ANALYSIS THE SECURITY OF SOME CIPHERS IN INDUSTRIAL APPLICATIONS OF WIRELESS SENSORS NETWORKS

Khalid Fadhil Jasim[1], Mohammad Hussein Shukur[2], Abdullah Abdulabbas Nahi Alrabeeah[3], and Laith R. Fleih[4]

[1,2,3,4]*Department of Computer Science, Cihan University-Erbil, Kurdistan Region, Iraq*
[1]khalid.jassim@cihanuniversity.edu.iq,
[2]mohammed.shukur@cihanuniversity.edu.iq,
[3]abduallah.nahi@cihanuniversity.edu.iq,
[4]laith.flaih@cihanuniversity.edu.iq

***Abstract*— The wireless sensor networks played substantial role in many fields such as pollution monitoring system, health care system, military operations system, agriculture industries, bridges monitoring, and wastewater treatment systems. Various types of data are exchanged via these networks which can be exploited by intruders or unauthorized users. Hence, there is a demand to protect the data confidentiality in these networks. The cipher algorithms can be used to protect the data confidentiality in these networks. This research presents some applications of wireless networks. Moreover, the research focused on study some cipher algorithms and different features of these ciphers. In this context, the encryption keys, input block, encryption process, and components of these algorithms have been covered. Thus, these cipher algorithms can provide suitable level of protection for the WSN networks.**

Keywords- Encryption algorithms; Wireless Networks Initialization Operations; Data Confidentiality

I. INTRODUCTION

In the previous years, the Wireless Sensors Networks (WSN) have been adopted in different areas such as environment applications, scientific monitor systems, and health care systems. These networks depend on a number of sensor nodes which are connected via the radio frequencies. The design of sensor node consists of sensors, transceiver unit, microcontroller unit, power resource, and memory storage. In different WSN applications, the sensor nodes are used for data collections from the field and transmit the collected data to the remote servers. Also, it can be used in various activities comprising (industry, railway control systems, smart city, home automation, traffic control, measuring systems, medical monitoring systems, and environment sensors). The nodes in (WSN) are constrained devices that have small storage memory, low consumption of power, restricted battery life, and limited computation power [1]. For instance, the WSN networks are used in agriculture industries, in which the sensor nodes are used to collect the data for field temperature, condition of crop, and weather humidity. The collected information via WSN networks will help to take suitable decisions for fertilization and irrigation operations that improve corps production [2]. In transportation field, the high speed trains pass via bridges, the vibrations and loads of trains will cause damages to the structures of bridges. Therefore, the WSN networks have been adopted in the monitoring systems of bridges structures, and to collect data about bridges health states and dynamic response so as to mitigate and prevent the collapses accidents of these bridges [3]. Jimenez et al. [4] proposed wastewater treatment system that can be used in irrigation operations. This system designed based on WSN networks, data analysis algorithm and communication protocol. The proposed system can be utilized to detect pollution stains and salinity of water. In the field of gardening (e.g. golf courses), it is important to manage soil moisture in order to increase the efficiency of using water. In recent years the remote sensing technique have been applied to measure the moisture of soil. In this context, Mauri et al. [5] introduced a method that depends on WSN networks and remote sensing technique so as to generate indexes for soil moisture and can be used in golf courses. The WSN networks used in different applications and aspects in smart cities, and for monitor the environmental aspects. Also, routing protocols in WSN networks possess significant role in data transmission in smart cities applications [6].

Moreover, the WSN networks employed in different types of health care applications. The sensor nods support flexible methods to collect information about human body (e.g. blood pressure, brain activity, heart activity, and level of oxygen in the body). These health care applications, with the support of WSN networks, can help the health centers to monitor the patients and diseases in wide areas [7]. On the other hand, the sensitive information of patients should be kept secret and not disclosed to unauthorized people. The authors in [8] have been proposed a scheme to protect the privacy of patients in these health care applications.

