Lightweight Cryptographic for Securing Constrained Resource IoT Devices

Zouheir Labbi, Mohamed Senhadji, Ahmed Maarof, Mostafa Belkasmi

Abstract**:** ***Internet of Things IoT become a recent concept of communication technologies and a novel computing paradigm. The idea is to connect a variety of objects or things (e.g., RFID tags, NFC tags, sensors, etc.), which can interact and exchange data with each other anywhere and everywhere over the internet. With the evolution of IoT, the volume of data interchanged among connecting IoT devices is increasing at a remarkable scale due to the increase in number of the connected objects. Most of IoT devices are constrained devices and low resources that handling confidential and sensitive data. Therefore, using conventional cryptographic methods are unsuitable due to many issues and challenges like limited computational power, memory space, energy resources, performance cost, and security requirement. For that, lightweight cryptographic primitives (LWC) have been introduced. Many kinds of research continue moving forward to find a suitable algorithm that meets the specific demands of the IoT application. This paper provides an overview of the LWC primitives for IoT environment and presents various LWC algorithms based on their key dimension, block size, structures and number of rounds. We examine also the security viewpoint for the constrained IoT environment focusing on the relevant research challenges, difficulties and solutions. Finally, we proposed a secure scheme for improving the constrained IoT environment and conclude by discussing the open issues.***

Keywords : Internet-of-things (IoT), Cryptographic, Lightweight, Encryption, Resource constrained

I. INTRODUCTION

Progress in sensing, communication and computing have transformed the internet for people toward the Internet of Things (IoT). The word covers an extensive perspective, that represents the evolution of internet technology to support many connected devices [1]. IoT is becoming an influential part of our daily livings that gradually led toward an imaginary space of the virtual world. Several systems of interconnected computing devices, like sensors, RFID and NFC tags, digital items, etc. which offer the capacity to transmit information across a connected network with the absence of any human interactions.

According to the newest estimations, more than 26 billion IoT units and devices which exclude PCs, tablets, and smartphones will be connected through the cloud platform by 2020 [2]. This is a good announcement for investors, operators and every player interested in the benefits and advantages of IoT, by the fact that it is involving a growth in the number of businesses and creating additional interesting opportunities.

As IoT is growing rapidly, a massive volume of data is communicated throughout a complex and huge network. However, there are still many challenges and risks that need to be addressed such as how to handle, encrypt/decrypt of huge volumes of data, processing power with energy consumption and address security menaces. these smart devices usually have constrained resources or can be called low-resource devices which characterized by their small memory, low computation power, restricted battery life and limited power supply. Consequently, conventional and standard cryptographic primitives become not suitable for smart devices with low resources. Case in point is RSA algorithm with 1204-bit [3] which cannot be performed in RFID tags. The uncomfortable restrictions enabled the necessities of developing a new branch of cryptographic algorithm, that offers robust security technique (encryption and decryption) through low processing power and other features for the ubiquitous computing. This new area of research is associated with lightweight cryptography.

NIST considers lightweight cryptography as a subsidiary of cryptography which intends to offer solutions for rapidly evolving applications based on low power-constrained devices [4]. The traditional cryptographic algorithm can perform in fine fettle in servers, computers, and some mobile phones. otherwise, lightweight cryptography platforms are required for devices of the perception layer are like sensing devices, sensor networks, smart cards, RFID tags and embedded system.

IoT supports building networks and creating connections between different devices or objects in the heterogeneous environment without or rather lesser human interventions. IoT security can also be susceptible to several attacks as each device can have illegal access to the network which affects and crash the network privacy and security parameters. Besides to these topics, all low-resource devices have restricted battery life, less computation power, a small memory space, and small bandwidth. As a result, an effective and suitable security solution is expected to avoid crunching the IoT smart devices. This paper is planned as follows. An introduction about the lightweight cryptographic primitives for low-resource device is given in section 2. Section 3 discusses security challenges and counter-measures in IoT. Section 4 discuss the proposed scheme. Finally, our research is concluded in Section 5.

Revised Manuscript Received on February 28, 2020.

***** Correspondence Author

Zouheir Labbi*, ICES Laboratory, ENSIAS, Mohammed V University, Rabat, Morocco. Email: zouhir.labbi@gmail.com

Mohamed Senhadji, ICES Laboratory, ENSIAS, Mohammed V University, Rabat, Morocco. Email: m.senhadji@um5s.net.ma

Ahmed Maarof, ICES Laboratory, ENSIAS, Mohammed V University, Rabat, Morocco. Email: ahmed.maarof@gmail.com

Mostafa Belkasmi, ICES Laboratory, ENSIAS, Mohammed V University, Rabat, Morocco. m.belkasmi@um5s.net.ma

II. OVERVIEW OF LIGHTWEIGHT CRYPTOGRAPHY PRIMITIVES

Lightweight cryptography (LWC) is a popular member within cryptography family that aims to develop a specified efficient cryptographic mechanism for devices with limited resources in terms of memory space and power. LWC is considered as a lighter form of conventional cryptography [5]. This branch of cryptography looks forward adjusting the current computationally intense operations of conventional cryptography algorithms to these constrained devices, by reducing the size of the fundamental parameters, that involves key size, block size, at an acceptable rate with minimum memory and energy consumptions and few computational cycles, without negotiating on security.

