From:	Bart Mennink <b.mennink@cs.ru.nl>
Sent:	Friday, March 20, 2020 5:06 AM
To:	lightweight-crypto
Cc:	b.mennink@cs.ru.nl; Christoph Dobraunig
Subject:	ROUND 2 OFFICIAL COMMENT: PHOTON-Beetle
Attachments:	photon-beetle-attack.pdf

Dear all,

We noted an inconsistency in the security claims of PHOTON-Beetle, leading to a generic key recovery attack faster than the claimed bounds.
Please find the corresponding note in attach. The inconsistency seems to stem from the fact that the earlier security proof of Beetle only captured this attack for the case of verification queries; the newest proof fixed this issue, but the change seems to be overlooked in the design document of PHOTON-Beetle.

We point out that our observation does not seriously threaten PHOTON-Beetle and that the problem is easily resolved by updating the security claims.

Best regards,
Christoph and Bart.

Key Recovery Attack on PHOTON-Beetle

Christoph Dobraunig and Bart Mennink

[1] Graz University of Technology, Graz, Austria
christoph@dobraunig.com
[2] Digital Security Group, Radboud University, Nijmegen, The Netherlands
b.mennink@cs.ru.nl

1 Beetle

The PHOTON-Beetle submission [1] to the NIST Lightweight Cryptography competition uses a variant of the Beetle is an authenticated encryption scheme by Chakraborti et al. [2]. We will describe a key recovery attack for a specific version of the mode, namely with *no* associated data and *no* message block. For this specific case, the mode is depicted in Figure 1. Here, f is the 256-bit Photon permutation [4], it gets as input a 128-bit key, a 128-bit nonce, and it outputs a 128-bit tag.

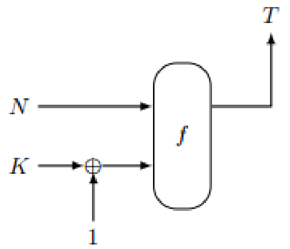

Fig. 1: Beetle mode for no associated data and no message block.

2 Attack

The key recovery attack is performed as follows:

(1) Make q_e queries for different nonces N_i to get tags T_i;
(2) Find an α-fold collision in the tags, i.e., such that α values i satisfy $T_i = T^\star$ for some $T^\star$;
(3) Make q_p queries $p^{-1}(T^\star \| Z_j)$ for varying Z_j. If the outcome is of the form $N_i \| K^\star$ for some of the i's in the α-fold collision, verify the key by making one more encryption query.

We will argue that the attack is expected to succeed for $(q_e, q_p) \approx (2^{122.8}, 2^{124})$. A well-established result [5] says that for

$$q_e = \left(\alpha! \cdot 2^{128(\alpha-1)}\right)^{1/\alpha}$$

an α-fold collision on the 128-bit tag is found with probability about 1/2. Concretely, for $\alpha = 16$ and $q_e \approx 2^{122.8}$, a 16-fold collision can be obtained with probability around 1/2. From this, the key recovery in step (3) takes $q_p \approx 2^{128}/16 = 2^{124}$ primitive queries.

3 Interpretation

The NIST PHOTON-Beetle submission [1, Section 4] claims IND-CPA security up to 128 bits (both data and time) and IND-CTXT security up to 121 bits (both data and time). One might argue that these bounds are simplifications, the true bounds of Beetle apply [2,3] and these true bounds do expose a natural constant loss, but the difference between 128 and 121 in the NIST submission seems well-chosen. The difference, as explained in [1, Section 4.2], is defined by the fraction $\frac{rq_p}{2^{128}}$, a term that precisely captures above attack. Our attack, however, makes no verification queries and hence shows that this fraction must also be taken into account for confidentiality.

We conclude by admitting that, naturally, our attack forms no threat in the attack space outlined by the NIST call for proposals, i.e., in a setting where the data complexity is bounded to around 2^{50} bytes. The problem is easily resolved by updating the security claims.

References

1. Bao, Z., Chakraborti, A., Datta, N., Guo, J., Nandi, M., Peyrin, T., Yasuda, K.: PHOTON-Beetle Authenticated Encryption and Hash Family. Submission to NIST Lightweight Cryptography (2019)
2. Chakraborti, A., Datta, N., Nandi, M., Yasuda, K.: Beetle Family of Lightweight and Secure Authenticated Encryption Ciphers. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2018(2), 218–241 (2018), https://doi.org/10.13154/tches.v2018.i2.218-241
3. Chakraborti, A., Datta, N., Nandi, M., Yasuda, K.: Beetle Family of Lightweight and Secure Authenticated Encryption Ciphers. Cryptology ePrint Archive, Report 2018/805 (2018)
4. Guo, J., Peyrin, T., Poschmann, A.: The PHOTON Family of Lightweight Hash Functions. In: Rogaway, P. (ed.) Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings. Lecture Notes in Computer Science, vol. 6841, pp. 222–239. Springer (2011), https://doi.org/10.1007/978-3-642-22792-9_13
5. Suzuki, K., Tonien, D., Kurosawa, K., Toyota, K.: Birthday Paradox for Multi-collisions. In: Rhee, M.S., Lee, B. (eds.) Information Security and Cryptology - ICISC 2006, 9th International Conference, Busan, Korea, November 30 - December 1, 2006, Proceedings. Lecture Notes in Computer Science, vol. 4296, pp. 29–40. Springer (2006), https://doi.org/10.1007/11927587_5

From: MEGE, Alexandre <alexandre.mege@airbus.com>
Sent: Thursday, April 8, 2021 4:43 AM
To: lightweight-crypto
Cc: lwc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: PHOTON-Beetle

Dear All,

It seems the Collision Security of PHOTON-Beetle-Hash is lower than the 112 bit stated value.

This reduced security results from 2 sources in the algorithms: Domain separation bits & first iteration with larger rate than next iterations

1) Domain Separation bits

The domain separation bits are Xored to the capacity part when the final message block is processed.

The constant Xored has a value of 1 or 2 depending on whether the final block is full or partial.

The domain separation bit for a full final block can be used as additional rate bits to search for collisions at the final or intermediate blocks of a message.

Using this separation bit increases the effective rate for collisions to 33 bits, and the capacity is reduced to 223 bits.

The probability of this event can be bounded by $\frac{q^2}{2^{256-33}} = \frac{q^2}{2^{223}}$.

Thus, using the Domain separation bits to search for collision reduces the collision security to 111.5 bits.

2) First iteration with larger rate

The first iteration of PHOTON-Beetle-Hash has a rate of 128 bits. Taking into account the domain separation bit, the effective rate for collisions for the first iteration is 129 bits.

This can be used to improve the collision probability, with a collision attack being achieved when two blocks have the same capacity part, or a block having the same part as the capacity for the first block.

This second collision has a probability of by $\frac{q}{2^{256-129}} = \frac{q}{2^{127}}$

The impact on security of this second collisions is marginal.

Best regards,

Alexandre Mège