WAS Science Nature
WASSN

ISSN: 2766 - 7715
WAS PRESS

Article

Evaluation of Lightweight Block Ciphers Based on General Feistel Structure (GFS)

Bassam. W. Aboshosha[1,*], Mohamed M. Dessouky[2], Rabie. A. Ramadan[3], Ayman El-Sayed[2], and Fatma H. Galalb[2]

[1] Department of Computer Engineering, Higher Institute of Engineering, Elshorouk Academy, Cairo , Egypt; bassam.ahmed32@gmail.com
[2] Department of Computer Engineering, Menofia University, Menoufia, Egypt
[3] Computer Engineering Dept. Cairo University, Cairo, Egypt and University of Hail, Hail , KSA

* Correspondence: bassam.ahmed32@gmail.com

Received: 1-08-2018; Accepted: 1-09-2018; Published: 20-09-2018

Abstract: Recently, lightweight block cipher has become a hot topic, which is a key technology to ensure the security of communications among constrained devices such as WSNs, RFID, and IoT. Therefore, hundreds of lightweight block ciphers have been proposed. The architecture of these ciphers is influenced by the balance between protection, efficiency, and costs. Therefore, efficient evaluation methods should be established. This paper outlines the performance analysis of three generalized Feistel lightweight block crypto ciphers - CLEFIA, PICCOLO, and TWINE. Various benchmark parameters, such as area, throughput, and power, need to be considered to analyze such algorithms. The algorithms are also tested for various key and plaintext sizes. This comparison sets the base for other algorithms to be tested and evaluated. It also encourages the researchers to look after different lightweight algorithms that could be utilized the best in certain applications instead of generalizing their purposes. Moreover, it shows the performance of the selected algorithms on Hardware, where most of the proposed algorithms are examined on software only.

Keywords: Constraint devices; lightweight cryptographic; IoT; WSNs; RFID; GFS.

1. Introduction

The Internet is the international architecture for communication systems that connects computer networks using the TCP/IP protocol suite. It makes it possible for various computer networks to be connected revolutionizing the communication among various devices as well as people. Wireless communications is one of the most important revolutions in the Internet. An approximate 47% of the world population has Internet access and around 75% of the world's own wireless devices. The Internet of Things (IoT) is the latest innovation in which it focuses on the concept of linking both smart machines and sensors via the internet IoT is expected to offer new applications which will create tremendous improvements in physical and virtual environments through Machine-to-Machine (M2M) communication. On the other hand, Internet of things faces numerous challenges like bandwidth, security, privacy, computing power, battery power supply, memory, scalability and many more among which privacy and security is the most important things to be considered in this environment as we cannot trust all the users in IoT. Cryptography can help to provide security assertion, which is necessary for protecting against the unauthorized access and different types of attacks. Since standard security methods such as an advanced data encryption standard (DES) and

advanced encryption standard (AES) cannot be used such constrained devices. Therefore, a certain class of cryptographic algorithms known as Lightweight Cryptography (LWC) is chosen to be an ideal candidate for these environments.

There are numerous Lightweight crypto block ciphers available; these ciphers have been designed based on different structures like, Feistel Structure, SP Network, Lai Massey and ARX Structure. Authenticated ciphers have their characteristics in software and hardware consistency and energy efficiency.

In this paper, we look into the implementation of three lightweight block ciphers, namely PICCOLO, CLEFIA, and TWINE, which belong to the Generalized lightweight Feistel Network (GFN) (which is a tradeoff between security and light weightiness) [3]. This work is inspired by [8], where the authors compared the same algorithms using different perspectives. Also, the algorithms are implemented on different hardware platforms. The authors of [8] implemented the algorithms on STM32F4 MCU and ARM Cortex-M4 with the following characteristics. STM32F401RE is considered a powerful device compared to Arduino Uno with ATmega328P – 8 bit AVR family microcontroller.

