From: Rotella Yann <yann.rotella@gmail.com>
Sent: Thursday, August 15, 2019 8:39 AM
To: lightweight-crypto
Cc: lwc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: Pyjamask
Attachments: main.pdf; sagescryptmonomials.py

Dear all,

We think we have an attack on full Pyjamask-96, the internal block cipher used in one of the version of Pyjamask. Our attack requires however a lot of data and does not threat the security of the proposed Pyjamask AE submission.

Moreover, our attack only works on the 96-bit version and not the 128. We verified our attack on a round reduced version (7 rounds).

Please see attached the documentation and code needed to understand our cryptanalysis.

Best regards,

Christoph Dobraunig, Yann Rotella and Jan Schoone

From: Rotella Yann <yann.rotella@gmail.com>
Sent: Wednesday, August 28, 2019 11:29 AM
To: lightweight-crypto
Cc: lwc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: Pyjamask

Dear all,
We found a flaw in our 14 round attacks, as we miscalculated the complexity of solving the system of equations. Hence, the complexity of what we decribed in the paper present on the mailing list is invalid (only for the 14 round attack) and is above the cost of the exhaustive search.
We're sorry for the designers and hope NIST will consider this e-mail for the fairness of the competition.

Best regards,

Christoph, Yann and Jan