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.
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
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