Recent Advances and Trends in Lightweight Cryptography for IoT Security

Nilupulee A. Gunathilake, Ahmed Al-Dubai, William J. Buchanan
School of Computing, Edinburgh Napier University, United Kingdom
nilupulee.gunathilake@napier.ac.uk, a.al-dubai@napier.ac.uk, b.buchanan@napier.ac.uk

Abstract—**Lightweight cryptography is a novel diversion from conventional cryptography to minimise its high level of resource requirements, thus it would impeccably fit in the internet-of-things (IoT) environment. The IoT platform is constrained in terms of physical size, internal capacity, other storage allocations like RAM/ROM and data rates. The devices are often battery powered, hence maintenance of the charged energy at least for a few years is essential. However, provision of sufficient security is challenging because the existing cryptographic methods are too heavy to adopt in the IoT. Consequently, an interest arose in the recent past to construct new cryptographic algorithms in a lightweight scale, but the attempts are still struggling to gain robustness against improved IoT threats and hazards.**

There exists a lack of literature studies to offer overall and up-to-date knowledge on lightweight cryptography. Therefore, this effort is to bridge the areas in the subject by summarising the content we explored during our complete survey recently. This work contains the development of lightweight cryptographic algorithms, its current advancements and futuristic enhancements. In contrast, this covers the history, parametric limitations of the invented methods, research progresses of cryptology as well as cryptanalysis.

Index Terms—**IoT, lightweight cryptography, side-channel attack**

I. Introduction

In modern cryptography, AES (Advanced Encryption Standard), DES (Data Encryption Standard) and RSA (Rivest-Shamir-Adleman) are effective in general purpose computing due to their compatibility with the resource requirements, *i.e., high-end processors, large internal capacities in Giga/TeraByte, etc*. The nature of the internet-of-things (IoT) is quite distinct because of its constrained resource management, *i.e., low-end processors, small data rates in kbps, etc*. Therefore, execution of the conventional methods on IoT devices would cause degradation of device performance and/or malfunction over the overall application deliverables, *i.e., fast battery drainage, high latency, etc*. Thus, a whole new perspective of cryptographic vision towards lightweight inventions for IoT security is crucial.

The interest in lightweight cryptography has been there in research for about ten years now. Nevertheless, the conventional cryptography also initially began on a lightweight scale a few decades back, compatible with the very first microprocessor which was 4b, *i.e., A5/1, CMEA, DSC, etc* [1]. Each of those method was either broken or reverse engineered eventually, due to simplicity of their operations. IoT threats and hazards are probably much more advanced and sophisticated, hence the aim must be increased security for decreased resource requirements. In contrast, safety assurance over IoT transmission technologies/protocols is an unavoidable necessity for accurate encryption/decryption and encoding/decoding, *i.e., ZigBee, BLE, LoRaWAN, etc*.

Lightweight cryptography is categorised as symmetric, asymmetric and hash. In the present, many symmetric and hash implementations are available to try in practical systems, *i.e., PRESENT, KLEIN, PHOTON, etc.*, whereas a few asymmetric algorithms are accessible in comparison, *i.e., elliptic light (ELLI) derived from elliptic curve cryptography (ECC)*. Because of the difficulties associated with traditional public key methods in such a constrained platform, it is extremely challenging to innovate ways to gain asymmetric adaptability. Even so, researchers continue to conduct asymmetric approaches in order to provide a better quality-of-service (QoS) via post-quantum[1] as well as lattice-based[2] cryptography, *i.e., cryptoGPS, ALIKE, etc*.

The predictions in 2000s were that it would be problematic to implement lightweight hash functions, but hybrid techniques via a combination of conventional hash methods and lightweight block ciphers would be a solution [2]. However, several lightweight hash inventions have been introduced theoretically later, yet their performance to be verified practically. There has been an immense attention given to block ciphers from the beginning, and stream ciphers became trending after a while. Moreover, sponge-based (SP) hash/message authentication code (MAC), individual authenticated ciphers (authenticated encryption - AE), SP based AE and block cipher (BC) based AE are available in academic and industrial researches [3]. Fig.1 illustrates the scale of the lightweight algorithms published from 1994 – 2019.

