

# Efficient hardware implementation for lightweight Loong algorithm using FPGA

Marwa Subhi Ibrahim<sup>1,2</sup>, Yasir Amer Abbas<sup>2</sup>, Mudhafar Hussein Ali<sup>1</sup>

<sup>1</sup>Department of Computer Engineering, College of Engineering, Al-Iraqia University, Baghdad, Iraq

<sup>2</sup>Department of Computer Engineering, College of Engineering, Diyala University, Diyala, Iraq

## Article Info

### Article history:

Received Sep 10, 2022

Revised Dec 5, 2022

Accepted Dec 10, 2022

### Keywords:

Field programmable gate array

Hardware architecture

Lightweight

Loong

VHDL

## ABSTRACT

Recently low-resource devices such as radio frequency identification (RFID), internet of things (IoT), and wireless sensor networks (WSN) using lightweight cryptography (LWC) to protect devices. Created or design low-resource devices with a lightweight cryptographic technique should take into account important factors such as the battery life and the amount of data to be processed. This paper provides a new hardware designed for Loong lightweight cryptographic algorithm that takes into account the previously described constraints. The new hardware architecture for Loong algorithm with resource sharing to reduce system designed. The proposed approach is implemented using ISE Xilinx V14.7 using Virtex 4 field programmable gate array (FPGA) platform. The synthesis analysis for ISE showed the throughput of 851.264 Mbps with efficiency of 2.282 Mbps/slice, and a power consumption of 0.193 Watt. The implementation designed show the all-algorithms size consists of 373 slices, and the maximum possible operating frequency is 212.816 MHz. To the best of our knowledge, this is the first time that Loong algorithm has been implemented on FPGA using very high-speed integrated circuit hardware description language (VHDL).

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



## Corresponding Author:

Marwa Subhi Ibrahim

Department of Computer Engineering, College of Engineering, Diyala University

Baqubah, Diyala, Iraq

Email: marwasubhialawsi@outlook.com

## 1. INTRODUCTION

Computer networks play an important role in our daily lives. Used by various applications such as the world wide web (WWW), electronic messaging or the transfer of computer files, they allow us to acquire information as well as to communicate and exchange data permanently. It is now possible to connect any object of our daily life to a network, and we speak of Internet of things to designate all of these connected objects. The internet of things (IoT) has many application areas and thus offers immense potential for companies [1], industries and users. The lightweight cryptography algorithms used for develop many applications like electronic clinical record prototype that designed to work with low-performance devices. These electronic clinical record seek to secure the information without losing optimal performance and ensure low computational consumption [2].

The block cipher is one of important types of lightweight cryptography algorithm, such as RoadRunner [3], shadow [4], KLEIN [5], AES [6], GOST [7], LBlock [8], SFN [9], Midori [10], TWINE [11], and SPARX [12], which provide us with smaller block sizes than conventional lightweight cryptography (LWC), most key sizes ranging from 80 bits to 112-bit keys according to what was established in the National Institute Standards Technology (NIST), simpler rounds with an 8-bit S-box preference and programming simpler keys that generate sub-keys that increase of memory, latency, and power consumption [13]. Tools have

very limited resources, memory, power consumption, and processing speed capacities. Because of these limitations, traditional encryption cannot be used on devices with low storage space. As a direct result, the concept of "lightweight cryptography" was considered. As a result of the rapid development of new technologies gaining popularity, an entirely new form of encryption known as "lightweight" has been created. Due to the complexity of the computational operations required in traditional cryptography. The goal of lightweight cryptography is to reduce hardware-oriented and software-oriented implementation costs. Lightweight cryptography refers to an encryption technology designed for use in rapidly expanding applications that rely heavily on technology with limited resources [14].

In this paper, we analyze the security issues of connected objects, linked on the one hand to the large amount of data they handle, and on the other to the fact that they are often in a hostile environment and physically accessible. Then new hardware architecture implemented using field-programmable gate array (FPGA) platforms for Loong lightweight block cipher algorithms. The rest of the paper is organized as follows: section 2 we will explain the concept of lightweight block cipher algorithms, in section 3 we will review some of the LWC concepts, in section 4 we will present our model for LWC based on FPGA, and finally we will conclude our work in section 5. Recently many lightweight block cipher algorithms are implemented using FPGA board for IoT application. Many of lightweight block ciphers have been proposed e.g. PRINCE [15], LED [16], mCrypton [17], and PRESENT [18]. All of these ciphers are designed and aimed at specifically for extremely constrained environments such as radio frequency identification (RFID) tags and sensor networks. Abbas *et al.* [15] the authors design new FPGA IP-core which is to speed-up the performance of PRINCE. LED is a symmetric block cipher whose block size is 64 bits and its internal architecture is based on the substitution-permutation network (SPN). It is designed in two versions based on the key size; 64-bit key (LED-64) and 128-bit key (LED-128). Its number of rounds is based on the size of the encryption key; LED-64 has 32 rounds while LED-128 has 48 rounds [16]. The mCrypton algorithm is a 64-bit lightweight block cipher cryptographic algorithm. Substitution permutation (SP) structure is used in design of mCrypton algorithm architecture [17]. A set of existing optimized lightweight cryptographic architectures are discussed here. Singh *et al.* [8] for LBlock is a 64-bit block cipher with an 80-bit key and 32 rounds. Mhaouch *et al.* [18] for the present the cipher is based on a substitution-permutation network (SPN). Present supports 64-bit input data blocks and key sizes of 80 and 128 bits. In [19] LILLIPUT cipher transforms 64-bits of plaintext into 64-bits of cipher text with 80-bits of the key. Anusha and Shastrimath [20] introduced XTEA which includes 64-bit block size (Plain text) and 128-bit key size. Zeebaree [21] for DES, data are encrypted in 64-bit blocks using a 56-bit key. So that the comparison would be as precise as possible, they used the same security level, technology, and hardware/software implementation complexity factors (chip area, throughput, latency, and power consumption) for each of the block ciphers under consideration [22], [23].

