From: Rotella Yann <yann.rotella@gmail.com>
Sent: Friday, May 03, 2019 5:43 AM
To: lightweight-crypto
Cc: lwc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: Bleep64
Attachments: ref.zip

Dear All,

In Bleep64, it seems that there is not only problems on the initialization phase pointed out by Samuel Neves.

Indeed, we think we are able to do Tag forgeries with very high probability of success.

We observed very strong differential properties on Bleep64 that allow us to do tag forgery attack targeting the decryption process.
By looking carefully at the algorithm specification, we found that applying a signed difference of +1 at round i will propagate with very high probability on the i+2 ciphertext block, allowing us to produce the same state value for ciphertexts C_1||C_2||C_3 and C_1-1||C_2||C_3+1.

Hence, if an attacker sees a message C_1||C_2||C_3||T, then T will be a valid tag for the same key and nonce and for the specific message C_1-1||C_2||C_3+1 with very high probability.
The only effect that will not pass with probability one is the compatibility of the 2's complement addition and 1's complement addition which is very unlikely to appear.

See the attached code for our attack, where we found that for 10 000 runs, this property holds 9 928 times.
Hence, integrity is not preserved by Bleep64.

Kind regards,

Christoph Dobraunig and Yann Rotella

From: MEGE, Alexandre <alexandre.mege@airbus.com>
Sent: Monday, June 10, 2019 12:31 PM
To: lightweight-crypto
Cc: lwc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: Bleep64

Dear All,

It seems the reference implementation of BLEEP64 is susceptible to forgery attacks.

This issue is visible in the KAT provided with the submission. It seems to happen between messages with AD and PT with 0x00 data at the tail.

Ex:

Count = 1

Key = 000102030405060708090A0B0C0D0E0F

Nonce = 000102030405060708090A0B

PT =

AD =

CT = **3D8536BA75CFAA02**

Count = 2

Key = 000102030405060708090A0B0C0D0E0F

Nonce = 000102030405060708090A0B

PT =

AD = 00

CT = **3D8536BA75CFAA02**

Count = 34

Key = 000102030405060708090A0B0C0D0E0F

Nonce = 000102030405060708090A0B

PT = 00

AD =

CT = **3D8536BA75CFAA02**DA

Count = 35

Key = 000102030405060708090A0B0C0D0E0F

Nonce = 000102030405060708090A0B

PT = 00

AD = 00

CT = **3D8536BA75CFAA02**DA

Best regards,

Alexandre Mège

From: Harry Bartlett <h.bartlett@qut.edu.au>
Sent: Wednesday, June 19, 2019 2:39 AM
To: lightweight-crypto
Cc: lwc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: Bleep64

Hi all:

we have done further analysis on the forgery attack described by Christoph and Yann. Our analysis confirms the validity of their attack and shows that it can be extended straightforwardly to a range of attacks with high success probability.

More specifically,

1. If a ciphertext block with even index (C_{2i}) is changed by an amount d, then an adjusting change of -d can be made at any later even-indexed block C_{2i+2k} and the final state will be unchanged with high probability.

2. If the same changes are made on ciphertext blocks with odd indices (C_{2i+1}, $C_{2i+2k+1}$), the success probability is lower (and decreases with increasing k), because the MSB of the state word y may be affected (which will affect the state contents unpredictably via the optional shift register update).

3. Case 1 can also be extended such that any set of numbers $d_1, \ldots, d_j$ with $\text{Sum}(d_i) = 0 \pmod{2^{32}}$ can be added to distinct ciphertext blocks with even indices, with high probability that the final state is unchanged.

If we assume that the relevant state words are uniformly distributed, the success probability for attacks 1 and 2 can be shown to be as follows:

(1) $1 - 2^{-31}.d + 2^{-63}.d^2 \sim= 1 - 2^{-31}.d$

(2) $(1 - 2^{-31}.d + 2^{-64}.d)[1 - 2d/(2^{32} - 1)]^k$
$+ 2^{-64}.d^2.[1 + (2 - 2d)/(2^{32} - 1)]^k$
$\sim= 1 - 2^{-31}.(k+1)d$

For case 2, we assume $d < 2^{31}$. For both cases, we assume $d << 2^{31}$ for the approximation.

We note that the success rate for case 1 is never lower than 0.5 (for $d = 2^{31}$) and is extremely high (>0.999) even for d as large as $2^{21} \sim= 2*10^6$. Clearly there is a huge scope for forgeries with this cipher.

Regards,

Harry Bartlett, Ed Dawson, Leonie Simpson, Kenneth Wong.

Queensland University of Technology