Is ASCON the best choice regarding the Side-channel Analysis?

Matúš Olekšák, Vojtěch Miškovský
Department of Digital Design
Faculty of Information Technology
CTU in Prague, Czech Republic
{oleksmat,miskovoj}@fit.cvut.cz

***Abstract*—The National Institute of Standards and Technology (NIST) started challenge for the new standard of lightweight encryption to meet the requirements of IoT devices. One of the requirements for the upcoming standard was resistance against side-channel attacks. This year, they chose ASCON as the winner from the final ten. In this work, we present an overview of each finalist and how ASCON stands against the other finalists regarding side-channel attacks resistance in the research to date.**

***Index Terms*—ASCON, side-channel analysis, lightweight cryptography**

I. Introduction

Since Internet of Things (IoT) is becoming widely used, it is required to ensure data are transmitted securely. IoT devices typically do not have much computation power and are battery-powered. This implies the need for lightweight encryption standard. Recently, the National Institute of Standards and Technology (NIST) found new standard for lightweight encryption [1]. One of the requirements for the upcoming standard was resistance against side-channel attacks, since they are one of the main threats for embedded devices. For this reason, it is necessary to analyze the finalists, whether they are certainly resistant to side-channel attacks.

Main reason, why side-channel attacks are getting popular, is because they are a serious threat and are very powerful, since they can break cryptographically secure algorithms. Its principle is that physical properties of running cryptographic device are dependent on the data being processed. The side channel can be, e.g., power consumption [2], electromagnetic radiation [3] or even sound [4].

II. Goals

The first goal of this research is a basic overview of NIST lightweight encryption finalists. It is a study of algorithms with related reasearch of their side-channel analysis. Main contribution of this research is the discovery of possible side-channel attacks on the following finalists.

List of summarized goals:

- Research of those finalists
- Search of existing research on side-channel analysis of those finalists
- Comparison of side-channel security between ASCON and other finalists

III. Lightweight Cryptography Standard

A. ASCON

ASCON [5] algorithm family is capable of authenticated encryption with associated data and hashing. All members of the algorithm family operate on a 320-bit state, which is divided into 5 64-bit registers x_0-x_4. Permutation function consists of bitwise Boolean functions (AND, NOT, XOR) and rotations on 64-bit words.

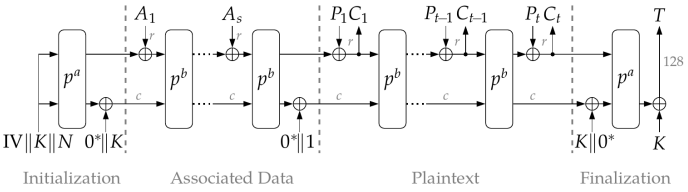

Fig. 1. Encryption diagram of ASCON. [5]

1) Side-channel Attacks: There is related work on side-channel resistance [6], in which authors successfully discovered key from unprotected implementation with 500 power traces on average. They attacked on S-Box output of ASCON-x-low-area design. With ASCON-fast design, authors had to attack on whole round transformation, since it all happens in single clock cycle. They combined 128 distinct power analysis attacks using SAT solver and found secret key with 1000 power traces on average. But attack on protected implementation (ASCON TI) was not successful even with over 1 million power traces captured.

Another attack performed on ASCON is called SCARL (Side-Channel Analysis with Reinforcement Learning) [7] and is based on deep learning. Authors used lightweight implementation on Artix-7 FPGA. They tried DPA and CPA attack with 40000 power traces, but the attack was not successful. On the other hand, SCARL attack needed only 24000 power traces in order to discover the secret key.

IV. NIST Finalists

A. Elephant

Elephant [8] is an authenticated encryption scheme, with nonce-based encrypt-then-MAC construction. There are 3 variants: Dumbo (160 bits), Jumbo (176 bits) and Delirium (200 bits). Main difference between variants is the used permutation

function. Dumbo and Jumbo use Spongent permutation, as opposed to Delirium, which uses Keccak permutation. The first two variants are well-suited for hardware implementation and the third one is intended for software implementation.