## 2. METHOD

### 2.1. Loong algorithm

SPN-based Loong includes a 128-bit key block addition to the 64-bit key. The values of 16, 20, and 32 according to the round number (RN) system. The length of each of the three keys is what determines which of the three algorithms Loong-64, Loong-80, and Loong-128 is applied to the encryption process. Because Loong was the first algorithm to develop the round function technique, we are able to write "SubCells!" and "MixRows!" AddRoundKey. This symmetrical and lightweight block cipher has been given the name Loong. It gets its name from the fact that its round function uses two different SubCells algorithms. AddRoundKey, Sub-Cells, MixRows, and MixColumns are some of the sub-functions that are available to you when you use the round function [24]. A number of round features, including AddRoundKey, SubCells, MixRows, and MixColumns, are available in Figure 1.

It is common knowledge that the AES technique utilizes the SPN structure as its foundation. In contrast to the Feistel network structure, the SPN network structure is able to produce round functions despite having a greater degree of confusion and diffusion than the latter. In comparison to other forms of computer programming, SPN-based algorithms offer superior levels of both productivity and dependability. In contrast, the process of encrypting and decrypting data is approached in a different manner by algorithms that are based on SPN [25]. In order to solve this problem, we propose that the SPN adopt a new organizational structure. In this newly designed SPN architecture, the operations of encrypting information with a cipher and decrypting it are exactly the same, Thus the Loong structure is highly efficient and secure.

As a direct consequence of this, the SPN structure used by the Loong has been entirely rethought and revised. SubCells (SC), MixRows (MR), MixColumns (MC), and AddRoundKey (AR) are the four round transformations that make up Loong's round transformations (ARK) as show in Figure 2. To best characterize these constituents, the word "involutionary" is the one that works best [24]. The example that follows is an illustration of the round function used in Loong's encryption.

$$\left( \begin{array}{l} ENC_{RN}[RC^0, \dots, RC^{RN}] = ARK(RK, RC^0) \\ o(\bigcirc_{r=1}^{RN} SC \circ MR \circ MC \circ SC \circ ARK(RK, RC^{RN})) \end{array} \right) [24] \quad (1)$$

As a result, the encryption and decryption of Loong are identical. Decryption uses round constants in the opposite order as encryption. We are required to give evidence that the encryption and decryption technologies are equivalent [24].

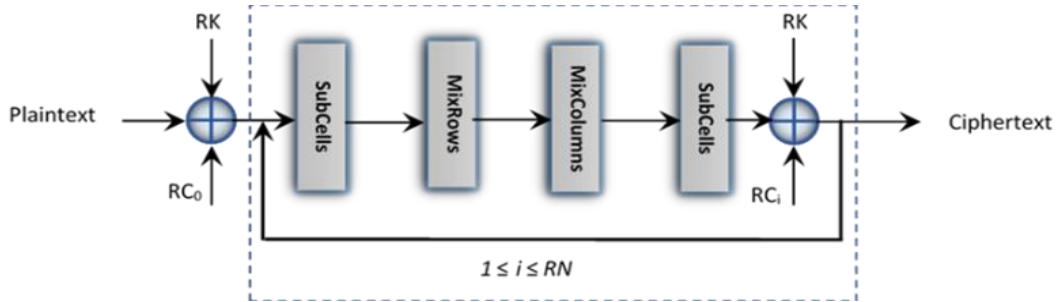


Figure 1. Process function of Loong algorithm [24]

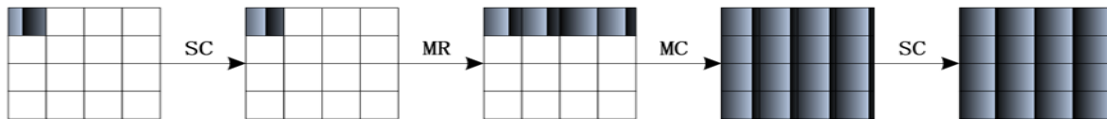


Figure 2. Diffusion effect in Loong [24]