Table 1. STM32F401RE specifications

Core	ARM 32 Cortex M4
CPU Frequency	84 MHz (84,000,0000 cycles per sec)
Flash Memory	512 KBytes
SRAM	96 KBytes
Security	MPU(Memory Protection Unit)
USB Type	USB OTG FS
Supply Voltage (v) max	3.6
Supply Current (per MHz)	137(μA)

The paper investigates their structures and evaluates their performance. This paper sets the base for other lightweight algorithms to be tested and evaluated. It also encourages the community to look after different lightweight algorithms that could be utilized best in certain applications instead of generalizing their purposes. Nevertheless, implementing such lightweight algorithms on hardware could be a challenging process, and we might end up with no suitability of such algorithms if implemented on hardware. In this paper, we investigate such issues as well.

The paper is organized as follows: In the next Section 2, an Overview of these ciphers is presented with their specifications and security. Section 3 describes ciphers hardware implementations. Finally, the analysis and comparison between the three mentioned algorithms using important metrics will be presented in Section 4..

2. Overview of Different LWCS Based on GFN

This section goes through the security and specifications of previously mentioned algorithms: PICCOLO, CLEFIA, and TWINE block cryptographic algorithms. PICCOLO is a lightweight block cipher that adopts a GFN structure with two versions, PICCOLO-80 and PICCOLO-128 [53]. The structure of PICCOLO block cipher is given in Fig 1a. The algorithm is divided into the data processing part and the key scheduling part. The data processing shows that 64-bit plaintext with four 16-bit whitening keys and 2r 16-bit round keys are used to encrypt the plaintext, where r is the number of rounds. To improve diffusion, Piccolo uses a byte permutation between rounds. Piccolo's Feistel function consists of two S-box layers separated by a diffusion matrix. The text is decrypted in a similar fashion, with only changes made to the order of round keys and whitening keys selection. In each round, the previous stage's output is permuted (shuffled on words of 8 bits) and given as input to the next stage. In the main preparation portion, the input key is split into five 16-bit of 80-

bit key and Eight 16-bit keys for 128-bit key, which have Four 16-bit whitening keys and 2r 16-bit round keys [7].

TWINE is a lightweight block cipher that is based on GFN with 16 (4-bit) branches. It uses 64-bit block size and supports two key sizes: 80-bit and 128-bits. In the data processing part of the algorithm, 64-bit ciphertext are generated out of 36 (32-bit) round keys and 64-bit plaintext. It has a very simple round structure wherein each round, eight F-functions are called, which simply consists of a key addition and the application of a 4-bit S-box, as shown in Fig 1b. The linear layer is a nibble permutation with a high diffusion, which permutes the 16 blocks. The cipher's design aims at the small footprint in hardware implementations and small ROM/RAM consumption in software. For TWINE, the decryption utilizes the same S-Box, the central method of encryption, but the diffusion layer is the inverse of the encryption. In the main TWINE scheduling portion, the input key producing 36 (32-bit) round keys uses 35 (6-bit) constants. TWINE's main schedule includes a round primary process on the fly by updating the key state sequentially. using such method, the hardware footprint is reduced and consequently the performance is enhanced. Because the round keys are sequentially updated, bit permutation or intermediate key generation is not necessary.

CLEFIA is a lightweight block cipher developed by Sony. It supports 128-bit block size with three different key sizes: 128-bit, 192-bit, 256-bits. The structure of CLEFIA is as shown in Fig 1c. This algorithm is currently available as an ISO-compliant lightweight crypto cipher. The basic element of the algorithm is the GFN (d, r), where d is representative of the data branch, and r is the round. CLEFIA data processing part requires four 32-bit whitening key, 2r 32-bit round key, and 128-bit encryption plaintext. The two F-functions (4x4 diffusion matrix) are used, which are simple substitution and permutation. Key scheduling part takes the input key to derive the intermediate key. CLEFIA 128 uses the constants GFN (4, 12) and 60 (32 bit) while CLEFIA192 uses the constants of GFN (8, 10), and 84(32-bit). At the same time, ClEFIA256 uses the constants GFN (8, 10) and 92(32-bit). The Double Swap function replaces these intermediate keys after two rounds the entry key to four whitening keys and 2nd round keys is expanded to intermedia keys.

