ISSN 2278-3091
Volume 8, No.3, May - June 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse47832019.pdf
https://doi.org/10.30534/ijatcse/2019/47832019

A Review on Performance Evaluation Criteria and Tools for Lightweight Block Ciphers

Deepti Sehrawat[1], Nasib Singh Gill[2]
[1,2]Department of Computer Science & Applications, Maharshi Dayanand University, Rohtak, Haryana (India)
dips.scorpio@gmail.com, nasibsgill@gmail.com

ABSTRACT

Internet of Things (IoT) has become a powerful paradigm that has made significant progress in almost all areas. It has attracted worldwide attention in the smart computing environment. Security is considered as one of the most important concerns of constraint end nodes. Providing solutions to these resource constraint devices through ordinary cryptographic solutions is not sufficient. To fulfill this gap, a relatively new field of cryptography called lightweight cryptography came into existence. Besides, ISO/IEC provides various standards related to ICT. There are several parameters for both hardware and software implementations that are set to assess the ciphers. This paper presents criteria posed by these standards that can be considered by a cipher designer so as to include cipher in this standard. A software implementation of security algorithms consider some evaluation parameters. Such performance evaluation criteria, some metrics and performance evaluation tools relevant in this context are also presented in this paper.

Key words : LBC, lightweight block cipher evaluation parameters, LBC metrics, LBC performance evaluation tools, security standards.

1. INTRODUCTION

IoT (Internet of Things) is an innovative paradigm in the setup of modern wireless telecommunication. Evolution of IoT begins with the RFID technology that allows the transmission of information via wireless communications [1]. RFID and sensors are the main participating elements in IoT smart environment. Resource-efficient crypto solutions become fundamental for realizing security in RFID tags and sensors which are the key technologies in IoT. Furthermore, wireless networks are more prone to attacks than the wired network [2]. A number of attacks can be applied to IoT based applications and to provide sufficient protection against these attacks good cryptographic solutions must be made available to these devices [3, 4]. Besides, embedded devices are memory available, low energy consumption, and etc. For such resource constraint environment of IoT, traditional security algorithms are not suitable. In this direction, to provide security for IoT based applications, lightweight cryptography came into existence [5]. These can be implemented either through software implementation or through hardware implementations. Software oriented cipher designs provide more flexibility at lower costs on manufacturing and maintenance as compared to hardware implementations [6]. This is because of its ability to provide efficient end-to-end communications [7]. Two international standards: ISO “International Organization for Standardization" and IEC "International Electro technical Commission" are meant for issuing and maintaining the standards related to ICT [8]. ISO/IEC 29192 is for standardization of lightweight ciphers. This paper presents the requirements posed by these standards on lightweight security solutions in order to include them in these standards.

The rest of the paper is structured as follows: section 2 presents the main standards relevant to lightweight cryptography. Inclusion criteria as set by ISO/IEC for the inclusion of a cipher in their list are presented in section 3. Section 4 details various performance evaluation parameters followed by performance evaluation tools which are given in section 5. Section 6 summarizes the features of good lightweight ciphers.

2. ISO/IEC CRYPTOGRAPHIC STANDARDS

Main aims of ISO/IEC are the issuance and maintenance of standards for ICT [9]. A number of standards are given by the ISO/ IEC. This section covers only those standards which are relevant to lightweight cryptography especially block ciphers and can be referred for creating algorithms for a smart environment in IoT, these are:

2.1 ISO/IEC 29167: “Information technology – Automatic identification and data capture techniques”

Symmetric ciphers used for "air interface communications", i.e. RFID tags are dealt in this standard

[10]. RFID "Radio Frequency Identification" tags are the main components in IoT having a unique identifier to distinguish from other RFID tags in the network. RFID chips are used as sensors which are inserted in or attached to objects and monitor and respond on specific conditions for which they are meant. So these RFID tags and sensors play an important role in IoT.

ISO/IEC 29167 Part 10 describes AES-128 block cipher algorithm which is widely used as a base in many lightweight block ciphers. AES follows WTS "Wide Trail Strategy" having two invertible steps in round transformations. In the first step, local non-linear transformation is performed where any of the output bit depends on only a limited number of input bits. The second step performs a linear mixing transformation to achieve high diffusion.

ISO/IEC 29167 Part 11 describes PRESENT-80, an SPN block cipher which is optimized for Hardware implementations. An XOR operation is applied in each round for both round key and post-whitening key. PRESENT cipher is also included in ISO/IEC 29192-2.

ISO/IEC 29167 part 13 describes GRAIN-128A, a stream cipher which was proposed as an improvement over GRAIN 128 cipher by enhancing the security and optional message authentication.

Other parts of the ISO/IEC 29167 standard deal with public key cryptography.

2.2 ISO/IEC 29192: "Information technology — Security techniques — Lightweight cryptography"

Some criteria are set for deciding whether to include a newly submitted technique into the existing list of standards or not. Typically it takes around 3-4 years for standardizing a technique. The ISO/IEC 29192 comprises the following parts [8]. Each part specifies their role in the standardization process and is meant for a different purpose.

A. Part 1: General

In this part, lightweight cryptography implementation and security requirements are specified. Classification of a lightweight cipher is also defined. It is defined by combining certain properties for hardware and software implementation along with some common properties. It includes chip area, program code size (ROM size), energy consumption, RAM size, execution time or speed, communication bandwidth, short input performance, and latency. Part 1 of ISO/IEC 29192 considers block ciphers and stream ciphers as symmetric key lightweight ciphers. It also defines three schemes for lightweight cryptographic mechanisms which use asymmetric techniques, these schemes are: "authentication and key exchange", "identity-based signature" and "challenge-response authentication".