### 2.1.1. Encryption process using Loong algorithm

SPN-based A 64-bit block in Loong is equivalent to a 64-bit round number, while an 80-bit key block is equivalent to a 64-bit round number, and a 128-bit key block is equivalent to a 128-bit round number (RN). The length of the three keys is used to determine which of the three Loong designations an algorithm is given: Loong-64, Loong-80, or Loong-128 [24]. The fundamental difference between Loong's encryption and decryption techniques is that the former uses round constants in the opposite sequence of the latter. This is the case while encrypting data. A number of round features, including AddRoundKey, SubCells, MixRows, and MixColumns, are available in Loong as shown in Figure 3. Provides an explanation of the intricate encryption process that Loong employed [24].

The method of enciphering data with the Loong cipher can also be referred to as  $ENC_{RN}$ . Plaintext is what  $ENC_{RN}$  takes in as its input, and the plaintext itself can be segmented into multiple 64-bit plaintext blocks in addition to a primary key if necessary. The encryption procedures for Loong-64, Loong-80, and Loong-128 are each represented by  $ENC_{16}$ ,  $ENC_{20}$ , and  $ENC_{32}$ , respectively [24].

$$ENC_{RN} : \begin{cases} \{0,1\}^{64} \times \{0,1\}^{K_{RN}} \rightarrow \{0,1\}^{64} \\ (plaintext, key) \rightarrow ciphertext \end{cases} [24] \quad (2)$$

In this particular instance, RN is equal to 16, 20, and 32, and the total value of K16, K20, and K32 is equal to 64. In Algorithm 1, the  $ENC_{RN}$  is illustrated by making use of a 64-bit Round Key (RK), which is a topic that is covered in key scheduling.

#### Algorithm 1. Loong routine

```

 $ENC_{RN}$ 
Input: Plaintext, RK, RC;
Output: Ciphertext;
1: state ← Plaintext;
2: AddRoundKey (state, RK, RC);
3: for i=1 to RN do
4: SubCells (state);
5: MixRows (state);
6: MixColumns (state);
7: SubCells (state);
8: AddRoundKey (state, RK, RC);
    
```

```

9: endfor
10: Ciphertext ← state;
11: Return Ciphertext;
    
```

**2.1.2. Decryption process**

This approach, which is the same process as the Loong cipher's inverse, is used to construct both the Loong cipher and its inverse. The process of encrypting and decrypting data follows the same pattern when it comes to the flow of the data. Long messages can be decrypted if the round constants are read backwards from the sequence in which they were written [24]. This method is known as "reverse reading." This Loong decryption is very quick and user-friendly as a direct result of this, thanks to the fact that it uses a direct consequence see Figure 4.

