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