B. Part 2: Block Ciphers

Number ISO/IEC 29192-2 (2012) specifies two block ciphers, PRESENT, and CLEFIA which are suitable for applications requiring lightweight cryptographic implementations. Both ciphers are given in the year 2007 [11]. An amendment was proposed in the year 2014 to consider two more ciphers, SIMON and SPECK to fall into this standard. A minimum block size of 46 bits and a minimum key size of 96 bits was included in the first working draft (WD1st) in the year 2015. These ciphers are described below:

PRESENT: A SPN lightweight block cipher suitable for enormously resource-constrained environments is optimized for hardware implementation with 64-bit of block size and a key size of 80/ 128 bits with 31 rounds is PRESENT. XOR operation is applied in each round with a post-whitening key. For substitution layer, same 4-bit S-box is applied 16 times in parallel to introduce non-linearity and its permutation layer uses a bit permutation. This cipher has a better throughput of 200 Kbps and GE (1570) is low as compared to other ciphers [12]-[14]. PRESENT provides low-cost diffusion in only hardware implementation whereas, for software implementation, it is not so efficient. The S-box is also hardware implementation choice and does not provide resistance to adequate security [15]. S-box of PRESENT is weak and is amongst 8% worst S-boxes regarding clustering of one-bit linear trails [16]. Key scheduling uses a single S-box lookup along with an addition counter and a rotation. Hardware implementation of PRESENT cipher replaces 8 distinct S-boxes with only a single one which is carefully selected [8]. The PRESENT lightweight block cipher is also comparable to prominent compact stream ciphers [17]. PRESENT has a compact design and is, therefore, less protected hence some attacks are successfully implemented on this prominent cipher including related-key rectangle attack, side channel attack [18]-[21]. Gate required of PRESENT is comparable to Grain and Trivium stream ciphers which have compact hardware implementations [22]. RAM memory requirement of PRESENT is least and its 80-bit key requires about 480 GEs, and 64-bit state requires only 780 GEs and a total of 1570 GEs [23]-[25]. So far various attacks are applied on PRESENT such as differential attack, statistical saturation attack, integral attack, zero correlation attack, and etc. [26].

CLEFIA: CLEFIA has a block size of 128 bits and it supports key sizes of 128/ 192/ 256 bits. It is targeted for ASIC implementations which are given by matching traditional ciphers along with the new innovative security algorithms. 4-branch Generalized Feistel Structure allows a compact implementation of F-functions in both hardware and software implementations. In CLEFIA, there is a sharing of functions between data scheduling and key scheduling parts and as a result reduction in the gate size and low cost [27]. It comprises the DSM (Diffusion Switching Mechanism) technique thus improve flexibility and performance in software and hardware implementations. DSM also provides

resistance against linear and differential attacks. Improved resistance to certain attacks is achieved by using two S-boxes system. Partial/half key whitening is applied to lower the key addition cost. It is applied to only two of four data lines at the beginning and at the end of the data processing part [28]. A good balance for security, speed, and cost is maintained in this cipher. CLEFIA makes use of two different diffusion matrices which provides a guard against linear and differential attacks [29]. Key scheduling of CLEFIA makes use of large tables due to which its memory size and execution time is greater than that of the PRESENT cipher. CLEFIA is utilized for data protection in various resource constraints applications like industries setups, smart medical devices, MANETs [30]. Comparable higher RAM consumption of CLEFIA is because of large tables in key scheduling. LED, lightweight block cipher has better power consumption as compared to CLEFIA because of the fixed key and simple round operations [31, 32]. CLEFIA allows very proficient implementation in a diversity of environments. Some block ciphers are also inspired from CLEFIA like in [25]. Sufficient cryptanalysis is done over CLEFIA and there exist several attacks on it like zero-correlation, linear cryptanalysis, improbable differential attack and Integral attack [33]-[35].

SIMON: SIMON is a family of lightweight Feistel block ciphers which offer excellent performance in hardware implementations. It provides ten algorithms by supporting block sizes/ key sizes of 32/64; 48/72, 96; 64/ 96, 128; 96/96, 144 and 128/128, 192, 256. It applies bitwise XOR, bitwise AND and left circular shift operations on n-bit words in SIMON 2n encryption and decryption. SIMON do not make use of any key whitening as applied in CLEFIA, its first and last round act to bring in the first and last round keys without performing cryptography [36]-[38]. Different attacks are successfully implemented on SIMON like linear, differential, truncated differential [39], related key attacks [40]-[44].

SPECK: SPECK is a family of LBCs tuned for optimized software implementations and provided ten algorithms to support block sizes/ key sizes of 32/64; 48/72, 96; 64/96, 128; 96/96, 144 and 128/128, 192, 256 [37]. Its round function is similar to the mixing function of THREEFISH cipher. It has an ARX structure and circular-shift uses bit permutations. Decryption is not a costly operation in ARX based ciphers, it simply reverses the order of operations. Modular subtraction in place of modular addition is used in the decryption process. SPECK make use of a combination of two Feistel-like maps with respect to two different types of addition. SPECK round-wise key addition in SPECK prevents it from slide attack and meet-in-the-middle attack over a sensible number of rounds [45]. Linear and differential attacks are implemented on SPECK [46]-[48].

C. Part 3: Stream Ciphers

Similarly, two stream ciphers, Trivium and Enocoro are part of ISO/IEC 29192-3 standard. Stream ciphers are symmetric key ciphers and are mainly used in those applications where plaintext size is unknown. Although, stream ciphers have a simple and speedy implementation in hardware but due to lengthy initialization phase and also due to some of the communication protocols that do not utilize stream ciphers, these are less preferred over block ciphers and as a result does not receive much attention [6, 49].