Lightweight cryptography is subdivided considering its applications/limitations as follows [4];

- **Ultra-lightweight**: Tailored in specific areas of the algorithm, *i.e., selected microcontrollers (μC)/cipher sections/operations – PRESENT, Grain (low gate count in hardware), Quarma (low latency in hardware) and Chaskey (high speed on μCs)*
- **Ubiquitous lightweight**: Compatible with wide variety of platforms, *i.e., 8b to 32b μCs – Ascon, GIMLI and*

[1] cryptographic primitives that involve quantum phenomena

[2] cryptographic primitives that involve lattices

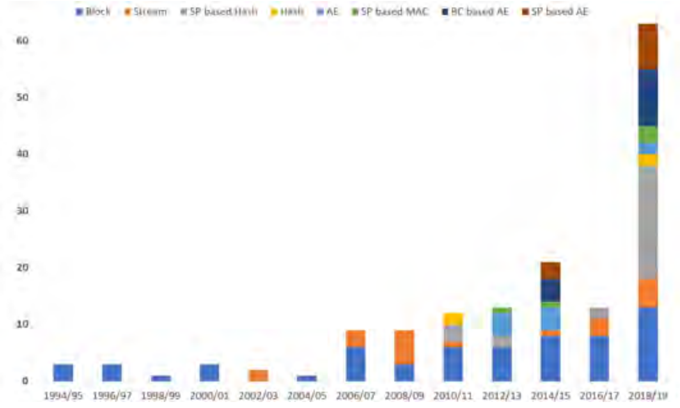

Fig. 1. Published lightweight algorithms from 1994-2019

AES

A. *Our Contribution*

Inventions, observations and adaption of lightweight cryptography are still emerging, so that the outcomes are rapidly being updated over vastly distributed areas. Therefore, literature studies are very useful references for researchers to acquire up-to-date information. Recent survey publications are mainly regarding a narrowed down subject area (specific algorithmic group/experimental type). Thus, our effort is to bridge all areas associated in lightweight cryptography to offer a comprehensive overview.

This complete survey summarises the history, development of all available algorithm types followed by standardisation process, benchmarking and finally, security analysis including side-channel leakage. This work also mentions the identified research gaps to be improved in the future.

II. Lightweight Cryptography

A. *History*

The preliminary applications of lightweight algorithms go back to late 1980s. Many of those were broken just after those were published. Their upgraded versions continued in use, but eventually many were replaced by AES due to its superior strength and flexibility. Table 3 of [1] includes some ciphers used in history that were in lightweight scale.

B. *Development*

The trends in cryptography contain both linear and non-linear operations. Non-linearity offers unpredictability to cryptographic outputs whereas linearity is for provision of diffusion, *i.e., absolute dependability in round-based functionalities*. In lightweight primitives, the impending trends are as in Table I along with some of the examples.

The gain of small hardware footprints depends on the programming language too. Consequently, attention has been refocused on the use of assembly language in implementations. In fact, the ultimate level of lightweight-ness would be possible if security functions are executed by lightweight scripting languages, *i.e., lo, wren, squirrel, etc*. There is no evidence of any initial attempt taken regarding the matter.

TABLE I
Lightweight ciphers based on trending method

Trend	Type	Examples
LUT	Non-linear	Piccolo, PRESENT and Prince
Bit-sliced based	Non-linear	3-Way, Ascon, Fantomas and iScream
ARX based	Non-linear	Chaskey, Hight, Speck and XTEA
MDS matrices	Linear	CLEFIA, LED, Lesamnta-LW and PHOTON
Bit permutations	Linear	FLY, RECTANGLE, RoadRunneR and Piccolo
XOR and rotations	Linear	Blake2s/b, GIMLI, GLUON and Noekeon
***LUT**: Look Up Table, **ARX**: Addition-Rotation-XOR, **MDS**: Maximum Distance Separable*		

III. Symmetric light-weight Crypto

These are usually adopted from a conventional algorithm and their improved light-weight architecture is introduced as either versions or in a new name, *i.e., AES based light-weight techniques [5]–[7], Prince and PRESENT derived from AES s-box* [8]. The majority is still in their trial phases because of deficiency, inadaptability in IoT devices and inaccuracy in decryption results.