Some unauthorized users (e.g. intruders or opponents) can access the connection between the WSN networks and sensor nodes via eavesdropping operations (e.g. active and passive attacks). Also, some hacking operations may be exploited to attack the security protocols in these networks. Therefore, there is a demand to protect the data exchanged in these networks. It is important to protect the data confidentiality, authenticity and data integrity for the WSN networks. For instance, the sensor nodes may be attacked by the hackers to extract sensitive data (e.g. secret encryption keys) which affect on data confidentiality. It is also a significant issue to use secure authentication protocol in the connection between the sensor nodes and base stations which can prevent the use of legitimate nodes by intruders. The transmitted data in WSN networks must be accurate, correct, and without modification so as to protect the data integrity in these networks [9,10].

The symmetric cipher algorithms rely on stream cipher and block cipher techniques. In this context, the symmetric cipher algorithms can be used to protect the data confidentiality in IoT devices and the IoT involves various components (e.g. Wireless Networks, Sensors Nodes, Radio Frequency Identification Devices (RFID), and Actuators) [11][25]. Also, these algorithms can be used to protect the data exchanged in the WSN networks and support secure transmissions among the sensor nodes and WSN networks.

DOI:http://doi.org/10.24086/cocos2022/paper.513

The encryption and decryption operations depend on the same secret key that must be shared via the WSN networks with secure and protected links [12]. Hence, this paper concentrates on study and analysis various components of cipher algorithms which may be utilized for secure data transmissions in the WSN networks.

The research is organized as follows. Section I introduced WSN networks, sensor nodes, encryption algorithms and some applications of WSN networks in various fields. Section II presents study of LED cipher and concentrates on encryption key, block size, rounds and the 4 operations in this cipher. Section III analyze the components of PRESENT cipher (e.g. input block, secret keys, encryption process and S-Box). Section IV describes versions of PICCOLO cipher, input block, subkeys, rounds and encryption process of this algorithm. Some versions of SIMON cipher, block size, secret keys and round function are presented in Section V. Section VI presents 3 versions of SPARX cipher, input block, secret keys, steps, rounds and encryption process. Section VII describes 3 types of LEA cipher, rounds, secret keys, round function and encryption process. Section VIII provides the discussion of WSN networks and the six cipher algorithms. Lastly, we present conclusions of this research in section IX.

II. LED Cipher Algorithm

The LED block cipher algorithm depends on different encryption keys (e.g. length of Enc. Key equal 64, 80, 96 & 128- bits). The input block (with length = 64 bits) and the number of rounds includes (32 and 48 rounds) [13]. For example, the LED-64 operates on (64 bits) input data or plaintext (P). The input data arranged as 16 (4 bits) values (P0, P1, … , P15, which means each Pi represented by 4 bits) and organized in state matrix (4x4 Matrix, Fig. 1) as follows [14]:

P0	P1	P2	P3
P4	P5	P6	P7
P8	P9	P10	P11
P12	P13	P14	P15

Figure 1: Plaintext Matrix in LED cipher.

LED-64 relies on (64 bits) key (K), the elements of this key are arranged as 16 (4 bits) values (K0, K1, … , K15) and organized in matrix (4 x 4 Matrix). Moreover, this cipher use 8 steps, each step consists of 4 rounds and 4 operations (AddConstant, SubCells, ShiftRows and MixColumnSerial). These 4 operations are applied on the above mentioned input state matrix during encryption process. Also, LED cipher depends on S Box with 16 Hex values (Table 1). For example if the input (x = 0) then the output (S(x) = C). In the data encryption, the input data matrix is processed by the above mentioned 4 operations and after 8 steps the output ciphertext matrix, or encrypted data matrix, is produced.