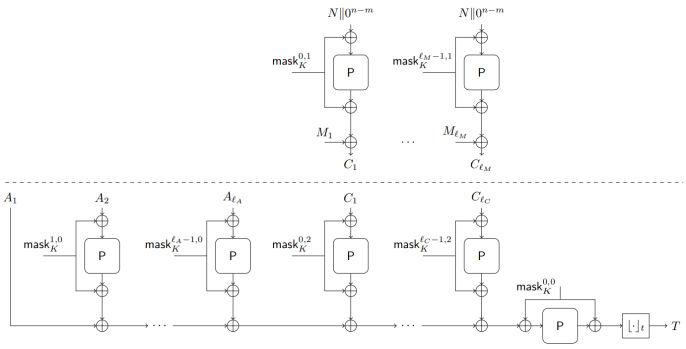

Fig. 2. Encryption diagram of Elephant. [8]

1) Side-channel Attacks: There are two unique publications related to side-channel attacks on Elephant. The first one [9] is not about particular attack, but it is about Test Vector Leakage Assessment using Welch's t-test of unprotected and protected implementations. The unprotected implementation exceeded the 4.5 threshold with only 2000 power traces. However, the protected implementation did not exceed threshold even with 100 000 power traces.

The first released Elephant attack [10] is based on CPA. It is meant for Dumbo and Jumbo variants. The author used ARM Cortex-M4 microcontroller and only around 30 power traces were needed for full key discovery. Reference C implementation was used without any protection.

B. GIFT-COFB

GIFT-COFB [11] is another Authenticated Encryption with Associated Data candidate. It uses COmbined FeedBack (COFB) mode with GIFT block cipher. COFB mode needs only single block cipher call for each input block and it has a small state size – $1.5n + k$ bits for n-bit block and k-bit key.

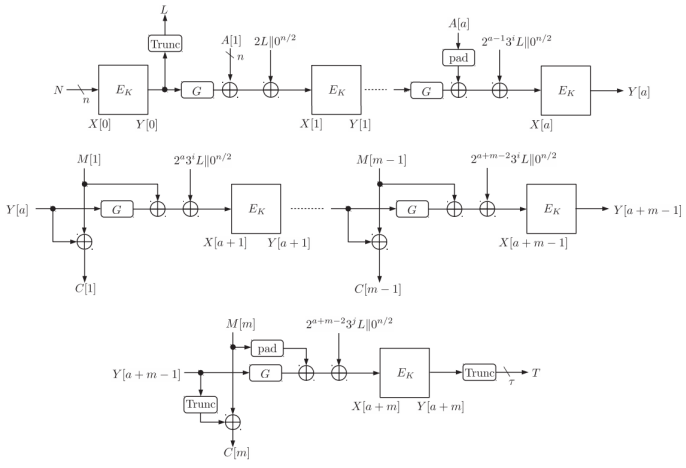

Fig. 3. Encryption diagram of GIFT-COFB. [11]

1) Side-channel attacks: There are not many publications about side-channel attack related to GIFT. There are Leakage Assessment Metrics of GIFT Block Ciphers [12], which compare PICCOLO, GIFT, and PRESENT ciphers in terms of resiliency to CPA attack. Experimental results are from 8-bit XMEGA target on ChipWhisperer platform.

Another related publication is Differential No-Fault Analysis of Bit Permutation-Based Ciphers Assisted by Side Channel [13]. It is quite revolutionary approach of side-channel attack, it combines Differential Fault Analysis, with Side-Channel Assisted Differential Plaintext Attacks. According to authors, in order to recover last round key, the attacker needs $2^{18.39}$ encryptions, which is achievable.

C. Grain-128AEAD

Grain-128AEAD [14] is a member of Grain stream cipher family. The specification is closely based on Grain-128a, introduced in 2011, has already been analyzed in literature for several years. Grain-128AEADv2 consists of two main building blocks. The first is a pre-output generator, which is constructed using a Linear Feedback Shift Register (LFSR), a Non-linear Feedback Shift Register (NFSR), and a pre-output function, while the last is an authenticator generator consisting of a shift register and an accumulator.