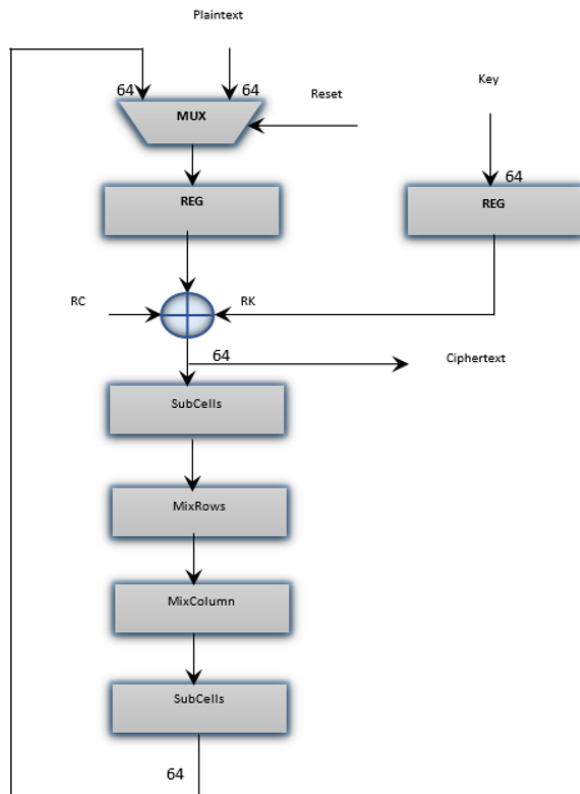


Figure 3. Encryption Loong algorithm

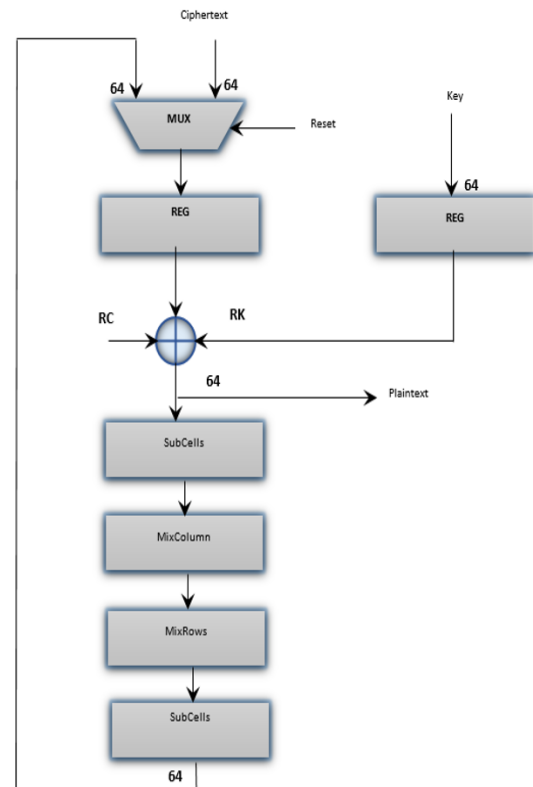


Figure 4. Decryption Loong algorithm

**2.2. FPGA implementation**

The field-programmable gate array, also known as an FPGA, is used to implement the lightweight block cipher encryption and hash function in hardware [25]. The hardware designed with different architectures. Also the architecture that is based on iterative looping has as its primary goal the reduction in the total number of hardware resources that are required for the design [26]. As a consequence of this, the design of loop unrolling no longer necessitates a number of round transformations equal to the algorithm's round count; rather, it only necessitates a single round transformation and the associated registers [27], [28]. This change was brought about as a result of the fact that loop unrolling no longer requires a number of round transformations equal to the algorithm's round count. Because of this, it is suitable for use in applications that are on a more limited scale [29]. The clock will be allowed to completely revolve around its axis once for each round of the competition. In order for this design to work as intended, the flow of operations needs to be controlled by a block of control logic as well [30], [31]. An FPGA is made up of a matrix of programmable logic units that may be reconfigured complex logic blocks (CLBs). The development of digital systems makes considerable use of FPGAs [18]. An FPGA is made up of a matrix of programmable logic units that may be reconfigured. Loop unrolling no longer requires a number of round transformations equal to the algorithm's round count. Because of this, it is suitable for use in applications that are on a more limited scale. The very

high-speed integrated circuit hardware description language (VHDL) language is used to implement the LWC Loong algorithm. Figure 5 shows the RTL top module for our proposal system. The proposal designed consist from four input ports and only one output port. The proposal designed base on FPGA Virtex 4 platforms.

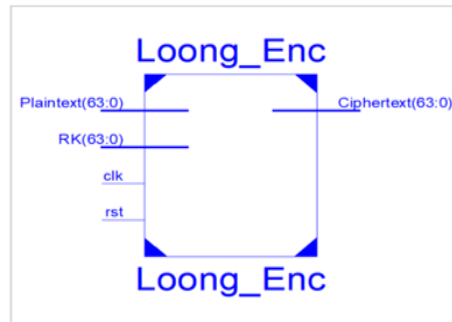


Figure 5. Top module of Loong RTL

### 3. THE LOONG HARDWARE COMPONENT

Loong is a lightweight block cipher algorithm that supports a block length of 64 bits with a key size of (64/80/128) bits. It consists of AddRoundKey, SubCells, MixRows, MixColumns, SubCells and AddRoundKey. The Loong algorithm decryption unit is about similar to the encryption design but the only variance between the encryption and the decryption is using round-constants in inverse order.

#### 3.1. Subcell

The hardware implementation of 64-bit S-Box is presented in Figure 6. The input/ouput of S-Box component is 64-bit contains sixteen subcell (Sbox) with 4-bit input/output. The D Flip Flop are used to implemented the Subcell to reduce the hardware footprint.

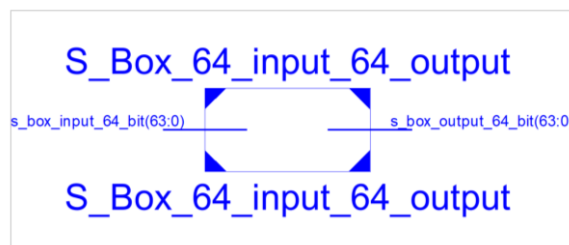


Figure 6. RTL of Subcell

#### 3.2. MixRo

The hardware implementation of 64-bit MixRow is presented in Figure 7. The encryption process is used sixteen Multiplexers. Each Multiplexer used 4-bit input and 1-bit output.

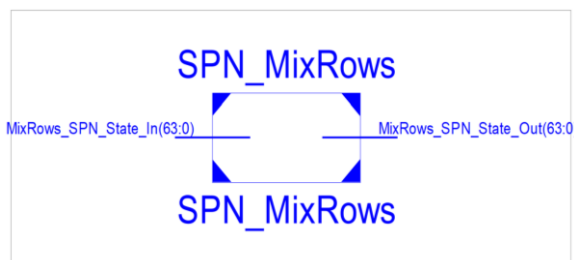


Figure 7. RTL of MixRow

### 3.3. MixColumn

Figure 8 show RTL of 64-bit MixColumn. The encryption process is used sixteen Multipliers. Each Multiplier is used 4-bit input and 1-bit output.