Table 1: S-Box in LED and PRESENT Ciphers

x	0	1	2	3	4	5	6	7
S(x)	C	5	6	B	9	0	A	D
x	8	9	A	B	C	D	E	F
S(x)	3	E	F	8	4	7	1	2

III. Present Cipher Algorithm

PRESENT is block cipher encryption algorithm (Fig. 2) and it is suitable for ultra-lightweight devices [15]. This block cipher is based on SPN design (Substitution Permutation Network), input block (64 bits), secret key (e.g. lengths of Enc. Keys equal 80, and 128 bits) and the process for perform the encryption includes 31 rounds. The encryption process consists of round key part, substitution box (S-Box , nonlinear part) and permutation (Per , linear part). In round key part, the elements of input data block B_i are Xored with the elements of round key K_i.

$$B'_i = B_i \text{ xor } K_i \quad (0 \leq i \leq 31)$$

In S-Box substitution part, the 64 bits output (B'_i) from round key part arranged into 16 (4 bits). Each (4 bits) used as input to S-Box (Table 1) and produce (4 bits) output. In permutation (Per) part, the output (64 bits) from S-Box part used as input to permutation (Per) and rearrange these bits according to defined permutation table (e.g. Per[0] = 0, Per[1] = 16, Per[2] = 32, … , Per[62] = 47, Per[63] = 63 etc.) [16].

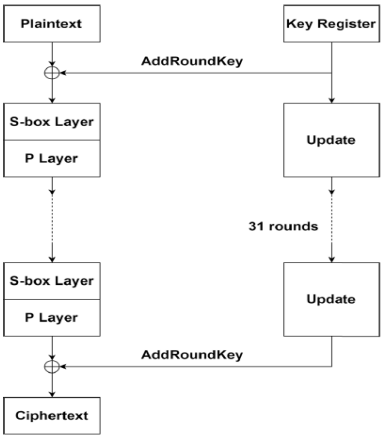

Figure 2: PRESENT Cipher .

IV. Piccolo Cipher Algorithm

PICCOLO is block cipher designed with 2 versions (Piccolo-80 and Piccolo-128) based on Feistel Cipher techniques [17]. Piccolo-80 use input block (64 bits), secret

DOI:http://doi.org/10.24086/cocos2022/paper.513

key (80 bits) and 25 rounds. The 80 bits of secret key are arranged into sub keys (k0, k1,k2, k3, k4, and each ki consists of 16 bits). Piccolo-128 adopt input block (64 bits), secret key (128 bits) and 31 rounds. The 128 bits of secret key are arranged into sub keys (k0, k1,k2, … k7, and each ki consists of 16 bits). Also, the algorithm depend on mix key function (WKi), this function implemented in the begin and in the end of the algorithm. The details of data encryption are shown in (Fig. 3).

Figure 3: Encryption Process in PICCOLO.

The encryption process include input data with (64 bits), and after perform the encryption steps will produce the encrypted data (64 bits). Moreover, the round permutation can process 8 values (e.g. X0, X1,X2, … , X7) , and produce 8 rearranged values (e.g. X2, X7,X4, … X5). Two substitution boxes (4x4 S-Box) and M matrix are used in F function of this cipher algorithm [18].

V. Simon Cipher Algorithm

The National Security Agency (NSA) designed SIMON block cipher algorithm [19]. This cipher algorithm was appropriate for hardware devices. Many versions designed of SIMON cipher (e.g. 1st version SIMON - 32/64, 2nd version SIMON - 64/128, and 3rd version SIMON - 128/256). For example, SIMON-32/64 depends on block of input data (32 bits), length of secret encryption key (with length = 64 bits), and (32) rounds. SIMON-128/256 relies on block of input (128 bits), encryption secret key (with length = 256 bits) and (72) rounds. The design use round function which includes 3 logic operations (AND operation, Circular Shift S^i operation , XOR operation, and all these operations applied with Bitwise computation) as shown in (Fig. 4).

Figure 4: Round function in SIMON.