Fig. 1 and Table I represent respectively the classification of LWC primitives and outline of the recent LWC algorithms being developed in the IoT context, based and characterized by their structures, block length, key size, and cycles number.

A. Lightweight Block Ciphers

A lightweight cryptographic cipher algorithm WG-8 was introduced by Fan Xinxin et al.'s research [6], which is adapted for low-resource devices from the Welch-gong cipher family. Many lightweight block ciphers are introduced in existing research to obtain the most suitable performance for items, such as RC-5 [7], AES-128 [8], TEA [9] and XTEA [10].

Habitually, to improve their performance, most of these algorithms were improved by simplifying and reducing the complexity of the conventional block ciphers.

For example, DESL [11], called also DES lightweighted, since it is derived from traditional DES. In DESL, only single S-box is used by the round function instead of iterating eight rounds to build the first and final permutation which eventually conducts to enhance the hardware implementation.

SPECK and SIMON [12] are flexible block ciphers algorithms that deliver a variety of key sizes that are suitable for the entire variety of lightweight purposes. [13] describes A number of block ciphers based on LWC philosophy:

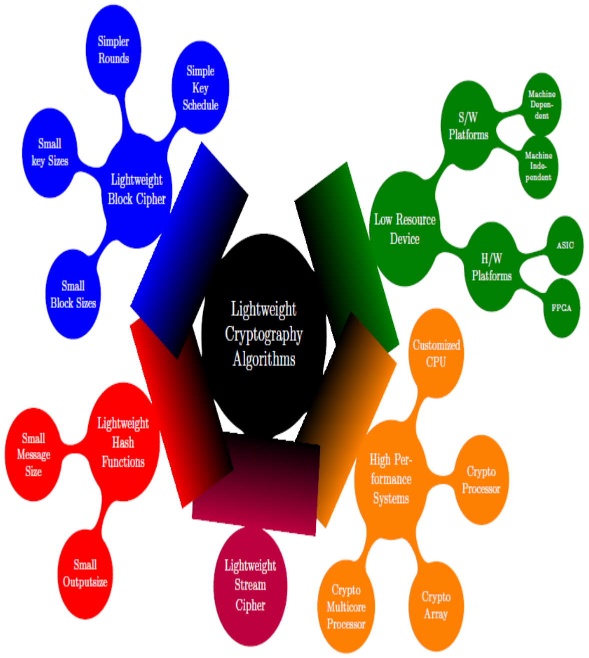

Fig. 1.Lightweight Cryptography primitives Classification

Table I. List of some LWC algorithms [13]

Algorithm	Structure	Block size	Key size	N. of rounds
AES	SPN	128	256/192/128	10/12/14
PRESENT	SPN	64	128/80	31
HIGHT	GFS	64	128	32
RC5	Feistel	128/64/32	2040-0	255-1
XTEA	Feistel	64	C	64
TEA	Feistel	64	128	64
Seed	Feistel	128	128	16
LEA	Feistel	64	256/192/128	32/28/24
Twine	Feistel	64	128/80	32
DES	Feistel	64	54	16
3DES	Feistel	64	168/112/56	48
DESL	Feistel	64	54	16
Humminbird2	SPN	16	256	4
Humminbird	SPN	16	256	4
Icebreg	SPN	64	128	16

- *Smaller block size:* With a minimum cost and to achieve the performance gains of lightweight block ciphers, the block size of plaintext should be small. for example, instead of use 128-bits for AES the block size should be at 64-its.
- *Smaller key length:* To reach power consumption with restricted battery life in a lightweight block cipher, the key size should be small. For instance, the key size of PRESENT [14] and Twine [15] have respectively 80-bits and 128/80-bits.
- *Simple rounds:* Generally, for low-resource conditions, lightweight block ciphers possess simple calculation operations and a limited number of rounds compared with standard and conventional block cipher algorithms. e.g., in a lightweight, a single 4-bit S-box has been utilised in place of 8-bit boxes inside conventional and traditional cryptography.

  Example of simple algorithms based on LWC are Hummingbird2 [16] which has no more than four rounds, and PRESENT which utilises 4-bit S-boxes.
- *Simple key schedules:* The key schedule used in each round, is a type of algorithm which computes the subkeys from the given key. Normally, the consumption of the complicated keys in term of energy and memory during their implementations is considerable compared to subkeys generated by simple key schedules which used by lightweight block cipher (e.g. for TEA, the block cipher purely divides a 128-bit key to four keys with 32-bit).

B. Lightweight Stream Ciphers

The stream ciphers encrypt the plaintext to produce ciphertext by combining each binary digit with the corresponding digit of the keystream (one bit at a time) [17]. The encryption process under stream ciphers uses one bit or byte at a time than a whole block under a block cipher, which considers stream ciphers faster and more convenient concerning real-time data, such as VoIP. The benefit of lightweight stream cipher consists of, low buffer size, low complexity and more important debit. Table II describes the three ciphers named in eSTREAM competition held by European Network of Excellence for Cryptology to identify new ciphers with large-scale adoption.

