

Re: VMPC

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2007-03/msg00818.html>

- *From:* "Wei Dai" <usenet@xxxxxxxxxx>
 - *Date:* Thu, 29 Mar 2007 01:21:48 GMT
-

On Mar 28, 2:16 pm, fortune.br...@xxxxxxxxxx wrote:

It is not a substitute for AES. But it is a wicked fast streaming algorithm that may have use.

The VMPC paper says it runs at 12.7 cycles per byte on a Pentium 4. I wouldn't call that "wicked fast" considering there are now many ciphers that take only 3 to 5 cycles per byte. See <http://www.ecrypt.eu.org/stream/perf/pentium-4-a/>.

So, Wei Dai, other than a possible distinguisher after a solid 18 petabytes of data have been observed (something as an attacker you will never get to see, BTW), where does the weakness come from?

I think the weakness is that the cipher now has no margin of security, so that even a small improvement in cryptanalytic technique may lead to a practical attack. Plus, the cipher is broken enough that with many faster unbroken ciphers around, it probably won't be receiving much further attention from academic cryptographers.

.