GIFT-COFB Final Round Updates

Subhadeep Banik[1], Avik Chakraborti[2], Akiko Inoue[4], Tetsu Iwata[3], Kazuhiko Minematsu[4], Mridul Nandi[5], Thomas Peyrin[6,7], Yu Sasaki[2], Siang Meng Sim[6], and Yosuke Todo[2]

[1] University of Lugano, Switzerland
[2] NTT, Japan
[3] Nagoya University, Japan
[4] NEC Corporation, Japan
[5] Indian Statistical Institute, India
[6] Nanyang Technological University, Singapore
[7] Temasek Laboratories NTU, Singapore

giftcofb@googlegroups.com

1 Third-party security analysis

Regarding GIFT-128 block cipher, third-party security evaluations have continued to be published since the last revision. With respect to linear attacks, the number of attacked rounds has increased significantly, but this does not change the fact that differential cryptanalysis remains more effective against GIFT-128. These attacks were discovered using automated evaluation tools and research on more efficient tools for the GIFT network have also been presented [20]. No progress has been made on differential cryptanalysis, and no new (unknown) cryptanalysis method has been discovered. This is a strong evidence of the reliability of GIFT-128. We give below some comments on a few references.

- Sun *et al.* [26] and its addendum [27] detected a 25-round linear cryptanalysis against GIFT-128. An attack taking into account the AEAD restrictions was also proposed, which recovers the key of GIFT-COFB if the primitive is reduced to 16 rounds. Note that differential cryptanalysis still works better on GIFT for the moment.
- Cui *et al.* proposed a 20-round linear cryptanalysis against GIFT-128 [10], which only works for a smaller number of rounds than previous results.
- The work by Khalesi and Ahmadian searches for minimum data complexity of the integral distinguisher [19]. Regarding GIFT-128, it confirms that the previously known result is actually the best.
- The paper by Hu *et al.* [12] proves the non-existence of impossible differential with one active superbox in both ends for 8-round reduced GIFT-128.
- The paper by Anubhab Baksi [3] presents the optimal linear bounds for 11 and 12 rounds of GIFT-128, extending from the best-known result on 10-rounds.

We recall that GIFT-128 has 40 rounds, while the best known attack can only reach 27 rounds (which does not apply to GIFT-COFB due to the data limitation, etc.). This leaves a very ample security margin.

The provable security aspects of GIFT-COFB and its variants have been studied and updated since the last revision of our specification document. We list the relevant works below.

- Khairallah [18] (ToSC 2022) presented an attack against a version of COFB mode shown in Journal of Cryptology [8]. Due to the difference in the modes, the presented attack is not applicable to GIFT-COFB.
- As an internal security evaluation of GIFT-COFB, Inoue, Iwata and Minematsu (IIM22, ACNS 2022 and NIST LWC workshop 2022) [14, 15] showed an attack that has a higher success probability than claimed. Their attack does not break the claimed bit security. A revised version of the proof (and the bound) maintaining the original bit security was presented in [5] (see the next section).
- Liu *et al.* [22] presented fault/side-channel attacks against unprotected implementation of GIFT-COFB.
- Reshma *et al.* [25] showed neural network-based distinguishers on reduced GIFT-COFB. The attack is very weak, as it only distinguishes between 2 and 6 rounds of GIFT-COFB's ciphertext from random data.

2 New security proofs/arguments

GIFT-COFB team revised the security proof of the mode and updated the bound by incorporating the fix suggested by IIM22. The fixed bound maintains the original bit security. The updated specification document (version 1.2) is posted at NIST LWC mailing list in May 2022[8]. The revised proof and the bound are shown in [5].

As an additional security feature, Inoue *et al.* [13] showed that GIFT-COFB has resilience against nonce misuse/repeat, which is a relaxed notion from the nonce misuse resistance introduced by Ashur *et al.* [2]. The presented bound is $n/4$ bits for $n = 128$, so not strong enough in general, but at least it does not lose everything in the event of nonce misuse. In contrast, the current NIST standard GCM has no resilience against nonce misuse. This work also supports the correctness of the design.

In summary, we actively reviewed the provable security of GIFT-COFB to increase the confidence in its security. As a result, we maintain the originally claimed bit security in a more transparent way.

[8] `https://groups.google.com/a/list.nist.gov/g/lwc-forum/c/7BmjTeE-NsY`

Table 1. Summary of third-party analysis result on GIFT. Rounds with asterisk (*) are optimal results. SK – single-key, RK – related-key, LC – linear cryptanalysis, DC – differential cryptanalysis.

