From: Peralta, Rene (Fed)
To: Perlner, Ray A. (Fed)
Subject: Re: Draft response on benign malleability
Date: Tuesday, August 29, 2017 1:30:45 PM

Hi Ray,

I would remove the comma from "literature, where"

Rene.

From: Perlner, Ray (Fed)
Sent: Tuesday, August 29, 2017 12:07 PM
To: Moody, Dustin (Fed)
Cc: internal-pqc
Subject: Draft response on benign malleability

We prefer that submitters implement their IND-CCA PKE and KEM schemes in the strict sense without benign malleability.

We are not, however, going to remove a scheme from consideration just because the submitted implementation failed to prevent benign malleability. (We may however ask for an implementation without benign malleability later in the process in such cases.) Finally, we would like to remind submitters that the NIST CFP allows submitters to provide KEMs or PKE schemes claiming only IND-CPA, and this is an option in cases where benign malleability cannot easily be prevented by the implementation (although we don't know of any postquantum IND-CCA schemes from the literature, where providing an implementation without benign malleability seems particularly hard.) If an IND-CPA scheme is provided, where the only barrier to IND-CCA is a difficult-to-implement-away benign malleability, we will consider the significance of this property on a case-by-case basis.

--Ray