Table II. Lightweight Stream Ciphers [18]

Cipher	Key size	Initialization Vector	Internal State
Grain	128/80	96/64	256/160
Trivium	80	80	288
MICKEY2	128/80	0-128/0-80	320/200

C. Lightweight cryptographic Hash Functions

A hash algorithm is a deterministic function that converts plaintext into ciphertext. Any modifications to the plaintext would generate a different ciphertext. Standard hash functions expect a huge and large internal state size which consume a significant value of power to perform the evaluation process [19]. To jump this difficulty many lightweight hash functions are proposed for small devices with constraints on energy and power like Spongent, PHOTON and Quark. Table III shows the distinct with conventional hash functions in term of their output sizes, message sizes and internal state.

Table III. List of some Lightweight Hash Functions

Cipher	Block/Rate	Digest	Internal State
Spongent	16/8	256/80	272-88
PHOTON	36/32/16	256/80	288-100
Lesamnta	128	256	256
Quark	36/32/16	256/176/136	256/176/136

D. Performance Metrics for Low Resource Devices

The quality of service prescribed by performance which rendered by resources-constrained of small devices to achieve the same security levels in an IoT environment. The metrics of the performance are represented in terms of latency or waiting time [19], power consumption, memory usage [20] and throughout. In this paragraph, we draw two kinds of lightweight cipher implementation in devices with low-resource.

- *Software Implementation:* Software implementation of LWC algorithms may be performed by running the code on the processor, generally a low-cost microcontroller with 8-bit, 16-bit [20]. The code language can be a machine (assembly) or independently such as Java and C [19]. The parameter's value on which implementations software under resource-constrained devices are based on power, speed and memory. The performance metrics of the software [20], [4] focus on the debit, number of the register needed in ROM and RAM and code size.
- *Hardware Implementation:* The performance metrics that characterize the hardware implementation of LWC algorithms are as follow [20]:
  - *Power consumption:* in Watts, required for resource device.
  - *Gate area:* is the physical area capacity needed into a circuit to run an LWC algorithm. The better Gate Equivalent value is the lower one (unit of gate area size).
  - *Latency:* in seconds, the time needed by the circuit to provide the output once the input has been set.

III. SECURITY CHALLENGES AND COUNTEMEASURES FOR IoT

A. Issues and Research Challenges

- *Research Challenges:* The principal challenge in IoT applications is ensuring confidentiality, security and data integrity. therefore, the major challenge is linked to the mechanism which performs authorization, authentication and key management. Additional challenges related to IoT environment are described as follows:
  - Lesser interventions from human can lead to logical/ physical attacks.
  - Several kinds of research done on the security vulnerabilities related to many attacks like reply attack, eavesdropping, DoS/DDoS and many more in IoT wireless sensor networks.
  - A challenge associated with resources constrained devices includes limited autonomy battery, power consumption, different platforms, bandwidth and complex security methods which may delay and affect the device performance.
- *Issues:* The evolution of IoT in social facilities, business companies, workplaces etc. who they face issues related to security and privacy that are the main causes of concern in the development of IoT platform.

As the algorithm's behavior based on conventional cryptography does not match well the IoT concept due to several resource constraints and requirements like power, limited battery, real-time performance etc. Hence, LWC becomes more suitable to run in an IoT system. Many types of research were developed in LWC especially based on asymmetry and symmetry algorithm, but they still some challenges to improve the power consumption, memory demand, execution time and assure real-time security. There was a short authentication in symmetric algorithms while the bigger key size of asymmetric algorithms consumes the memory space, spend resources of the IoT devices and influences real-time processing and data collecting.

B. Solutions and correction actions for IoT

1) lightweight Symmetric algorithm for IoT

- *AES:* Advanced encryption standard, also known by Rijndae cipher, launched by NIST and states three forms which are AES-192, AES-256 and AES-128. The operation of the encryption process comprises a 4×4 matrix with blocks size 128-bit. The design of its internal state consists of by mix column, sub byte, add round key and shift rows.
- *HIGHT:* High security and lightweight employs Feistel structure which leads to use a very basic and simple operation to generate the keys within the decryption and encryption. To improve the RFID system, a new parallel implementation was introduced by Lee and Lim that requires a few lines of code and less energy [21]. HIGHT is exposed to a vulnerable attack represented by a saturation attack.
- *TWINE:* This algorithm uses Feistel structure that requested in each round 8 times, XOR operation using subkey and perform 4×4 S-box.

Contrary to HIGHT, permutation and combination are more complicated in TWINE in order to speed up distribution. The permutation in TWINE requires only half the number of rounds like the circular offset so that the difference of a single sub-block diffuses all the sub-blocks

- *PRESENT:* contains 31 rounds and based on SP-network. This lightweight algorithm is developed and adopted for security purpose. PRESENT comprises two keys with 128 and 80 bits and block of 64 bits.

