

**Subject:** OFFICIAL COMMENT: Vortex - simple correlation on some of the output bits  
**From:** Niels Ferguson <niels@microsoft.com>  
**Date:** Sun, 14 Dec 2008 17:38:29 -0800  
**To:** "hash-function@nist.gov" <hash-function@nist.gov>  
**CC:** "hash-forum@nist.gov" <hash-forum@nist.gov>

I think I found a simple correlation on some of the output bits of Vortex.

The hash result is the output of the V function. I'll use the notation of Figure 4 in the Vortex documentation, and use  $X[0]$  to refer to the least significant bit of word X.

new\_B0 and new\_A0 are two of the output words of the function V.  
new\_B0[0] is a function of three bits B1[0], B0[0], and A0[0].  
new\_A0[0] is a function of three bits B0[0], A1[0], and A0[0].

These two functions share inputs and are correlated.  $\text{new\_B0}[0] = \text{new\_A0}[0]$  with probability 5/8. This leads to a trivially detectable output bias, and makes the hash function unsuitable for many applications, including key derivation and Hash\_DRBG from SP800-90.

Let's rename the four input bits to A, B, C, and D, and the two output bits to X and Y. We have:

$$X = (A \& D) \wedge B$$
$$Y = (B \& C) \wedge D$$

If  $A=0$  then  $X = B$  and  $Y = \text{<some expression>} \wedge D$  so both output bits are uncorrelated and unbiased.  
If  $C=0$  the same applies.

But if  $A=C=1$  we have

$$X = D \wedge B$$
$$Y = B \wedge D$$

and thus

$$X = Y$$

So 3/4 of the time the two output bits are unrelated, and 1/4 of the time they are the same, which leads to  $X=Y$  for 5/8 of all inputs.

I haven't verified this experimentally, but the submitters of Vortex agreed with this analysis.

Cheers!

Niels

---

**From:** Michael Kounavis [michael\_kounavis@hotmail.com]  
**Sent:** Saturday, May 30, 2009 3:40 AM  
**To:** hash-function@nist.gov  
**Cc:** hash-forum@nist.gov  
**Subject:** OFFICIAL COMMENT: Vortex - New paper and web page

Hello,

In response to the bit correlation remark posted by Niels and the other published attacks we have posted a new paper titled: "Security Enhancement of the Vortex Family of Hash Functions" that can be found in our algorithm's new web site: <http://math.haifa.ac.il/~vortex>

Regards  
Shay and Michael