A Small GIFT-COFB: Lightweight Bit-Serial Architectures

Andrea Caforio[1], Daniel Patrick Collins[1], Subhadeep Banik[2], Francesco Regazzoni[2,3]

[1] LASEC, École Polytechnique Fédérale de Lausanne, Switzerland
{andrea.caforio,daniel.collins}@epfl.ch
[2] Universita della Svizzera Italiana, Lugano, Switzerland
subhadeep.banik@usi.ch
[3] University of Amsterdam, Netherlands
f.regazzoni@uva.nl

Abstract. GIFT-COFB is a lightweight AEAD candidate and a submission to the ongoing NIST lightweight cryptography standardization process where it currently competes as a finalist. The construction processes 128-bit blocks with a key and nonce of the same size and has a small register footprint, only requiring a single additional 64-bit register. Besides the block cipher, the mode of operation deploys a bit permutation and a finite field multiplication with different constants. 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 this paper, we fill this gap regarding efficient field arithmetic in bit-serial circuits, and propose a lightweight circuit for GIFT-COFB that occupies less than 1500 GE, making it the to-date most area-efficient implementation of this construction. In a second step, we demonstrate how the additional operations in the mode can be executed concurrently with GIFT itself so that the total latency is significantly reduced whilst incurring only a modest area increase. Finally, we propose a first-order threshold implementation of GIFT-COFB, which we experimentally verify resists first-order side-channel analysis[4].

1 Introduction

Resource-constrained devices have become pervasive and ubiquitous commodities in recent years to the extent that the task of securing such gadgets spawned a dedicated branch of cryptographic research. Lightweight cryptography is a discipline that comprises the creation, analysis and implementation of resource-optimized cryptographic primitives in terms of criteria such as circuit area, power consumption and latency.

[4] This work is partially supported by the European Union Horizon 2020 research and innovation program under CPSoSAware project (grant No. 871738)

This proliferation of low-resource devices and their security requirements spurred the NIST Lightweight Cryptography competition [nis]. Commencing in 2018 and recently entering its ultimate round with ten competing candidate designs, the competition can nowadays be considered the essential driving force in this research field. GIFT-COFB [BCI+19] is one the finalists and thus an efficient implementation of this construction on hardware and software platforms is both timely and useful. The designers of this scheme have provided results for round-based circuits, i.e., which perform one round of the underlying block cipher encryption algorithm per clock cycle. However, such circuits, although they consume less energy [BBR15], induce a higher hardware footprint in gate count. Consequently, the minimum circuit area of GIFT-COFB remains unexplored.

A popular technique to reduce the hardware footprint of circuits is serialization. Serialized circuits operate with a datapath of width much less than the specified block size of the cipher, and therefore allow for specific resources of the circuit to be reused several times in each round. The byte-serial circuit (i.e., which advances one byte in the computation pipeline in each clock cycle) for AES-128 [DR02] by Moradi et al. [MPL+11], with area equivalent to around 2400 GE, remained for many years the most compact implementation of this block cipher. The implementation was subsequently extended to support both encryption and decryption capabilities as well as different key sizes [BBR16,BBR17,BB19].

A first generic technique to obtain bit-serial block cipher implementations, termed *bit-sliding*, was proposed in a work by Jean et al. [JMPS17] yielding, at the time, the smallest circuits for the ciphers AES-128, SKINNY [BJK+16] and PRESENT [BKL+07]. However, all these circuits required more clock cycles than the block size of the underlying block ciphers to execute one encryption round. The circuit for PRESENT was further compacted in [BBRV20] with a technique that made is possible to execute one round in exactly 64 clock cycles which is equal to the block size. This endeavour of computing a round function in the same number cycles as there are bits in the internal state was successfully extended to other ciphers including AES-128, SKINNY and GIFT-128 [BPP+17,BCB21]. This was achieved by not treating the round as a monolithic entity by deferring some operations to the time allotted to operations of the next round. Additionally, the authors proposed bit-serial circuits for some modes of operation such as SAEAES [NMMaS+19], SUNDAE-GIFT [BBP+19], Romulus [IKMP19], SKINNY-AEAD [BJK+19]. It is important to note that the canon of bit-serial works has pushed implementations to a point where the corresponding circuits are predominantly comprised of storage elements with almost negligible amounts of combinatorial parts that implement the actual logic of the algorithm.

1.1 Contributions

Unlike the bit-serial AEAD implementations proposed in [BCB21], GIFT-COFB involves finite field arithmetic for which there is no straightforward mapping into a bit-serial setting that is both circuit area and latency efficient. In this paper, we fill this gap by proposing *three* bit-serial circuits that stand as the to-date

most area-efficient GIFT-COFB implementations known in the literature. More specifically, our contributions are summarized as follows:

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, we 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: In a natural progression, we design a bit-serial first-order threshold implementation 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. We synthesise all of the proposed schemes on ASIC platforms using multiple standard cell libraries and compare our results to existing bit-serial implementations of NIST LWC candidate submissions, indicating our designs are among the smallest currently in the competition. A brief overview of the synthesis results is tabulated in Table 1.