2) Lightweight Asymmetric Algorithms for IoT

- *RSA (Rivest–Shamir–Adleman):* due to its big key size, this algorithm, in general, seems not suitable to LWC structure. RSA preserves the privacy of users and offers more security due to playing modulo operation and the use of two long prime numbers.
- *ECC:* the key size used by Elliptic Curve Cryptography algorithm is very smaller with less memory and offers a rapid processing speed and fast real-time computing. Hence, the hardware implementation can be accomplished into a small area (constrained devices) [22].

Tables IV, V present some illustrations of asymmetric and symmetric lightweight algorithms used in IoT environment based on their number of rounds, block size, code length, potential attacks, internal structures and key size and.

Table IV. Lightweight symmetric algorithms for internet of things

Asymmetric algorithm	Structure	Code length	Nb. Rounds	Block size	Key size	Possible attack
PRESENT	SPN	936	32	64	80	Differential
AES	SPN	2606	10	128	128	Man-in-midle
HEIGHT	GFS	5672	32	64	128	Saturation
TEA	Feistel	1140	32	64	128	Related key
RC5	ARX	Not fixed	20	32	16	Differential and Timing

Table V. Lightweight asymmetric algorithms for internet of things

Asymmetric algorithm	Length	Key size	Possible attack
ECC	8838	160	Timing
RSA	900	1024	Modules

IV. PROPOSED LIGHTWEIGHT ENCRYPTION (LWE) SCHEME FOR INTERNET OF THINGS

A. LWE Scheme

The proposed lightweight scheme (LWE) which suited for IoT devices, combines asymmetric and symmetric lightweight encryption algorithms.

Lightweight asymmetric algorithms offer stronger security compared to symmetric algorithms even if their requirements in term of computation complexity and larger key size in the constrained IoT context [23]. Therefore, develop an algorithm suitable and appropriate to resource-constrained IoT environment that deliver asymmetric and symmetric lightweight algorithms characteristics with small key size, less computation time, consume less power, less memory space, and assures the same security level.

Furthermore, smart space includes many devices which have limited computational power, battery power and memory space, however, other devices have adequate battery power, processing power and memory space. Consequently, the proposed scheme combines both cryptography aspects by taking into account all devices specifications dedicated IoT environment (see Fig. 2).

Fig. 2 illustrates a flowchart which considers IoT devices parameters as input and its outcome recommends the convenient encryption algorithm for this smart device. LWE scheme consists of four analysis phases that utilize as input four device parameters: memory space (MS) [24], data size (DS), battery power (BP), and computation power (CP) [24]. Each parameter has a threshold value which can be determined by a specific algorithm.

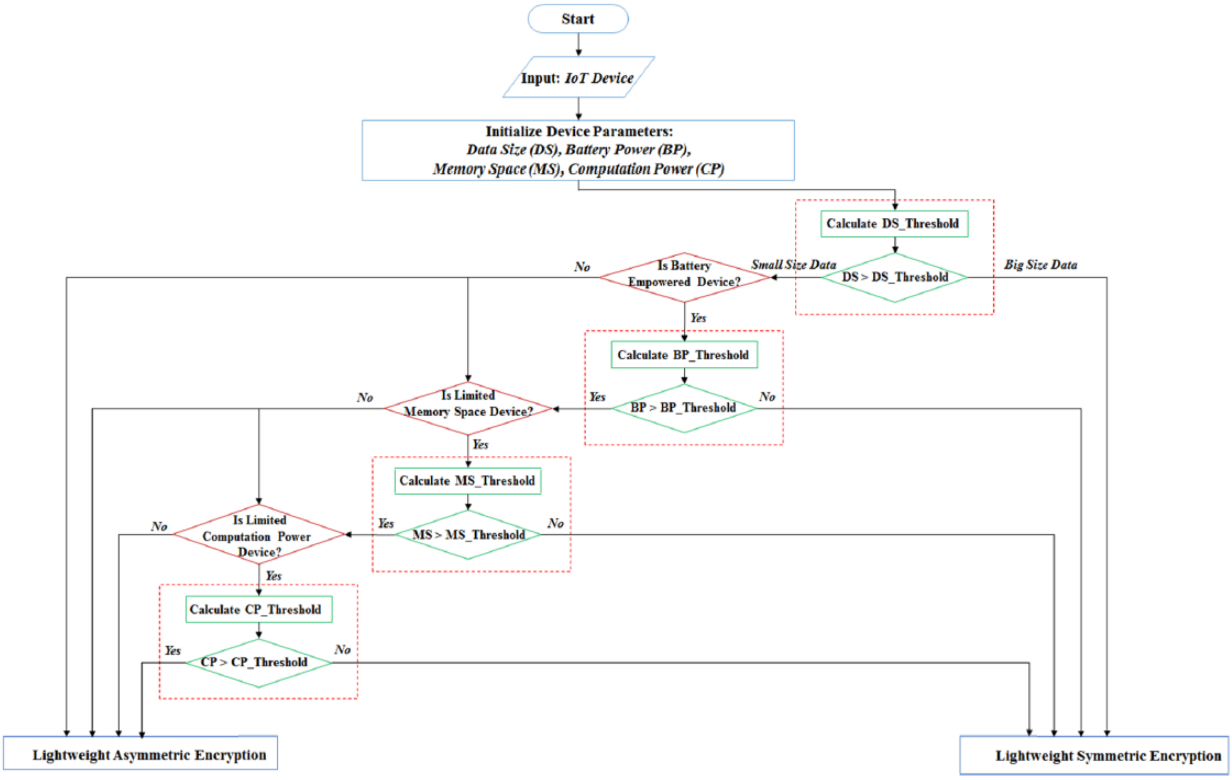
Start
Input: IoT Device
Initialize Device Parameters:
Data Size (DS), Battery Power (BP),
Memory Space (MS), Computation Power (CP)
Calculate DS_Threshold
DS > DS_Threshold
Small Size Data
Big Size Data
Is Battery Empowered Device?
No
Yes
Calculate BP_Threshold
BP > BP_Threshold
Yes
No
Is Limited Memory Space Device?
No
Yes
Calculate MS_Threshold
MS > MS_Threshold
Yes
No
Is Limited Computation Power Device?
No
Yes
Calculate CP_Threshold
CP > CP_Threshold
Yes
No
Lightweight Asymmetric Encryption
Lightweight Symmetric Encryption