Setting	Rounds	Approach	Prob.	Time	Data	Mem.	Ref.
Distinguisher							
SK	11	Integral	1	-	2^{127}	-	[11]
SK	11*	Integral	1	-	2^{127}	-	[19]
SK	9*	LC	2^{-44}	-	-	-	[16]
SK	10*	LC	2^{-52}	-	-	-	[16]
SK	15	LC	2^{-109}	-	-	-	[29]
SK	16	LC	2^{-122}	-	-	-	[10]
SK	19	LC	$2^{-117.43}$	-	-	-	[26]
SK	19	LC	$2^{-123.11}$	-	-	-	[27]
SK	9*	DC	$2^{-45.4}$	-	-	-	[23]
SK	10*	DC	$2^{-49.4}$	-	-	-	[23]
SK	11*	DC	$2^{-54.4}$	-	-	-	[23]
SK	12*	DC	$2^{-60.4}$	-	-	-	[23]
SK	13*	DC	$2^{-67.8}$	-	-	-	[23]
SK	14*	DC	$2^{-79.000}$	-	-	-	[16]
SK	15*	DC	$2^{-85.415}$	-	-	-	[16]
SK	16*	DC	$2^{-90.415}$	-	-	-	[16]
SK	17*	DC	$2^{-96.415}$	-	-	-	[16]
SK	18	DC	2^{-109}	-	-	-	[28]
SK	18*	DC	$2^{-103.415}$	-	-	-	[16]
SK	19	DC	$2^{-110.83}$	-	-	-	[16]
SK	20	DC	$2^{-121.415}$	-	-	-	[21]
SK	20	DC	$2^{-120.245}$	-	-	-	[17]
SK	20	DC	$2^{-121.813}$	-	-	-	[29]
SK	21	DC	$2^{-126.4}$	-	-	-	[23]
RK	7	DC	$2^{-15.83}$	-	-	-	[7]
RK	10	DC	$2^{-72.66}$	-	-	-	[7]
RK	19	Boomerang	$2^{-121.2}$	-	-	-	[24]
RK	19	Boomerang	$2^{-109.626}$	-	-	-	[17]
Key-Recovery							
SK	20	LC	-	$2^{112.28}$	2^{126}	2^{65}	[10]
SK	22	LC	-	2^{117}	2^{117}	2^{78}	[29]
SK	24	LC	-	$2^{124.45}$	$2^{122.55}$	2^{105}	[26]
SK	25	LC	-	$2^{124.75}$	$2^{126.77}$	2^{96}	[27]
SK	22	DC	-	2^{114}	2^{114}	2^{53}	[28]
SK	26	DC	-	$2^{124.415}$	2^{109}	2^{109}	[21]
SK	26	DC	-	$2^{123.245}$	$2^{123.245}$	2^{109}	[17]
SK	27	DC	-	$2^{124.83}$	$2^{123.53}$	2^{80}	[29]
RK	21	Boomerang	-	$2^{126.6}$	$2^{126.6}$	$2^{126.6}$	[24]
RK	22	Boomerang	-	$2^{112.63}$	$2^{112.63}$	2^{52}	[17]
RK	23	Rectangle	-	$2^{126.89}$	$2^{121.31}$	$2^{121.63}$	[17]

3 New software and hardware implementations

3.1 Bit serial implementation of GIFT-COFB

It is a well-known fact that implementing a hardware block cipher in a bit-serial manner, which advances only one bit in the computation pipeline in each clock cycle, results in the smallest circuits. Nevertheless, an efficient bit-serial circuit for a mode of operation that utilizes finite field arithmetic with multiple constants has yet to be demonstrated in the literature.

In a recent work [6], this issue regarding efficient field arithmetic in bit- serial circuits has been addressed. As a result lightweight circuit for GIFT-COFB is proposed, that occupies less than 1500 GE, making it the to-date most area-efficient implementation of this construction. In a second step, it is demonstrated how the additional operations in the mode can be executed concurrently with block cipher operations itself so that the total latency is significantly reduced whilst incurring only a modest area increase. Finally, a first-order threshold implementation of GIFT-COFB is proposed, in which first-order side-channel security is experimentally verified.

Summary: A total of 3 bit-serial circuits are proposed that stand as the to-date most area-efficient GIFT-COFB implementations known in the literature.

1. GIFT-COFB-SER-S: This circuit represents an effective transformation of the swap-and-rotate GIFT-128 scheme into the GIFT-COFB mode of operation minimizing its area footprint.
2. GIFT-COFB-SER-F: Subsequently, it was observed that the interspersing of block cipher invocations with calls to the finite field module as found in the baseline GIFT-COFB design can be reordered by leveraging its inherent mathematical structure in order to further optimize the overall latency of GIFT-COFB-SER-S while only incurring a modest area increase.
3. GIFT-COFB-SER-TI: A bit-serial first-order threshold implementation is proposed based on GIFT-COFB-SER-F whose security is experimentally verified through statistical tests on signal traces obtained by measuring the implemented circuit on a SAKURA-G side-channel evaluation FPGA board.
4. All of the proposed schemes are synthesized on ASIC platforms using multiple standard cell libraries and compared with results to existing bit-serial implementations of NIST LWC candidate submissions, indicating the designs are among the smallest currently in the competition. A brief overview of the synthesis results is tabulated in Table 2.