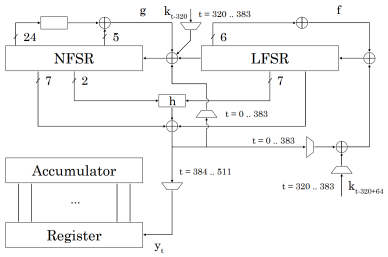

Fig. 4. Initialization diagram of Grain-128AEAD. [14]

1) Side-channel attacks: One of the published attacks [15] is the first usage of algebraic side-channel attack on stream cipher. Authors trasnformated partial side-channel leakage information into conjunctive normal form clauses and used SAT solver.

Another attack [16] is focused on protected variants of Grain family algorithms. It is combination of Differential Power Analysis and clock glitch. The leakage is exploited with power side channel during the initialization phase. Afterwards, it is combined with fault injection. Glitches were affecting 128th bit of the NFSR.

D. ISAP

ISAP [17] algorithm family is specifically designed with passive side-channel attack resistance in mind. It is nonce-based authenticated cipher with associated data. Authors recommend four instances: ISAP-A-128, ISAP-A-128A, ISAP-K-128 and ISAP-K-128A. The first two instances use 320-bit ASCON permutation, while the latter two use 400-bit KECCAK permutation. Leakage is limited because of sponge-based re-keying function, which is responsible for usage of fresh keys for processing new data.

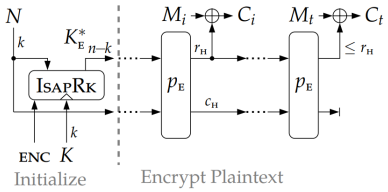

Fig. 5. Encryption diagram of ISAP. [17]

1) Side-channel attacks: There is only single one publication [18] about side-channel evaluation of ISAP. The author used software implementation by ISAP team, hardware implementation by IAIK, and hardware implementation by Ruhr-University Bochum. Afterwards, CPA attack was used, but it was not able to recover private key under given implementations.

E. PHOTON-Beetle

PHOTON-Beetle [19] is another authenticated encryption and hash family. Both modes can be parametrized by the rate of message absorption. It uses PHOTON_{256} permutation and sponge-based mode Beetle.

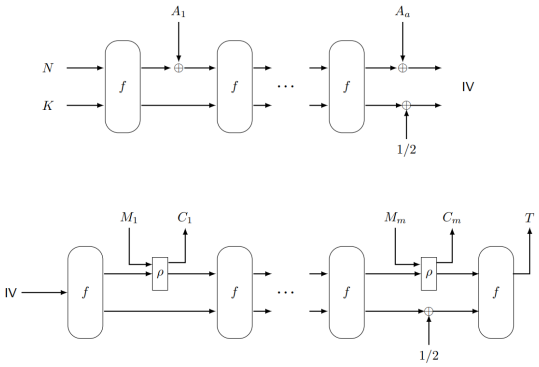

Fig. 6. Encryption diagram of PHOTON-Beetle. [19]

1) Side-channel attacks: There is known template attack [20] on PHOTON-Beetle. Author targeted on MixColumnSerial operation of the first round. It was captured about 20000 traces to generate templates. Authors used Hamming Weight as a leakage function, since they attacked on 4-bit elements, they divided traces into 5 sets. Authors observed, that even plugging device into different USB port of the same computer, which was used for template creation, resulted in incorrect predictions.

With 150 power traces captured, the successful key recovery rate was about 50% and it was achieved with exhaustive search of four most likely values returned from template attack. Without this search it was between 12% and 23%.

Recently published fault attack [21] describes two models - random fault and known fault. The first one needs $2^{37.15}$ of faulty queries and the second one only $2^{11.05}$, but attacker needs to know faulty value. Both of the attacks were successful.

F. Romulus

Another finalist is Romulus [22], which is based on tweakable block cipher Skinny. Four variants were submitted: Romulus-N (nonce-based AE), Romulus-M (nonce misuse-resistant), Romulus-T (leakage resilient) and Romulus-H (hash function).