TRIVIUM: Trivium is a simple, speedy, smallest and most efficient bit-oriented stream cipher which provides good security margin against attacks and requires low power hardware implementation [50, 51]. It is an ARX based cipher which uses 288-bit cyclic shift register parallelization techniques [52, 53]. In TRIVIUM, up to 264-bits of keystream along with 80-bit Initialization Vector (IV) can be generated from a single 80-bit secret key. Various attacks are applied on Trivium and analyzed like linear approximation [54], conditional differential attack, differential fault attack, statistical attack, algebraic analysis, fault attack [55], state recovery attack [56]. Trivium provides good resistance against linear sequential circuit approximation attack [57]-[60].

ENOCORO: ENOCORO is a family of hardware-oriented pseudo-random number generator. Enocoro-80 and Enocoro-128v1.1 are two versions of Enocoro security algorithms allowing key lengths of 80-bits and 128-bits respectively [61]. Authors in [62] claim that there exists a large class of weak keys in Enocoro-128v1.1 due to which it is vulnerable to related-key attacks.

D. Part 4: Mechanisms using Asymmetric Techniques

In this part of ISO /IEC 29192 standard, three lightweight mechanisms are specified which have used asymmetric techniques, these are: a) "Unilateral authentication mechanism" which lies on discrete logarithms on elliptic curves; b) "Authenticated lightweight key exchange (ALIKE) mechanism" for establishing of the session key and unilateral authentication; c) "Identity-based signature mechanism".

E. Part 5: Hash Functions

Three hash functions namely, Photon, Spongent, and Lesamnta-LW are included in ISO/IEC 29192-5 standard.

PHOTON: It is a family of compact lightweight hash function designed for 64-bit collision resistance security in hardware based implementation. It makes use of the column mixing layer in a serial way [63, 64]. There are five versions of PHOTON family, these are PHOTON-80/20/16, PHOTON128/16/16, PHOTON-160/36/36, PHOTON-224/32/32 and PHOTON-256/32/32 with internal permutations P100, P144, P196, P256, and P288 respectively.

SPONGENT: SPONGENT is a family of lightweight hash functions which allows hash sizes of 88, 128, 160, 224 and 256 bits, in total 13 variants. The first SPONGENT variant supporting 88 bits is only for preimage resistance and other four variants are based on a sponge construction instantiated. Its permutations are similar to that of PRESENT cipher and following the hermetic sponge strategy. An n-bit hash value is

obtained whenever a finite number of input bits is given [65]-[67].

Lesamnta-LW: It is a fast lightweight hash function supporting 256-bit hash size and is suitable for devices running on 8-bit microcontroller [68]. Lesamnta-LW is a compact design but there exists a known-key distinguisher attack [69].

F. Part 6: Message Authentication Codes (MACs)

At the time of writing the paper, this part is under consideration.

3. INCLUSION CRITERIA IN ISO/IEC STANDARDS

Annexure A of the ISO/IEC 29192 standard defines the criteria which can be considered by lightweight algorithms so as to include the algorithms in the standard [70]. It generally takes 3-4 years to standardize a new technique and considers the following criteria:

A. Security of Cryptographic Mechanism

Minimum security strength considered towards applications utilizing lightweight algorithms is 80-bit. Systems requiring security for longer periods requires a minimum of 112-bit security.

B. Hardware Implementation Properties

The chip area occupied by the cryptographic mechanism and the energy consumption are two parameters that are considered important for hardware targeted cryptographic algorithms. (Clear benefits over existing ISO standards, e.g. ISO/IEC 18033, ISO/IEC 9798, ISO/IEC 11770).

C. Software Implementation Properties

The code size and the RAM size requirement are considered towards inclusion in the standard. Ciphers having low resource utilization than existing lightweight standards on the same platform are possibly considered towards inclusion in the standard.

D. Some Common Properties

Some properties are common to both software implementation and hardware implementation of a cipher, these are:

a) The nature of any licensing issues affecting the cryptographic mechanism.
b) The maturity of the security algorithm is also considered as it is linked to other factors. A stable state publication of a proposed technique for a minimum of 4-5 years is required for initial consideration of a proposed technique. This time is specified so that sufficient cryptanalysis techniques have been applied to it and no weakness has been found.
c) It is desired that the requesting techniques provide sufficient security proofs for their specifications against possible and feasible attacks.
d) An industrial need is also considered if there is a practical demand for the technique to be standardized then its likelihood of inclusion increases.
e) Dependency from specific implementation also affects inclusion in the standard. The more independent a cipher is from its implementation in a specific technology, the more its probability of inclusion.

4. PERFORMANCE EVALUATION PARAMETERS

In lightweight cryptography huge variety of resource constraint devices uses different communication technologies. They have some limitations in the form of implementation memory size, speed, power, security, performance and as a result it is not possible to implement standard cryptographic solutions. So there are tradeoffs in implementation cost, speed, security, performance, and energy consumption in resource-constrained devices. In this era of pervasive computing, lightweight cryptography expects simple and fast security solutions [71].

Memory consumption (RAM and ROM size), speed and throughput are among the main primitives which are considered towards finding good lightweight algorithms [7]. These are specific to the hardware or software implementation of a security algorithm. Authors in [72] mentioned 6 metrics for evaluation of software implementation of lightweight ciphers, these are:

a) Code size, given in bytes
b) RAM usage, given in bytes
c) Cycle count in encryption, one block Cycles/byte
d) Cycle count in decryption, one block Cycles/byte
e) Energy consumed, given in μJ, and
f) A combined metric which is given after the normalization (by block size) using (1):

$$code\ size \times cycle\ count \quad (1)$$

There is a strong correlation between energy consumption and cycle count [72]. Lightweight algorithms implemented in software, targeted for micro-controllers usually consider some more performance evaluation parameters like:

a) Throughput measured in bytes per CPU cycle.
b) Power Consumption

Among all the primitives, memory elements set up a key part of the module's surface. Optimized software implementations result in fast speed thereby utilizing low power consumption [73]. Authors in [74] presented a Combined Metric (CM) indicating a tradeoff between implementation size and performance. A smaller size of metric indicates better cipher implementation. CM is given by using (2):

$$CM = (code\ size\ [bits] - encryption\ cycle\ count\ [cycles]) \quad (2)$$

Authors in [8] presented three different groups based on the values obtained from this Combined Metrics:

a) **Ultra-lightweight implementations:** "Requiring up to 4 KB ROM and 256 bytes RAM".
b) **Low-cost implementations:** "Requiring up to 4 KB ROM and 8 KB RAM."
c) **Lightweight implementations:** "Requiring up to 32 KB ROM and 8 KB RAM."