A. *Block ciphers*

These take the highest contribution. The most common block ciphers along with their ordinary parameters are in Table II. Additional ones may be referred in [1], [2], [9]–[11]. Among all, KLEIN, Lilliput, PRESENT, Rectangle and Skinny are known as ultra-light-weight because their key sizes, block sizes and computational rounds are in the least range. Also, XTEA which an extended version of TEA, is contemplated to be super-fast. Simon and Speck families [12] used to be very promising due to their satisfying scalability, but dissatisfaction in the security later.

TABLE II
Most common symmetric light-weight block ciphers

Cipher	Key (b)	Block Size (b)	Rounds
3-Way	96	96	11
AES	128/192/256	128	10/12/14
CLEFIA	128/192/256	128	18/22/26
GIFT	128	64/128	28/40
iScream	128	128	12/14
KLEIN [13]	64/80/96	64	12/16/20
LBlock	80	64	32
LEA	128/192/256	128	24/28/32
Lilliput	80	64	30
Midori	128	64/128	16/20
PRESENT	80/128	64	31
PRINCE	128	64	12
Qarma	128/256	64/128	16/24
RECTANGLE	80/128	64	25
Robin	128	128	16
SKINNY	64–384	64/128	32–56
SPARX	128/256	64/128	24–40
TEA	128	64	32
XTEA	128	64	64
Zorro	128	128	24

B. *Stream ciphers*

The current implementations are as in Table III. Enocoro-80, Grain and Trivium [2] are known to be well suited in terms of light-weight primitives. Even though A2U2 has the smallest key size, it would probably be insecure at this stage as sufficient robustness is benchmarked above 72-bit size in cryptography.

TABLE III
SYMMETRIC LIGHT-WEIGHT STREAM CIPHERS

Cipher	**Key (b)**	**IS (b)**	**IV (b)**
A2U2	61	95	64
Enocoro-80	80	176	64
Espresso	128	256	96
F-FCSR-H/16 v3	80/128	160/256	80/128
Grain	80/128	160/256	64/96
MICKEY v2	80/128	200/320	0–80/0–128
Plantlet	80	110	90
Sprout	80	89	70
Rabbit	128	513	64
SNOW 2.0	128/256	576	128
SNOW 3G	128	576	128
Trivium	80	288	80

C. Dedicated AE

Available AE methods are as in Table IV. A greater interest can be seen in ARCON, Ascon and Hummingbird-2 in the present because of their promising functionalities towards adequate security measures [14]. Nonetheless, Hummingbiard-2 is still vulnerable to differential attacks in a related key setting. Nonce misuses could be identified in Helix and FIDES was broken shortly after its publication. Full-round NORX v2 could be affected by forgery and key recovery attacks, thus, a later version was introduced to prevent those [15], [16].

TABLE IV
DEDICATED LIGHT-WEIGHT AE METHODS

Cipher	**Key (b)**	**IS (b)**	**IV (b)**
ACORN	128	293	128
ALE	128	128	128
ASC-1	256	384	56
Ascon	96/128	320	96/128
FIDES	80/96	80/96	160/192
Helix	256	160	128
Hummingbird-2	128	128	64
LAC	80	144	64
NORX32	128	512	128
Sablier	80	208	80
TriviA	128	384	128

D. MAC

These are the least contributors. However, the widely accepted one here is Chaskey which has 128b of IS, key and block sizes. It is an ARX based method which requires 3334.33 of GE plus an operating clock frequency of 1MHz for signing. The other one is SipHash which has 64b of key and block sizes along with 256 IS. The latest report of NIST [3] approves TuLP and LightMAC as well.

IV. ASYMMETRIC LIGHTWEIGHT CRYPTO

Research outcomes of asymmetric implementations are still at a preliminary stage. Satisfactory theoretical impacts can be seen in ECC [9], [17]–[19], ELLI [11] and hyper-elliptic curve cryptography (HECC) [20] that are based on mathematical elliptic curve. Those are approved by both ISO/IEC and NIST standards. Alternative efforts are seen in ALIKE and cryptoGPS recommended by ISO/IEC, post-quantum basis multivariate quadratic (MQ) algorithmic attempts by the NIST and N-th degree truncated polynomial ring (NTRU) which is a lattice crypto technique.

Among those, ECC is known to have short key length, low processing time on 8-bit μC and small signatures [19]. NTRU is more efficient on 3000 of GE while maintaining short signatures in general, but flexibility is highly required due to its instability [21]. On the other hand, MQ algorithms are struggling with robustness, enormous key lengths and unaffordability yet.

