SUNDAE-GIFT: Status Update

Subhadeep Banik, Andrey Bogdanov, Thomas Peyrin, Yu Sasaki,
Siang Meng Sim, Elmar Tischhauser, and Yosuke Todo

1 New Proofs

None planned at the moment.

2 New Software/Hardware Implementations

2.1 Bit Serial/ Nibble Serial architectures

We are glad to report extremely lightweight implementations of SUNDAE-GIFT on ASIC platforms. The content reported in this section has already appeared in [1]. In the variant of GIFT used in SUNDAE-GIFT, the cipher state is reordered and interpreted as a two-dimensional array.

2.2 1-Bit Datapath

In [1], the authors report an efficient implementation of GIFT using a 1 bit datapath that takes 128 cycles to implement 1 round of the cipher. This is an improvement over the 160 cycle/round implementation originally reported in [3]. The circuit diagrams are presented in Figures 1 and 2. The 4-bit key pipeline can be seamlessly adapted from the 1-bit counterpart by simply turning the single-bit swaps into nibble swaps. As we had 5 swaps in the single-bit version we now have $4 \cdot 5 = 20$ swaps, i.e. 40 scan flip-flops. In Table 1 we list the synthesis results for our 1-bit and 4-bit GIFT circuits.

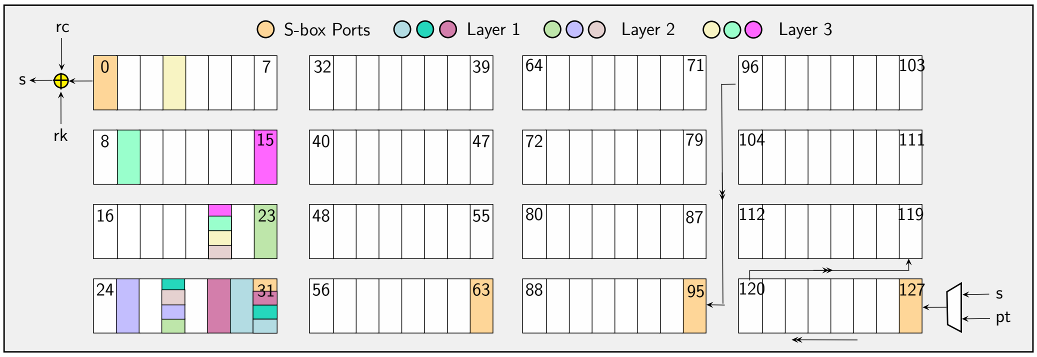

Fig. 1: 128-cycle, bit-serial GIFT round function implementation using nine swaps.

2.3 SUNDAE-GIFT

The SUNDAE-GIFT is a bare-bones construction that does not require any additional registers aside the ones used within the block cipher. After the encryption of the init vector each data block is mixed into the AEAD state between the encryption calls. A field multiplication over

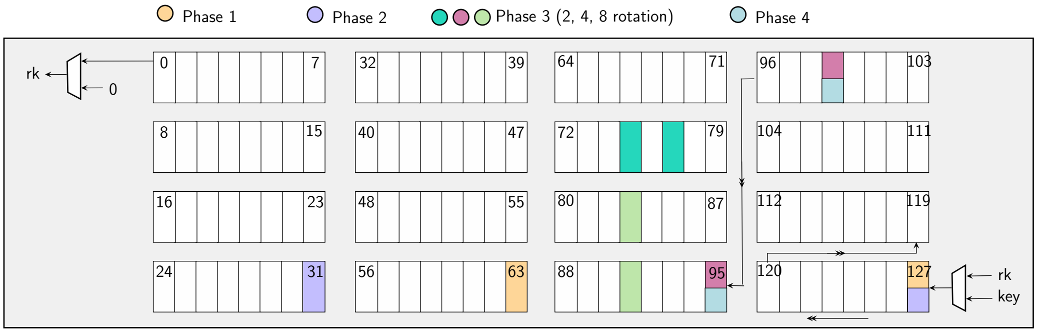

Fig. 2: 128-cycle, bit-serial GIFT key schedule implementation using five swaps.

