First-order masked ARMv7-M implementations of GIFT-COFB AEAD scheme

Alexandre Adomnicai

March 15, 2022

Abstract

This document briefly describes first-oder masked implementations of GIFT-COFB on ARMv7-M architectures which have been developped within the context of the NIST LWC standardization project.

1 Context

In 2018, the National Institute of Standards and Technology (NIST) initiated a process that started in 2018, with the goal of selecting the future Authenticated Encryption with Associated Data (AEAD) standard(s) for constrained environments [?]. AEAD algorithms ensure confidentiality, integrity, and authenticity of data in a single primitive. An important selection criterion, on top of security and performance, is the resilience against side-channel attacks since embedded devices are typical targets for such attacks. In order to assist the NIST in evaluating the LWC finalists in this regard, the Cryptographic Engineering Research Group from George Mason University issued a call for protected implementation of NIST LWC finalists[1]. The submissions have to follow a specific API so that it facilitates side-channel evaluations from the security labs involved in the process. The implementations described in this document were developped in this context and focus on GIFT-COFB [BCI+21][2], one of the 10 NIST LWC finalists, which is based on the GIFT-128 block cipher [BPP+17].

2 Implementation details

The first-order secure implementations presented in this document are based on a previous work employing an advanced bitslicing technique named *fixslicing* [ANP20]. Therefore, all the code consists of bitwise operations only, which eases the integration of Boolean masking. Non-linear operations (i.e. `AND` and `OR` gates) are computed without additional randomness using the techniques detailed in Algorithms 1 and 2.

Algorithm 1: First-order Boolean masked `AND` gate without additional randomness from [BDCU17]

Input: (x_1, x_2) s.t. $x = x_1 \oplus x_2$; (y_1, y_2) s.t. $y = y_1 \oplus y_2$
Output: (z_1, z_2) s.t. $z = x \wedge y = z_1 \oplus z_2$
$z_1 = (x_1 \wedge y_1) \oplus (x_1 \vee \neg y_2)$
$z_2 = (x_2 \vee y_1) \oplus (x_2 \vee \neg y_2)$
return (z_1, z_2)

[1] https://cryptography.gmu.edu/athena/LWC/Call_for_Protected_Software_Implementations.pdf

[2] https://www.isical.ac.in/~lightweight/COFB/

Algorithm 2: First-order Boolean masked `OR` gate without additional randomness from [BDCU17]

Input: (x_1, x_2) s.t. $x = x_1 \oplus x_2$; (y_1, y_2) s.t. $y = y_1 \oplus y_2$
Output: (z_1, z_2) s.t. $z = x \vee y = z_1 \oplus z_2$

$z_1 = (x_1 \wedge y_1) \oplus (x_1 \vee y_2)$
$z_2 = (x_2 \wedge y_1) \oplus (x_2 \wedge y_2)$
return (z_1, z_2)

The key is the only input which is split into 2 shares by the `generate_shares_encrypt` and `generate_shares_decrypt` functions. Since the key schedule is computed on both shares independently within a single assembly function call. At the GIFT-128 level, the internal state is also split into 2 shares, where the initial shares are initialized to zero (i.e. the input block is not masked).

Note that no hiding countermeasures have been integrated to these implementations so far.

3 Results of the preliminary security evaluation

No premilinary security evaluation has been undertaken.

References

[ANP20] Alexandre Adomnicai, Zakaria Najm, and Thomas Peyrin. Fixslicing: A new GIFT representation fast constant-time implementations of GIFT and GIFT-COFB on ARM cortex-m. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2020(3):402–427, 2020.

[BCI+21] Subhadeep Banik, Avik Chakraborti, Tetsu Iwata, Kazuhiko Minematsu, Mridul Nandi, Thomas Peyrin, Yu Sasaki, Siang Meng Sim, and Yosuke Todo. GIFT-COFB v1.1. Submission to the NIST Lightweight Cryptography project, 2021.

[BDCU17] Alex Biryukov, Daniel Dinu, Yann Le Corre, and Aleksei Udovenko. Optimal First-Order Boolean Masking for Embedded IoT Devices. In Thomas Eisenbarth and Yannick Teglia, editors, *Smart Card Research and Advanced Applications - 16th International Conference, CARDIS 2017*, volume 10728 of *Lecture Notes in Computer Science*, pages 22–41. Springer, 2017.

[BPP+17] Subhadeep Banik, Sumit Kumar Pandey, Thomas Peyrin, Yu Sasaki, Siang Meng Sim, and Yosuke Todo. GIFT: A Small Present - Towards Reaching the Limit of Lightweight Encryption. In *Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings*, volume 10529 of *Lecture Notes in Computer Science*, pages 321–345. Springer, 2017.