The round function use input data with 2 words (Xi and Xi+1). Then apply Bitwise operations on these words. The operations include Left Circular Shift (S^1 by 1 bit, S^8 by 8 bits, and S^2 by 2 bits), Bitwise AND, XOR, and round key Ki. The output of round function consists of 2 words (Xi+1 and Xi+2) [20].

VI. Sparx Cipher Algorithm

SPARX is classified as block cipher encryption algorithm. This cipher depends on input block of data (with size = n) and encryption key (with size = k). Therefore the algorithm represented by SPARX-n/k [21]. The input data (plaintexts) and the output data (ciphertexts) include w words (w = n/32). Also, the elements of encryption key are separated into a number of words (v: v 32

DOI:http://doi.org/10.24086/cocos2022/paper.513

Figure 5: Encryption Process in SPARX Cipher.

Moreover, this cipher algorithm designed with 3 versions (1st version SPARX (64 / 128), 2nd version SPARX (128 / 128) and 3rd version SPARX (128 / 256) [22]. For example, first version of SPARX with (64/128 bits) involves block size (64 bits), key size (128 bits), operates with words (w: w = 2), words of key (v: v = 4), steps (n_s=8), rounds/step (r_a=3), and total rounds (24). The parameters of the 3 versions of SPARX cipher are explained in (Table 2).

Table 2: Versions of SPARX cipher.

Parameter	SPARX-64/128	SPARX-128/128	SPARX-128/256
Block Size	64 bits	128 bits	128 bits
Key Size	128 bits	128 bits	256 bits
Rounds	24	32	40
Steps ns	8	8	10
Round/step	3	4	4

VII. LEA CIPHER ALGORITHM

The LEA is block cipher algorithm suitable for software applications and provides data encryption with high bit rate. This cipher algorithm designed with 3 types (e.g. 1st type LEA - 128, 2nd type LEA - 192, and 3rd type LEA - 256) [23]. The design of first type of LEA with (128 bits) includes (24) rounds, encryption secret key (Enc. Key with length equal 128 bits) and input block (with size equal 128 bits). The LEA-192 consists of 28 rounds, encryption secret key (with length equal 192 bits) and input block (with size equal 128 bits). The design of LEA-256 depends on (32) rounds, encryption secret key (with length equal 256 bits) and input block (with size equal 128 bits). Also, this cipher contains round function and this function consists of 3 rotation operations (ROR3, ROR5, ROL9), 6 XOR operations and 3 Modular Addition (Mod 2^{32}). The algorithm perform data encryption with different steps. First, the input block (with 128 bits) organized as sequence of words (e.g. four words: Xj [0],Xj [1], Xj [2],Xj [3]), apply the mentioned operations of round function on the 4 words, repeat this process in each round j, then after the last round 4 words of encrypted data are produced (Fig. 6) [24].

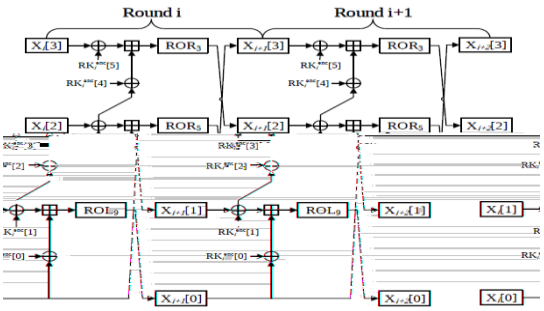

Figure 6: Encryption Process in LEA Cipher.

VIII. DISCUSSION

In recent years the WSN networks have been evolved and implemented in different fields. These networks used in agriculture industries to improve corps production, in bridges monitoring to prevent the collapse's accidents, wastewater treatment systems, gardening to control soil moisture, and in health care systems to monitor the patients and diseases. Moreover, there is a need to protect the transmitted data between the WSN networks and sensor nodes, and prevent the unauthorized users (e.g. hackers, intruders or opponents) from access these networks. The symmetric ciphers algorithms can be used to protect the data transmitted via the WSN networks and can provide secure data communications. Therefore, in this research we focused on study of some ciphers that can be used to protect data confidentiality in these networks.