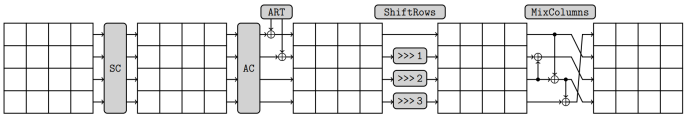

Fig. 7. Diagram of Romulus round function. [22]

1) Side-channel attacks: There are two publications about side-channel attacks on Romulus-N. The first one [20] describes CPA attack. Author attacked on SubCells of the second round to discover the 8 most significant bytes of the key, since it is the first round after secret key was added. To get the 8 least significant bytes of the key, it was needed to attack on SubCells at the third round as it is the first time this part of secret key is used. The attack is successful between 69% and 85% with number of traces between 1800 and 2400.

The second publication [23] is about side-channel leakage assessment of first order masked Romulus-N. Authors performed Welch's t-test, X^2-test and deep learning leakage assessment. With Welch's t-test and X^2-test, there were some statistically significant results only in case of checking last bit of the first byte of the input nonce in hardware implementation. But in software implementation, there were no statistically significant results. Because of that, authors focused on software implementation with deep learning leakage assessment. They achieved over 98% accurancy in checking last bit of the first byte of the input nonce and intermediate value. Authors also treid CPA and template attack, but they were unsuccessful.

G. SPARKLE

SPARKLE [24] family consists of AEAD algorithm called SCHWAEMM and hash algorithm ESCH. ESCH is available in two instances: 256-bit (based on SPARKLE384) and 384-bit (based on SPARKLE512). SPARKLE is based on SPARX, but it has wider block size and a fixed key size. As the name suggests, it is an ARX algorithm with operations on 32-bit words.

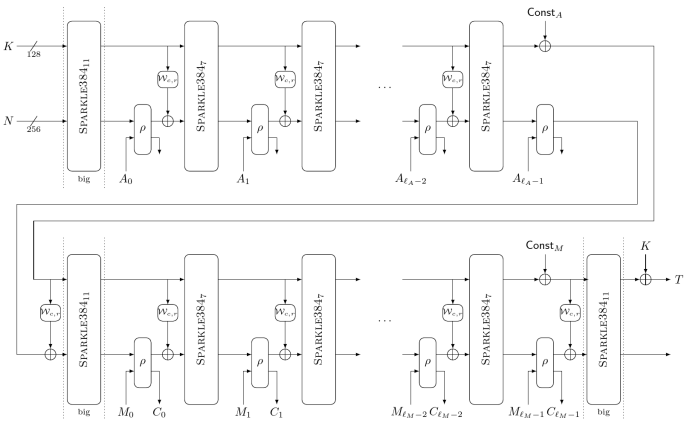

Fig. 8. Encryption diagram of Sparkle. [24]

1) Side-channel attacks: First publication [26] related to side-channel attacks on SPARKLE was about implementation of protected version of SCHWAEMM and COMET-CHAM. Authors have not tried to attack on either unprotected or protected version of mentioned algorithms, they only measured power traces and calculated t-test values. They demostrated that unprotected versions exceed threshold of $|4.5|$, but protected version does not. Protection was based on 3-share TI KSA scheme.

Second and the latest publication [25] is about CPA and DLPA on SCHWAEMM256-128. Authors implemented SCHWAEMM256-128 on an unspecified device and measured 2000 traces for each of 320 different private keys. However, they were unable to recover keys through CPA nor DLPA.

H. TinyJambu

TinyJambu [27] is a small state variant of JAMBU mode. It has only 128-bit state and 32-bit message block size. TinyJambu supports 128-bit, 192-bit and 256-bit key sizes. All variants use 96-bit nonce and 64-bit tag. Permutation is based on nonlinear feedback shift register.

