From: Moody, Dustin (Fed)
To: Kelsey, John M. (Fed)
Subject: Re: nitpick
Date: Monday, March 7, 2022 8:53:41 AM

Sounds good. I agree Fiat-Shamir with aborts is what I've heard said the most.

Dustin

From: Kelsey, John M. (Fed) <john.kelsey@nist.gov>
Sent: Saturday, March 5, 2022 12:36 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: nitpick

Dustin,

The Dilithium team refers to their approach as Fiat-Shamir with aborts, which I think is the term of art. It amounts to generating a challenge for a Fiat-Shamir signature, but then trying again if the response would reveal too much information about the private key or would lead to a failure in verification. (I just think of it as a kind of rejection sampling, but I'm not immersed in the lattice crypto literature.)

--John