

From: (b) (6)
To: [Moody, Dustin \(Fed\)](mailto:Moody.Dustin(Fed)@nist.gov)
Subject: Re: Notes
Date: Tuesday, February 6, 2018 2:04:23 PM

okay. thanks.

On Tue, Feb 6, 2018 at 1:58 PM, Moody, Dustin (Fed) <dustin.moody@nist.gov> wrote:

Do you want me to forward this to internal-pqc?

From: Daniel Smith [mailto:(b) (6)]
Sent: Tuesday, February 06, 2018 1:57 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Notes

Hi, Dustin,

I have a comment on the NSA notes on our process. The thing that caught my attention was the comment about suspicion on sampling from non-uniform distributions.

I'm curious what they have in mind here. There are standard transformations one can use to fairly sample from most distributions via a transform from a uniform distribution. I'm curious if they think that our testing suite is weak against non-uniform distributions. I suspect that we can avoid issues with this by implementing sampling from non-uniform distributions via a transformation from an i.i.d uniform series and using our testing suite on the uniform data. (Alternatively, we can test non-uniform data by using the reverse transform to convert it to uniform and then test for all kinds of properties, such as serial dependence.)

I found this comment very confusing. If it is the case that NIST SP-800-22 is weak against non-uniform distributions, this is something that we should know (and something that the NSA should be obligated to report, I think, under 15 U.S. Code § 278g-3). Also, it would be very strange for NIST SP-800-22 to be weak against non-uniform distributions, since we can just "uniformize" the distributions and run the same tests. It makes no sense.

I'm curious if anyone else had any thoughts on this.

(Sorry to email just you, but I'm away from my NIST machine, right now.)

Cheers,

Daniel