Subject: OFFICIAL COMMENT: Abacus
From: "Neil Sholer" <neil@wavestrong.com>
Date: Tue, 23 Dec 2008 06:37:48 -0800
To: <hash-function@nist.gov>
CC: <hash-forum@nist.gov>

Hi all,

I would like to announce a parametric change to my submission algorithm, "Abacus".

The change is as follows:

1. Change the length of the rb[], rc[], and rd[] registers to 65, 66, and 67 bytes, respectively.
2. Change the tap positions of rb[], rc[], and rd[] to be at 62, 56, and 38, respectively.

This has the effect of increasing Abacus's internal state size from 136 bytes to 203 bytes (i.e. from 1088 bits to 1624 bits). Also, the change should make Abacus resistant to the attack of Nikolic and Khovratovich.

I would appreciate comments on this change. In particular, does it meet NIST's requirements for a "trivial fix"?

Thank You,
Neil Sholer