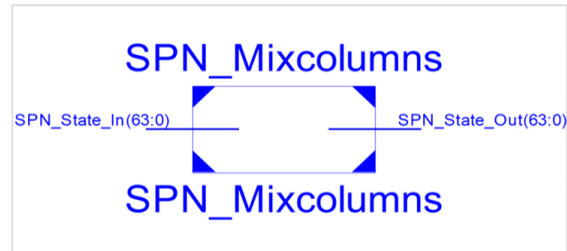


Figure 8. RTL of MixColumn

### 3.4. AddRoundkey

The last component show in the Figure 9 described the implementation of Add round key that used two time every round. The input/output is 64-bit, first time the plaintext XOR with round key. Second time with every round the output from Mix column component is XOR with round key (RK) and the round constants (RC).

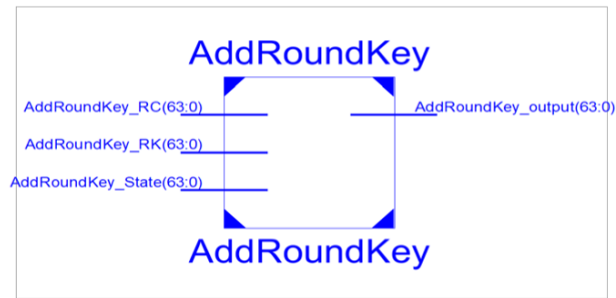


Figure 9. RTL of AddRoundKey

## 4. RESULTS AND DISCUSSION

The main target of this paper is implement small hardware design for Loong algorithm with low of latency. The amount of data that is transferred during permutation designed using wire only as well as row-to-column conversion. The new architecture designed and implemented using ISE, then ISim simulation program was used to execute the Loong algorithm with test vectors. The plaintext and key size is 64-bit. Figure 10 shows the outputs of the simulation that was run on the most current three system components that were constructed, as well as the results of the most recent data that was input into the design. A relatively low number of slices is required in order for the proposed architecture to function properly and successfully meet the goals of high frequency and high throughput. When working in shift mode, it is possible to reduce the total number of slices by making use of the lookup table (LUT) technique. The LUT is responsible for transferring data by shuffling the order of the input and output data places. The shift operation that makes use of LUTs can be carried out in a single cycle of the clock if necessary. As show in Figure 11 show the decryption process.

When utilizing this design, it is necessary to utilize a total of sixteen clock cycles in order to process the inputs and produce the cipher text. The results of running the simulation on the remaining three parts of the system that is being envisioned along with the last round of data input. It has been proved that the proposed pipeline architecture is effective even with a constrained number of slices when it comes to the execution of tasks that need high frequency and high throughput. During shift operations, the number of slices may be cut down to a more manageable level thanks to the LUT technique. A LUT will shift both the input data values and the output data values whenever it is given the instruction to perform a shift operation. It is possible for the shift operation that makes use of LUTs to be finished in a single cycle of the clock. Reducing the number of slices used in the creation of a design for RFID or IoT applications. Area is defined as the total number of

slices. The results of the design architecture performance are displayed in Table 1. These results have a high throughput with small area and small energy. In addition, the implementation for proposal design show throughput 851.264 Mbps, efficiency of 2.28 Mbps per slice, and total power consumption of 0.193 mW.