Table 1: Synthesis figures for 1-bit and 4-bit GIFT circuits. Table taken from [1]

Library	Area (μm^2)	Area (GE)	Power (μW)	Latency		Energy	Throughput
			@ 10 MHz	round	total	(nJ)	Mbps
			1-Bit				
STM 90 nm	4863.5	1108	48.7	128	5248	25.5	9.09
UMC 90 nm	4410.8	1332	49.8	128	5248	26.1	9.77
TSMC 90 nm	4176.5	1480	45.1	128	5248	23.7	12.51
Nangate 15 nm	402.3	2047	15.4	128	5248	8.1	178.92
Nangate 45 nm	1432.1	1791	122.3	128	5248	64.2	29.82
			4-Bit				
STM 90 nm	6280.5	1430	61.4	32	1312	5.1	8.98
UMC 90 nm	5779.7	1779	60.9	32	1312	4.4	7.73
TSMC 90 nm	5135.6	1819	50.8	32	1312	4.3	9.73
Nangate 15 nm	481.5	2449	17.1	32	1312	1.9	166.14
Nangate 45 nm	1704.5	2130	152.9	32	1312	13.9	28.72

$GF(2^{128})$ is applied after the last associated data has been added to the state. Analogously, the same multiplication is performed for the last message block. The multiplication is either ×2 when the last AD or message block have been padded or ×4 whenever the last blocks are complete. More formally, the multiplication ×2 is encoded as a byte-wise shift and the addition of the most significant byte into other bytes of the state such that if $B_0||B_1||\dots||B_{15}$ represent the 16 bytes of the intermediate AEAD state with B_0 being the most significant byte we have that

$$2 \times (B_0||B_1||\dots||B_{15}) = B_1||B_2||\dots B_{10}||B_{11} \oplus B_0||B_{12}||B_{13} \oplus B_0||B_{14}||B_{15} \oplus B_0||B_0,$$

and $4 \times (B_0||B_1||\dots||B_{15}) = 2 \times (2 \times (B_0||B_1||\dots||B_{15}))$. The tag is produced after processing all AD and message blocks and the ciphertext blocks are generated by reprocessing the message blocks afterwards. A schematic of the SUNDAE is depicted in Figure 3.

The simplicity of SUNDAE can be exploited in a bit-serial implementation to attain a circuit with very low overhead in terms of area. In fact, aside a more involved control logic the sole addition to the GIFT circuit is the field multiplication. The 1-bit version of SUNDAE can seamlessly be amended to a 4-bit datapath design by changing the bit swaps to nibble swaps. After synthesis the resulting SUNDAE architecture is the to-date smallest authenticated encryption circuit at around 1200 gate equivalents for the STM 90 nm process which is only a 8 percent increased compared to the bit-serial GIFT implementation.

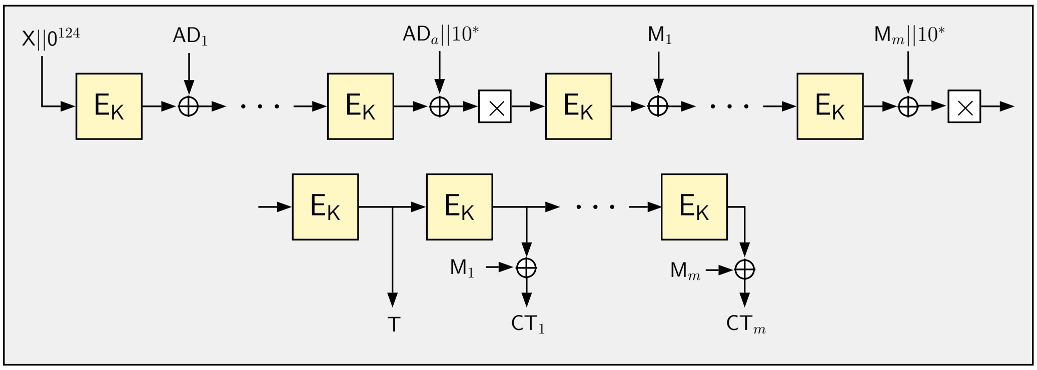

Fig. 3: SUNDAE high-level overview. The figure depicts the processing of two message and two associated data blocks. X denotes a 4-bit parameter based on the length of the nonce and whether there are no AD or message blocks.

2.4 Round based/Unrolled architectures

SUNDAE-GIFT uses the GIFT block cipher in its core and processes 128-bit blocks with a key of the same size. The nonce is variably-size and included in the first associated data block. SUNDAE does not require any additional registers, except naturally the one for the block cipher state, with the output to the core being multiplied over GF(2^{128}).

We compared SUNDAE-GIFT with 9 other modes of operation in the 2nd round of the NIST LWC competition. The results in this section appear in [5]. We experimented with different round unrolled architectures of the core block cipher used in the design (from round-based to fully unrolled) using the TSMC 90nm standard cell library. Figure 4 charts the optimal energy per 128-bit block value for each degree of unrolling r and candidate. As can be seen although SUNDAE is a rate 1/2 mode it performs well wrt to other modes wrt energy consumption. Table details the simulation results.