Fig. 2.Proposed scheme

The proposed LWE scheme follows the hierarchy levels concept. All smart home devices integrate processors which collects the data, perform the appropriate instructions, and formulate the targets information of device that proves the model of hierarchal structured [25]. The LWE scheme provides two encryption algorithms as output (lightweight symmetric and asymmetric encryption) depend on the device parameters evaluation. Both algorithms are the light release of conventional algorithms proved by their smaller number of rounds, key size, block size and code length. Which make the proposed scheme adequate and suitable for constrained IoT devices like RFID (Radio-frequency Identification), WSN (Wireless Sensor Network) and many more.

After initializing the four parameters, LWE scheme starts firstly by calculating the communicated data quantity through the network. If the data quantity is large, which means that is bigger than the threshold rate. In this case, the recommended output is lightweight symmetric encryption according to the present research [26][27], else, our scheme continues by executing the next processing phase which is represented by checking the parameter of IoT device battery. Equations (1) and (2) may affect respectively the computational power, memory space, and battery power of IoT device [30]. Table VI illustrates the notation of these equations.

If the calculated value of the battery power is smaller than the threshold and based on the research work [31], the proposed scheme recommended and advised lightweight symmetric encryption as the recommended method. And if the IoT device has sufficient battery power, the process pasts to analysis the memory space under the next phase.

For memory size analysis phase, the metrics part is a platform-dependent, like code length, that related to the selected processor and its instruction set. The number of shifts or/and the addition of XOR operation can also influence the memory size. The encryption process does not require much memory if it does not utilize substitution boxes. The following equation expresses the design throughput:

TableVI. notations

Notation	Metric
NB	Block size
GE	Gate equivalent
TB	Time to encrypt one block
A	Design area
CB	Cycles Nb. to encrypt one block
F	Frequency
Th	Throughput

$$Th = \frac{N_B}{T_B} = \frac{N_B \times F}{C_B} \qquad (1)$$

The function of design frequency is represented by Throughput. Round's number (cycles) linked to the instruction set saved into the processor memory. Hence, each processor has its own number of cycles and frequency differ.

The memory reservation to store the data in IoT devices differs from limited memory and enough memory. The LWE scheme verifies if the device possesses restricted memory for analysis computation power, if not, the encryption process used in this case is lightweight asymmetric encryption [32].

The last phase of LWE scheme analysis considers the device computational power as efficiency metric, that is calculated by the report of the rate of flow computed upon the area at a fixed clock frequency [29].

This parameter estimates also the area cost and requisite to handle a unique ciphertext bit.

The performance efficiency is represented by the following equation:

$$Efficiency = \frac{Th}{A} = \frac{N_B}{T_B \times A} = \frac{N_B \times F}{C_B \times A} \qquad (2)$$

LWE scheme compares the threshold value with the device computational power by taking into account the efficiency points of the device. According to the present search performed in [26][28], if the value of computation power exceeds the threshold value, the recommended algorithm for this device is lightweight asymmetric encryption, otherwise, our scheme selects lightweight symmetric encryption.

V. RESULT ANALYSIS

A. Services Scenario Example

The proposed scheme is planned and designed to be adopted for resource-constrained devices with restricted memory storage and battery lifetime and can also feasible within smart home system. It is also suitable for several genre of smart space like for example smart home applications (Fig. 3). Multiple IoT devices in smart home with different processing power, memory spaces and battery abilities are interconnected and interact with each other.

Fig. 3 presents an example scenario in a smart home network based on smart sensor node, that communicates the encrypted message by applying LWE scheme. This proposed scenario is described during the following section.

The smart sensor in this scenario transmits into the smart home network the light message accordingly to their limited memory, battery and computation power. Table VII shows the values sensor node parameter including the calculated value of threshold for memory space, power of battery and computation power.

