www.revistageintec.net
ISSN: 2237-0722
revista GEINTEC Gestão, Inovação e Tecnologias

Ultra-Lightweight Block Cipher in Medical Internet of Things for Secure Machine-to-Machine Communication Using FPGA

Mahendra Balkrishna Salunke[1]; Parikshit Narendra Mahalle[2]; Gitanjali Rahul Shinde[3]
[1]Research Scholar, Smt. Kashibai Navale College of Engineering, SPPU, Pune, India.
[1]msalunke@gmail.com
[2]Professor, Vishwakarma Institute of Information Technology, SPPU, Pune, India.
[3]Assistant Professor, Smt. Kashibai Navale College of Engineering, SPPU, Pune, India.

Abstract
With the swift growth of internet applications with the Internet of Things (IoT), medical sensors and online medical service has become mandatory part of every use case in the recent years. The health care system has become more connected with the increasing use of IoT devices, and these medical devices introduce vulnerabilities into health care organizations. Recently, there are significant cyber-threats against the medical IoT and some resisting elements of cryptosystem that cloud help to combat these threats. Hence, in medical IoT, security and privacy of patients are among the major areas of concern. However, such methods are very complex to implement in Field Programmable Gate Array (FPGA) platforms. This paper proposes an ultra-lightweight block ciphers (ULBC) for medical IoT applications. The first contribution of ULBC algorithm is to propose the chaotic Whale optimization (CWO) algorithm for key management, which improves the security and reduce hardware cost by reducing the number of iteration rounds. The second contribution is to introduce the flexible design of modified ULBC algorithm that provides an area, power and delay efficient design with attack free feature. The flexible design avoids the reconfigurable runtime, power; and it is surely different from existing block ciphers. Finally, the ULBC algorithm is synthesized in Xilinx tool with different FPGA families and the performance is compared with existing lightweight ciphers in terms of maximum clock frequency, power consumption and hardware utilization.

Key-words: Medical IoT, ULBC, FPGA, Block Ciphers, CWO.

1. Introduction

The services offered by wireless and smart communications have made the user's life easy and IoTs has become as an integral part their life. It is also helping medical domain to facilitate useful medical operations and tasks in the best possible way. For an example, medical tests done using smart

and tiny devices connected wirelessly gives faster results. Such kind of technology will definitely ensure the improvement in healthcare of users [1]. Though medical IoT is providing useful services, but these smart and tiny devices have few important weaknesses. Therefore, addressing the security issues in medical IoT and finding the mitigation solution to these issues are important. For encryption, the encoding technologies are useful [2].

Considering constrained devices, the integration of cryptographic algorithms and primitives are investigated in Lightweight Cryptography [3] - [5]. As per the National Institute of Standards Technology (NIST), lightweight cryptography is a subset of cryptography that has different objectives to cater smart applications built on less power consumption.

The outline of this paper contains different sections as mentioned below.

Section 2 presents the motivation to perform this research work. Section 3 discusses the state of the art technologies related to lightweight ciphers and the gap analysis. Section 4 presents proposed methodology along with its design in detail. In section 5, the detailed description of proposed ultra-lightweight block ciphers is discussed in detail. This section also gives the proper mathematical models of the proposed cipher scheme. The simulation results and performance analysis are presented in Section 6. Finally, the section 7 gives conclusions of this paper.

2. Motivation

Cloud based medical IoT is demanding and offered many services to hospitals and other stakeholders. However, there are many security attacks observed on medical IoT. These attacks help the unauthorized users to gain access to personal and medical information in a network. Hence security and privacy are at highest risks. The main objective of the proposed ultra-lightweight block ciphers FPGA design is to elucidate the security issues in the medical information over medical IoT network.

3. Related Works

Xuan et al. [6] have presented Eight Sighted Figure (ESF) as a lightweight cipher which match with the requirements of resource constraint execution environment like radio frequency identification (RFID), wireless sensor network (WSN), etc. For implementation and synthesis, VHDL and 0.18 µm CMOS technology is used in the design phase of ESF. It takes different gate equivalents

(GEs) based on KATAN and KTANTAN. To former design it takes 1054 GEs areas and 688 for later design of ESF.

Other research by At et al. [7] have given a detailed discussion on the cipher that includes ChaCha (as a stream cipher), Treefish (block cipher) and BLAKE and Skein (hash function) which uses mathematical operations. The implementation and synthesis is done on a target device called as Xilinx Virtex6 XC6VLX75T-2 and it takes 168 slices and maximum clock frequency is 304MHz.

Zhang et al. [8] have proposed "RECTANGLE" which is a lightweight block cipher that permits fast implementations and lightweight in nature using bit-slice methods. The implementation and synthesis of RECTANGLE design are done by implementing by VHDL and 0.13µm CMOS technology. To mention about GE area consumption, it takes 1054 GE 64-bit block length and 80-bit key size. On the other side, it takes 2063.5 GE areas for 128-bit key size keeping the same block length.