Furthermore, the LED cipher is block cipher algorithm can provide suitable data protection. The design includes state matrix (4x4 matrix), apply 4 operations (first: AddConstant operation, second: SubCells operation, third: ShiftRows operation, and fourth: MixColumnSerial operation), and use Substitution Box that contains 16 Hex values (Table 1). Also, this cipher depends on 4 encryption keys (Table 3), input data (64 bits), number of rounds include (32, 48), depends on Substitution Permutation Network (SPN) technique and the design of this algorithm can be implemented by hardware or software programs.

The PRESENT cipher can be used as data confidentiality algorithm. The design of this cipher contains round key part, substitution box (S-Box) and permutation (P). This cipher adopts 2 encryption keys (Table 3), input data (64 bits), 31 rounds, relies on SPN technique and this cipher algorithm is suitable for hardware implementation.

PICCOLO Cipher is block cipher also can be used to protect the data in WSN networks. This cipher includes various components such as 2 (S Boxes), matrix M, Generate Round Key (K), Add Function (S), Add Round Key (S, rKi) and RP (S) (RP: Round Permutation). This cipher involves 2 encryption keys (80 and 128 bits), input block (64 bits), rounds (25 and 31), depends on Feistel cipher technique and suitable for hardware implementation (Table 3).

SIMON is block cipher that provides data encryption for secure data transmissions. This block cipher relies on round function, Left Circular Shift, Bitwise AND, Bitwise XOR, and round key Ki. The encryption algorithm designed with different encryption keys (64, 128 and 256 bits), input blocks (32, 64 and 128 bits), rounds (32, 44 and 72), and adopted Feistel cipher. Also, this cipher can be implemented by hardware and software.

SPARX cipher starts with 2 inputs of plaintext (w words) and encryption key (v words). These 2 inputs processed by 4 loops, update key state, apply linear mixing layer, and addition of final key. This cipher provides flexible encryption process. Also, this encryption algorithm can operates with the 3 encryption keys (Table 3), 3 input blocks, rounds (24, 32, and 40 bits). The design depends on Feistel cipher, and suitable for software implementation.

DOI:http://doi.org/10.24086/cocos2022/paper.513

LEA cipher constructed with 3 types (e.g. 1st type LEA - 128, 2nd type LEA - 192, and 3rd type LEA - 256). The design of this cipher based on round function, this function involves 3 rotation operations (ROR3, ROR5, ROL9), 6 XOR operations and 3 Modular Addition (Mod 2^{32}). The 3 versions depend on 3 encryption keys (128, 192, and 256 bits), input block (128 bits), rounds (24,28, and 32), and adopt Feistel cipher. These versions can be implemented by software and hardware.

According to the increasing demands on resource constrained devices such as WSN networks, sensor nodes, RFID devices, smart cards and FPGA devices, all the mentioned lightweight encryption ciphers algorithms are practical solution to protect the data in these resource constrained devices.

Table 3: Encryption Algorithms.

Type Of Cipher	Encryption Key (Bits)	Input Block (Bits)	No. of Rounds	Structure/ Design of Cipher
LED	64/80/96/128	64	32/48	SPN/HW,SW
PRESENT	80/128	64	31	SPN/HW
PICCOLO	80/128	64	25/31	Feistel/HW
SIMON	64/128/256	32/64/128	32/44/72	Feistel/HW,SW
SPARX	128/128/256	64/128/128	24/32/40	Feistel/SW
LEA	128/192/256	128/128/128	24/28/32	Feistel/SW,HW

