 -0200
To: hash-function@nist.gov
CC: hash-forum@nist.gov

Dear all:
Yesterday Florian Mendel and Martin Schläffer sent us a pseudo-collision and collision attack on a hash function very similar to TIB3.
This work showed us a mistake in our testing suite, and we have been able to find a pseudo-collision attack in the actual TIB3-256 which can be extended to a collision attack on the hash function with complexity we estimate is 2**116. This is due to the underlying cipher having a differential characteristic of low weight we had previously not seen because of the mistake in our testing suite. TIB3-512 is also vulnerable to this pseudo-collision attack.

TIB3 can be easily modified to block the attack, but given the rules of the game, we understand the probability of getting to the second round is very low (we estimate this probability to be 2**(-128*number of contestants)).

Credit is due to Florian and Martin. We are sure they are working now in the actual TIB3, and soon they will publish their results.

Miguel Montes and Daniel Penazzi

Subject: Re: OFFICIAL COMMENT: TIB3
From: Martin Schläffer <martin.schlaeffer@iaik.tugraz.at>
Date: Tue, 20 Jan 2009 09:41:57 -0500
To: Multiple recipients of list <hash-forum@nist.gov>

Dear all,

Miguel Montes wrote:
> Credit is due to Florian and Martin. We are sure they are working now in the actual TIB3, and soon they will publish their results.

Thanks for the credit, we have published the results in the sha3zoo now:
http://ehash.iaik.tugraz.at/uploads/2/2b/Tib3-pseudo.pdf

Martin

Subject: Re: OFFICIAL COMMENT: TIB3
From: "Wei Dai" <weidai@weidai.com>
Date: Sun, 25 Jan 2009 17:03:18 -0500
To: Multiple recipients of list <hash-forum@nist.gov>

> Yesterday Florian Mendel and Martin Schläffer sent us a pseudo-collision and
> collision attack on a hash function very similar to TIB3.
> This work showed us a mistake in our testing suite, and we have been able to
> find a pseudo-collision attack in the actual TIB3-256 which can be extended
> to a collision attack on the hash function with complexity we estimate is
> 2**116. This is due to the underlying cipher having a differential
> characteristic of low weight we had previously not seen because of the
> mistake in our testing suite. TIB3-512 is also vulnerable to this
> pseudo-collision attack.

Miguel and Daniel, can you please describe the collision attack on TIB3-256 with estimate complexity of 2**116?

I have read Florian and Martin's paper, which gives a collision attack with estimated complexity of 2**122.5. However, the description of the extension from pseudo-collision to collision seems incomplete, and I cannot figure out how to fill in the blanks in a way that achieves complexity less than 2**127. I sent the authors a query a couple of days ago, but have not heard back from them yet.

I just noticed that you gave an even lower estimate of 2**116, which would seem to improve upon Florian and Martin's techniques. Please share the attack so I and others can learn from it.

Subject: Re: OFFICIAL COMMENT: TIB3
From: Miguel Montes <miguel.montes@gmail.com>
Date: Mon, 26 Jan 2009 11:29:58 -0500
To: Multiple recipients of list <hash-forum@nist.gov>

That number (2**116) was wrong. We found the same characteristics as Florian and Martin. There are slightly more than 2**11 characteristics, so we rounded to 12. (256/2)-12 = 116. It should be (256-12)/2, (or (256-11)/2, as in their paper).

Miguel Montes

On Sun, Jan 25, 2009 at 8:01 PM, Wei Dai <weidai@weidai.com> wrote:

> Yesterday Florian Mendel and Martin Schläffer sent us a pseudo-collision and collision attack on a hash function very similar to TIB3.
> This work showed us a mistake in our testing suite, and we have been able to find a pseudo-collision attack in the actual TIB3-256 which can be extended to a collision attack on the hash function with complexity we estimate is 2**116. This is due to the underlying cipher having a differential characteristic of low weight we had previously not seen because of the mistake in our testing suite. TIB3-512 is also vulnerable to this pseudo-collision attack.

Miguel and Daniel, can you please describe the collision attack on TIB3-256 with estimate complexity of 2**116?

I have read Florian and Martin's paper, which gives a collision attack with estimated complexity of 2**122.5. However, the description of the extension from pseudo-collision to collision seems incomplete, and I cannot figure out how to fill in the blanks in a way that achieves complexity less than 2**127. I sent the authors a query a couple of days ago, but have not heard back from them yet.

I just noticed that you gave an even lower estimate of 2**116, which would seem to improve upon Florian and Martin's techniques. Please share the attack so I and others can learn from it.