From: MEGE, Alexandre <alexandre.mege@airbus.com>
Sent: Monday, June 10, 2019 12:34 PM
To: lightweight-crypto
Cc: lwc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: SIMPLE

Dear All,

It seems simple is vulnerable to forgery attack.

This vulnerability comes from the absence of domain separation between AD and PT processing.

A forgery attack can be created where the padding pattern separating AD and PT data is moved from the correct pattern limit to a decoy pattern embedded in the PT data.

This attack could be solved by using different tweaks for processing the AD and PT part of the input data.

All simple versions seem to be vulnerable.

Ex for simple 128aes10:

Key = 000102030405060708090A0B0C0D0E0F

Nonce = 000102030405060708090A0B0C0D0E

PT = **00000101020203030404050506060701**01**00000101020203030404050506060607**

AD = **00000101020203030404050506060607**

CT = **4D9454CE9579FEE8296A1248821D32**E37C8AA6533A40ABFC792FCFC76AAB8B**B7DDCF79BD269250972DD3FB193590FB**

Key = 000102030405060708090A0B0C0D0E0F

Nonce = 000102030405060708090A0B0C0D0E

PT = **00000101020203030404050506060607**

AD = **00000101020203030404050506060607**01000001**01020203030404050506060607**

CT = **4D9454CE9579FEE8296A1248821D32B7DDCF79BD269250972DD3FB193590FB**

Best regards,

Alexandre Mège