From: MEGE, Alexandre <alexandre.mege@airbus.com>
Sent: Monday, June 3, 2019 5:32 AM
To: lightweight-crypto
Cc: lwc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: Fountain

Dear All,

I have found some tag collision with Fountain reference code.
It seems those collisions are produced when the middle byte of AD changes from 0x80 to 0x01, with same pattern as PT on left and right of this Byte.

Examples:

Key = 000102030405060708090A0B0C0D0E0F
Nonce = 000102030405060708090A0B
PT = 00000101020203030404050506060607
AD = 000001010202030304040505060606078000000101020203030404050506060607
CT = 5274801E6C0131A255F74245E8C0F3384B52EEF66E37734A0789C378FC0A26

Key = 000102030405060708090A0B0C0D0E0F
Nonce = 000102030405060708090A0B
PT = 00000101020203030404050506060607
AD = 000001010202030304040505060606070100000101020203030404050506060607
CT = 5274801E6C0131A255F74245E8C0F3384B52EEF66E37734A0789C378FC0A26

And

Key = 000102030405060708090A0B0C0D0E0F
Nonce = 000102030405060708090A0B
PT = 000001
AD = 00000180000001
CT = 62F8E554A1CADFA82D4BF736FDD03550DCABFC

Key = 000102030405060708090A0B0C0D0E0F
Nonce = 000102030405060708090A0B
PT = 000001
AD = 00000101000001
CT = 62F8E554A1CADFA82D4BF736FDD03550DCABFC

Best regards,
Alexandre Mège

From: Zhang Bin <martin_zhangbin@hotmail.com>
Sent: Monday, June 3, 2019 9:58 AM
To: MEGE, Alexandre; lightweight-crypto
Cc: lwc-forum@list.nist.gov
Subject: 回复: OFFICIAL COMMENT: Fountain

Dear Alexandre,

Thanks for the interest on Fountain and for pointing out this implementation problem in Fountain's reference code, which is resulted from some typos on LFSR numbers inconsistent with the specification. Fountain is invertible by the design. The reference code will be revised soon and there is no change of Fountain's specification.

Best Regards,

Bin Zhang

发件人: MEGE, Alexandre <alexandre.mege@airbus.com>
发送时间: 2019 年 6 月 3 日 17:31
收件人: lightweight-crypto@nist.gov
抄送: lwc-forum@list.nist.gov
主题: [lwc-forum] OFFICIAL COMMENT: Fountain

Dear All,

I have found some tag collision with Fountain reference code.
It seems those collisions are produced when the middle byte of AD changes from 0x80 to 0x01, with same pattern as PT on left and right of this Byte.

Examples:

Key = 000102030405060708090A0B0C0D0E0F
Nonce = 000102030405060708090A0B
PT = 00000101020203030404050506060707
AD = 0000010102020303040405050606078000000101020203030404050506060 7
CT = 5274801E6C0131A255F74245E8C0F3384B52EEF66E37734A0789C378FC0A26

Key = 000102030405060708090A0B0C0D0E0F
Nonce = 000102030405060708090A0B
PT = 00000101020203030404050506060 7
AD = 0000010102020303040405050606070100000101020203030404050506060 7
CT = 5274801E6C0131A255F74245E8C0F3384B52EEF66E37734A0789C378FC0A26

And

Key = 000102030405060708090A0B0C0D0E0F

From:	raluca.e.posteuca@gmail.com
Sent:	Thursday, June 6, 2019 3:33 AM
To:	lightweight-crypto
Cc:	lwc-forum@list.nist.gov
Subject:	OFFICIAL COMMENT: Fountain

Dear author,

We have analyzed Fountain and we found the following results regarding its security.

For each (Key, IV) pair, with probability 2^(-32), after 48 steps of the initialization phase, there exists an internal state with the same properties as the output of the loading phase (the constants are in the same positions). Based on this observation, we have designed a slide attack, that leads to predictable ciphertexts (up to 40 bits long) with a time complexity of up to 12 × (2 ^ 80). Moreover, computing the ciphertexts' XOR, we can also recover up to 8 bits of the internal state and up to 4 equations involving bits of the internal state.