5. PERFORMANCE EVALUATION TOOLS

It is important to analyze the ciphers for their performance evaluation and against attacks. There are various tools that are available for analysis of lightweight ciphers. Some tools/ frameworks are suitable for hardware implementations like XPower analyzer whereas some tools are available for software targeted implementations. This section presents some widely used software evaluation frameworks. Some of these are available for open access.

A. FELICS

Authors in [74], presented a metric, FoM and a framework named FELICS for the evaluation of software-based lightweight ciphers. Metric FoM (Figure of Merit) can be used for ranking different ciphers. FELICS which stands for "Fair Evaluation of Lightweight Cryptographic Systems", is a free and open-source framework. Its modular structure consists of three modules, one module for block ciphers and the second module for stream ciphers, while the third module is a core module for both types of ciphers. It gives RAM size, ROM size and execution time of implementation as an output. This framework also allows comparisons of implementations for different microcontrollers viz. 8-bit AVR, a 16-bit MSP, and a 32-bit ARM. It provides the flash memory, section memory sizes and the total memory size [5, 75]. FELICS test a cipher in three different scenarios, these are cipher operation, communication protocol and challenge-handshake authentication protocol [76]. FELICS tool has been efficiently used by various researchers for the performance analysis of lightweight ciphers on different platforms [77]-[80].

B. BLOC

BLOC project gives six different metrics on 16-bit MSP430 microcontroller using simulator coming with mspdebug for performance evaluation of lightweight block ciphers by authors in [81] in 2011. The metrics are: cycle count for encryption + key, cycle count for decryption + key, cycles/ bytes for encryption + key, cycles/ bytes for decryption + key, code size in bytes and RAM usage in bytes. RAM requirements computed under this project gave erroneous results and hence it was shut down on March 31st, 2016.

C. ATLAS

"Automated TooL for Assembly analysiS" (ATLAS) is an automated easy and modular approach to analyze assembly implementations of a cipher by representing it as a graph. This graph is then efficiently used to find vulnerable spots. Through these vulnerable spots, fault propagation is then analyzed in a subgraph and gives equations for differential fault analysis. Thus, ATLAS gives subgraphs and equations [82].

D. XFC Framework

It is important to analyze the ciphers against attacks. Fault attacks like differential fault attack target to recover the secret key. Finding such fault attacks manually is a laborious task and it may take several months to years. Authors in [83] provided a framework for block ciphers that can be used to automatically predict the weak points present in a cipher design. The proposed framework, XFC "eXploitable Fault Characterization" makes use of colors for the analysis of fault propagation and exploitability. It predicts whether a differential attack would be possible or not on a particular cipher. It can also be used for predicting the key bits that can be derived from the attack. There are two stages in this model. In the first stage, a user enters the encryption specification and the fault model with the help of coloring scheme, find the fault propagation and its influence on the ciphertext. The 2nd stage finds the round keys by evaluating the exploitability of the fault. The complexity of the attack and derivable round keys are outputs of this model.

6. FEATURES OF GOOD LIGHTWEIGHT CIPHERS

Nowadays, a number of lightweight block ciphers are available and it is very tough to select the best among them because the suitability of any particular algorithm is application specific. But still, to consider a cipher better than its competitors requires some analysis and measuring their performance on same platform. Table 1 enlists some measures which are laid down by the standard organization for the inclusion of a lightweight block cipher in their standards.

Table 1: Criteria for good lightweight block ciphers (GEs: Gate Equivalents; μJ: Microjoule).

Criteria	Requirement
Security (in bits)	Minimum key size of 80-bits
Chip Area (in GEs)	Lower than existing standards
Energy Consumption (in μJ)	Lower than existing standards
Code size (ROM) (in bytes)	Lower than existing standards when compared on the same platform
RAM size (in bytes)	Lower than existing standards when compared on the same platform
Maturity (in years)	Minimum 4-5 years so that enough cryptanalysis has been applied
Resistance to attacks	Sufficient proofs against feasible attacks
Implementation Dependency	Lower

7. CONCLUSION

Designing a security algorithm for IoT enabled devices must consider the criteria provided by standard organizations from time to time. We have presented different criteria posed by standard organizations to consider a lightweight cipher. This paper reports prominent security solutions in IoT enabled constrained devices which are already standardized by these organizations. Some performance evaluation criteria, metrics and performance evaluation tools related to the evaluation of lightweight ciphers are also presented in this paper. The main aim of this paper is to demonstrate how to achieve efficient and optimal software implementation of lightweight block ciphers for IoT-enabled low-resource embedded devices. The work in this paper helps the researchers in the area of IoT security. This paper set a base for further research work and in the near future, we will propose a LBC for IoT enabled environment.

