From: Kelsey, John M. (Fed)
To: Moody, Dustin (Fed); internal-pqc
Subject: NSA PQC comments
Date: Tuesday, February 6, 2018 3:42:27 PM

Everyone,

It seems like they were concerned with how the validation labs would handle schemes that needed to generate a lot of non-uniform random numbers. What I think they were getting at is that the schemes for generating these numbers can leak information via timing or other side channels, and it's not clear that FIPS 140 validation would catch that.

--John

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Tuesday, February 6, 2018 at 2:07 PM
To: internal-pqc <internal-pqc@nist.gov>
Subject: FW: Notes

From: Daniel Smith (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