V. HASH FUNCTIONS

Numerous lightweight hashing resolutions exist where families of Keccak, Quark and SPONGENT [22] are enhancing their versions to improve their performance. Keccak is highly demanding due to its small digest and code size. Although PHOTON [23] is equally considered, its code is slightly longer. Table V contains typical parametric values of those. Some other methods are Armadillo, QUARK, Lesamnta-LW, GLUON and SPN-Hash [1], [3], [14]. The step-by-step internal mathematical process of lightweight hashing is available in [11].

TABLE V
MOST DEMANDING LIGHTWEIGHT HASH FUNCTIONS

Cipher	**Digest**	**Code (b)**	RAM (B)	**RAM (stack)**
Keccak1	160	752	5/45	3
Keccak2	256	608	18/92	4
PHOTON1	160	764	9/39	11
PHOTON2	256	1244	4/68	10
S-Quark	256	1106	4/60	5
D-Quark	176	974	2/42	5
SPONGENT1	256	364	16/96	5
SPONGENT2	160	598	10/60	6

VI. STANDARDISATION

The professional bodies involved in this can be classified into government agencies, regional organizations and international associations.

- Federal Information Processing Standards (FIPS) 185 and 197 by the USA
- Networked European Software and Services Initiative (NESSIE) and eSTREAM portfolio by the EU
- Cryptography Research and Evaluation Committees (CRYPTREC) by the government of Japan
- Telecommunications Technology Association (TTA) by South Korea
- GOST R 34.12-2015 by the government of Russia
- ISO/IEC international standards in issues of 29167, 29192-2, 29192-3, 29192-5, 18033-3 and 18033-4
- National Institute of Standards and Technology (NIST) standards in issues of NISTIR 8268 and NISTIR 8114

The NIST is conducting a global lightweight cryptography competition to verify performances [14]. The winners will be finalised before end of this year. In addition, post-quantum cryptography standardisation competition of theirs would probably provide useful insights on asymmetric lightweight cryptography.

VII. Benchmarking

Although there are not any defined threshold levels for lightweight-ness, the following are generally considered by the standardisation bodies [24];

- 80b is the minimum security strength whereas 112b is advocated for long time security requirements
- 25% - 30% of minimum security margin adaption
- Hardware implementation to be up to standardised levels, *i.e., chip area, etc.*
- Software execution to be verified through standardised benchmarking tools, *i.e., FELICS*
- Clear licensing and liability where necessary
- Maturity of the cryptographic mechanism, *i.e., entropy*

Fair Evaluation of Lightweight Cryptographic Systems (FELICS) [25] is the utmost benchmarking tool that is being upgraded regularly for software benchmarking. It compares code size, RAM consumption and throughput across algorithms over a variety of strategies. Then it summarises into a parameter called the figure of merit (FoM) where the lower, the better. Table 1 of [11] is an example for counter mode encryption of 128b. In addition, eXternal Benchmarking extension (XBX), BLOC project and CRYPTREC contribute in the field [1].

In hardware benchmarking, the metrics depend on the exact technological platform. The ATHENa (Automated Tool for Hardware EvaluatioN) project and CRYPTREC are the main partners in the arena.

VIII. Security Analysis

A. Cryptological Approaches

A survey [10] mentions that it is possible to gain a 12% reduction in area and a 20% increase in speed via AES optimisation. Another study [6] emphasises on an AES-128 modification on LoRaWAN by reducing rounds from 10 to 5, where 26.2% of encryption power consumption was minimised. It further proves its resistance to known-key, replay and eavesdropping attacks theoretically. The researches [5] and [26] propose trustworthy neighbourhood mechanisms to enhance effective security schemes depending on the connection history.

Successful trials can be seen in cryptographic key management methodologies that encourage each node on the network to have a different key [27], [28]. Then once a key is leaked, only that particular node would be at risk without compromising the entire network. The updatability over keys offers a better quality of service (QoS) which was impossible for some time in the past. In fact, a reduced number of GE enhances energy efficiency. The studies [29] and [27] prove the possibility of battery life maintainability from 5 to 10 years via their lightweight scheduling mechanisms. The study [29] faced an introduction of overheads when the security was better upgraded, but further optimisation lessened 43% of the overheads from the end devices and 48% from the network server edge.