REFERENCES

1. M. Devi and N. S. Gill. **Performance Evaluation of Dynamic Source Routing Protocol in Smart Environment,** *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 2, pp. 333-338, 2019. https://doi.org/10.30534/ijatcse/2019/37822019
2. P. Singh and N. S. Gill. **A Secure and Power-Aware Protocol for Wireless Ad Hoc Networks,** *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 1, pp. 34-41, 2018. https://doi.org/10.30534/ijatcse/2019/07812019
3. D. Sehrawat and N. S. Gill. **Deployment of IoT based smart environment: key issues and challenges,** *International Journal of Engineering & Technology*, vol. 7, no. 2, pp. 544-550, 2018.
4. D. Sehrawat and N. S. Gill. **Analysis of Security Attacks on Lightweight Block Ciphers and their Countermeasures,** *Journal of Engineering and Applied Sciences*, vol. 13, no. 20., pp. 8439-8447, 2018. DOI: 10.3923/jeasci.2018.8439.8447
5. M. Katagi, and S. Moriai. **Lightweight cryptography for the Internet of Things**, *Sony Corp.*, pp. 7-10, 2008. https://pdfs.semanticscholar.org/9595/b5b8db9777d5795625886418d38864f78bb3.pdf
6. D. Sehrawat and N. S. Gill. **Performance Evaluation of Newly Proposed Lightweight Cipher, BRIGHT,** *International Journal of Intelligent Engineering and Systems,* Vol. 12, 2019.
7. S. Singh, P. K Sharma, Pradip, S.Y. Moon, and J. H. Park. **Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions,** *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-18, 2017. DOI: 10.1007/s12652-017-0494-4
8. M. Matsui, and Y. Murakami. **Minimalism of software implementation,** in *Proc. International Workshop on Fast Software Encryption, Springer,* Berlin, Heidelberg, 2013, pp. 393-409.

   https://doi.org/10.1007/978-3-662-43933-3_20
9. C. Manifavas, G. Hatzivasilis, K. Fysarakis, and K. Rantos. **Lightweight cryptography for embedded systems–A comparative analysis**, *Data Privacy Management and Autonomous Spontaneous Security, DPM 2013, SETOP 2013. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg,* vol. 8247. pp. 333-349, 2014.

   https://doi.org/10.1007/978-3-642-54568-9_21
10. A. Biryukov, and L. Perrin. **State of the Art in Lightweight Symmetric Cryptography**, *IACR Cryptology ePrint Archive*, (2017):511, 2017. http://eprint.iacr.org/2017/511
11. ISO/IEC,29192-2:2012. https://www.iso.org/standard/56552.html
12. A. Bogdanov, *et al.* **PRESENT: An ultra-lightweight block cipher**, in *Proc. International Workshop on Cryptographic Hardware and Embedded Systems, Springer*, Berlin, Heidelberg, 2007, pp. 450-466. https://doi.org/10.1007/978-3-540-74735-2_31
13. S. Jana, J. Bhaumik, and M. K. Maiti. **Survey on Lightweight Block Cipher,** *International Journal of Soft Computing and Engineering*, vol. 3, no. 5, pp. 183-187, 2013.

    http://www.ijsce.org/wp-content/uploads/papers/v3i5/E1933113513.pdf
14. M. Mozaffari-Kermani, K. Tian, R. Azarderakhsh, and S. Bayat-Sarmadi. **Fault-resilient lightweight cryptographic block ciphers for secure embedded systems,** *IEEE Embedded Systems Letters*, vol. 6, no. 4, pp. 89-92, 2014. 10.1109/LES.2014.2365099
15. Z. Wentao, B. A. O. Zhenzhen, L. I. N. Dongdai, V. Rijmen, Y. Bohan, and I. Verbauwhede. **RECTANGLE : a bit-slice lightweight block cipher suitable for multiple platforms**, *Science China Information Sciences*, vol. 58, no. 12, pp. 1-15, 2015. https://doi.org/10.1007/s11432-015-5459-7
16. G. Leander. **On linear hulls, statistical saturation attacks, PRESENT and a cryptanalysis of PUFFIN,** *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6632, pp. 303-322, 2011.

    https://doi.org/10.1007/978-3-642-20465-4_18
17. W. Wu, and L. Zhang. **LBlock: A Lightweight Block Cipher,** in *Proc. International Conference on Applied Cryptography and Network Security, Springer*, Berlin,

Heidelberg, 2011, pp. 327-344. https://doi.org/10.1007/978-3-642-21554-4_19

18. D. Gu, J. Li, S. Li, Z. Ma, Z. Guo, and J. Liu. **Differential fault analysis on lightweight blockciphers with statistical cryptanalysis techniques,** in *Proc. - 2012 Work. Fault Diagnosis Toler. Cryptogr, IEEE Xplore.* FDTC, 2012, pp. 27–33. 10.1109/FDTC.2012.16

19. M. Renauld, F. Standaert, and C. X. Standaert. **Algebraic Side-Channel Attacks,** in *Proc. International Conference on Information Security and Cryptology, Springer,* Berlin, Heidelberg, 2010, pp. 393–410. https://doi.org/10.1007/978-3-642-16342-5_29

20. P. Yalla, E. Homsirikamol, and J. Kaps. **Comparison of Multi-Purpose Cores of Keccak and AES,** in: *Proc. 2015 Design, Automation & Test in Europe Conference & Exhibition, EDA Consortium,* 2015, pp. 585-588. https://dl.acm.org/citation.cfm?id=2755885

21. F. Zhang, X. Zhao, S. Guo, T. Wang, and Z. Shi. **Improved algebraic fault analysis: A case study on piccolo and applications to other lightweight block ciphers,** *Lecture Notes in Computer Science (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics),* vol. 7864, pp. 62-79, 2013. https://doi.org/10.1007/978-3-642-40026-1_5

22. K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, and T. Shirai. **Piccolo: An ultra-lightweight blockcipher,** *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics),* vol. 6917, pp. 342–357, 2011. https://doi.org/10.1007/978-3-642-23951-9_23

23. C. D. Cannière, O. Dunkelman, and M. Knežević. **KATAN and KTANTAN - A family of small and efficient hardware-oriented block ciphers,** *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics),* vol. 5747, pp. 272–288, 2009. https://doi.org/10.1007/978-3-642-04138-9_20