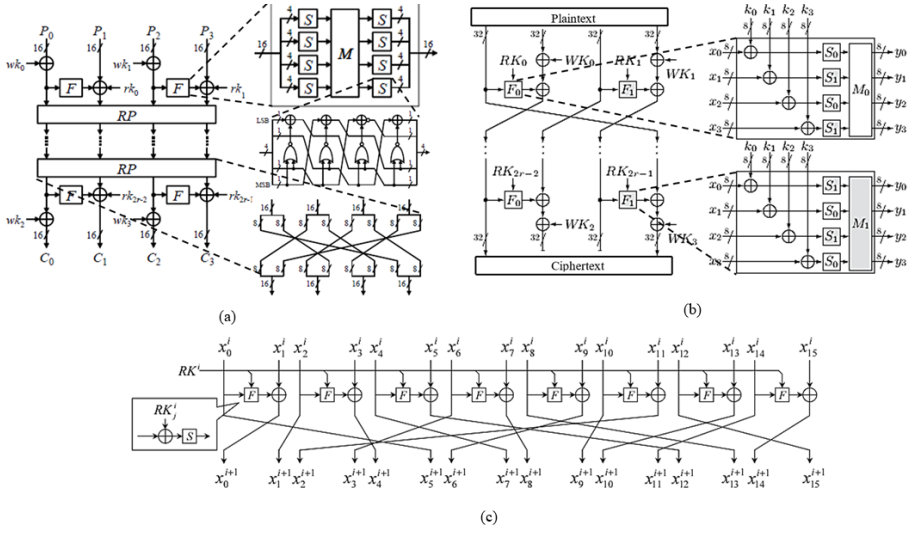

Figure 1. (a) PICCOLO Encryption Structure, (b) TWINE round structure, and (c) CLEFIA Encryption Structure

3. Hardware Implementations

There are different ways to implement a cryptographic circuit. This paper considers three basic implementation architectures, unrolled, round, and serial , as indicated in Fig 2. Efficient implementation has become one of the most challenging in different applications especially, constraint resources devices applications. Therefore, the following metrics have to be taken into consideration if the encryption schemes are implemented in hardware.

- Low gate area, measured in Gate Equivalents (GE), memory consumption, and implementation size reflect the gate area.
- High throughput; reflects the encryption process speed, and it measured in bits or bytes per second.
- Low latency, which defines the time taken to obtain the output of the circuit once its input has been set. It measured in seconds.
- Low power consumption; indicates the amount of power needed to use the circuit. It measured in Watts.

These four criteria compete with one another. For instance, a low latency tends to imply a higher area. Small implementation is also by far slow, while the most energy efficient is the largest.

The optimum tradeoff between these quantities depends greatly on the context. In fact, primitives have been proposed that have been optimized for different corners of the design space: some allow a very low latency implementation, others a very small one (in terms of GE), etc. Regardless of the exact platform, a given primitive may be implemented using different approaches. In the case of the hardware implementation of the three algorithms; Two types of implementation were evaluated: one performing only the encryption operation and the other performing both encryption and decryption with the same module in which a control signal switches the operations.

The block cipher algorithm can generally be divided into key scheduling and encryption/decryption functions. For the evaluation in this guideline, an implementation having both functions was built. The same clock-controlled the key scheduling function and the encryption/decryption function. Algorithms that require no registers for key scheduling were implemented without registers.

