From: Peralta, Rene C. (Fed)
To: Moody, Dustin (Fed)
Subject: Re: Rainbow and GeMSS
Date: Tuesday, September 21, 2021 12:13:58 PM

Thanks Dustin.

René.

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Tuesday, September 21, 2021 12:04 PM
To: Peralta, Rene C. (Fed) <rene.peralta@nist.gov>
Subject: Re: Rainbow and GeMSS

Rene,

Yes.

I wouldn't say that we've officially taken any action to that effect, but the cryptanalysis certainly calls their security claims into question. The Rainbow designers have tried to re-but the attack somewhat, but Ray and Daniel don't really buy their argument.

Dustin

From: Peralta, Rene C. (Fed) <rene.peralta@nist.gov>
Sent: Tuesday, September 21, 2021 11:59 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Rainbow and GeMSS

Hi Dustin,

The status of Rainbow and GeMSS is that we've lost confidence in them
due to cryptanalysis, right?

(I'm preparing a talk for tomorrow on PQC)

Thanks, René.