In the context of HIGHT and LED block ciphers, Subramanian et al. [9] have presented an approach based on signature and encoded operand re-computing methods. The implementation and synthesis is done on a target device called Xilinx Virtex7 7VX330tffg1157-3. It consumes 178 slices and 191 slices in LED and HIGHT design respectively. In the same environment, it takes 2.93mW 2.15mW power respectively.

Li et al. [10] have used integration Feistel network structure and SFN structure to design different encryption method. The implementation and synthesis of the proposed method, are performed on VHDL and UMC'S 0.13µm CMOS technology. It takes 1876.04 GEs with power consumption of 1.97 µW having 100 KHz clock frequency.

Another lightweight block cipher was proposed by Li et al. [11] called "QTL". This cipher supports both 64 and 128-bit size keys. The implementation and synthesis of QTL design are done on VHDL and SMIC 0.18µm CMOS technology, respectively. It takes 1025.52 GEs and 1206.52 GE area for QTL-64 and QTL-128 respectively.

Bansod et al. [12] have come up with a low power compact and ultra-lightweight block cipher called BORON. This solution works on 64-bit text and 138/80 bits of key length using a permutation and substitution based network. The implementation and synthesis of BORON are done on UMCL 0.18µm technology and takes 1939 GEs and 1626 GEs for 128-bit and 80-bit respectively.

Lara-Nino et al. [13] have proposed a hardware version of PRESENT. In a constrained environment, this solution overcomes the security issues by keeping lightweight cipher. The implementation and synthesis of PRESENT are done on Xilinx Virtex-5 and it consumes 375.66

MHz frequency, 201 and 265 slices of FFs and LUTs respectively. The power consumption of this solution is 245.78mW and 248.02mW for PRESENT-80 and PRESENT-128 respectively.

Chen et al. [14] have proposed Algebraic Fault Analysis (AFA) which is a bit-level of HIGHT. These faults are disconnected by a furtive Hardware Trojan (HT). The implementation and synthesis of this solution are done on Xilinx Virtex-5. It takes 245 slices FFs, 750 slice LUTs and 404 slice registers [15].

With the help of Simeck cipher, Bhoyar et al. [16] have proposed a lightweight block cipher. This solution is basically for IEEE 802.15.4 transceiver. Here, the input bits are processed in the parallel way and encryption takes place way before the process of modulation. Hence, this reduces the power required and work at a low frequency. For designing of this solution, it uses FPGA prototype. The power consumption is 100µW and 780µW.

Jarvinen et al. [17] have examined the conversions of weaker part of cryptography system into stronger part with the help of operations in the τ-adic domain. The implementation and synthesis of τ-adic design is done on VHDL and UMC 0.13µm CMOS technology, respectively. This solution consumes 827.75 GE area.

3.1. Gap Analysis

Considering the state of the art technologies, there is a huge difference in the implementations in the view hardware and software. A metric is one of the ways to identify the implementation parameters or properties to be considered during the phase of implementation [13] [14]. Table 1 shows the research gap analysis.

Table 1- Research Gap Analysis

References	Process	Key size (bits)	Area	Power	Maximum frequency
[6]	0.18µm	80	1054 GE	No	No
[7]	Virtex6	No	168 slices	No	304MHz
[8]	0.13µm	128	1054 GE	No	No
[9]	Virtex7	128	178 slices	2.93mW	No
[10]	0.13µm	128	1876.04 GE	1.97 µW	100KHz
[11]	0.18µm	128	1206.52 GE	No	No
[12]	0.18µm	128	1939 GE	No	No
[13]	Virtex5	128	153 Slices	245.78mW	375.66MHz
[14]	Virtex5	128	404 slices	No	No
[15]	0.18µm	64	2368 GE	No	No
[16]	0.13µm	64	174 slices	0.58mW	No
[17]	0.13µm	128	827.75 GE	No	No

4. Proposed Methodology and Design

4.1. Problem Methodology

Dalmasso et al. [18] have examined the importance and advantages of lightweight cryptography relative to hardware implementation using the classic algorithms. As the standard, AES, GIFT and PRESENT are optimized hardware versions along with some other methods. The security levels are compared (from low to high levels) with key length (80 and 128).