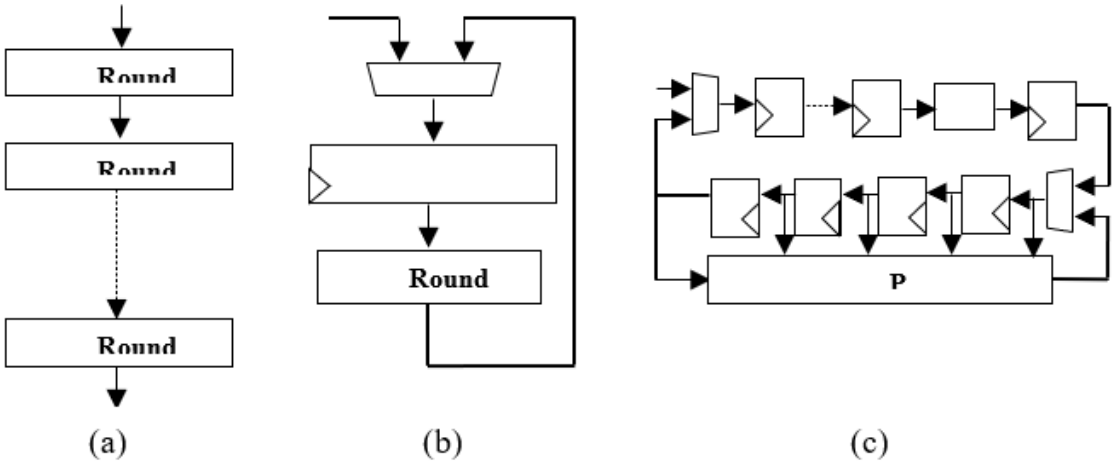

Figure 2. Basic Implementation Methods (4-a) unrolled, (4-b) round and (4-c) serial implementation

4. Performance Evaluation

Let us consider unrolled implementation which is popular when a low-latency is targeted as those allow a full evaluation in one clock cycle. The downside is then the far larger size of the circuit. Table 1 shows the unrolled implementations evaluation results of the three encryption algorithms CLEFIA, PICCOLO and TWINE. Figures 5a to 5d graphically compare the circuit sizes, excluding the target implementations' interface circuits, processing speeds, peak power, and leakage power.

As can be seen in Table 2, although CLEFIA uses 128 block and key size, it requires the largest area, and its peak power is also the largest. At the same time, it has the highest leakage power. On the other hand, although TWINE and PICCOLO-80 are almost similar in all of their characteristics, PICCOLO-80 is gaining 100% throughput, and its leakage power is much less than TWINE. Fig 3 confirms these results are visualizing the algorithm's performance during the encryption and decryption phases..

Table 2: Evaluation of Unrolled Implementation

Algorithm	Block Size (Bits)	Key Size (Bits)	Cycles/ block	frequency (MHz)	Throughput (Gbps)	Area (Kgate)	Peak power (mW)	Leakage power (µW)
Unrolled Encryption								
CLEFIA	128	128	1	5.7	0.7	**74.6**	**195.5**	**891.0**
PICCOLO-80	64	80	1	18	1.2	19.4	61.0	224.8
TWINE	64	80	1	24.8	**1.6**	19.5	43.8	221.2
Unrolled Encryption / Decryption								
CLEFIA	128	128	1	5.7	0.7	**74.3**	195.5	891.0
PICCOLO-80	64	80	1	16.3	1.0	22.8	64.8	264.0
TWINE	64	80	1	13.1	0.8	25.6	50.9	292.2

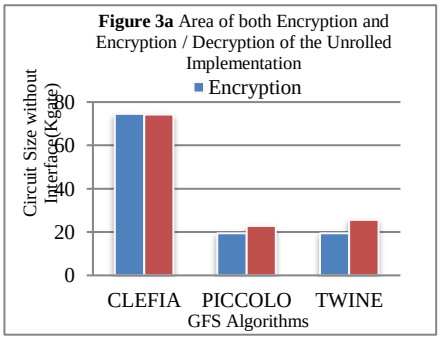

Figure 3a Area of both Encryption and Encryption / Decryption of the Unrolled Implementation