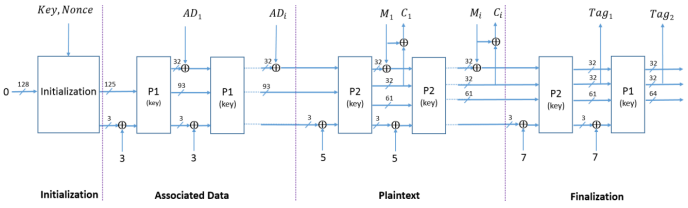

Fig. 9. Encryption diagram of TinyJambu. [27]

1) Side-channel attacks: There is one known publication [28] about Differential Analysis aided Power Attack. In case of 32-bit architecture, authors were capable of discovery of 32 bits of private key. It is because of possibility to affect only 32 bits of NFSR.

Another publication [29] is related to Test Vector Leakage Assessment of TinyJambu and protected implementation. The platform of NewAE CW305 SCA board with FPGA Artix-7 was used for testing. Protection was achieved with Domain-Oriented Masking. Protected version with measured 1 million power traces did not exceed threshold of $|4.5|$ of t-test value.

I. Xoodyak

The alphabetically last finalist is Xoodyak [30]. It uses XOODOO permutation with 384-bit state, which is represented by 3 planes of 128 bits each. Design is inspired by KECCAK-p and has several mechanisms to protect against side-channel attacks.

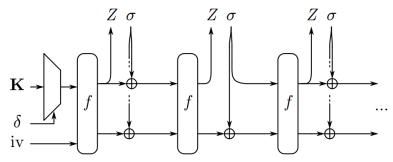

Fig. 10. Diagram of keyed duplex construction of Xoodyak. [30]

1) Side-channel attacks: The only side-channel attack [32] is CPA inspired by DPA attack called Keyak, which was based on Keccak-p. Measurement was made on Piñata development board with STM32F4. However, the publication is quite brief on Xoodyak CPA attack description.

Another side-channel related publication [31] is about countermeasure for side-channel leakage, which was primarily made for fault injection countermeasure. It was implemented on SAKURA-G target board with Spartan-6 FPGA. Results show, that side-channel leakage was lowered by 30%, but it does not offer acceptable protection yet as a stand-alone countermeasure.

V. Conclusion

Side-channel attacks against ASCON has already been proposed and proved to be effective. That means, there are some weak spots in terms of side-channel security. Threshold implementation of ASCON has been proposed, which is resistant to side-channel attack according to authors, but the area increased from 2.57 kGE to 7.97 kGE and power consumption increased from 15 μW to 45 μW [6].

Algorithm	Publications	Attacks	Successful Attacks
ASCON	4	3	3
Elephant	3	2	1
GIFT-COFB	3	3	3
Grain-128AEAD	3	3	3
ISAP	3	1	0
PHOTON-Beetle	2	2	2
Romulus	2	1	1
Sparkle	2	1	0
TinyJAMBU	2	1	1
Xoodyak	3	1	0

TABLE I
TABLE SUMMARIZING NUMBER OF SIDE-CHANNEL RELATED PUBLICATIONS.

Table I shows, that there has been at least three successful attacks presented in public literature prior to the final candidate selection. In fact, ASCON happened to be among the most successfully attacked candidates. This implies, that ASCON was not great choice in terms of side-channel attack resistance. Regarding the fact, that there are other finalists, which were not successfully attacked using side-channel attacks yet, the SCA resistance of ASCON is not the reason of its selection as the NIST standard for lightweight cryptography. This may represent a weak spot of this standard in the future.

VI. Aknowledgement

This research has been supported by the project SGS20/211/OHK3/3T/18 of CTU in Prague, and Student Summer Research Program 2022 of FIT CTU in Prague.

References

[1] Announcing Lightweight Cryptography Selection — CSRC. 2021., https://csrc.nist.gov/News/2023/lightweight-cryptography-nist-selects-ascon
[2] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential Power Analysis. 1998.,https://www.paulkocher.com/doc/DifferentialPowerAnalysis.pdf
[3] Anh Do, Soe Thet Ko, Aung Thu Htet. Electromagnetic Side-Channel Analysis on the Intel Atom Processor. 2013., https://web.wpi.edu/Images/CMS/ECE/MQP_Report_EM_Analysis__6.pdf