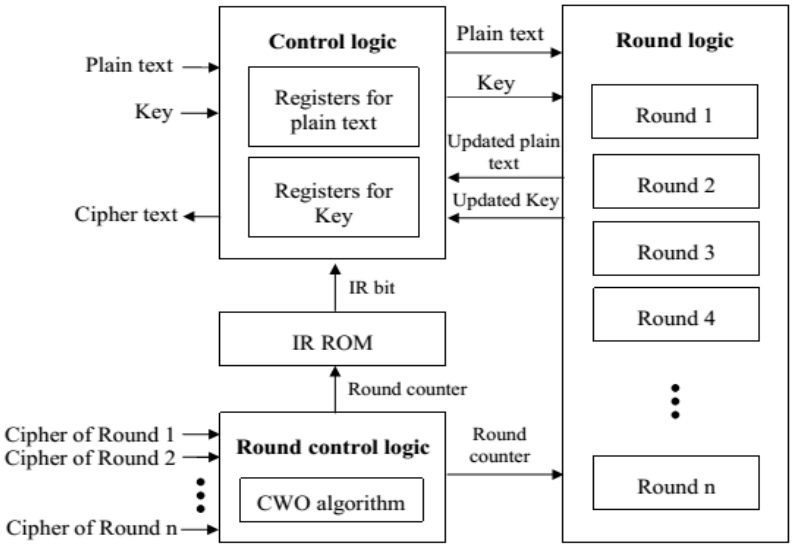
For the low resources, or constrained devices, it is important to use the block lightweight ciphers [18]. Hence, an ultra-lightweight block cipher (ULBC) is proposed for medical IoT applications. The proposed ULBC algorithm's contributions are highlighted as follows:

1. To improve the security, the key management in this ULBC algorithm uses Chaotic Whale Optimization (CWO);
2. The proposed algorithm is flexible in design for internal modules that gives area, power and delay without compromising on attacks. The objective of flexible design is to avoid the reconfiguration of internal block structures at runtime. This makes the solution unique from the existing block ciphers;
3. The proposed solution is an ultra-lightweight block cipher which was synthesized in Xilinx tool having FPGA families. At the end, the performance is compared with existing ciphers with the parameters like power consumption, maximum clock frequency, and hardware utilization;

4.2. System Model of Proposed Ultra-lightweight Block Cipher

An ultra-lightweight block ciphers (ULBC) is proposed here with the round optimization and flexible design constraints. Generally, the hardware architecture of ULBC comprises two blocks. First is control logic and second is round logic. The control logic handles registers and round controller process; and the round logic performs nonlinear functions of ULBC. The ULBC design utilizes CWO algorithm for the round logic controller. The system model of ULBC design is shown in Figure 1.

Figure 1- ULBC Design Model



In the rounds logic, CWO algorithm is being used along with the constraints like: number of rounds, cipher text and its hide and threshold rate, importantly, these constraints are captured during each round of round logic. The non-similarity between cipher text and plain text is defined by the hide rate. For the comparison purpose, the hide rate threshold is utilized and it is based on the history of cipher text of ULBC. The objective of CWO algorithm is to compute high hide rate cipher text within limited round logics. Another problem in existing ciphers is reconfigurable design, which reduced by the flexible control logic with their flexible memory devices.

5. FPGA Design of Ultra-lightweight Block Cipher

This section gives an elaboration on the basic operations performed in both the ULBC design. Then, the detailed working function of the CWO algorithm with round logic reduction on basic ciphers is mentioned as follows.

5.1. Basics of ULBC Ciphers

Mostly, ULBC ciphers [18] comprises 254 rounds and functions 80-bit key size and works for blocks having different size in bits like 32, 48 and 64. The initial step of this algorithm is loading and integration of two registers R1 and R2 having variable length with the plaintext. This is accompanied by a key of size 80-bit. The reason to keep the variable length of registers R1 and R2 is that they the

Received: 09.05.2021 – Accepted: 30.05.2021

values are different from all the block size. In each round, these nonlinear functions (A1 and A2) are calculated which used the register values. The formula for A1 and A2 is as below:

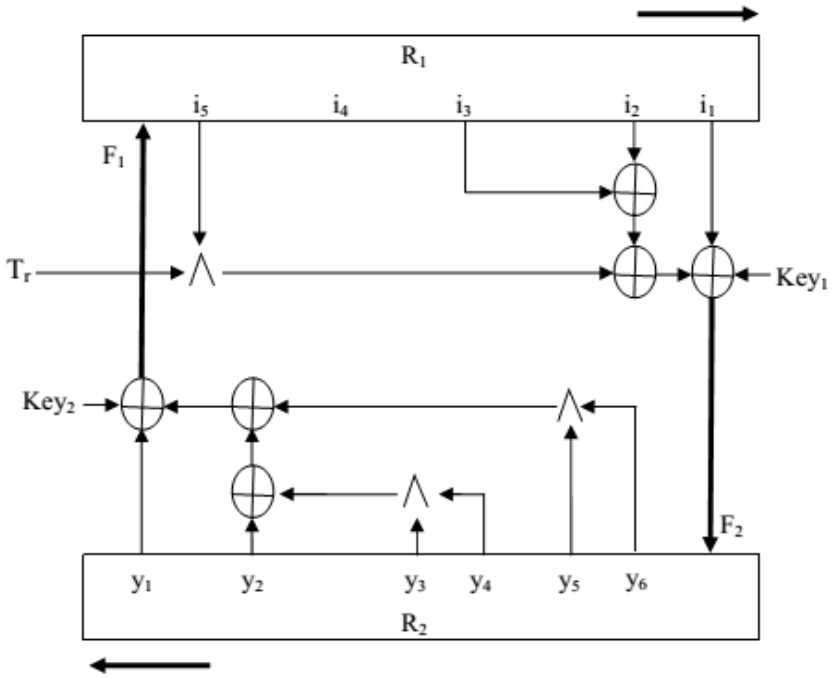
$$A_1 = A_1[i_1] \oplus A_1[i_2] \oplus (A_1[i_3] \wedge A_1[i_4]) \oplus (A_1[i_5] \wedge IA) \oplus key_1 \quad (1)$$

$$A_2 = A_2[j_1] \oplus A_2[j_2] \oplus (A_2[j_3] \wedge A_2[j_4]) \oplus (A_2[j_5] \wedge A_2[j_6]) \oplus key_2 \quad (2)$$

Here, IR stands for irregular update rule which is pre-computed and most significant bit is Linear Feedback Shift Register's (LFSR). The important elements i and j are the size of registers which is variable for all block sizes [18]. Two sub-key bits are Key1 and Key2 represented as $key_1 = key_{2x}$ and $key_2 = key_{2x+1}$ for ith iteration. . Using 80-bit key, the yth bit, is generated as:

$$Key = \begin{cases} key_x; & for\ x = 0,1,2,\ldots 79 \\ key_y; & y = key_{y-80} \oplus key_{y-61} \oplus key_{y-50} \oplus key_{y-13} \end{cases} \quad (3)$$

Figure 2- Round logic module of KATAN/KTANTAN *Ciphers*



The F1 and F2 functions in ULBC ciphers are applied for 1 time, 2 times and 3 times for ULBC bits as 32-bit, 48-bit and 64-bit respectively. The ULBC algorithm is same except the process of key scheduling since the key is not changed and only to select sub key bits in the most flexible way. The five words each key is $G_4 \| G_3 \| G_2 \| G_1 \| G_0$ having 16 bits size. Following is the formula used to calculate sub key bits:

$$key_1 = \overline{\mathrm{JK}_3} \wedge \overline{\mathrm{JK}_2} \wedge mux_{16\times1}\left(w_0, \mathrm{JK}_7\mathrm{JK}_6\mathrm{JK}_5\mathrm{JK}_4\right) \oplus \left(\mathrm{JK}_3 \vee \mathrm{JK}_2\right) \wedge mux_{4\times1}\left(key_1, \mathrm{JK}_1\mathrm{JK}_0\right) \quad (4)$$

$$key_2 = \overline{\mathrm{JK}_3} \wedge \mathrm{JK}_2 \wedge mux_{16\times1}\left(w_4, \mathrm{JK}_7\mathrm{JK}_6\mathrm{JK}_5\right) \oplus \left(\mathrm{JK}_3 \vee \overline{\mathrm{JK}_2}\right) \wedge mux_{4\times1}\left(key_2, \overline{\mathrm{JK}_1\mathrm{JK}_0}\right) \quad (5)$$

Figure 2 represents the round logic, functional model and the above formulas are used in the same model. In this proposed ULBC cipher, same round logic with controller is used in an external way along with the flexible register for reconfigurable evasion.

5.2. Key Management System Using CWO Algorithm

The heuristic CWO algorithm is based on population and has an objective to optimize global multi-model functions. To share the information and its exchange among solutions, it uses the mutation operator. The evolutionary functions and parameters like subtraction, addition, comparison and their performance are better than other algorithms. The minimum function to reduce the problem without losing its generality is presented as:

$$\text{minimize} f(x) = f(x_1, x_2, \ldots, x_i) \quad (6)$$

Where i is D dimensional vector and f is a true point of confinement of certifiable respected clashes.

$$x_{i,j} = x_{i,low} + rand(0,1) \cdot \left(x_{i,high} - x_{i,low}\right) \qquad i = 1,2,\ldots\ldots D;\ j = 1,\ 2,\ldots\ldots N_p \quad (7)$$

CWO first changes the best plan vector (target vector), from the present masses by including the scaled differentiation of two vectors from the present people with the crack vector. The selection of records is done considering they are not same and have no relation to atom documents. The change scale factor F is a positive certified number, regularly shy of what one. The technique of monstrosity vector age is represented by condition 2 and depicted in Figure 1.