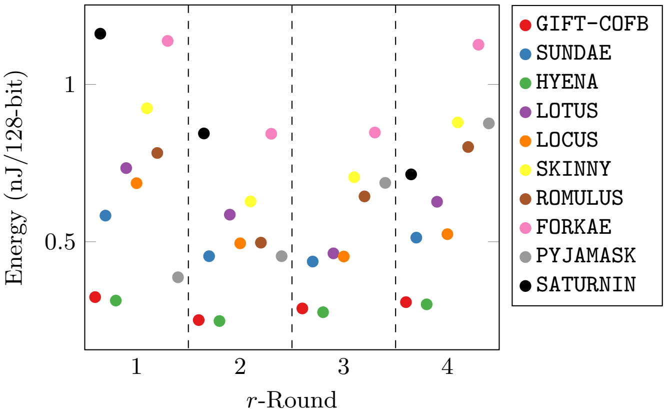

Fig. 4: Energy consumption (nJ/128-bit) comparison chart for the r-round partially-unrolled implementations with $r \in \{1, 2, 3, 4\}$. For each candidate the best obtained energy value obtained through techniques is used.

Table 2: Low-latency synthesis figures for selected AEAD Schemes. Energy and throughput calculated for processing 1024 bits of plaintext and 128 bits of AD. Table taken from [1]

Library	Area	Area	Power(μW)	Latency	Energy	Throughput
	(μm^2)	(GE)	(@ 10 MHz)	(cycles)	(nJ)	(Mbit/s)
SUNDAE 1-Bit						
STM 90 nm	5273.9	1201	50.1	92800	464.9	4.80
UMC 90 nm	4729.9	1508	51.1	92800	474.2	5.00
TSMC 90 nm	4444.6	1663	45.9	92800	426.0	5.75
Nangate 15 nm	426.6	2170	15.9	92800	147.6	90.80
Nangate 45 nm	1527.9	1915	130.3	92800	1209.2	15.13
SUNDAE 4-Bit						
STM 90 nm	6969.8	1587	63.9	23136	91.12	14.78
UMC 90 nm	6109.7	1948	63.5	23136	95.4	13.97
TSMC 90 nm	5640.6	1998	52.1	23136	93.8	13.67
Nangate 15 nm	541.4	2754	19.45	23136	30.2	299.93
Nangate 45 nm	1871.3	2345	168.16	23136	234.2	53.67
SAEAES 1-Bit						
STM 90 nm	5938.0	1350	77.2	24448	188.7	6.58
UMC 90 nm	5381.4	1716	66.9	24448	163.6	10.22
TSMC 90 nm	4942.7	1751	56.9	24448	139.1	7.63
Nangate 15 nm	464.3	2362	18.8	24448	46.0	152.69
Nangate 45 nm	1653.5	2067	148.8	24448	363.8	22.76
SAEAES 8-Bit						
STM 90 nm	5938.0	1350	77.2	24448	188.7	6.58
UMC 90 nm	5381.4	1716	66.9	24448	163.6	10.22
TSMC 90 nm	4942.7	1751	56.9	24448	139.1	7.63
Nangate 15 nm	464.3	2362	18.8	24448	46.0	152.69
Nangate 45 nm	1653.5	2067	148.8	24448	363.8	22.76
ROMULUS 1-Bit						
STM 90 nm	7812.7	1779	79.1	55431	438.4	6.35
UMC 90 nm	7155.6	2282	81.6	55431	452.31	6.78
TSMC 90 nm	6658.8	2359	74.0	55431	410.2	9.99
Nangate 15 nm	650.8	3310	25.0	55431	138.6	161.22
Nangate 45 nm	2304.1	2887	199.0	55431	1103.0	21.28
ROMULUS 8-Bit						
STM 90 nm	7812.7	1779	79.1	55431	438.4	6.35
UMC 90 nm	7155.6	2282	81.6	55431	452.31	6.78
TSMC 90 nm	6658.8	2359	74.0	55431	410.2	9.99
Nangate 15 nm	650.8	3310	25.0	55431	138.6	161.22
Nangate 45 nm	2304.1	2887	199.0	55431	1103.0	21.28
SKINNY AEAD 1-Bit						
STM 90 nm	7812.7	1779	79.1	55431	438.4	6.35
UMC 90 nm	7155.6	2282	81.6	55431	452.31	6.78
TSMC 90 nm	6658.8	2359	74.0	55431	410.2	9.99
Nangate 15 nm	650.8	3310	25.0	55431	138.6	161.22
Nangate 45 nm	2304.1	2887	199.0	55431	1103.0	21.28
SKINNY AEAD 8-Bit						
STM 90 nm	16606.7	3783	149	9856	438.4	39.9
UMC 90 nm	15161.0	4834	155	9856	452.31	25.1
TSMC 90 nm	13943.4	4940	137	9856	410.2	38.6
Nangate 15 nm	1381.2	7025	31.9	9856	138.6	569.9
Nangate 45 nm	4793.3	6007	410.75	9856	1103.0	101.4