IX. Conclusion

This research presented analysis study of some applications of wireless sensor networks in different fields, and some cipher algorithms that can be used for the data security in these networks. WSN networks deployed in agriculture industries, bridges monitoring, wastewater treatment systems, gardening, military systems, and in health care systems. Moreover, some cipher algorithms such as LED, PRESENT, PICCOLO, SIMON, SPARX and LEA can be used for data confidentiality in wireless sensor networks. Thus, this research introduced analysis study of these ciphers. These ciphers relied on different lengths of encryption keys ranged (80 bits to 256 bits) which enhance the security of these ciphers. These algorithms can process various input lengths of data (32 bits to 128 bits). Various lengths of rounds (24 to 72 rounds) used in these algorithms that improve the security of encrypted data. The cipher algorithms designed based on two significant techniques the Feistel Cipher and Substitution and Permutation Networks (SPN). Furthermore, software and hardware designs can be adopted for implementing these cipher algorithms. As a result, these cipher algorithms can support practical solutions for the data security in WSN networks. Finally, we offer 6 cipher algorithms and the customer can select based on the available resources and the application field.

References

[1] Lee, Cheng_Chi. "Security & Privacy in Wireless Sensor Networks: Advances and Challenges. " *Sensors* 20, no. 3 (2020): 744.

[2] Kumar, Nagesh, and Brijbhushan Sharma. "Opportunities and Challenges with WSN's in Smart Technologies: A Smart Agriculture Perspective." In_ *Handbook of Wireless Sensor Networks: Issues and Challenges_ in Current Scenario's*, pp. 441-463. Springer, Cham, 2020.

[3] Deng, Nianchun. "Study on Dynamic Characteristic of Train_bridge Coupling Based on Wireless Sensor Network." *Journal of Internet Technology_* 20, no. 2 (2019): 555-562.

[4] Jimenez, Jose M., Lorena P., Laura G., Jaime L., Pedro V. Mauri, and Pascal L. "New Protocol and Architecture for a Wastewater Treatment System Intended for Irrigation." *Applied Sciences_* 11, no. 8 (2021): 3648.

[5] Mauri, Pedro V., Lorena P., David M., Laura G., Jaime L., and Jose F. Marin. "The Combined Use of Remote Sensing and Wireless Sensor Network to Estimate Soil Moisture in Golf Course." *Applied Sciences_* 11, no. 24 (2021): 11769.

[6] Ismail, Reem J., Khalid F. Jasim, Samar J. Ismael, and Soma AM Solaimanzadeh. "Enhancing Wireless Sensor Networks Routing Protocols Based on Cross Layer Interaction." *Cihan University_Erbil Scientific Journal* 5, no. 2 (2021): 52-55.

[7] Saleh, Yasmine N.M, Claude C. Ch., Ayman A. Abdel_Hamid, and Abdel_Hamid Soliman. "Privacy Preservation for Wireless Sensor Networks in Healthcare_ State of the Art, and Open Research Challenges." *arXiv preprint arXiv:2012.12958* (2020).

[8] Sharma, Nidhi, and Ravindara B. "Privacy Preservation in WSN for Healthcare Application." *Procedia computer science_* 132 (2018): 1243-1252.

[9] Bhushan, Bharat, & Gadadhar S. "Recent Advances in Attacks, Technical Challenges, Vulnerabilities and their Countermeasures in Wireless Sensor Networks." *Wireless Personal Communications_* 98, no. 2 (2018): 2037-2077.

[10] Pragadeswaran , S. "Wireless Sensor Networks Security Issues, Security Needs and Different Types of Attacks Based on Layers: A Survey." *International Journal of Advanced Engineering Science and Information Technology* _5, no. 5 (2021).

[11] Jasim, Khalid F., Reem J. Ismail, Abdullah A. Nahi Al-Rabeeah, and Soma Solaimanzadeh. "Analysis the Structures of Some Symmetric Cipher Algorithms Suitable for the Security of IoT Devices." *Cihan University_Erbil Scientific Journal* 5, no. 2 (2021): 13-19.