Moreover, we are also aware of the following implementations:

- a protected implementation of GIFT-COFB [1]
- a white-box implementations of GIFT-128 [9]

Table 2. Synthesis results overview for lightweight block cipher based NIST LWC competitors using the STM 90 nm cell library at a clock frequency of 10 MHz. Latency and energy correspond to the encryption of 128 bits of AD and 1024 message bits. Highlighted schemes are NIST LWC finalists.

	Datapath	Area	Latency	Power	Energy	Reference
	Bits	GE	Cycles	μW	nJ	
SUNDAE-GIFT	1	1201	92544	55.48	513.4	[4]
SAEAES	1	1350	24448	84.47	206.5	[4]
Romulus	1	1778	55431	82.28	456.1	[4]
SKINNY-AEAD	1	3589	72960	143.7	1048	[4]
GIFT-COFB	128	3927	400	156.3	6.254	[5]
GIFT-COFB-SER-S	1	1443	54784	50.11	275.8	[6]
GIFT-COFB-SER-F	1	1485	51328	62.15	319.8	[6]
GIFT-COFB-SER-TI	1	3384	51328	158.1	813.5	[6]

4 Target applications

GIFT-COFB performs extremely well in all hardware situations (low area, low energy, low power), and also very well in software due to its fixsliced representation.

5 Others

Akiko Inoue (NEC) joined the team of GIFT-COFB.

References

1. Balanced Dual-Mask Protection Scheme for GIFT Cipher Against Power Attacks. In: 2022 IEEE 40th VLSI Test Symposium (VTS). pp. 1–6 (2022). https://doi.org/10.1109/VTS52500.2021.9794230
2. Ashur, T., Dunkelman, O., Luykx, A.: Boosting authenticated encryption robustness with minimal modifications. In: CRYPTO (3). Lecture Notes in Computer Science, vol. 10403, pp. 3–33. Springer (2017)
3. Baksi, A.: New insights on differential and linear bounds using mixed integer linear programming. In: Maimut, D., Oprina, A., Sauveron, D. (eds.) Innovative Security Solutions for Information Technology and Communications - 13th International Conference, SecITC 2020, Bucharest, Romania, November 19-20, 2020, Revised Selected Papers. Lecture Notes in Computer Science, vol. 12596, pp. 41–54. Springer (2020). https://doi.org/10.1007/978-3-030-69255-1“˙4, `https://doi.org/10.1007/978-3-030-69255-1\_4`
4. Balli, F., Caforio, A., Banik, S.: The area-latency symbiosis: Towards improved serial encryption circuits. IACR Trans. Cryptogr. Hardw. Embed. Syst. **2021**(1), 239–278 (2021). https://doi.org/10.46586/tches.v2021.i1.239-278