For instance, the data from the smart home system may be detected by a smart sensor device. Presume a sensor node desires transmit a data to a separate sensing unit. Table VII express the parameters which is considered in LWE scheme for efficient and secure communication. The value of threshold battery power is 11.66 mW and the battery power of sensor node (data 2) is 10 mW which is below the calculated threshold. This case conducts to use the lightweight symmetric encryption as output algorithm. The battery power value in data3 is bigger than the threshold parameter, which proceeds and pasts to the memory phase analysis.

The throughput during this phase is considered to calculate the threshold value. The Table VII shows that the average of the memory spaces threshold value for several devices for IoT system is 3310.66 bytes and as the memory value of the sensor node (data 1) is 4740 bytes, which is higher than the threshold value. Consequently, the process will go to the computation analysis phase, else lightweight symmetric encryption will be applied. Compensation power takes into account the smart sensor processor frequency. The computation parameter threshold value shown in Table VII is 399MHz. by examining the computation power value for data 2 and data 3 the output encryption algorithm of LWE approach is lightweight symmetric. Otherwise, lightweight asymmetric encryption will be applied for data 1.

Table VII. Parameters values of smart sensor [29]

Parameter	**Data (3)**	**Data (2)**	**Data (1)**	**Threshold value (average)**
Computation power (MHz) based on frequency	363	377	444	399
Memory space (byte) based on throughput	2997	2195	4740	3310,66
power of Battery (mW)	12	10	13	11,66

B. Discussion and Issues

Even the importance of many contributions in cryptographic scheme and implementation, there are still fields to be analyzed in forthcoming research works. We surveyed and summarized in the previous sections several existing lightweight algorithms dedicated for IoT devices with low-resources. This paragraph intends to highlight the associated research topics related to lightweight and conventional cryptographies. We describe also in this section the addressed issues as follow.

1) Cryptography implementations and cipher structure

The implementation of the cryptography studied within this work makes it possible to reveal the global performance for different cryptographic designs. Though, a dependence on technologies and tools deform the outcomes and finishing by huge deviations among the investigations. Hence, start thinking about another approach is necessary, by proposing a new cryptosystem that should be compared with the present conventional cryptography. The recent model serves to enhance the quality of investigation in the field of lightweight cryptography. To optimize the cryptographic energy, a hardware impact design energy is proposed by Mohd et al. which attained the optimal energy of Katan cipher implemented in 32 rounds [30]. Furthermore, they advised making a design more compacted by taking into account the physical, architectural, and algorithmic issues. The model comprises a conventional structure of Feistel with slow diffusion as cipher structure. Also adjusting between the complexity of the round and increased the number of rounds, pipelining, and unrolling/rolling rounds. Furthermore, a middleware framework called PalCom was suggested by [33] to exchange a lightweight data for IoT environment.

2) Issues related to key length and block length

The evolution of lightweight approach dedicated to resource restrained is based on the significant role performed by the block and the key size. The size of ciphertext is increased automatically when increasing the key size, and as result, the computational power, in this case, becomes more important. The same is valid for block size. Attackers can use a particular key to destroy the algorithm by applying the multikey attack. The property of confidentiality is put under risk if the key is well got by attackers.