[4] Daniel Genkin, Adi Shamir, Eran Tromer. RSA key extraction via low-bandwidth acoustic cryptanalysis. 2014., https://link.springer.com/chapter/10.1007/978-3-662-44371-2_25

[5] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, Martin Schläffer. Ascon v1.2. 2021., https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/ascon-spec-final.pdf

[6] Hannes Gross, Erich Wenger, Christoph Dobraunig, Christoph Ehrenhöfer. Ascon hardware implementations and side-channel evaluation. 2017., https://doi.org/10.1016/j.micpro.2016.10.006

[7] Keyvan Ramezanpour, Paul Ampadu, William Diehl. SCARL: Side-Channel Analysis with Reinforcement Learning on the Ascon Authenticated Cipher. 2020., https://doi.org/10.48550/arxiv.2006.03995

[8] Tim Beyne, Yu Long Chen, Christoph Dobraunig, Bart Mennink. Elephant v2. 2021., https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/elephant-spec-final.pdf

[9] Richard Haeussler. Implementation, Benchmarking, and Protection of Lightweight Cryptography Candidates. 2021. PhD Thesis. http://ebot.gmu.edu/bitstream/handle/1920/12134/Haeussler_thesis_2021.pdf

[10] Louis Vialar. Fast Side-Channel Key-Recovery Attack against Elephant Dumbo. 2022. https://eprint.iacr.org/2022/446.pdf

[11] Subhadeep Banik, Avik Chakraborti, Tetsu Iwata, Kazuhiko Minematsu, Mridul Nandi, Thomas Peyrin, Yu Sasaki, Siang Meng Sim, Yosuke Todo. GIFT-COFB v1.1. 2021., https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/gift-cofb-spec-final.pdf

[12] William Unger, Liljana Babinkostova, Mike Borowczak and Robert Erbes. Side-channel Leakage Assessment Metrics: A Case Study of GIFT Block Ciphers, 2021 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2021, pp. 236-241, https://doi.org/10.1109/ISVLSI51109.2021.00051

[13] Xiaolu Hou, Jakub Breier and Shivam Bhasin. DNFA: Differential No-Fault Analysis of Bit Permutation Based Ciphers Assisted by Side-Channel, 2021 Design, Automation & Test in Europe Conference & Exhibition (DATE), 2021, pp. 182-187, https://doi.org/10.23919/DATE51398.2021.9474154.

[14] Martin Hell, Thomas Johansson, Willi Meier, Jonathan Sönnerup, Hirotaka Yoshida, Alexander Maximov. Grain-128AEADv2 - A lightweight AEAD stream cipher. 2021., https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/grain-128aead-spec-final.pdf

[15] Asif Raza Kazmi, Mehreen Afzal, Muhammad Faisal Amjad, Haider Abbas and Xiaodong Yang, Algebraic Side Channel Attack on Trivium and Grain Ciphers, in IEEE Access, vol. 5, pp. 23958-23968, 2017, https://doi.org/10.1109/ACCESS.2017.2766234.

[16] Abhishek Chakraborty, Bodhisatwa Mazumdar and Debdeep Mukhopadhay, Combined Side-Channel and Fault Analysis Attack on Protected Grain Family of Stream Ciphers, Cryptology ePrint Archive, Paper 2015/602, 2015, https://eprint.iacr.org/2015/602

[17] Christoph Dobraunig, Maria Eichlseder, Stefan Mangard, Florian Mendel, Bart Mennink, Robert Primas, Thomas Unterluggauer. ISAP v2.0. 2021., https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/isap-spec-final.pdf

[18] Yuhang Ji. Side-channel Evaluation of ISAP. 2022., https://cryptography.gmu.edu/athena/LWC/Reports/SJTU/SJTU_Report_HW_4_candidates_RUB.pdf

[19] Zhenzhen Bao, Avik Chakraborti, Nilanjan Datta, Jian Guo, Mridul Nandi, Thomas Peyrin, Kan Yasuda. PHOTON-Beetle. 2021., https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/photon-beetle-spec-final.pdf

