Subject: OFFICIAL COMMENT: Waterfall
From: "Scott Fluhrer" <sfluhrer@cisco.com>
Date: Fri, 19 Dec 2008 17:58:14 -0500
To: <hash-function@nist.gov>
CC: <hash-forum@nist.gov>

I have submitted initial cryptographical results at http://eprint.iacr.org/2008/531.pdf . If these results are correct, this shows a weakness in collision resistance.

Subject: OFFICIAL COMMENT: Waterfall is broken
From: "Bob Hattersley" <bob.hattersley@optaconsulting.co.uk>
Date: Sat, 20 Dec 2008 06:55:42 -0500
To: Multiple recipients of list <hash-forum@nist.gov>

Scott Fluhrer of Cisco has found a 2^70 collision attack on Waterfall. His paper is available on ePrint. I hereby withdraw from the competition.

I realise that I failed to think clearly about collision attacks at all. I believe the first and second preimage resistance is unaffected, but the collision weakness is fundamental - I can't see any way of patching it up. So you will be spared any embarrassing attempts to tune numbers of rounds etc.. I don't think there is much useful to be dragged from the wreckage except perhaps the message "don't try this".

Bob Hattersley

Subject: Re: OFFICIAL COMMENT: Waterfall is broken
From: Richard Outerbridge <outer@sympatico.ca>
Date: Sat, 20 Dec 2008 20:40:43 -0500
To: Multiple recipients of list <hash-forum@nist.gov>

On Dec 20, 2008, at 06:55, Bob Hattersley wrote:

> Scott Fluhrer of Cisco has found a 2^{70} collision attack on Waterfall. His paper is available on ePrint. I hereby withdraw from the competition.
>
> I realise that I failed to think clearly about collision attacks at all. I believe the first and second preimage resistance is unaffected, but the collision weakness is fundamental - I can't see any way of patching it up. So you will be spared any embarrassing attempts to tune numbers of rounds etc.. I don't think there is much useful to be dragged from the wreckage except perhaps the message "don't try this".
>
> Bob Hattersley

Hey, thanks for trying.

Richard