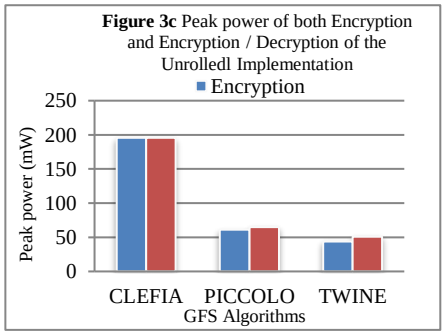

Figure 3c Peak power of both Encryption and Encryption / Decryption of the Unrolledl Implementation

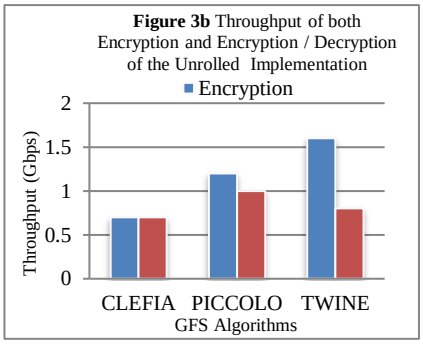

Figure 3b Throughput of both Encryption and Encryption / Decryption of the Unrolled Implementation

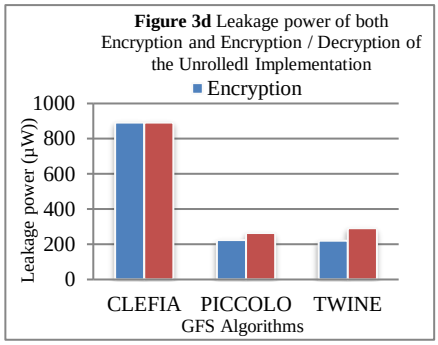

Figure 3d Leakage power of both Encryption and Encryption / Decryption of the Unrolledl Implementation

Figure 3. Unrolled Implementation Evaluations

Serialized and round-based implementations are recommended for lightweight hardware implementation. In serial implementation, although it has a minimal number of gate equivalents (GE) and the most efficient power consumption, it has the slowest performance. In some critical applications, the serial implementation performance is not acceptable, especially; for real-time IoT applications. In the case of round-based implementation, it has high throughput, low latency, small area, and low power consumption.

As can be seen in Table 3, the round implementations of three algorithms are presented. Although CLEFIA has the most power leakage, it has the best throughput; it is a tradeoff between the area size, power leakage, and throughput. Fig 4 could be better visualizing the results. However, in constrained devices, size and power could be the most important factors to be considered. So, in this case, using one of these algorithms depends on the nature of the applications.

Table 3 Evaluation of Round Implementation

Algorithm	Block Size (Bits)	Key Size (Bits)	Cycles/ block	frequency (MHz)	Throughput (Gbps)	Area (Kgate)	Peak power (mW)	Leakage power (µW)
Round Encryption								
CLEFIA	128	128	19	145.8	0.982	10.1	39.8	99.6
PICCOLO-80	64	80	27	262.5	0.622	3.5	3.4	34.2
TWINE	64	80	36	311.5	0.554	4.4	4.6	40.0
Round Encryption / Decryption								
CLEFIA	128	128	19	143.1	0.964	9.9	38.1	99.0
PICCOLO-80	64	80	27	261.8	0.621	3.8	3.3	38.5
TWINE	64	80	36	302.1	0.537	4.7	4.5	42.8

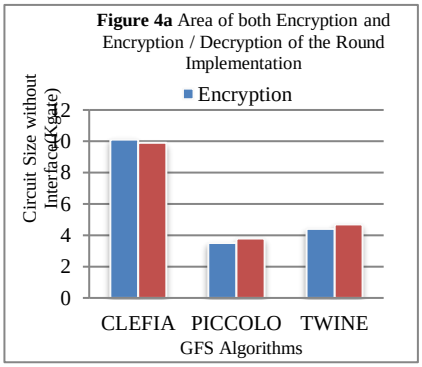

Figure 4a Area of both Encryption and Encryption / Decryption of the Round Implementation

