Kerman, Sara J. (Fed)

From: Lorenz Panny <l.s.panny@tue.nl>
Sent: Thursday, December 21, 2017 5:00 PM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: Guess Again

Follow Up Flag: Follow up
Flag Status: Completed

Dear all,

the following Python script quickly recovers the message from a given "Guess Again" ciphertext without knowledge of the private key:

https://yx7.cc/files/guessedonce.py.txt

I have only tried the attack on the ciphertexts in the known-answer tests file so far, but I think there is no reason to believe that it does not work in general.
Notice that the attack is solely based on statistical properties of the ciphertext and does not even require the public key. The script expects the contents of the KAT archive in the same direc- tory (but can easily be modified to decrypt other ciphertexts).

-- Lorenz