2.5 Threshold Implementations

The s-box of GIFT belongs to the cubic class $\mathcal{C}_{172}$ which is decomposable into 2 quadratics. The algebraic expressions of the output shares of both the 3 and 4-share TI can be found in [8]. Table 4 lists the simulation results using the same measurement setup as the unshared round-based implementations. It can be seen that SUNDAE-GIFT offers both low area and competitive energy efficiency when compared with other modes of operation. The results in this section appear in [5].

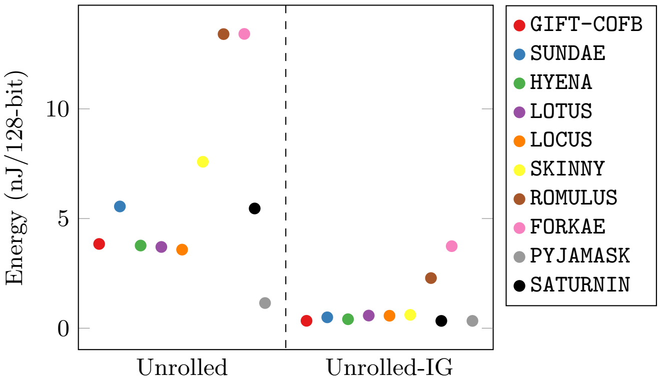

Fig. 5: Energy consumption (nJ/128-bit) comparison chart for the fully-unrolled implementations with and without inverse-gating.

Table 3: Various SUNDAE implementations with no clock-gating. Latency and energy is given for processing a single authenticated data block followed by eight message blocks. IG denotes "inverse-gated" implementation as per the generic energy reduction technique explained in [2]

Candidate	Implementation	Latency (cycles)	Area (GE)	TP_{max} (Mbps)	Power (μW)	Energy (nJ/128-bit)
SUNDAE	1-Round	720	3548	430.11	69.4	0.583
	2-Round	360	4313	642.57	107.8	0.454
	3-Round	252	5136	769.42	147.7	**0.437**
	4-Round	180	5858	863.70	242.5	0.513
	Unrolled	18	34571	1145.93	12045.5	5.551
	Unrolled-IG	18	42419	395.01	1076.7	0.496

3 New 3rd Party Analysis

As far as our knowledge goes, there have not been any cryptanalytic advance reported against SUNDAE-GIFT so far. In July 2019, there was a comment [13] from Alexandre Mege in regards to the internal state collision in SUNDAE-GIFT. But as one of our team members Thomas Peyrin had replied, that is a generic birthday attack and within our security bound. Hence, there is no violation to our security claims and no modification is made.

In short, our underlying 40-round block cipher GIFT [3] remains secure with high security margin. We have summarized the latest third-party cryptanalysis results in Table 5. [16] is the corrected version of [17] with the 22-round differential cryptanalysis on GIFT, the original 23-round attack was invalid. Although GIFT did not make related-key security claims, third-party analysis [6, 12] have shown that GIFT is actually resistance against related-key attacks.

4 Target applications and use cases

SUNDAE's structure is based on SIV [15], however it is optimized for lightweight settings: it uses one key, consists of a cascade of block cipher calls, and its only additional operations consist of XOR and multiplication by fixed constants. The use of efficient intermediate functions is inspired by GCBC [14]. Using an n-bit block cipher, aside from storage for

Table 4: Measurements for the 1-round threshold implementations. The schemes using GIFT are colored in light gray whereas, SKINNY based schemes are in white. Table taken from [5]