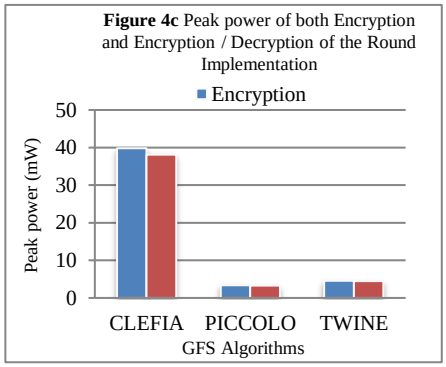

Figure 4c Peak power of both Encryption and Encryption / Decryption of the Round Implementation

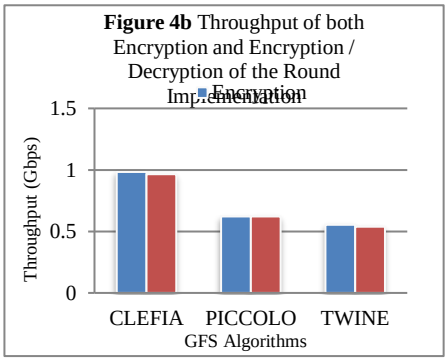

Figure 4b Throughput of both Encryption and Encryption / Decryption of the Round Implementation

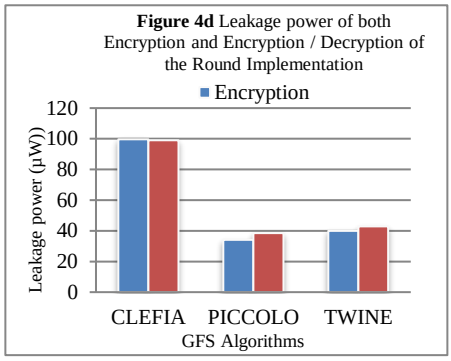

Figure 4d Leakage power of both Encryption and Encryption / Decryption of the Round Implementation

Figure 4. Round Implementation Evaluations

As shown in Table 4, PICCOLO-80 could be the worst for the serial implementation in terms of the cycles taken per block; the requirements are much less than the other two algorithms. At the same time, CLEFIA is the most secure algorithm among the three selected algorithms since it uses 128 key size and its throughput is much better than other algorithms. Also, CLEFIA is comparable to the PICCOLO-80 and TWINE in terms of the required area, peak power, and power leakage. Therefore, CLEFIA is our recommendation for serial implementation. For better visualization of the results, Fig 5 depicts the encryption and decryption performance of the algorithms.

Table 4 Evaluation of Serial Implementation

Algorithm	Block Size (Bits)	Key Size (Bits)	Cycles/ block	frequency (MHz)	Throughput (Gbps)	Area (Kgate)	Peak power (mW)	Leakage power (µW)
Serial Encryption								
CLEFIA	128	128	175	114.2	83.5	6.2	13.1	61.3
PICCOLO-80	64	80	433	300.3	44.4	3.5	2.0	28.5
TWINE	64	80	324	277.8	54.9	4.1	2.8	29.6
Serial Encryption / Decryption								
CLEFIA	128	128	175	113.1	82.7	6.8	12.5	59.3
PICCOLO-80	64	80	433	292.4	43.2	3.7	2.0	23.4
TWI	64	80	324	270.3	53.4	4.2	2.6	28.4

