

From: [Kerman, Sara J. \(Fed\)](#)
To: [Moody, Dustin \(Fed\)](#); [Dworkin, Morris J. \(Fed\)](#)
Subject: RE: 2015 PQC workshop
Date: Monday, April 15, 2019 1:20:28 PM

I don't think we provided webcast/recording of this one. I don't have any speaker waiver forms – which have to be signed before being recorded.

Sara

From: Moody, Dustin (Fed)
Sent: Monday, April 15, 2019 9:15 AM
To: Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>
Cc: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: 2015 PQC workshop

Morrie,

I went back and checked our 2015 PQC workshop, to see what we had on stateful hash-based signatures. We had the following:

- Hash-based Signatures: An outline for a new standard Andreas Hulsing, Stefan-Lukas Gazdag, Denis Butin, Johannes Buchmann
- Let Live and Let Die - Handling the state of Hash-based signatures Stefan-Lukas Gazdag, Denis Butin, Johannes Buchmann
- PANEL: Shoring up the Infrastructure: A strategy for Standardizing Hash Signatures panelists: Andreas Hulsing, David McGrew, Aziz Mohaisen, Russ Housley
- Keynote address by David McGrew: Living with postquantum cryptography

I've attached the papers submitted, the panel proposal, and the slides for the talks that I could find. I don't think we have any video or audio (at least I couldn't find any).

Dustin