Candidate	Conf.	Shares	Latency	Area	TP_{max}	Power	Energy
		#	(cycles)	(GE)	(Mbps)	(mW)	(nJ/128-bit)
GIFT-COFB	CG-RB	3	800	16386	208.9	0.214	2.243
	CG-RB	4	400	25850	350.8	0.358	**1.875**
SUNDAE	RB	3	1440	13297	145.7	0.215	3.719
	RB	4	720	21848	285.2	0.357	**2.999**
HYENA	CG-RB	3	800	14769	344.9	0.212	2.216
	CG-RB	4	400	24540	497.4	0.358	**1.875**
LOTUS	CG	3	2072	14176	121.7	0.145	3.581
	CG	4	1036	19712	133.0	0.262	**3.232**
LOCUS	CG	3	2072	12366	121.7	0.137	3.362
	CG	4	1036	17597	176.8	0.255	**3.148**
SKINNY	CG	3	2240	18501	92.83	0.2264	6.134
ROMULUS	CG-RB	3	2056	13450	130.00	0.1865	4.656
FORKAE	CG	3	3008	17008	76.60	0.2483	8.304
PYJAMASK	CG-RB	3	348	42001	620.2	0.472	1.825
	CG-RB	4	180	64577	927.6	0.814	**1.628**

the key, CLOC requires $2n$-bit state, JAMBU $1.5n$-bit state, and COFB $1.5n$-bit state, whereas SUNDAE only uses an n-bit state.

SUNDAE's performance is fundamentally limited by the fact that it requires two block cipher calls per data block, hence SUNDAE works best for communication which consists of short messages. For a message consisting of one block of nonce, associated data, and plaintext, COFB uses 3 block cipher calls, CLOC requires 4, JAMBU 5, and SUNDAE 5 as well (which can be reduced to 4 if one block cipher call can be precomputed). However, SUNDAE's strength lies in settings where communication outweighs computational costs: if the combination of associated data and plaintext is never repeated, the nonce is no longer needed, and communication or synchronization costs are reduced, in addition to reducing the block cipher calls to 4.

SUNDAE is inherently serial, and although the client side is important, it is not everything, especially given GCM-SIV's excellent performance using AES-NI on Haswell and Skylake. Even though parallel modes inherently profit most from modern parallel architectures, the Comb scheduling technique proposed in [4] can mitigate this issue even for serial modes, at least on the server side. Furthermore there is a variant SUNDAE-GIFT-0 that does not need IV or nonce. This could be useful for really constrained environments where the generation of IV is not available or unreliable.

5 Planned tweak proposals

None at the moment.

Setting	Rounds	Approach	Probability	Time	Data	Memory	Ref.
Distinguisher							
SK	11	Integral	1	-	2^{127}	-	[7]
SK	9^*	LC	2^{-44}	-	-	-	[9]
SK	10^*	LC	2^{-52}	-	-	-	[9]
SK	9^*	DC	$2^{-45.4}$	-	-	-	[11]
SK	10^*	DC	$2^{-49.4}$	-	-	-	[11]
SK	11^*	DC	$2^{-54.4}$	-	-	-	[11]
SK	12^*	DC	$2^{-60.4}$	-	-	-	[11]
SK	13^*	DC	$2^{-67.8}$	-	-	-	[11]
SK	14^*	DC	$2^{-79.000}$	-	-	-	[9]
SK	15^*	DC	$2^{-85.415}$	-	-	-	[9]
SK	16^*	DC	$2^{-90.415}$	-	-	-	[9]
SK	17^*	DC	$2^{-96.415}$	-	-	-	[9]
SK	18	DC	2^{-109}	-	-	-	[16]
SK	18^*	DC	$2^{-103.415}$	-	-	-	[9]
SK	19	DC	$2^{-110.83}$	-	-	-	[9]
SK	20	DC	$2^{-121.415}$	-	-	-	[10]
SK	21	DC	$2^{-126.4}$	-	-	-	[11]
RK	7	DC	$2^{-15.83}$	-	-	-	[6]
RK	10	DC	$2^{-72.66}$	-	-	-	[6]
RK	19	Boomerang	$2^{-121.2}$	-	-	-	[12]
Key-Recovery							
SK	22	DC	2^{-109}	2^{114}	2^{114}	2^{53}	[16]
SK	26	DC	$2^{-121.415}$	$2^{124.415}$	2^{109}	2^{109}	[10]
RK	21	RK-Boomerang	$2^{-121.2}$	$2^{126.6}$	$2^{126.6}$	$2^{126.6}$	[12]

Table 5: 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.

Acknowledgments

Subhadeep Banik is supported by the Ambizione grant PZ00P2_179921, awarded by the Swiss National Science Foundation. Thomas Peyrin is supported by the Temasek Labs grant (DSOCL16194). The authors would like to thank Atul Luykx for the meaningful discussions with regards to this submission.