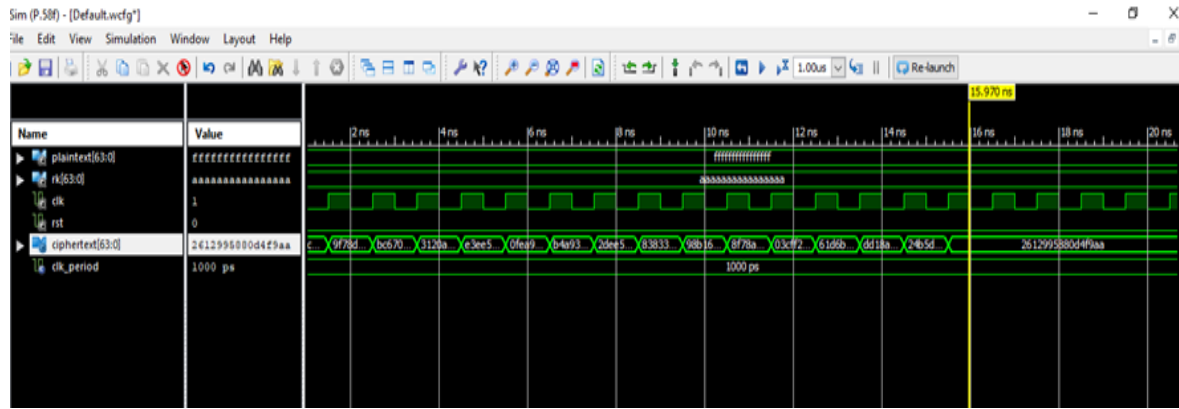


Figure 10. Simulation of Loong encryption

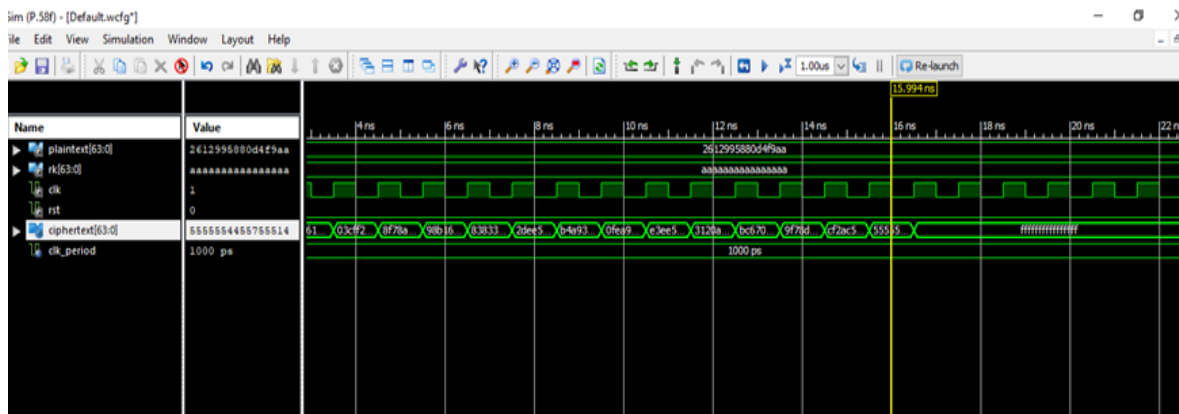


Figure 11. Simulation of Loong decryption

Table 1. Compares the encryption and decryption resources given by Loong to those provide

Algorithm	Block size	FPGA Device	Max. Freq. (MHz)	Throughput (Mbps)	Total Slices	Efficiency	Power (mWatt)
Proposed Loong	64	Virtex-4	212.816	851.264	373	2.282	0.193
LBLOCK [8]	64	Virtex-4	315.00	635.021	158	4.02	0.878
PRESENT [21]	64	Virtex-4	364.56	171.56	152	0.041	248.02
LILLIPUT [22]	64	Virtex-4	654.24	465.24	3313	-----	285.00
TEEA [23]	64	Artix-7	263.762	80.43	238	0.34	0.222

### 5. CONCLUSION

Efficient hardware architecture for the Loong lightweight encryption algorithm is designed and implemented in this paper. The area and power are optimized for our new architecture based on FPGAs. The utilization of a resource structure that is shared by using multiple component to process algorithms. All component is designed to execute through sixteen clock cycles. The results for implement Loong algorithm using Xilinx Virtex-4 FPGA show that number of slices is 373 with an operating frequency 212.816 MHz and a power consumption of 0.192 mWatt. In addition, a total throughput of 851.264 Mbps with a slice efficiency of 2.282 Mbps/slice. Finally the result of hardware proposal designed for LWC Loong algorithm shows that it is appropriate for mobile and small devices.

