From: Alperin-Sheriff, Jacob (Fed)
To: Moody, Dustin (Fed)
Subject: Re: another paper that probably breaks it
Date: Tuesday, July 11, 2017 4:19:47 PM

Actually, looking at Section 1.2, they clearly have no clue what's going on, as they seem to be trying to prove invulnerability to attacks.

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Tuesday, July 11, 2017 at 3:26 PM
To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>
Subject: another paper that probably breaks it

http://sucra.saitama-u.ac.jp/modules/xoonips/download.php/A1002281.pdf?file_id=1273