References

1. Balli, F., Caforio, A., Banik, S.: Low-latency meets low-area: An improved bit-sliding technique for AES, SKINNY and GIFT. IACR Cryptol. ePrint Arch. **2020** (2020) 608
2. Banik, S., Bogdanov, A., Regazzoni, F., Isobe, T., Hiwatari, H., Akishita, T.: Inverse gating for low energy encryption. In: 2018 IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2018, Washington, DC, USA, April 30 - May 4, 2018, IEEE Computer Society (2018) 173–176
3. Banik, S., Pandey, S.K., Peyrin, T., Sasaki, Y., Sim, S.M., Todo, Y.: GIFT: A small present - towards reaching the limit of lightweight encryption. In Fischer, W., Homma, N., eds.:

Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings. Lecture Notes in Computer Science, Springer (2017) 321–345

4. Bogdanov, A., Lauridsen, M.M., Tischhauser, E.: Comb to pipeline: Fast software encryption revisited. In Leander, G., ed.: Fast Software Encryption - 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers. Volume 9054 of Lecture Notes in Computer Science., Springer (2015) 150–171
5. Caforio, A., Balli, F., Banik, S.: Energy analysis of lightweight AEAD circuits. Accepted in Ceryptography and Network Security (CANS) 2020
6. Cao, M., Zhang, W.: Related-Key Differential Cryptanalysis of the Reduced-Round Block Cipher GIFT. IEEE Access **7** (2019) 175769–175778
7. Eskandari, Z., Kidmose, A.B., Kölbl, S., Tiessen, T.: Finding integral distinguishers with ease. In Cid, C., Jr., M.J.J., eds.: Selected Areas in Cryptography - SAC 2018 - 25th International Conference, Calgary, AB, Canada, August 15-17, 2018, Revised Selected Papers. Volume 11349 of Lecture Notes in Computer Science., Springer (2018) 115–138 https://eprint.iacr.org/2018/688.
8. Jati, A., Gupta, N., Chattopadhyay, A., Sanadhya, S.K., Chang, D.: Threshold implementations of GIFT: A trade-off analysis. IEEE Trans. Information Forensics and Security **15** (2020) 2110–2120
9. 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. IACR Cryptol. ePrint Arch. **2019** (2019) 1190 https://eprint.iacr.org/2019/1190.
10. 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** (2019) 49
11. 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. IACR Cryptol. ePrint Arch. **2019** (2019) 25
12. Liu, Y., Sasaki, Y.: Related-Key Boomerang Attacks on GIFT with Automated Trail Search Including BCT Effect. In Jang-Jaccard, J., Guo, F., eds.: Information Security and Privacy - 24th Australasian Conference, ACISP 2019, Christchurch, New Zealand, July 3-5, 2019, Proceedings. Volume 11547 of Lecture Notes in Computer Science., Springer (2019) 555–572 https://eprint.iacr.org/2019/669.
13. Mege, A.: (July 9, 2019) OFFICIAL COMMENT: SUNDAE-GIFT. Official comments received on SUNDAE-GIFT. (2019) https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-1/official-comments/SUNDAE-GIFT-official-comment.pdf.
14. Nandi, M.: Fast and secure cbc-type MAC algorithms. In Dunkelman, O., ed.: Fast Software Encryption, 16th International Workshop, FSE 2009, Leuven, Belgium, February 22-25, 2009, Revised Selected Papers. Volume 5665 of Lecture Notes in Computer Science., Springer (2009) 375–393
15. Rogaway, P., Shrimpton, T.: A provable-security treatment of the key-wrap problem. In Vaudenay, S., ed.: Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings. Volume 4004 of Lecture Notes in Computer Science., Springer (2006) 373–390
16. Zhu, B., Dong, X., Yu, H.: MILP-based Differential Attack on Round-reduced GIFT. IACR Cryptol. ePrint Arch. **2018** (2018) 390 https://eprint.iacr.org/2018/390. A corrected version of [17].
17. Zhu, B., Dong, X., Yu, H.: MILP-Based Differential Attack on Round-Reduced GIFT. In Matsui, M., ed.: Topics in Cryptology - CT-RSA 2019 - The Cryptographers' Track at the RSA Conference 2019, San Francisco, CA, USA, March 4-8, 2019, Proceedings. Volume 11405 of Lecture Notes in Computer Science., Springer (2019) 372–390