From: lwc-forum@list.nist.gov on behalf of Jan Schoone <schoonemath@gmail.com>
Sent: Thursday, February 20, 2020 9:16 AM
To: lwc-forum
Subject: [lwc-forum] OFFICIAL COMMENT: Pyjamask
Attachments: pyj_subm.pdf

Since the previous official comment on Pyjamask (15-08-19), we have worked on our attack on Pyjamask-96 and found that we now indeed have the attack claimed before on the full Pyjamask-96 blockcipher. In the attached paper (that will appear in ToSC 2020 Issue 1), you can read more about it. It does not break the AEAD scheme, but the attack works on 7 out of the 14 rounds.

--