## REFERENCES




- [1] A. K. Sahu, S. Sharma, and D. Puthal, "Lightweight multi-party authentication and key agreement protocol in IoT-based E-healthcare service," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 17, no. 2s, pp. 1–20, 2021, doi: 10.1145/3398039.
- [2] A. Alamer, B. Soh, A. H. Alahmadi, and D. E. Brumbaugh, "Prototype device with lightweight protocol for secure RFID communication without reliable connectivity," *IEEE Access*, vol. 7, pp. 168337–168356, 2019, doi: 10.1109/ACCESS.2019.2954413.
- [3] P. Pachange and G. Bansod, "A fast and efficient datapath designs of lightweight cipher RoadRunneR on FPGA's for resource constrained environments," in *2019 6th International Conference on Internet of Things: Systems, Management and Security, IOTSMS 2019*, 2019, pp. 65–72. doi: 10.1109/IOTSMS48152.2019.8939241.
- [4] P. Prakasam, M. Madheswaran, K. P. Sujith, and M. S. Sayeed, "Low latency, area and optimal power hybrid lightweight cryptography authentication scheme for internet of things applications," *Wireless Personal Communications*, vol. 126, no. 1, pp. 351–365, 2022, doi: 10.1007/s11277-022-09748-1.
- [5] P. Singh, B. Acharya, and R. K. Chaurasiya, "High throughput architecture for KLEIN block cipher in FPGA," *2019 9th Annual Information Technology, Electromechanical Engineering and Microelectronics Conference (IEMECON)*, pp. 64–69, 2019, doi: 10.1109/IEMECONX.2019.8877021.
- [6] A. Kumar and S. Mozar, "Lecture Notes in Electrical Engineering," in *3rd International Conference on Communications and Cyber Physical Engineering, ICCCE 2020*, 2021, vol. 698, doi: 10.1007/978-981-15-7961-5.
- [7] A. Dmukh, D. Trifonov, and A. Chookhno, "Modification of the key schedule of the 2-GOST block cipher and its implementation on FPGA," *Journal of Computer Virology and Hacking Techniques volume*, vol. 18, no. 1, pp. 49–59, 2022, doi: 10.1007/s11416-021-00406-x.
- [8] P. Singh, B. Acharya, and R. K. Chaurasiya, "Low-area and high-speed hardware architectures of LBlock cipher for Internet of Things image encryption," *Journal of Electronic Imaging*, vol. 31, no. 03, p. 33012, 2022, doi: 10.1117/1.jei.31.3.033012.
- [9] L. Li, B. Liu, Y. Zhou, and Y. Zou, "SFN: A new lightweight block cipher," *Microprocessors and Microsystems*, vol. 60, pp. 138–150, 2018, doi: 10.1016/j.micpro.2018.04.009.
- [10] S. Banik *et al.*, "Midori: A block cipher for low energy," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2015, vol. 9453, pp. 411–436. doi: 10.1007/978-3-662-48800-3\_17.
- [11] T. Suzuki, K. Minematsu, S. Morioka, and E. Kobayashi, "A lightweight block cipher for multiple platforms," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2013, vol. 7707 LNCS, pp. 339–354. doi: 10.1007/978-3-642-35999-6\_22.
- [12] D. Dinu, L. Perrin, A. Udovenko, V. Velichkov, J. Großschädl, and A. Biryukov, "Design strategies for ARX with provable bounds: SPARX and LAX," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2016, vol. 10031 LNCS, pp. 484–513. doi: 10.1007/978-3-662-53887-6\_18.
- [13] P. Chodowicz and K. Gaj, "Very compact FPGA implementation of the AES algorithm," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2003, vol. 2779, pp. 319–333. doi: 10.1007/978-3-540-45238-6\_26.
- [14] B. J. Mohd, T. Hayajneh, and A. V. Vasilakos, "A survey on lightweight block ciphers for low-resource devices: comparative study and open issues," *Journal of Network and Computer Applications*, vol. 58, pp. 73–93, 2015, doi: 10.1016/j.jnca.2015.09.001.
- [15] Y. A. Abbas, R. Jidin, N. Jamil, M. R. Z'aba, and M. E. Rusli, "PRINCE IP-core on field programmable gate arrays (FPGA)," *Research Journal Of Applied Sciences, Engineering And Technology*, vol. 10, no. 8, pp. 914–922, 2015, doi: 10.19026/rjaset.10.2447.
- [16] M. Al-Shatari, F. A. Hussin, A. A. Aziz, G. Witjaksono, M. S. Rohmad, and X. T. Tran, "An efficient implementation of LED Block Cipher on FPGA," *2019 First International Conference of Intelligent Computing and Engineering (ICOICE)*, 2019, pp. 9–13, doi: 10.1109/ICOICE48418.2019.9035193.
- [17] Y. A. Abbas, A. S. Hameed, S. H. Alwan, and M. A. Fadel, "Efficient hardware implementation for lightweight mCrypton algorithm using FPGA," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 23, no. 3, pp. 1674–1680, 2021, doi: 10.11591/ijeecs.v23.i3.pp1674-1680.
- [18] A. Mhaouch, W. Elhamzi, and M. Atri, "lightweight hardware architectures for the Piccolo block cipher in FPGA," *22020 5th International Conference on Advanced Technologies for Signal and Image Processing (ATSIP)*, vol. 64, no. 9, pp. 2544–2555, 2020, doi: 10.1109/ATSIP49331.2020.9231586.
- [19] P. Singh, B. Acharya, and R. K. Chaurasiya, "Pipelined architectures of LILLIPUT block cipher for RFID logistic applications," in *Proceedings - 2019 International Conference on Computing, Communication, and Intelligent Systems, ICCIS 2019*, 2019, vol. 2019-Janua, pp. 452–457. doi: 10.1109/ICCIS48478.2019.8974530.
- [20] R. Anusha and V. V. D. Shastrimath, "LCBC-XTEA: high throughput lightweight cryptographic block cipher model for low-cost RFID systems," *Advances in Intelligent Systems and Computing*, 2019, vol. 986, pp. 185–196. doi: 10.1007/978-3-030-19813-8\_20.
- [21] S. R. M. Zeebaree, "DES encryption and decryption algorithm implementation based on FPGA," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 18, no. 2, pp. 774–781, 2020, doi: 10.11591/ijeecs.v18.i2.pp774-781.
- [22] D. J. Rani and S. E. Roslin, "Light weight cryptographic algorithms for medical internet of things (IoT) - A review," in *Proceedings of 2016 Online International Conference on Green Engineering and Technologies, IC-GET 2016*, 2017, pp. 1–6. doi: 10.1109/GET.2016.7916703.
- [23] A. A. Yazdeen, S. R. M. Zeebaree, M. M. Sadeeq, S. F. Kak, O. M. Ahmed, and R. R. Zebari, "FPGA Implementations for Data Encryption and Decryption via Concurrent and Parallel Computation: A Review," *Qubahan Academic Journal*, vol. 1, no. 2, pp. 8–16, 2021, doi: 10.48161/qaj.v1n2a38.
- [24] B. T. Liu, L. Li, R. X. Wu, M. M. Xie, and Q. P. Li, "Loong: a family of involutational lightweight block cipher based on spn structure," *IEEE Access*, vol. 7, pp. 136023–136035, 2019, doi: 10.1109/ACCESS.2019.2940330.
- [25] J. Daemen and V. Rijmen, *The Design of Rijndael*, vol. 2. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002. doi: 10.1007/978-3-662-60769-5.
- [26] P. Yalla and J. P. Kaps, "Lightweight cryptography for FPGAs," in *ReConFig'09 - 2009 International Conference on ReConfigurable Computing and FPGAs*, 2009, pp. 225–230. doi: 10.1109/ReConFig.2009.54.
- [27] A. Korobeynikov, "Effective implementation of 'Kuznyechik' block cipher on FPGA with OpenCL platform," in *Proceedings of the 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2019*, 2019, pp. 1683–1686. doi: 10.1109/ElConRus.2019.8656872.