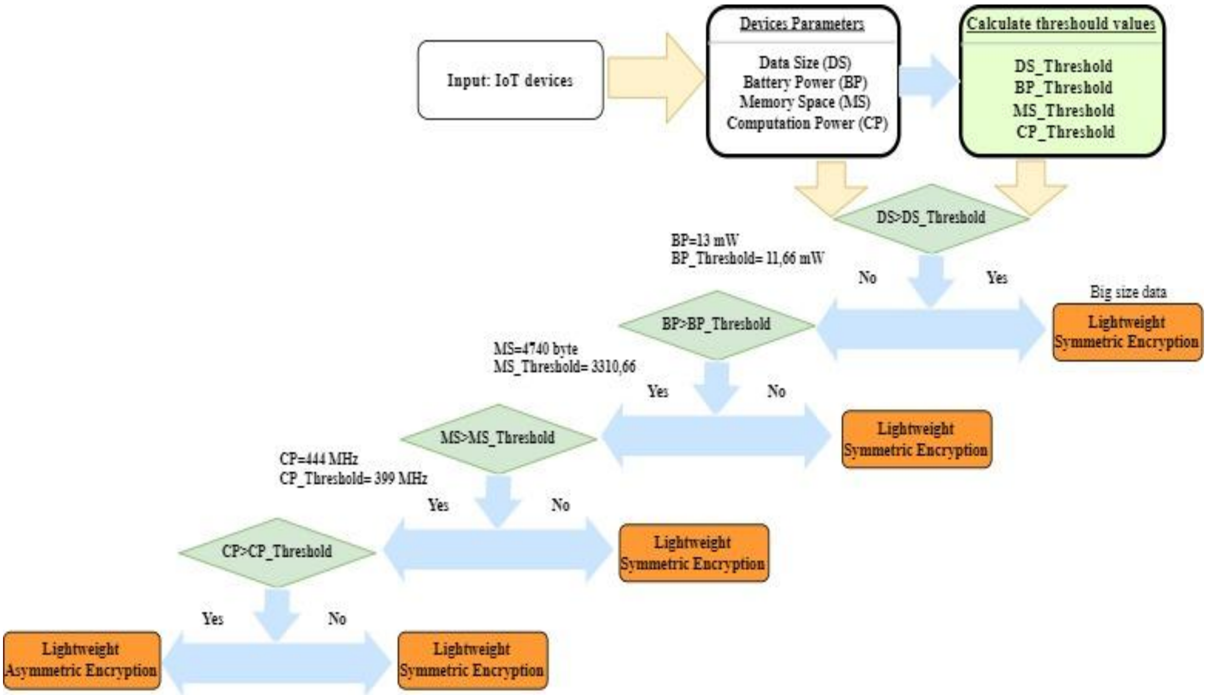

Fig. 3.Scenario proposed for smart home

3) Novel attacks

Many solutions are proposed to preclude and identify attacks that affect the security level and destroy the implemented models [34]. Thus, to be resistant to attacks the capacity of cipher must be modernized. The great problem in resource restrained system is the HT (Hardware Trojan. Which affect the implanted circuit by its physical behavior throughout the fabrication/ design phase. A Supplemented unsolved problem provides the necessity to evolve a universal pattern which consolidates design of HT and hardware to evaluate the complexities and trade-offs of security.

4) Security level

The level of security for constrained device is adaptable as well as its resources structure, which increase the attention and the interest of security metrics. Generally, there is no metric for security can precisely estimate the level of security for cryptographic field. In fact, encryption process is a topic to the decryption which represented by adopting a list to break the encryption process. According to successful listed of attacks, the security level can be classified as less secure, safe or moderate. Nonetheless, popular security systems still need improvements and require more clearly set security standards for performing cryptographic security for constrained resources devices in the IoT systems still need enhancements and expect more definitely set parameters for performing cryptographic security.

VI. CONCLUSION

We have elaborated in detail, in this work over the new branch of conventional cryptography named lightweight cryptographic algorithms, as numerous devices with low-resource for IoT system perform computations methods and restricted in term of autonomy, energy consumption and memory. They also face the challenges of privacy and security and counting the matter by which conduct to preserve the security among IoT employers. Moreover, we have reviewed several types of cryptographic algorithms with lightweight option that can be implemented whether hardware or software. A number of algorithms list are susceptible to several sorts of attacks which conduct to evolve safe and strong lightweight encryption algorithms with small size of key and demand less computation power and fast processing. In this paper we proposed a new approach which may be employed into smart environment. We discussed as well as the opened points concerning block size, key size, cipher structure, implementation, security metrics, and new attacks.

Our expectation will examine the cost of these solutions and study the integration possibility into restricted IoT system. furthermore, we expect to improve the algorithm used for computing the value of threshold for individual device parameter, that has been previously presented within this work.

REFERENCES

1. C. Maxim, et al, “Internet of Things (IoT): Research, Simulators, and Testbeds”. IEEE Internet of Things Journal, 2018, vol. 5, no 3, pp. 1637-1647.
2. L. In, and K. Lee, “The internet of things: investments, Applications and challenges for enterprises”. Business Horizons, vol. 58, no. 4, 2015, pp. 431-440.
3. B. Padmavathi, et al, “performance analysis of AES, RSA and DES algoirithm with LSB substution”. IJSR, India, 2013.
4. M. Kerry, et al, Repoert on lightweight cryeptography. NISITIR, pp 1-28, 2017.
5. J. B. William, et al, “Lightweight cryptography methods”. Journal of Cyber Security Technology, 2017, vol. 1, no. 3-4, pp.187-201.
6. F. Xinxin, et al, “Weg-8: lightweieght streeam cipher for resources-constriained smart devices”. Proceeding of ICHNQRSR, 2013, Springer, Berlin, pp. 617-632.
7. R. L. Ronald, “The RC5 encryption algorithm”. International Workshop on FSE, 1994, Springer, Berlin, pp. 86-96.
8. I. Kengo, et al, “Analysis on equivalent in current source of AES128 circuits for HD power in model verification”. International Symposium on EMC’14, Tokyo, IEEE, 2014, pp. 302-305.
9. W. J. David, et al, “TEA, an encryption algorithm”. International Workshop on FSE, Springer, Berlin, pp. 363–366, 1994.