Best regards,

Raluca Posteuca

COSIC, KU Leuven

From: Zhang Bin <martin_zhangbin@hotmail.com>
Sent: Thursday, June 6, 2019 10:21 PM
To: raluca.e.posteuca@gmail.com; lightweight-crypto
Cc: lwc-forum@list.nist.gov
Subject: 回复: [lwc-forum] OFFICIAL COMMENT: Fountain
Attachments: New reference code of Fountain v1.zip

Dear all,

Please find the new reference code for Fountain and the report file as attached, which corrected the previous mentioned implementation errors that are inconsistent with the specification, and may affect the reading of the report and cross-checking of the design. There is no change of Fountain's specification, only the test vectors in Chapter 7 of the report file are revised accordingly. There is also a Chapter 8 in the document to record the change log.

Please refer to the attached package for the details. Thanks.

Dear Raluca,

Thanks for the interest on Fountain and the analysis. I would appreciate if the details of the mentioned attack could be provided.

Best Regards,

Bin Zhang

发件人: raluca.e.posteuca@gmail.com <raluca.e.posteuca@gmail.com>
发送时间: 2019 年 6 月 6 日 15:32
收件人: lightweight-crypto@nist.gov
抄送: lwc-forum@list.nist.gov
主题: [lwc-forum] OFFICIAL COMMENT: Fountain

Dear author,
We have analyzed Fountain and we found the following results regarding its security.
For each (Key, IV) pair, with probability 2^(-32), after 48 steps of the initialization phase, there exists an internal state with the same properties as the output of the loading phase (the constants are in the same positions). Based on this observation, we have designed a slide attack, that leads to predictable ciphertexts (up to 40 bits long) with a time complexity of up to 12 × (2 ^ 80). Moreover, computing the ciphertexts' XOR, we can also recover up to 8 bits of the internal state and up to 4 equations involving bits of the internal state.
Best regards,
Raluca Posteuca
COSIC, KU Leuven

From: Zhang Bin <martin_zhangbin@hotmail.com>
Sent: Thursday, June 20, 2019 10:24 PM
To: raluca.e.posteuca@gmail.com; lightweight-crypto
Cc: lwc-forum@list.nist.gov
Subject: 回复: [lwc-forum] OFFICIAL COMMENT: Fountain

Dear Raluca,

Thanks again for the interest on Fountain. Since the details of the designed slide attack have not been revealed so far, I just present some analysis on the feasibility of launching a slide attack on Fountain.

The first concern is how to identify the slide pairs when the key is unknown and what is the complexity for doing so. Precisely, in the single key model (in which Fountain has claimed 112-bit security), after 48 steps of initialization, the nonlinear feedbacks has affected 192 state bits, and the least significant two bytes of each register are shifted results from itself. If the attacker manipulates the three IV byte positions, IV_0, IV_4 and IV_8 by choosing the appropriate IV's such that IV_0=IV'_3, IV_4=IV'_7 and IV_8=IV'_11 to meet these three bytes sliding conditions, he still has to deal with the other state bits to meet the sliding conditions, that is the two states are slidable if and only if the full 256-bit state conditions are satisfied, not only the 32-bit constants conditions. But now all the other 256-3*8=232 bit positions are either affected by the unknown key or are the shifted constant values and the 192 feedback positions correspond to a non-linear system of algebraic equations. Thus, the probability that (key, IV) and (key, IV') are slide pairs is 2^(-232) after the manipulating the IV values, not 2^(-32) when the key is unknown. Thus to detect such a slide pair with the appropriate IVs, one has to randomly change the value of IVs to meet the 232 bit conditions, which will have a complexity much higher than 2^(112). Besides, if we take into account the data/memory complexities for fulfilling this task, the complexity will definitely exceed the 112-bit bound.