$$MV_i = x_{best} + F \cdot \left(x_{i,r_1} - x_{i,r_2}\right)\ r_1, r_2 \in \{1,2,\ldots N_p\} \quad (8)$$

In order to increase the diversity of the parameter vector, the crossover operation is realistic to the original individuals and to the mutant vector MV_i and $x_{i,j}$. The resultant trial vector $TV_{i,j}$ is computed as follows:

$$TV_{i,j} = \begin{cases} MV_{i,j} & \text{if rand}(0,1) \le \text{CR} \\ x_{i,j} & \text{Otherwise} \end{cases} \quad (9)$$

CR (crossover parameter) is responsible to handle the fractions of parameters that helping the mutant vector to get a final trial vector. Further, the characteristics of the mutant vector parameter are

inherited by the trial vector as per the random selection of the index. Based on the location approximation scheme and the NNI (nearest-neighbor-interpolation) the fitness computation process is modified.

Algorithm 1 - Chaotic Whale Optimization (CWO) Algorithm

Algorithm 1: chaotic whale optimization (CWO) algorithm

Start

Round=0

1: **Create a random initial population**

for i =1 to D do

for j =1 to NP do

$x_{i,j}^{0} = x_{i}^{min} + rand_{i}[0,1] \cdot \left(x_{i}^{max} - x_{i}^{min}\right)$

end for

end for

Compute fitness function for each individual of

2: **population**

for j =1 to NP do

$f\left(x_{j}^{0}\right)$

end for

generate initial trial vectors

for round=1 to max. round do

for j=1 to NP do

Select randomly $r_1, r_2, r_3 \in [1, NP],\ r_1 \neq r_2 \neq r_3 \neq i$

Received: 09.05.2021 – Accepted: 30.05.2021

3. Perform crossover and mutation

for i=1 to D do

if (rand [0, 1] <CR) then

$$MV_{i,j}^{t} = x_{i,r_1}^{t} + F \cdot \left(x_{i,r_2}^{t} - x_{i,r_3}^{t}\right)$$

else

$$MV_{i,j}^{t} = x_{i,j}^{0}$$

end if

end for

end for

Selection process

4. If $\left(f\left(MV^{t}\right) \leq f\left(x_j^{0}\right)\right)$ **then**

$$x_j^{t} = MV_{i,j}^{t}$$

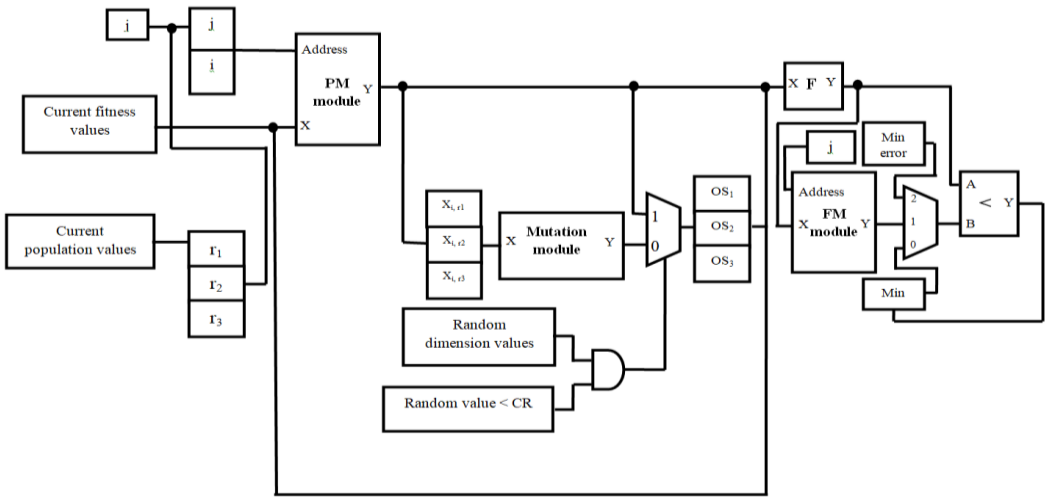
end if

end for

end for

The contraption utilization of the CWO game plan contains the sub-modules, for instance, (1) to store individuals "Primary Memory Module" (PM) (2) to store, fitness function values "Fitness Memory Module" (FM) (3) "Mutation and Crossover Module" (4) "Fitness Function Module" and (5) "Control Module". The entire scale arrangement of CWO is represented in Figure 3.