[20] Louis VIALAR; DES GLYCINES, Chemin. Side Channel Analysis of NIST Lightweight Cryptography Candidates., https://ceyal.me/thesis.pdf

[21] Jana Amit, Paul Goutam. 2022. Differential Fault Attack on PHOTON-Beetle. In Proceedings of the 2022 Workshop on Attacks and Solutions in Hardware Security (ASHES'22). Association for Computing Machinery, New York, NY, USA, 25–34. https://doi.org/10.1145/3560834.3563824

[22] Tetsu Iwata, Mustafa Khairallah, Kazuhiko Minematsu, Thomas Peyrin, Chun Guo. Romulus v1.3. 2021., https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/romulus-spec-final.pdf

[23] Dawu Gu, et al. Side-Channel Evaluation on Protected Implementations of Several NIST LWC Finalists. 2022. https://cryptography.gmu.edu/athena/LWC/Reports/SJTU/SJTU_Report_HW_4_candidates_RUB.pdf

[24] Christof Beierle, Alex Biryukov, Luan Cardoso dos Santos, Johann Großschädl, Léo Perrin, Aleksei Udovenko, Vesselin Velichkov, Qingju Wang, Amir Moradi, Aein Rezaei Shahmirzadi. Schwaemm and Esch: Lightweight Authenticated Encryption and Hashing using the Sparkle Permutation Family. 2021., https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/sparkle-spec-final.pdf

[25] Cassi Chen, et al. CPA and DLPA on Hardware Implementations of SCHWAEMM and GIFT., https://www.michelliao.com/content/files/2022/11/Side_Channel_Attacks_and_Neural_Networks.pdf

[26] Flora Coleman, Behnaz Rezvani, Sachin Sachin and William Diehl, Side Channel Resistance at a Cost: A Comparison of ARX-Based Authenticated Encryption, 2020 30th International Conference on Field-Programmable Logic and Applications (FPL), Gothenburg, Sweden, 2020, pp. 193-199, https://doi.org/10.1109/FPL50879.2020.00040.

[27] Hongjun Wu, Tao Huang. TinyJAMBU v2. 2021., https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/tinyjambu-spec-final.pdf

[28] Shivam Bhasin, et al. Survey on the Effectiveness of DAPA-Related Attacks against Shift Register Based AEAD Schemes. Cryptology ePrint Archive, 2022. https://eprint.iacr.org/2022/561.pdf

[29] Abubakr Abdulgadir, et al. Side-Channel Resistant Implementations of Three Finalists of the NIST Lightweight Cryptography Standardization Process: Elephant, TinyJAMBU, and Xoodyak. 2022. https://csrc.nist.gov/csrc/media/Events/2022/lightweight-cryptography-workshop-2022/documents/papers/side-channel-resistant-implementations-of-three-finalists-of-the-nist-lwc-standardization-process.pdf

[30] Joan Daemen, Seth Hoffert, Michaël Peeters, Gilles Van Assche, Ronny Van Keer, Silvia Mella. Xoodyak v2. 2021., https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/xoodyak-spec-final.pdf

[31] Lejla Batina, et al. Side-Channel Evaluation Report on Implementations of Several NIST LWC Finalists. 2022. https://cryptography.gmu.edu/athena/LWC/Reports/Radboud/Radboud_Report_SW_3_candidates.pdf

[32] Konstantina Miteloudi, Łukasz Chmielewski, Lejla Batina, Nele Mentens, "Evaluating the ROCKY Countermeasure for Side-Channel Leakage," 2021 IFIP/IEEE 29th International Conference on Very Large Scale Integration (VLSI-SoC), Singapore, Singapore, 2021, pp. 1-6, https://doi.org/10.1109/VLSI-SoC53125.2021.9606973

[33] Guozhen Liu, Jingwen Lu, Huina Li, Peng Tang, Weidong Qiu. Preimage Attacks Against Lightweight Scheme Xoodyak Based on Deep Learning. In: Arai, K. (eds) Advances in Information and Communication. FICC 2021. Advances in Intelligent Systems and Computing, vol 1364. Springer, Cham. https://doi.org/10.1007/978-3-030-73103-8_45