B. Cryptanalysis Approaches

A study [30] presents the first third-party cryptanalysis of BORON block cipher against differential and linear criteria. The studies [31], [32] and [33] analyse the robustness of Ascon v1.2, COMET and ESTATE respectively.

The researches [34] and [13] observe that KLEIN is an ultra-lightweight side-channel resistant crypto because of its Substitution-Permutation Network (SPN) structure. The analysis [34] validates its results up to first-order attacks, also stating that it may be still vulnerable to higher-order incidents due to the exponential growth in data complexity. An AI-based approach over AES and PRESENT was taken by [35] concludes that there is not any significant difference in side-channel vulnerability between AES and PRESENT in comparison to both 4b and 8b S-box constructions. Another study [36] demonstrates optimal leakage models for ciphertext-only fault attacks (CFA) for SIMON, PRINCE and AES. A correlation power analysis (CPA) on PRESENT [37] was able to derive the first 8B of the encryption key. The highest percentage of work involves either CAP or differential power analysis (DPA). Only a few studies on electromagnetic (EM) analysis are available. One of the successful experiments is a differential EM analysis (DEMA) of PRESENT [38]. It verifies the tamper resistance using several selection functions. Other vital impactors like optical, clock, cache and so on, based work are yet unavailable.

IX. Conclusions

Adequate IoT security still struggles to provide compatible cryptographic primitives in terms of lightweight to cope with possible and futuristic IoT hazards and threats. The concept of lightweight cryptography was introduced to overcome the challenge.

Lightweight cryptographic functions are still emerging to deliver precise privacy and data protection via accurate encryption and decryption models. There exist numerous proposed lightweight ciphers in all forms (symmetric, asymmetric and hash) though, many are still under verification and commercially not available, *i.e., PRESENT, KLEIN, Grain v2, ECC, etc*. This work particularly identifies a lack of consideration over physical leakage analysis at the current status.

Government agencies, regional organisations and international associations are involved in standardisation process where ISO/IEC and NIST are the leading contributors. FELICS is the predominating benchmarking tool for software implementations whereas hardware implementations are case dependent. Also, improvement of lightweight scripting languages would probably cause achieving the ultimate level of lightweight-ness.

References

[1] A. Biryukov and P. Léo, "State of the Art in Lightweight Symmetric Cryptography," *IACR Cryptology ePrint Archive*, pp. 511–566, 11 2017. [Online]. Available: https://www.semanticscholar.org/paper/State-of-the-Art-in-Lightweight-Symmetric-Biryukov-Perrin/532441547d905feae7a65f635594585c96d2987b

[2] M. Katagi and S. Moriai, "Lightweight Cryptography for the Internet of Things," *Sony Corporation*, pp. 7–10, 2008. [Online]. Available: http://www.iab.org/wp-content/IAB-uploads/2011/03/Kaftan.pdf

[3] N. I. R. 8114, "Report on Lightweight Cryptography," 03 2017. [Online]. Available: https://csrc.nist.gov/CSRC/media/Publications/nistir/8114/draft/documents/nistir_8114_draft.pdf

[4] N. A. Gunathilake, W. J. Buchanan, and R. Asif, "Next Generation Lightweight Cryptography for Smart IoT Devices: Implementation, Challenges and Applications," in *IEEE 5th World Forum on Internet of Things (WF-IoT)*, 04 2019, pp. 707–710, doi: 10.1109/WF-IoT.2019.8767250.

[5] S. Naoui, M. Elhdhili, and L. Saidane, "Enhancing the security of the IoT LoraWAN architecture," 11 2016, pp. 1–7, doi: 10.1109/PEMWN.2016.7842904.

[6] K. Tsai, Y. Huang, F. Leu, I. You, Y. Huang, and C. Tsai, "AES-128 Based Secure Low Power Communication for LoRaWAN IoT Environments," *IEEE Access*, vol. 6, pp. 45 325–45 334, 2018, doi: 10.1109/ACCESS.2018.2852563.

[7] X. Fei, K. Li, and W. Yang, "A Fast Parallel Cryptography Algorithm based on AES-NI, volume = 31, journal = Journal of Intelligent Fuzzy Systems, note = doi: 10.3233/JIFS-169039," pp. 1–9, 07 2016.

