Analyzing the Provable Security Bounds of GIFT-COFB and Photon-Beetle[★]

Akiko Inoue[1], Tetsu Iwata[2], and Kazuhiko Minematsu[1]

[1] NEC, Kawasaki, Japan
a_inoue@nec.com,k-minematsu@nec.com
[2] Nagoya University, Nagoya, Japan
tetsu.iwata@nagoya-u.jp

Abstract. We study the provable security claims of two NIST Lightweight Cryptography (LwC) finalists, GIFT-COFB and Photon-Beetle, and present several attacks whose complexities contradict their claimed bounds in their final round specification documents. For GIFT-COFB, we show an attack using q_e encryption queries and no decryption query to break privacy (IND-CPA). The success probability is $O(q_e/2^{n/2})$ for n-bit block while the claimed bound contains $O(q_e^2/2^n)$. This positively solves an open question posed in [Khairallah, ePrint 2021/648 (also accepted at FSE 2022)]. For Photon-Beetle, we show an attack using q_e encryption queries (using a small number of input blocks) followed by a single decryption query and no primitive query to break authenticity (INT-CTXT). The success probability is $O(q_e^2/2^b)$ for a b-bit block permutation, and it is significantly larger than what the claimed bound tells, which is independent of the number of encryption queries. We also show a simple tag guessing attack that violates the INT-CTXT bound when the rate $r = 32$. Then, we analyze other (improved/modified) bounds of Photon-Beetle shown in the subsequent papers [Chakraborty et al., ToSC 2020(2) and Chakraborty et al., ePrint 2019/1475]. As a side result of our security analysis of Photon-Beetle, we point out that a simple and efficient forgery attack is possible in the related-key setting.

We emphasize that our results do not contradict the claimed "bit security" in the LwC specification documents for any of the schemes that we studied. That is, we do not negate the claims that GIFT-COFB is $(n/2 - \log n)$-bit secure for $n = 128$, and Photon-Beetle is $(b/2 - \log b/2)$-bit secure for $b = 256$ and $r = 128$, where r is a rate. We also note that the security against related-key attacks is not included in the security requirements of NIST LwC, and is not claimed by the designers.

Keywords: Authenticated Encryption · Lightweight Cryptography · Provable Security · NIST

[★] This paper has been accepted to ACNS 2022 under the same title, and the proceedings version will be published in LNCS series by Springer.