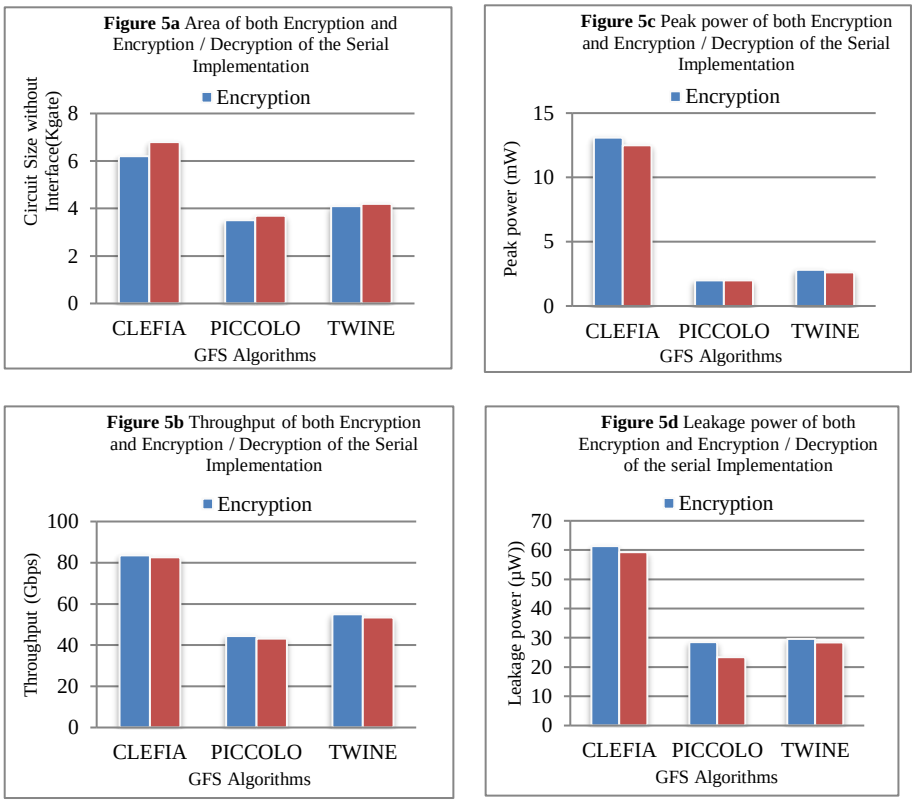

Figure 5. Serial Implementation Evaluations

5. Conclusions

A performance evaluation of different lightweight block ciphers, CLEFIA, PICCOLO and TWINE, which are based on GFN structure, is given in this paper. The evaluation metrics are the circuit sizes excluding the interface circuits, throughput, peak power, and leakage power of the different ways of implementation. The performance evaluation presented in this paper shows that the lightweight algorithms' hardware implementation could produce different points of view in utilizing the algorithms in real-world applications that software implementation could not be the best choice. Our future work targets different types of algorithms and different hardware platforms.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest."

References

1. Stallings, W. Cryptography and Network Security: Principles and Practice 0133354695, 9780133354690.
2. Author 1, A.; Author 2, B. Title of the chapter. In *Book Title*, 2nd ed.; Editor 1, A., Editor 2, B., Eds.; Publisher: Publisher Location, Country, 2007; Volume 3, pp. 154–196.
3. Ramadan, R., & Medhat, K. (2021). Intrusion Detection Based Learning in Wireless Sensor Networks. PLOMS AI, 1(2).
4. Lai, X., Massey, J. L., & Murphy, S. (1991, April). Markov ciphers and differential cryptanalysis. In Workshop on the Theory and Application of of Cryptographic Techniques (pp. 17-38). Springer, Berlin, Heidelberg.
5. Trappe, W. (2006). Introduction to cryptography with coding theory. Pearson Education India.
6. Schneier, B. (1993, December). Description of a new variable-length key, 64-bit block cipher (Blowfish). In International Workshop on Fast Software Encryption (pp. 191-204). Springer, Berlin, Heidelberg.
7. Daemen, J., & Rijmen, V. (2001). Reijndael: The Advanced Encryption Standard. Dr. Dobb's Journal: Software Tools for the Professional Programmer, 26(3), 137-139.
8. Ertaul, L., & Rajegowda, S. K. (2017). Performance analysis of CLEFIA, PICCOLO, TWINE Lightweight block ciphers in IoT environment. In Proceedings of the International Conference on Security and Management (SAM) (pp. 25-31). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).