- [28] Y. A. Abbas, R. Jidin, N. Jamil, and M. R. Zaba, "Reusable data-path architecture for encryption-then-authentication on FPGA," *International Review on Computers and Software (IRECOS)*, vol. 11, no. 1, pp. 56–63, 2016, doi: 10.15866/irecos.v11i1.8367.
- [29] M. Sbeiti, M. Silbermann, A. Poschmann, and C. Paar, "Design space exploration of present implementations for FPGAS," in *Proceedings - 2009 5th Southern Conference on Programmable Logic, SPL 2009*, 2009, pp. 141–145. doi: 10.1109/SPL.2009.4914893.
- [30] Y. N. Hatif, Y. A. Abbas, and M. H. Ali, "Lightweight ANU-II block cipher on field programmable gate array," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 3, pp. 2194–2205, Apr. 2022, doi: 10.11591/ijece.v12i3.pp2194-2205.
- [31] F. X. Standaert, G. Piret, G. Rouvroy, and J. J. Quisquater, "FPGA implementations of the ICEBERG block cipher," in *Integration, the VLSI Journal*, 2007, vol. 40, no. 1, pp. 20–27. doi: 10.1016/j.vlsi.2005.12.008.

## BIOGRAPHIES OF AUTHORS






**Marwa Subhi Ibrahim**    received the B.Sc. (From the first group in the undergraduate stage) degree in Computer Engineering from University of Diyala, Iraq, in 2007. She is a staff member in Diyala University, Iraq. She is currently a M.Sc. student in Al Iraqia University, College of Engineering, Iraq. His research interests are in computer engineering, web applications, lightweight cryptography, FPGA, artificial intelligence and image processing. She can be contacted at email: marwasubhialawsi@outlook.com.



**Yasir Amer Abbas**    was awarded the Bachelor of Science (First Class Hons.) Degree and Master of Science Degree in Computer Engineering from the University of Technology, Iraq, in the year 2000 and 2005, respectively. His Ph.D in Computer Engineering from the Universiti Tenaga Nasional, Malaysia at 2016. Currently he is a Assist. Prof. in the Computer Engineering Department, College of Engineering, University of Diyala, Iraq. His research interests are in the fields of computer engineering including, Computer Architectures, embedded systems hardware-software co-design and Lightweight cryptography. He is a member of the IEEE and the IEEE Computer Society since 2012. He can be contacted at email: dr.yasiral-zubaidi@uodiyala.edu.iq.



**Mudhafar Hussein Ali**    received his B.Sc. in electrical and electronics engineering and his M.Sc. in laser and optoelectronics engineering from AL Rasheed College of Engineering and Science, University of Technology, Iraq, in 1996 and 2004, respectively. His employment experience includes the Research and Development Center in Ministry of Science and Technology. His special fields of interest include fiber amplifiers, laser systems and applications. By 2004, he was a chief of engineers at the Ministry of Science and Technology/Renewable Energy Center. In 2015, he received his Ph.D in communications engineering from Universiti Tenaga Nasional. Since 2016, he has been a staff member in the Network Engineering Department, College of Engineering, Al Iraqia University, Iraq. He can be contacted at email: muthafarh@yahoo.com.