24. B. J. Mohd, T. Hayajneh, and A. V. Vasilakos. **A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues,** *J. Netw. Comput. Appl.,* vol. 58, pp. 73-93, 2015. https://doi.org/10.1016/j.jnca.2015.09.001

25. S. K. Ojha, N. Kumar, K. Jain, and Sangeeta. **TWIS–A Lightweight Block Cipher,** *Information Systems Security. Springer,* vol. 5905, pp. 280-291, 2009. https://doi.org/10.1007/978-3-642-10772-6_21

26. C. Blondeau, and K. Nyberg. **Links between truncated differential and multidimensional linear properties of block ciphers and underlying attack complexities,** *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics),* vol. 8441, pp. 165-182, 2014.

https://doi.org/10.1007/978-3-642-55220-5_10

27. L. Knudsen and D. Wagner. **Integral cryptanalysis,** *in Proc. International Workshop on Fast Software Encryption, Springer,* Berlin, Heidelberg, 2002, pp. 112-127. https://doi.org/10.1007/3-540-45661-9_9

28. Sony Corporation, 2007: https://www.sony.net/Products/cryptography/clefia/download/data/clefia-design-1.0.pdf

29. T. Shirai1, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata. **The 128-bit blockcipher CLEFIA,** in *Proc. International Workshop on Fast Software Encryption, Springer,* Berlin, Heidelberg, 2007, pp. 181-195. https://doi.org/10.1007/978-3-540-74619-5_12

30. M. M. Kermani, and R. Azarderakhsh. **Efficient fault diagnosis schemes for reliable lightweight cryptographic ISO/IEC standard CLEFIA benchmarked on ASIC and FPGA,** *IEEE Transactions on Industrial Electronics,* vol. 60, no. 12, pp. 5925-5932, 2013. 10.1109/TIE.2012.2228144

31. L. Batina *et al.* **Dietary Recommendations for Lightweight Block Ciphers: Power, Energy and Area Analysis of Recently Developed Architectures,** *Lect. Notes Comput. Sci. Springer*-Verlag Berlin Heidelberg, vol. 8262. Pp. 103-112, 2013. https://doi.org/10.1007/978-3-642-41332-2_7

32. S. Kolay, and D. Mukhopadhyay. **Khudra : A New Lightweight Block Cipher for FPGAs,** *Lect. Notes Comput. Sci. Springer,* Cham, vol. 8804, pp. 126-145, 2014. https://doi.org/10.1007/978-3-319-12060-7_9

33. A. Bogdanov, H. Geng, M. Wang, L. Wen, and B. Collard. **Zero-Correlation Linear Cryptanalysis with FFT and Improved Attacks on ISO Standards Camellia and CLEFIA,** *Lect. Notes Comput. Sci. Springer,* Berlin, Heidelberg, vol. 8282, pp. 306–323, 2014. https://doi.org/10.1007/978-3-662-43414-7_16

34. Y. Sasaki, and L. Wang. **Meet-in-the-middle technique for integral attacks against feistel ciphers,** *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics),* vol. 7707, pp. 234–251, 2013. https://doi.org/10.1007/978-3-642-35999-6_16

35. C. Tezcan. **The improbable differential attack: Cryptanalysis of reduced round CLEFIA,** *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics),* vol. 6498, pp. 197–209, 2010. https://doi.org/10.1007/978-3-642-17401-8_15

36. A. Aysu, E. Gulcan, and P. Schaumont. **SIMON Says, Break the Area Records for Symmetric Key Block Ciphers on FPGAs,** *IEEE Embed. Syst. Lett.,* vol. 6, no. 2, pp. 37–40, 2014. 10.1109/LES.2014.2314961

37. R. Beaulieu, D. Shors, J. Smith, S. T. Clark, B. Weeks, and L. Wingers. **The SIMON and SPECK block ciphers on AVR 8-bit microcontrollers,** in *Proc. International Workshop on Lightweight Cryptography for Security and Privacy*, *Springer*, Cham, 2014, pp. 3-20.

https://doi.org/10.1007/978-3-319-16363-5_1

38. R. Beaulieu, D. Shors, J. Smith, S. T. Clark, B. Weeks, and L. Wingers. **The SIMON and SPECK lightweight block ciphers,** in *Proc. Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE*, 2015, pp. 1-6. 10.1145/2744769.2747946

39. T. Mourouzis, G. Song, N. Courtois, and M. Christofi. **Advanced Differential Cryptanalysis of Reduced-Round SIMON64 / 128 Using Large-Round Statistical Distinguishers,** *Cryptology ePrint Archive, Report*, 2015/481 (2015). http://eprint.iacr.org/

40. M. A. Abdelraheem, J. Alizadeh, H. A. Alkhzaimi, M. R. Aref, N. Bagheri, and P. Gauravaram. **Improved linear cryptanalysis of reduced-round SIMON-32 and SIMON-48,** *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9462, pp. 153–179, 2015. https://doi.org/10.1007/978-3-319-26617-6_9

41. F. Abed, E. List, S. Lucks, and J. Wenzel. **Differential and Linear Cryptanalysis of Reduced-Round SIMON,** *IACR Cryptol. ePrint Arch., Report* 2013/526, 2013. https://pdfs.semanticscholar.org/59c7/b77ca5ee6cd0cd7b74fe41fb8744b84025f5.pdf

42. C. Cid, and C. Rechberger. **Differential Analysis of Block Ciphers SIMON and SPECK,** *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8540, pp. 546–570, 2015. https://doi.org/10.1007/978-3-662-46706-0_28

43. S. Sun, L. Hu, P. Wang, K. Qiao, and L. Song. **Automatic Security Evaluation and (Related-key) Differential Characteristic Search: Application to SIMON, PRESENT, LBlock, DES(L) and Other Bit-oriented Block Ciphers,** *Lecture Notes in Computer Science, Springer, Berlin, Heidelberg*, vol. 8873, pp. 158–178, 2014. https://doi.org/10.1007/978-3-662-45611-8_9