[8] T. Goyal, V. Sahula, and D. Kumawat, "Energy Efficient Lightweight Cryptography Algorithms for IoT Devices," *IETE Journal of Research*, pp. 1–14, 11 2019, doi: 10.1080/03772063.2019.1670103.

[9] S. Dhanda, B. Singh, and P. Jindal, "Lightweight Cryptography: A Solution to Secure IoT," *Wireless Personal Communications*, pp. 1–34, 01 2020, doi: 10.1007/s11277-020-07134-3.

[10] I. K. Dutta, B. Ghosh, and M. Bayoumi, "Lightweight Cryptography for Internet of Insecure Things: A Survey," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, 01 2019, pp. 0475–0481, doi: 10.1109/CCWC.2019.8666557.

[11] W. J. Buchanan, S. Li, and R. Asif, "Lightweight Cryptography Methods," *Journal of Cyber Security Technology*, vol. 1, no. 3–4, pp. 187–201, 10 2017, doi: 10.1080/23742917.2017.1384917.

[12] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "The SIMON and SPECK Families of Lightweight Block Ciphers," in *52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, San Francisco, CA, 2015, pp. 1–6, doi: 10.1145/2744769.2747946.

[13] Z. Gong, S. Nikova, and Y. Law, *KLEIN: A New Family of Lightweight Block Ciphers*, ser. CTIT Technical Report Series. entre for Telematics and Information Technology (CTIT), 5 2010, no. TR-CTIT-10-33.

[14] N. I. of Standards and Technology. (2019, 11) Lightweight Cryptography Workshop 2019 - Accepted Papers. NIST. [Online]. Available: https://csrc.nist.gov/Events/2019/lightweight-cryptography-workshop-2019

[15] C.-I. Fan, T.-P. Chiang, and R.-H. Hsu, "Lightweight Authentication and Key Exchange Protocols with Forward Secrecy for Digital Home," *Journal of Computers*, vol. 18, pp. 61–73, 05 2007.

[16] T. Eisenbarth and S. Kumar, "A Survey of Lightweight-Cryptography Implementations," *Design Test of Computers, IEEE*, vol. 24, pp. 522–533, 12 2007, doi: 10.1109/MDT.2007.178.

[17] C. Lara-Nino, A. Díaz-Pérez, and M. Morales-Sandoval, "Elliptic Curve Lightweight Cryptography: a Survey," *IEEE Access*, vol. PP, pp. 1–1, 11 2018, doi: 10.1109/ACCESS.2018.2881444.

[18] D. Atkins and P. Gunnells, "Algebraic Eraser: A Lightweight Efficient Asymmetric Key Agreement Protocol for Use in No-power, Low-power and IoT Devices," 2015. [Online]. Available: https://www.semanticscholar.org/paper/Algebraic-EraserTM-

[19] A. Poschmann, *Lightweight Cryptography: Cryptographic Engineering for a Pervasive World*, PhD Thesis, Ruhr-University Bochum, 2009, doi: 10.1.1.182.1450.

[20] K. Nagendran, T. Nadesan, P. Chandrika, and R. Chethana, "Hyper Elliptic Curve Cryptography (HECC) to Ensure Data Security in the Cloud," 01 2018, doi: 10.14419/ijet.v7i4.19.22045.

[21] R. Xu, C. Cheng, Y. Qin, and T. Jiang, "Lighting the way to a Smart World: Lattice-Based Cryptography for Internet of Things," vol. abs/1805.04880, 2018. [Online]. Available: https://arxiv.org/pdf/1805.04880.pdf

[22] A. Bogdanov, M. Knezevic, G. Leander, D. Toz, K. Varici, and I. Verbauwhede, "Spongent: The Design Space of Lightweight Cryptographic Hashing," *IEEE Transactions on Computers*, vol. 62, no. 10, pp. 2041–2053, 2012.

[23] J. Guo, T. Peyrin, and A. Poschmann, "The PHOTON Family of lightweight Hash functions," vol. 2011, 08 2011, pp. 222–239, doi: 10.1007/978-3-642-22792-9_13.

