From: MEGE, Alexandre <alexandre.mege@airbus.com>
Sent: Wednesday, June 5, 2019 4:00 AM
To: lightweight-crypto
Cc: lwc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: Sycon

Dear All,

It seems syconaer96128v1 will output same Tag for two packets in some cases if the only differences are in the last bytes of Associated Data D and the values are 80(00) and 00(00) .

It seems there are also collisions in some cases with Associated Data tails being 0x8080,0x 0180 , 0x0080

I was not able to reproduce it for syconaer64128v1.

Best regard,

Alexandre Mege

Ex for syconaer96128v1

Key = 000102030405060708090A0B0C0D0E0F

Nonce = 000102030405060708090A0B0C0D0E0F

PT =

AD = 000001010202030304040505060607**80**

CT = **00495ED7B0C4D7C68EEF975200245441**

Key = 000102030405060708090A0B0C0D0E0F

Nonce = 000102030405060708090A0B0C0D0E0F

PT =

AD = 000001010202030304040505060607**00**

CT = **00495ED7B0C4D7C68EEF975200245441**

And with non empty PT:

Key = 000102030405060708090A0B0C0D0E0F

Nonce = 2A2B2C2D2E2F30313233343536373839

PT = 00

AD = 00000101020203030404050506060707<u>80000000</u>

CT = **<u>5D45F0FC363C8C53A8A549D2A08A4BB455</u>**

Key = 000102030405060708090A0B0C0D0E0F

Nonce = 2A2B2C2D2E2F30313233343536373839

PT = 00

AD = 00000101020203030404050506060707<u>00000000</u>

CT = **<u>5D45F0FC363C8C53A8A549D2A08A4BB455</u>**

And with Associated Data tails being 0x8080,0x 0180 , 0x0080

Key = 00000000000000000001010101010101

Nonce = 2A2B2C2D2E2F30313233343536373839

PT = 00

AD = 00000000000000000000000000000000**<u>0180</u>**

CT = **<u>7511E8F37303ADC8E7A352537D60342912</u>**

Key = 00000000000000000001010101010101

Nonce = 2A2B2C2D2E2F30313233343536373839

PT = 00

AD = 00000000000000000000000000000000**<u>8080</u>**

CT = **<u>7511E8F37303ADC8E7A352537D60342912</u>**

Key = 0000000000000000000010101010101

Nonce = 2A2B2C2D2E2F30313233343536373839

PT = 00

AD = 00000000000000000000000000000000**0080**

CT = **7511E8F37303ADC8E7A352537D60342912**

From: Sumanta Sarkar <sumanta.sarkar@gmail.com>
Sent: Thursday, June 6, 2019 12:21 PM
To: Alexandre; lightweight-crypto
Cc: lwc-forum@list.nist.gov
Subject: [lwc-forum] OFFICIAL COMMENT: Sycon
Attachments: sycon-update-6June.tar.gz

Dear Alexandre and All,

Thanks to Alexandre for pointing out this issue. We would like to inform you that the collision that you have observed is due to an implementation error. The error was in line number 97 of the "encrypt.c" file of syconaer96128v1:

state[i]^=ad[num_ad_block*8+(u64)i];

The correct code needs 12 instead of 8. So this line should be replaced with

state[i]^=ad[num_ad_block*NUMRATEBYTES+(u64)i];

where NUMRATEBYTES is already defined as 12.

Please find the updated implementation as well as the change log attached, and note that our specification does not need any change due to this finding.

Thanks
Sycon Team