Figure 3- The entire scale hardware arrangement in the proposed CWO algorithm



Received: 09.05.2021 – Accepted: 30.05.2021

Each sub-module of the proposed CWO algorithm is listed and discussed as below:

(1) Module 1: Primary Memory

(2) Module 2: Fitness Memory

(3) Module 3: Mutation and Crossover

(4) Module 4: Fitness Function

(5) Module 5: Control

5.2.1. Module 1: Primary Memory (PM)

This module is accountable to store the population and uses a memory circuit. The size of population size defined the memory size and it is represented as:

$$PM = NP \times D \text{ words} \tag{10}$$

Also, the memory size is calculated as follows if 64 bits (8 bytes) are used to define each word,

$$PM = NP \times D \times 8 \text{ bytes} \tag{11}$$

5.2.2. Module 2: Fitness Memory (FM)

This module is responsible to calculate size, which is similar to PM but it stores only value for the indivisible. The formula for FM is represented as:

$$FM = NP \text{ words} \tag{12}$$

Also, the memory size (FM) is calculated as follows if 64 bits (8 bytes) are used to define each word,

$$FM = NP \times 8 \text{ bytes} \tag{13}$$

5.2.3. Module 3: Mutation and Crossover

The mutation and crossover modules are mathematically represented by equations 14 and 15. However, equation 16 represents the floating point values and operations that used to decide mutation module.

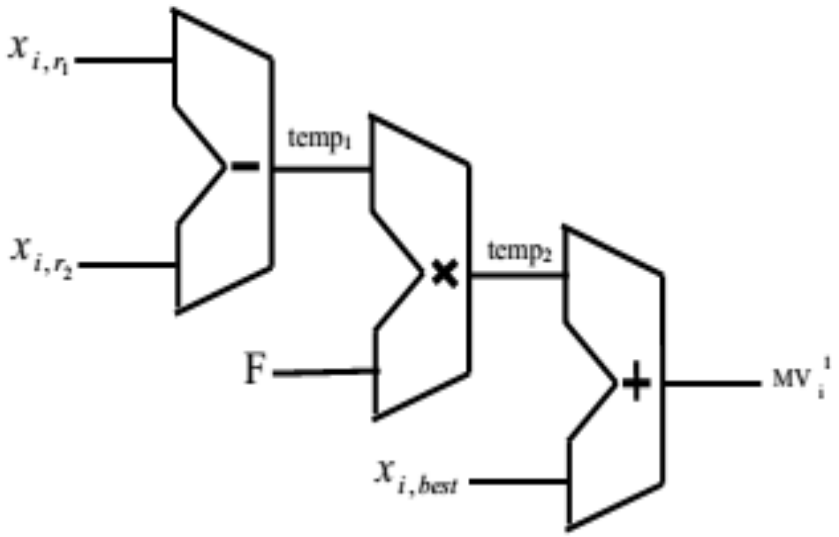
$$temp_1 = x^0_{i,r_1} - x^0_{i,r_2} \tag{14}$$

$$temp_2 = F \times temp_1 \tag{15}$$

Received: 09.05.2021 – Accepted: 30.05.2021

$$MV_i^1 = x_{i,best}^0 + temp_2 \quad (16)$$

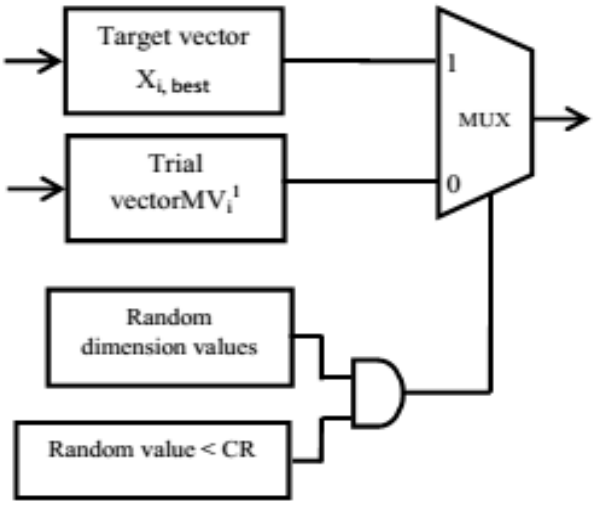
Figure 4- Module 3: Mutation



These sequences of operations are implemented using floating point functions like subtraction, multiplication and addition. As shown in the Figure 4, complete module can be implemented. For the subsequent rounds, the mutant trial vector is generated from this module.

Once the mutation is done, then the next step is crossover. Here, for all dimensions, the random numbers are generated. It checks the condition and will go to next multiplexer block if the condition is true. The decision of multiplexer to go forward or backward is completely depends on the CR value. Module 3 crossover is depicted in Figure 5.