[24] S. Renner, E. Pozzobon, and J. Mottok. (2019, 11) Benchmarking Software Implementations of 1st Round Candidates of the NIST LWC Project on Microcontrollers. National Institute of Standards and Technology (NIST). [Online]. Available: https://csrc.nist.gov/CSRC/media/Events/lightweight-cryptography-workshop-2019/documents/papers/benchmarking-software-implementations-lwc2019.pdf

[25] K. L. Gouguec. (2019, 11) FELICS-AE: A Framework to Benchmark Lightweight Authenticated Block Ciphers. National Institute of Standards and Technology (NIST). [Online]. Available: https://csrc.nist.gov/CSRC/media/Events/lightweight-cryptography-workshop-2019/documents/papers/felics-ae-lwc2019.pdf

[26] S. Naoui, M. E. Elhdhili, and L. A. Saidane, "Trusted Third Party Based Key Management for Enhancing LoRaWAN Security," in *IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)*, 10 2017, pp. 1306–1313, doi: 10.1109/AICCSA.2017.73.

[27] B. Reynders, Q. Wang, P. Tuset-Peiro, X. Vilajosana, and S. Pollin, "Improving Reliability and Scalability of LoRaWANs Through Lightweight Scheduling," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1830–1842, 2018.

[28] X. Yang, E. Karampatzakis, C. Doerr, and F. Kuipers, "Security Vulnerabilities in LoRaWAN," 04 2018, pp. 129–140, doi: 10.1109/IoTDI.2018.00022.

[29] R. Sanchez-Iborra, J. Sánchez-Gómez, S. Pérez, P. J. Fernández, J. Santa, J. L. Hernández-Ramos, and A. F. Skarmeta, "Enhancing LoRaWAN security through a Lightweight and Authenticated Key Management Approach," *Sensors*, vol. 18, no. 6, p. 1833, 2018.

[30] H. Liang and M. Wang, "Cryptanalysis of the Lightweight Block Cipher BORON," *Security and Communication Networks*, vol. 2019, pp. 1–12, 12 2019, doi: 10.1155/2019/7862738.

[31] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer. (2019, 11) Ascon v1.2 – Analysis of Security and Efficiency. National Institute of Standards and Technology (NIST). [Online]. Available: https://csrc.nist.gov/CSRC/media/Presentations/ascon-v1-2-analysis-of-security-and-efficiency/images-media/session2-mendel-analysis-of-security.pdf

[32] S. Gueron, A. Jha, and M. Nandi. (2019, 11) On the Security of COMET Authenticated Encryption Scheme. National Institute of Standards and Technology (NIST). [Online]. Available: https://csrc.nist.gov/CSRC/media/Events/lightweight-cryptography-workshop-2019/documents/papers/on-sthe-security-of-comet-lwc2019.pdf

[33] A. Chakraborti, N. Datta, A. Jha, C. M. Lopez, M. Nandi, and Y. Sasaki. (2019, 11) ESTATE Authenticated Encryption Mode: Hardware Benchmarking and Security Analysis. National Institute of Standards and Technology (NIST). [Online]. Available: https://csrc.nist.gov/CSRC/media/Events/lightweight-cryptography-workshop-2019/documents/papers/estate-authenticated-encryption-mode-lwc2019.pdf

[34] W. Li, "An Ultra-lightweight Side-channel Resistant Crypto for Pervasive Devices," vol. 10, pp. 173–186, 01 2015, doi: 10.14257/ijmue.2015.10.11.17.

[35] A. Heuser, S. Picek, S. Guilley, and N. Mentens, "Side-Channel Analysis of Lightweight Ciphers: Does Lightweight Equal Easy?" pp. 91–104, 07 2017, doi: 10.1007/978-3-319-62024-4_7.

[36] A. Singh, M. Kar, V. C. K. Chekuri, S. K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Enhanced Power and Electromagnetic SCA Resistance of Encryption Engines via a Security-Aware Integrated All-Digital LDO," *IEEE Journal of Solid-State Circuits*, 2019.

[37] O. Lo, W. J. Buchanan, and D. Carson, "Correlation Power Analysis on the PRESENT Block Cipher on an Embedded Device," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, 2018, pp. 6–11, doi: 10.1145/3230833.3232801.

[38] Y. Nozaki, T. Iwase, Y. Ikezaki, and M. Yoshikawa, "Differential Electromagnetic Analysis for PRESENT and its Evaluation with Several Selection Functions," *Journal of International Council on Electrical Engineering*, vol. 7, no. 1, pp. 137–141, 2017, doi: 10.1080/22348972.2017.1344014.