In the relate-key model (in which Fountain has made no claims), similar analysis also holds and it seems difficult to generate the slide pairs and the complexity for doing so is well above the 112-bit security bound.

If we assume the adversary is able to solve the non-linear algebraic system which describes the inherent relation between the sliding state pairs, we cannot assure that the captured keystream is just related to the specific value and the complexity to find the exact sliding partner is well above the claimed security bound.

Thus if I am not wrong, based on the above analysis, Fountain is immune to the slide attacks.

Best Regards,

Bin Zhang

发件人: raluca.e.posteuca@gmail.com <raluca.e.posteuca@gmail.com>
发送时间: 2019 年 6 月 6 日 15:32
收件人: lightweight-crypto@nist.gov
抄送: lwc-forum@list.nist.gov
主题: [lwc-forum] OFFICIAL COMMENT: Fountain

Dear author,
We have analyzed Fountain and we found the following results regarding its security.
For each (Key, IV) pair, with probability 2^(-32), after 48 steps of the initialization phase, there exists an internal state with the same properties as the output of the loading phase (the constants are in the same positions). Based on this observation, we have designed a slide attack, that leads to predictable ciphertexts (up to 40 bits long) with a time

From: raluca.e.posteuca@gmail.com
Sent: Wednesday, August 14, 2019 2:10 AM
To: lightweight-crypto
Cc: lwc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: Fountain

Dear all,

Sorry for the late answer. Please find details regarding the related- key differential slide attack on Fountain v1 at https://eprint.iacr.org/2019/920.pdf.

Kind regards,
Raluca Posteuca

From: Zhang Bin <martin_zhangbin@hotmail.com>
Sent: Thursday, August 22, 2019 6:31 AM
To: raluca.e.posteuca@gmail.com; lightweight-crypto
Cc: lwc-forum@list.nist.gov
Subject: 回复: [lwc-forum] OFFICIAL COMMENT: Fountain

Dear Raluca,

Thanks again for the interest on Fountain and for analyzing it against related-key differential slide attack, though Fountain has made no claims in related-key model so far.

If I am not wrong, the known-key case is different from the secret key case when mounting a slide attack. The analysis presented in my last post on Fountain in the forum on 21/06/2019 could be extended to the related-key model as well. When the key is unknown, the two states are slidable if and only if the full 256-bit conditions are satisfied, not only the 32-bit constants conditions. The probability that (key_1, IV_1) and (key_2, IV_2) are slide pairs is 2^(-232), not 2^(-32) when the key is unknown, though the probability 2^(-32) is verified in experiments in the known-key case. Thus when preparing the data set in the secret key case, 2^80 is not enough for the data complexity, the actual complexity will be well above the 2^112 bound.

Besides, in order to overcome the difficulty of identifying the related-key slide pairs when the key is unknown and the related key is associated with it by a non-linear system of algebraic equations, the attacker uses an oracle which could extract the intermediate state update information under one key/iv pair and do the second encryption with a different key/iv pair (Section 4.2, the two hypotheses part). This side-channel information will release the high-complexity (well above 2^112) burden to identify the slide pair in the normal/standard related-key model.
I think such a side-channel information will make the presented attack less relevant to the security of Fountain.

The second result is some state transition properties of Fountain in the known-key model. When the key is known in an authenticated cipher, the security is already compromised completely.

Best Regards,

Bin Zhang

发件人: raluca.e.posteuca@gmail.com <raluca.e.posteuca@gmail.com>
发送时间: 2019 年 8 月 14 日 14:10
收件人: lightweight-crypto@nist.gov <lightweight-crypto@nist.gov>
抄送: lwc-forum@list.nist.gov <lwc-forum@list.nist.gov>
主题: [lwc-forum] OFFICIAL COMMENT: Fountain

Dear all,

Sorry for the late answer. Please find details regarding the related- key differential slide attack on Fountain v1 at https://eprint.iacr.org/2019/920.pdf.

Kind regards,
Raluca Posteuca