Figure 5- Module 3: Crossover



Received: 09.05.2021 – Accepted: 30.05.2021

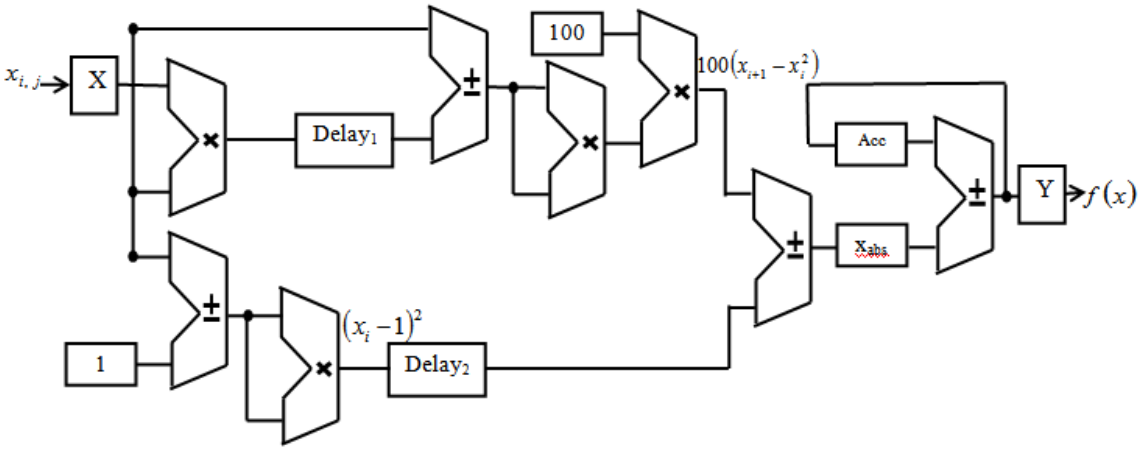
5.2.4. Module 4: Fitness Function

The application dependent module is Fitness computation. Hence, this gets changed if the application also gets changed. To compute fitness, it uses six mathematical formulas or functions and is represented as:

$$f(x) = \sum_{i=1}^{D} \left| 100\left(x_{i+1} - x_i^2\right) + \left(x_i - 1\right)^2 \right| \qquad (17)$$

The blocks of the fitness function module based on Rosenbrock's function are shown in Figure 6.

Figure 6 - Blocks of Fitness Function Module based on Rosenbrock's Function



5.2.5. Module 5: Control

This module is accountable to decide read and write operation on registers. This module controls the operation using control inputs of this module and selects the desired element of the desired input. Control unit this module manages control signals to perform the algorithm correctly.

6. Results and Discussion

Considering the throughput, it is vital to examine different lightweight cryptography algorithms at a given throughput and selected protocol. Firstly, the proposed ULBC algorithm's design implementation will be reviewed. In this paper, the proposed algorithm is better than the existing ciphers. The proposed algorithm is implemented on Xilinx Kintex FPGA and the relative performance of the proposed algorithm and existing ciphers are compared using parameters like area

consumption, power consumption, and throughput. In the Xilinx, the XST tools are used to synthesize the designs of the proposed algorithms and maps it into the target device. The designed architecture process and its verification are done using ISIM simulator. The experiments have been executed on a computer having a configuration like Windows 10 OS, 8GB RAM and Core i5 Intel processor. The throughput and area are impacted depending on the operating frequency and the FPGA technology. The selected nominal frequency is 100 MHz for the target platform which has given fair results. Therefore, the area is investigated using the slice and throughput (T) is computed as below:

$$T = \frac{(F * D_s)}{C} \tag{18}$$

The energy-per-bit is calculated as follows,

$$E = \frac{C * P}{F * D_s} \tag{19}$$

Table 1 depicts the comparison of performance between the proposed ULBC algorithm and different devices. It clearly shows that the performance metrics of proposed multi-favor NoC router with Kintex7 FPGA device consumes lower device utilization (40 slice registers, 100 flip-flops, and 72 slice LUTs) as compared to other implementations of the devices. The maximum frequency attained is 702.5 MHz in the Kintex 7 FPGA family. Also, the energy attained is 18 pJ/bit at the Kintex7 FPGA family as compared to other FPGA families.

Table 2- Performance Comparison of proposed ULBC Algorithm

Performance metrics	FPGA devices		
	Kintex7	Virtex6	Virtex7
Number of Slice Registers	40	52	49
Number of Flip-Flops	100	114	102
Number of slice LUTs	72	103	89
Maximum Frequency (MHZ)	702.5	687	698
Energy (pJ/bit)	18.09	20.9	19.4