Table 1: 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	[BCB21]
SAEAES	1	1350	24448	84.47	206.5	[BCB21]
Romulus	1	1778	55431	82.28	456.1	[BCB21]
SKINNY-AEAD	1	3589	72960	143.7	1048	[BCB21]
GIFT-COFB	128	5621	400	471.5	18.90	[CBB20]
GIFT-COFB-SER-S	1	1443	54784	50.11	275.8	Section **??**
GIFT-COFB-SER-F	1	1485	51328	62.15	319.8	Section **??**
GIFT-COFB-SER-TI	1	3384	51328	158.1	813.5	Section **??**

References

BB19. Fatih Balli and Subhadeep Banik. Six shades of AES. In Johannes Buchmann, Abderrahmane Nitaj, and Tajje-eddine Rachidi, editors, *Progress in Cryptology - AFRICACRYPT 2019 - 11th International Conference*

on Cryptology in Africa, Rabat, Morocco, July 9-11, 2019, Proceedings, volume 11627 of *Lecture Notes in Computer Science*, pages 311–329. Springer, 2019.

BBP+19. Subhadeep Banik, Andrey Bogdanov, Thomas Peyrin, Yu Sasaki, Siang Meng Sim, Elmar Tischhauser, and Yosuke Todo. Sundae-gift v1.0. *NIST Lightweight Cryptography Project*, 2019.

BBR15. Subhadeep Banik, Andrey Bogdanov, and Francesco Regazzoni. Exploring energy efficiency of lightweight block ciphers. In *Selected Areas in Cryptography - SAC 2015 - 22nd International Conference, Sackville, NB, Canada, August 12-14, 2015, Revised Selected Papers*, pages 178–194, 2015.

BBR16. Subhadeep Banik, Andrey Bogdanov, and Francesco Regazzoni. Atomic-aes: A compact implementation of the AES encryption/decryption core. In *Progress in Cryptology - INDOCRYPT 2016 - 17th International Conference on Cryptology in India, Kolkata, India, December 11-14, 2016, Proceedings*, pages 173–190, 2016.

BBR17. Subhadeep Banik, Andrey Bogdanov, and Francesco Regazzoni. Compact Circuits for Combined AES Encryption/Decryption. *Journal of Cryptographic Engineering*, pages 1–15, 2017.

BBRV20. Subhadeep Banik, Fatih Balli, Francesco Regazzoni, and Serge Vaudenay. Swap and rotate: Lightweight linear layers for spn-based blockciphers. *IACR Trans. Symmetric Cryptol.*, 2020(1):185–232, 2020.

BCB21. Fatih Balli, Andrea Caforio, and Subhadeep Banik. The area-latency symbiosis: Towards improved serial encryption circuits. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2021(1):239–278, 2021.

BCI+19. Subhadeep Banik, Avik Chakraborti, Tetsu Iwata, Kazuhiko Minematsu, Mridul Nandi, Thomas Peyrin, Yu Sasaki, Siang Meng Sim, and Yosuke Todo. Gift-cofb v1.0. *NIST Lightweight Cryptography Project*, 2019.

BJK+16. Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. The SKINNY family of block ciphers and its low-latency variant MANTIS. In *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*, pages 123–153, 2016.

BJK+19. Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. Skinny-aead and skinny-hash. *NIST Lightweight Cryptography Project*, 2019.

BKL+07. Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. PRESENT: an ultra-lightweight block cipher. In *Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings*, pages 450–466, 2007.

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*, pages 321–345, 2017.

CBB20. Andrea Caforio, Fatih Balli, and Subhadeep Banik. Energy analysis of lightweight AEAD circuits. In Stephan Krenn, Haya Shulman, and Serge Vaudenay, editors, *Cryptology and Network Security - 19th International Conference, CANS 2020, Vienna, Austria, December 14-16, 2020, Proceedings*, volume 12579 of *Lecture Notes in Computer Science*, pages 23–42. Springer, 2020.

DR02. Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Information Security and Cryptography. Springer, 2002.

IKMP19. Tetsu Iwata, Mustafa Khairallah, Kazuhiko Minematsu, and Thomas Peyrin. Romulus v1.2. *NIST Lightweight Cryptography Project*, 2019.

JMPS17. Jérémy Jean, Amir Moradi, Thomas Peyrin, and Pascal Sasdrich. Bit-sliding: A generic technique for bit-serial implementations of spn-based primitives - applications to aes, PRESENT and SKINNY. In *Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings*, pages 687–707, 2017.

MPL+11. Amir Moradi, Axel Poschmann, San Ling, Christof Paar, and Huaxiong Wang. Pushing the limits: A very compact and a threshold implementation of AES. In *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings*, pages 69–88, 2011.

nis. Nist lightweight cryptography project. https://csrc.nist.gov/projects/lightweight-cryptography.

NMMaS+19. Yusuke Naito, Yasuyuki Sakai Mitsuru Matsui and, Daisuke Suzuki, Kazuo Sakiyama, and Takeshi Sugawara. SAEAES. *NIST Lightweight Cryptography Project*, 2019.