44. H. Tupsamudre, S. Bisht, and D. Mukhopadhyay. **Differential fault analysis on the families of SIMON and SPECK ciphers,** in Proc. *workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC*, 2014, pp. 40–48.

http://doi.ieeecomputersociety.org/10.1109/FDTC.2014.14

45. F. Abed, E. List, S. Lucks, and J. Wenzel. **Cryptanalysis of the Speck Family of Block Ciphers,** *IACR Cryptol. ePrint Arch, pp.* 1–14, 2013. https://eprint.iacr.org/2013/568.pdf

46. A. Biryukov, A. Roy, and V. Velichkov. **Differential analysis of block ciphers Simon and Speck,** *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8540, pp. 546–570, 2015.

https://doi.org/10.1007/978-3-662-46706-0_28

47. A. Biryukov, V. Velichkov, and Y. Le Corre. **Automatic search for the best trails in ARX: Application to block cipher SPECK,** *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9783, no. 2008, pp. 289–310, 2016. https://doi.org/10.1007/978-3-662-52993-5_15

48. I. Dinur. **Improved Differential Cryptanalysis of Round-Reduced Speck,** in *Proc. International Conference on Computational Intelligence and Security, CIS*, 2010, pp. 367–371. https://doi.org/10.1007/978-3-319-13051-4_9

49. Y. Luo, Q. Chai, G. Gong, and X. Lai. **A lightweight stream cipher WG-7 for RFID encryption and authentication,** in *Proc. Global Telecommunications Conference (GLOBECOM 2010), IEEE*, 2010, pp. 1-6. 10.1109/GLOCOM.2010.5684215

50. M. Feldhofer. **Comparison of Low-Power Implementations of Trivium and Grain,** in Proc. The State of the Art of Stream Ciphers, Workshop Record, 2007, 236–246.

https://www.cosic.esat.kuleuven.be/ecrypt/stream/papersdir/2007/027.pdf

51. T. Good, W. Chelton, and M. Benaissa. **Review of stream cipher candidates from a low resource hardware perspective,** in *Proc. Stream Ciphers Revisited, SASC 2006, Work. Rec.*, 2006, pp. 125–148. http://www.ecrypt.eu.org/stvl/sasc2006/SASC2006full.pdf

52. J. M. Mora-Gutiérrez, C. J. Jiménez-Fernández, and M. Valencia-Barrero**. Low power implementation of Trivium stream cipher,** *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7606, pp. 113–120, 2013. https://doi.org/10.1007/978-3-642-36157-9_12

53. W. Record. **TRIVIUM - A Stream Cipher Construction Inspired by Block Cipher Design Principles,** in *Proc. International Conference on Information Security, Springer*, Berlin, Heidelberg, 2006, pp. 171-186.

https://doi.org/10.1007/11836810_13

54. M. S. Turan, and O. Kara. **Linear approximations for 2-Round Trivium,** in *Proc. First International Conference on Security of Information and Networks (SIN 2007)*, 2007, pp. 96-105.

55. C. J. Jim, and A. T. S. Cipher. **Fault Attack on FPGA implementations of Trivium Stream Cipher,** in *Proc. IEEE International Symposium on Circuits and Systems (ISCAS)*, 2016, pp. 562-565. 10.1109/ISCAS.2016.7527302

56. A. Maximov, and A. Biryukov. **Two Trivial Attacks on Trivium,** in *Proc. International Workshop on Selected Areas in Cryptography*, 2007, pp. 36-55. https://doi.org/10.1007/978-3-540-77360-3_3

57. H. Englund, T. Johansson, S. Turan, and Meltem. **A Framework for Chosen IV Statistical Analysis of Stream Ciphers,** in *Proc. International Conference on Cryptology in India, Springer*, Berlin, Heidelberg, 2007, pp. 268–281.

    https://doi.org/10.1007/978-3-540-77026-8_20

58. S. Khazaei, and M. Hassanzadeh. **Linear Sequential Circuit Approximation of the TRIVIUM Stream Cipher,** *ECRYPT Stream Cipher Project*, EU, Rep, 63, 2005.
    https://pdfs.semanticscholar.org/b3ef/0156061493974b77547f981534c845d02b36.pdf

59. S. Knellwolf, W. Meier and M. N. Plasencia. **Conditional differential cryptanalysis of trivium and KATAN,** *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7118, no. 8065, 2012, pp. 200–212. https://doi.org/10.1007/978-3-642-28496-0_12

60. C. McDonald, C. Charnes, and J. Pieprzyk. **An Algebraic Analysis of Trivium Ciphers based on the Boolean Satisfiability Problem,** in *Proc. 4th International Workshop on Boolean Functions: Cryptography and Applications*, 2007, pp. 173-184. https://eprint.iacr.org/2007/129.pdf

61. D. Watanabe, K. Ideguchi, J. Kitahara, K. Muto, H. Furuichi, and T. Kaneko. **Enocoro-80: A hardware oriented stream cipher,** in *Proc. ARES 2008 - 3rd International Conference on Availability, Security, and Reliability*, 2008, pp. 1294–1300. http://doi.ieeecomputersociety.org/10.1109/ARES.2008.84

62. D. Watanabe, T. Owada, K. Okamoto, Y. Igarashi, and T. Kaneko. **Update on Enocoro stream cipher,** in *Proc. IEEE International Symposium on Information Theory and its Applications (ISITA), ISITA/ISSSTA, 2010*, pp. 778-783. 10.1109/ISITA.2010.5649627

63. J. Guo, T. Peyrin, and A. Poschmann. **The PHOTON family of lightweight hash functions.** In *Proc. Annual Cryptology Conference, Springer*, Berlin, Heidelberg, 2011, pp. 222-239.