10. Y. Jack, et al, “Xtea encryption-based novel RFID security protocol”. 24th CCECE, 2011, IEEE, pp. 58-62.
11. L. Gregor, et al, “New lightweight DES variants”. International Workshop on FSE, Springer, Berlin, pp 196-210, 2007.
12. B. Ray, et al, “The SPECK and SIMON lightweight block ciphers”. 52nd ACM/EDAC/IEEE, IEEE, 2015, Design Automation Conference (DAC), pp 1-6.
13. “Lightweight block ciphers”. Université du Luxembourg. https://www.cryptolux.org/index .php/Lightweight_Block_Ciphers. Accessed 22 July 2019
14. B. Andrey, et al, “PRESENT: an ultralightweight block cipher”. International CHES Workshop, Springer, pp. 450-466, 2007.
15. H. Jaber, et al, “A comprehensive survey on evaluation lightweight symmetric ciphers: software and hardware implementation”. Advances in Computer Science: International Journal, 2016, vol. 5, no 4, pp. 31-41.
16. M. Bassam J, et al, “A survey lightweight block ciphers for low resources devices: a comparative study & open issues”. Journal of Network and Computer Applications, 2015, vol. 58, p. 73-93.
17. D.Dumitru Daniel, “Secure and Efficient Implimentations of thee Lightweieght Symmitric Cryptogreaphic Primiteves”. University of Luxembourg, 2017, pp. 278.
18. D. Lennart, et al, “Comparison of Lightweight Stream Ciphers: MICKEY 2.0, WG-8, Grain and Trivium”.
19. S., Saurabh, et al, “Advanced lightweight and encryption algorithms in IoT devices: challenge, survey and solutions”. Journal of Ambient Intelligence & Humanized Computing, 2017, pp. 1-18.
20. B.Alex, et al, “State of the Art of Lightweight Symmetric Cryptography”. 2017.
21. L.Je-Hoon, et al, “Paralel archetecture fer heigh speeed blocck cipher, HEIGHT”. International Journals of Security and Applications, 2014, vol. 8, no 2, pp. 59-66.
22. E. Thomas, et al, “A survey of a lightweight cryptography implementations”. IEEE Design & Test of Computers, 2007, vol. 24, no 6, pp. 522-533.
23. S. Maity, JH. Park, “Powering IoT devices: novel design & analysis technique”. Journal Converg 7, 2016, pp. 1-18.
24. D. Alan, “Component of smaert deveice and a smart deveice interaction”. Telecom Sofware Systeems Grroup, 2003, pp. 1-18.
25. Hood, GW, et al. US Patente N. 7,574,735. Patente USand Tradeemark Offices, DC, pp. 1–28, 2010.
26. M. Ranjeet, et al, “Dynnamic selections of a symetric key crypetographic algorithm securiing data bassed on the variious parameter”. ArXiv preprint:1406.6221, 2014.
27. MA. Mushtaque, “A Comparrative annalysis on differents parammeters of the encryeption algorithm informations secureity”. Internationnal Journale IJCSE, 2014, 2(4), pp. 76-82.
28. T. Ritu, S. Agrawal, “Comparative study of asymmetric and symmetric cryptography technique”. IJAFRC, 2014, vol. 1, no 6, pp. 68-76.
29. K. Stéphanie, et al, “Toward greean crypetography: comparaison of lightweieght cipher freom the energey viewpoient”. Internationnal Worksshop on CHES, 2012, Springer, Berlin, pp. 390-407.
30. M. Bassam Jamil, et al, “Optimization and modelling of FPGA implementation of Katan Cipher”. 6th International Conference on ICICS, IEEE, 2015. p. 68-72.
31. K. Jong-Min, et al, “Power adaptive of data encryption for energy efficient and secure communication in solare powered wireless sensor network”. Journal of Sensors, 2016, vol. 2016.
32. C. Sourabh, et al, “A comparative survey of asymmetric and symmetric key cryptography”. International Conference ICECCE. IEEE, 2014. pp. 83-93.
33. N. Behailu, et al, “LIISA 2.0: lighetweight intirnet of thing services buss architeceture utilising noode centreic netwoerking”. Journale of Ambeient Intelleigence aend Humaenized Compueting, 2016, vol. 7, no 3, pp. 305-319.
34. B. Swarup, et al. “Protection against the hardware trojan attack: toward comprehensive solution”. IEEE Design & Test, 2013, vol. 30, no 3, pp. 6-17.

AUTHORS PROFILE

Zouheir Labbi Since 2014, he is working toward a Ph.D. degree in Computer Science and Engineering at Department of Computer Science ENSIAS, Rabat, Morocco. His interests are security in low cost RFID and application of RFID technologies in Internet of things (IoTs). Since 2006, Zouheir Labbi has worked as support and software engineer for Alcatel-Lucent, now he is as fixed network presales services team at NOKIA.

Mohamed Senhadji is currently an Assistant Professor at the communication networks department of ENSIAS, Mohammed V University, Morocco. He gives several courses at ENSIAS school such Computer Architecture, Assembly, Microprocessors and Implementation Networks, Physical security and smart card. His research interests lie with the field of wireless networking, RFID technologies, Internet of Things (IoTs) and Ad-hoc networks

Ahmed Maarof is working toward a Ph.D. degree at college of Engineering, ENSIAS, Mohammed V University. His interests are security in low cost RFID security and Lightweight cryptography for Internet of things (IoTs), low power circuit design techniques for passive tags. Since 2006, Ahmed Maarof has worked as sub-Contractor hardware and software engineer for several company, Texas instruments, ONsemiconductor, Wolfson, ST-Ericsson, Zodiac Aerospace and Freescale, now he is a sub-contractor hardware engineer for NXP.

Mostafa Belkasmi is a professor at ENSIAS Rabat; head of Telecom and Embedded Systems Team at SIME Lab. He had PhD at Toulouse University in 1991(France). His current research interests include, RFID technologies, Internet of Things (IoTs), mobile and wireless communications, interconnections for 3G and 4G, and Information and Coding Theory.