[12] Sun, Da_Zhi, and Yi M. "On the Security of Symmetric Encryption Against Mass Surveillance." *IEEE Access* 8 (2020): 175625-175636.

[13] Yao, Yuan, M. Yang, Pantea K., and Patrick S. "Dimming Down LED: An Open-source Threshold Implementation on Light Encryption Device (LED) Block Cipher." *arXiv_ preprint arXiv:2108.12079* (2021).

[14] Rai, Vikash K., Boreddy V. , Somanath T., and Jimson M. "Correlation Power Analysis and Effective Defense Approach on Light Encryption Device Block Cipher." *Security and Privacy_* 2, no. 5 (2019): e87.

[15] Gunathilake , Nilupulee A.,Ahmed Al_Dubai, William J. Buchanan , and Owen L. "Electromagnetic Analysis of an Ultra_Lightweight Cipher: PRESENT." *arXiv_ preprint arXiv:2106.15225* (2021).

[16] Luo, Haoxiang, Weijian C., Xinyue M., and Yifan W. "General Differential Fault Attack on PRESENT and GIFT Cipher with nibble. " *IEEE Access_* 9 (2021): 37697_37706.

[17] Mhaouch, Ayoub , Wajdi E., and Mohamed A. "Lightweight Hardware Architectures for the PICCOLO Block Cipher in FPGA. " In *2020 5th_International Conference on Advanced Technologies for Signal and Image Processing_(ATSIP)*, pp. 1-4. IEEE, 2020.

[18] Liu, Ya, Liang Ch., Fengyu Zh., Chunhua Su. , Zhiqiang L., Wei L., and Dawu G. "New Analysis of Reduced-Version of PICCOLO in the Single-Key Scenario." *KSII_Transactions on Internet and Information Systems (TIIS)* 13, no. 9 (2019): 4727-4741.

[19] Wang, Xuzi, Baofeng W., Lin H., and Dongdai L. "Searching for Impossible Subspace Trails and Improved Impossible Differential Characteristics for SIMON_like Block Ciphers." *Cybersecurity*_4, no. 1 (2021): 1-14.

DOI:http://doi.org/10.24086/cocos2022/paper.513

[20] Le, Duc-P., Sze Ling Y., and Khoongming K. "Algebraic Differential Fault Analysis on Simon Block Cipher. " *IEEE Transactions on Computers*_68, no. 11 (2019): 1561-1572.

[21] Alzakari, Sarah, and Poorvi V. "Linear and Partly-Pseudo-Linear Cryptanalysis of Reduced_Round SPARX Cipher. " In_*International Conference on Applications and Techniques in Information Security*, pp. 108-121. Springer, Singapore, 2020.

[22] Zhou, Dawei, Huaifeng C., Rui Z., and Ningning S. "Zero-Correlation Linear Cryptanalysis on SPARX - 64." *Journal of Sensors*_2021 (2021).

[23] Song, JinGyo, and Seog Seo. "Efficient Parallel Implementation of CTR Mode of ARX - Based Block Ciphers on ARMv8_Microcontrollers." Applied Sciences 11, no. 6 (2021): 2548.

[24] Kim, YoungBeom, Hyeokdong K., SangWoo A., Hwajeong S., and Seog Chung S. "Efficient implementation of ARX - based Block Ciphers on 8 - Bit AVR Microcontrollers. " Mathematics_8, no. 10 (2020): 1837.

[25] Al-Majdi, K., Salman, A., Abbas, N., Hashim, M., Taha, M., Nahi, A., Saleh, S. (2022). MLCM: An efficient image encryption technique for IoT application based on multi-layer chaotic maps. *International Journal of Nonlinear Analysis and Applications*, 13(2), 1591-1615. doi: 10.22075/ijnaa.2022.6571

DOI:http://doi.org/10.24086/cocos2022/paper.513