    https://doi.org/10.1007/978-3-642-22792-9_13

64. B. Tareq Hammad, N. Jamil, M. Ezanee Rusli, and M. Rezaaba. **A survey of Lightweight Cryptographic Hash Function,** *International Journal of Scientific & Engineering Research*, vol. 8, no. 7, pp. 806-814, 2017. https://www.ijser.org/researchpaper/A-survey-of-Lightweight-Cryptographic-Hash-Function.pdf

65. J. Balasch *et al.* **Compact implementation and performance evaluation of hash functions in attiny devices,** *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7771, pp. 158–172, 2013. https://doi.org/10.1007/978-3-642-37288-9_11

66. A. Bogdanov, M. Knežević, 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, 2013. 10.1109/TC.2012.196

67. A. Bogdanovl, M. Knezevic, G. Leander, K. Vancil, and I. Verbauwhede. **Spongent: A Lightweight Hash Function,** in *Proc. International Workshop on Cryptographic Hardware and Embedded Systems, Springer*, Berlin, Heidelberg, 2011, pp. 312-325. https://doi.org/10.1007/978-3-642-23951-9_21

68. S. Hirose, K. Ideguchi, H. Kuwakado, T. Owada, B. Preneel, and H. Yoshida. **An AES based 256-bit hash function for lightweight applications: Lesamnta-LW,** *IEICE transactions on fundamentals of electronics, communications and computer sciences*, vol. *95, no.* 1 pp. 89-99, 2012.

    https://doi.org/10.1587/transfun.E95.A.89

69. Y. Sasaki, and K. Aoki. **Open-key distinguishers for the internal block cipher of tweaked lesamnta,** *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 96, no. 1 pp. 141-149, 2013. 10.1587/transfun.E96.A.141

70. A. Biryukov, and L. Perrin. **State of the Art in Lightweight Symmetric Cryptography,** *IACR Cryptology ePrint Archive* (2017): 511, 2017. http://eprint.iacr.org/2017/511

71. W. J. Buchanan, S. Li, and R. Asif. **Lightweight cryptography methods,** *Journal of Cyber Security Technology*, vol. 1, no. 3-4, pp. 187-201, 2017. https://doi.org/10.1080/23742917.2017.1384917

72. T. Eisenbarth, *et al.* **Compact implementation and performance evaluation of block ciphers in AT tiny devices,** in *Proc. International Conference on Cryptology in Africa, Springer*, Berlin, Heidelberg, 2012, pp. 172-187.

    https://doi.org/10.1007/978-3-642-31410-0_11

73. D. Sehrawat and N. S. Gill. **Design Considerations of Lightweight Block Ciphers for Low-Cost Embedded Devices**, *International Journal of Recent Technology and Engineering*, vol. 8, no. 2, 2019. (To be Published)

74. A. A. Priyanka, and S. K. Pal. **A Survey of Cryptanalytic Attacks on Lightweight Block Ciphers,** *IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS),* vol. 2, no. 2, pp. 472-481, 2012.

    https://ijcsits.org/papers/Vol2no22012/43vol2no2.pdf

75. D. Dinu, A. Biryukov, J. Großsch¨adl, D. Khovratovich, Y. L. Corre, and L´. Perrin. **Felics–fair evaluation of lightweight cryptographic systems,** in *Proc. NIST Workshop on Lightweight Cryptography*, vol. 128, 2015. https://www.cryptolux.org/index.php/FELICS

76. T. Park, H. Seo, G. Lee, M. A.-A. Khandaker, Y. Nogami, and H. Kim. **Parallel Implementations of SIMON and SPECK, Revisited,** in *Proc. International Workshop on Information Security Applications, Springer*, Cham, 2017, pp. 283-294. https://doi.org/10.1007/978-3-319-93563-8_24

77. Z. Bao, P. Luo, and D. Lin. **Bitsliced implementations of the PRINCE, LED and RECTANGLE block ciphers on AVR 8-bit microcontrollers,** *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9543, pp. 18–36, 2016. 10.1007/978-3-319-29814-6_3

78. W. Diehl, F. Farahmand, P. Yalla, J. P. Kaps, and K. Gaj. **Comparison of hardware and software implementations of selected lightweight block ciphers,** in *Proc. IEEE 27th International Conference on Field Programmable Logic and Applications, FPL*, 2017, pp. 1-7. 10.23919/FPL.2017.8056808

79. E. M. Do Nascimento, and J. A. M. Xexeo. **A flexible authenticated lightweight cipher using Even-Mansour construction,** in *Proc. IEEE International Conference on Communications*, 2017, pp. 1-6. 10.1109/ICC.2017.7996734

80. S. Kotel, F. Sbiaa, M. Zeghid, M. Machhout, A. Baganne, and R. Tourki. **Performance Evaluation and Design Considerations of Lightweight Block Cipher for Low-Cost Embedded Devices,** in *Proc. 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, 2016, pp. 1-7. 10.1109/AICCSA.2016.7945695

81. M. Cazorla, K. Marquet, and M. Minier. **Survey and Benchmark of Lightweight Block Ciphers for Wireless Sensor Networks,** in *Proc. International Conference on Security and Cryptography (SECRYPT)*, IEEE, 2013, pp. 1-6. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7223213&isnumber=7223120

82. J. Breier, and X. Hou. **Automated Fault Analysis of Assembly Code (With a Case Study on PRESENT Implementation),** *Cryptology ePrint Archive*, pp.1-19, 2017.

83. K. Punit, C. Rebeiro, and A. Hazra. **XFC: A framework for eXploitable Fault Characterization in block ciphers,** in *Proc. IEEE Design Automation Conference (DAC)*, 2017, pp. 1-6. 10.1145/3061639.3062340