5. Banik, S., Chakraborti, A., Iwata, T., Minematsu, K., Nandi, M., Peyrin, T., Sasaki, Y., Sim, S.M., Todo, Y.: GIFT-COFB. IACR Cryptol. ePrint Arch. p. 738 (2020)
6. Caforio, A., Collins, D., Banik, S., Regazzoni, F.: A small gift-cofb: Lightweight bit-serial architectures. Cryptology ePrint Archive, Paper 2022/955 (2022), https://eprint.iacr.org/2022/955, (To appear at Africacrypt 2022)
7. Cao, M., Zhang, W.: Related-Key Differential Cryptanalysis of the Reduced-Round Block Cipher GIFT. IEEE Access **7**, 175769–175778 (2019)
8. Chakraborti, A., Iwata, T., Minematsu, K., Nandi, M.: Blockcipher-based authenticated encryption: How small can we go? J. Cryptol. **33**(3), 703–741 (2020)
9. Charlès, A., Gravouil, C.: Review of the White-Box Encodability of NIST Lightweight Finalists. Cryptology ePrint Archive, Paper 2022/804 (2022), https://eprint.iacr.org/2022/804, https://eprint.iacr.org/2022/804
10. Cui, Y., Xu, H., Wang, W.Q.: MILP-Based Linear Attacks on Round-Reduced GIFT. Chinese Journal of Electronics **31**(1), 89–98 (2022), https://doi.org/10.1049/cje.2020.00.113
11. Eskandari, Z., Kidmose, A.B., Kölbl, S., Tiessen, T.: Finding Integral Distinguishers with Ease. In: SAC. Lecture Notes in Computer Science, vol. 11349, pp. 115–138. Springer (2018)
12. Hu, K., Peyrin, T., Wang, M.: Finding all impossible differentials when considering the ddt. Cryptology ePrint Archive, Paper 2022/1034 (2022), https://eprint.iacr.org/2022/1034, to appear in the proceedings of SAC2022.
13. Inoue, A., Guo, C., Minematsu, K.: Nonce-misuse resilience of romulus-n and gift-cofb. Cryptology ePrint Archive, Paper 2022/1012 (2022), https://eprint.iacr.org/2022/1012, https://eprint.iacr.org/2022/1012
14. Inoue, A., Iwata, T., Minematsu, K.: Analyzing the provable security bounds of GIFT-COFB and photon-beetle. Fifth NIST Lightweight Cryptography Workshop 2022 (2022)
15. Inoue, A., Iwata, T., Minematsu, K.: Analyzing the provable security bounds of GIFT-COFB and photon-beetle. In: ACNS. Lecture Notes in Computer Science, vol. 13269, pp. 67–84. Springer (2022)
16. Ji, F., Zhang, W., Ding, T.: Improving Matsui's Search Algorithm for the Best Differential/Linear Trails and its Applications for DES, DESL and GIFT. The Computer Journal **64**(4), 610–627 (April 2021), available at IACR Cryptol. ePrint Arch. 2019/1190
17. Ji, F., Zhang, W., Zhou, C., Ding, T.: Improved (Related-key) Differential Cryptanalysis on GIFT. In: SAC. Lecture Notes in Computer Science, Springer (2021), to appear. The preprint version is available at IACR Cryptol. ePrint Arch. 2020/1242
18. Khairallah, M.: Security of COFB against Chosen Ciphertext Attacks. IACR Trans. Symmetric Cryptol. **2022**(1), 138–157 (2022)
19. Khalesi, A., Ahmadian, Z.: Provably minimum data complexity integral distinguisher based on conventional division property. Cryptology ePrint Archive, Paper 2022/752 (2022), https://eprint.iacr.org/2022/752, https://eprint.iacr.org/2022/752
20. Kim, S., Hong, D., Sung, J., Hong, S.: Accelerating the best trail search on aes-like ciphers. IACR Trans. Symmetric Cryptol. **2022**(2), 201–252 (2022). https://doi.org/10.46586/tosc.v2022.i2.201-252, https://doi.org/10.46586/tosc.v2022.i2.201-252
21. Li, L., Wu, W., Zheng, Y., Zhang, L.: The Relationship between the Construction and Solution of the MILP Models and Applications. IACR Cryptol. ePrint Arch. **2019**, 49 (2019)

22. Liu, S., Guan, J., Hu, B.: Fault attacks on authenticated encryption modes for GIFT. IET Inf. Secur. **16**(1), 51–63 (2022)
23. Liu, Y., Liang, H., Li, M., Huang, L., Hu, K., Yang, C., Wang, M.: STP Models of Optimal Differential and Linear Trail for S-box Based Ciphers. Science China Information Sciences **64**(159103) (May 2021), available at IACR Cryptol. ePrint Arch. 2019/25
24. Liu, Y., Sasaki, Y.: Related-Key Boomerang Attacks on GIFT with Automated Trail Search Including BCT Effect. In: ACISP. Lecture Notes in Computer Science, vol. 11547, pp. 555–572. Springer (2019)
25. Rajan, R., Roy, R.K., Sen, D., Mishra, G.: Deep learning-based differential distinguisher for lightweight cipher gift-cofb. In: Machine Intelligence and Smart Systems. pp. 397–406. Springer Nature Singapore, Singapore (2022)
26. Sun, L., Wang, W., Wang, M.: Linear cryptanalyses of three aeads with GIFT-128 as underlying primitives. IACR Trans. Symmetric Cryptol. **2021**(2), 199–221 (2021). https://doi.org/10.46586/tosc.v2021.i2.199-221, https://doi.org/10.46586/tosc.v2021.i2.199-221
27. Sun, L., Wang, W., Wang, M.: Addendum to linear cryptanalyses of three aeads with GIFT-128 as underlying primitives. IACR Cryptol. ePrint Arch. p. 151 (2022), https://eprint.iacr.org/2022/151
28. Zhu, B., Dong, X., Yu, H.: Milp-based differential attack on round-reduced gift. Cryptology ePrint Archive, Report 2018/390 (2018), https://eprint.iacr.org/2018/390
29. Zong, R., Dong, X., Chen, H., Luo, Y., Wang, S., Li, Z.: Towards Key-recovery-attack Friendly Distinguishers: Application to GIFT-128. IACR Trans. Symmetric Cryptol. **2021**(1), 156–184 (2021)