6.1. Performance Comparisons

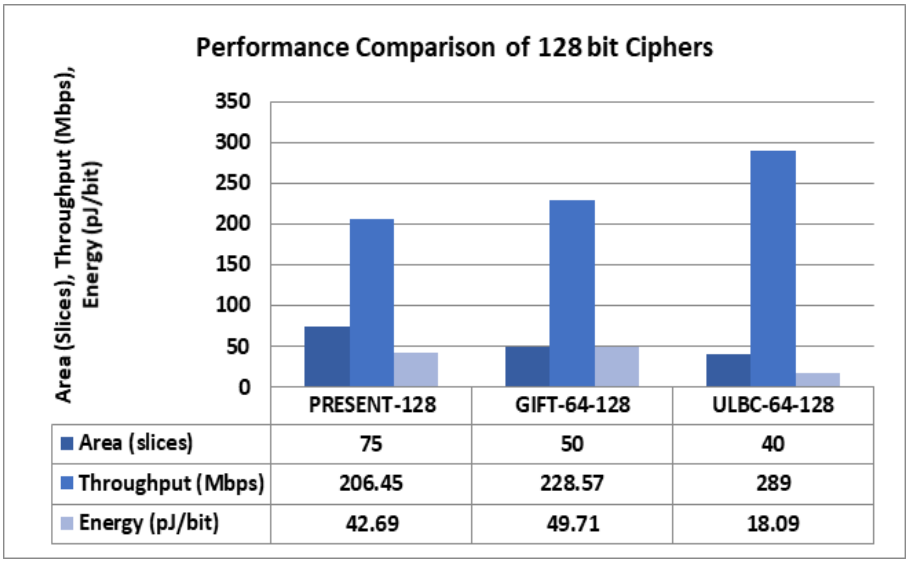
For comparing the performance of the proposed ULBC algorithm, the current block ciphers like PRESENT and GIFT are selected. Table 2 gives complete details on the comparison of the proposed algorithm and its existing ciphers on the parameters like throughput and area. The result shows that the throughput and the area of the proposed algorithm are effective as compared with existing ciphers. The histogram of the proposed algorithm and the existing ciphers are mentioned in

Figure 7. Kintext 7 device is used to implement the proposed algorithm and it clearly shows the less slices register consumption (40), low energy (18.09 pJ/bit) and high throughput (289 Mbps). The proposed algorithm's throughput is 32% higher than existing ciphers and there is an 18% reduction in the energy compared with existing ciphers.

Table 3 - Performance Comparison of Proposed and Existing Ciphers

Cipher	**Performance metrics**		
	Area (slices)	Throughput (Mbps)	Energy (pJ/bit)
PRESENT-128	75	206.45	42.69
GIFT-64-128	50	228.57	49.71
ULBC-64-128	40	289	18.09

Figure 7- Performance *Comparison* of *Block Ciphers*



7. Conclusion & Future Outlook

In this paper, the proposed algorithm is ultra-lightweight block ciphers (ULBC) for medical IoT applications. To enhance the security concerns and reduce hardware cost, the proposed algorithm uses the Chaotic Whale Optimization (CWO) key management having a minimum number of rounds. The proposed algorithm is flexible in design and attack free that provides low power, low area and low delay. The advantage of the proposed algorithm is that it avoids reconfiguration at runtime and hence is different from the existing ciphers. The paper shows the performance comparison with existing ciphers using Xilinx tool for Comparison the parameters are throughput, area, and energy consumption. The result shows that the proposed algorithm ULBC is efficient and lightweight.

References

Rachedi, Abderrezak et al; "IEEE Access Special Section Editorial: The Plethora of Research in Internet of Things (IoT)", *IEEE Access,* vol. 4, pp. 9575-9579, 2016.

Zhao, Shuai; Yu, Le; Cheng, Bo; "An Event-Driven Service Provisioning Mechanism for IoT (Internet of Things) System Interaction", *IEEE Access,* vol. 4, pp. 5038-5051, 2016.

Maimut, Diana; Ouafi, Khaled; "Lightweight Cryptography for RFID Tags", *IEEE Security & Privacy Magazine,* vol. 10, no. 2, pp. 76-79, 2012.

Eisenbarth, Thomas et al; "A Survey of Lightweight-Cryptography Implementations", *IEEE Design & Test of Computers,* vol. 24, no. 6, pp. 522-533, 2007.

Tan, Chiu et al; "IBE-Lite: A Lightweight Identity-Based Cryptography for Body Sensor Networks", *IEEE Transactions on Information Technology in Biomedicine,* vol. 13, no. 6, pp. 926-932, 2009.

LIU, Xuan et al; "Eight-sided fortress: a lightweight block cipher", *The Journal of China Universities of Posts and Telecommunications,* vol. 21, no. 1, pp. 104-128, 2014.

At, Nuray et al; "Compact Hardware Implementations of ChaCha, BLAKE, Threefish, and Skein on FPGA", *IEEE Transactions on Circuits and Systems I: Regular Papers,* vol. 61, no. 2, pp. 485-498, 2014.

Zhang, Wentao et al; "RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms", *Science China Information Sciences,* vol. 58, no. 12, pp. 1-15, 2015.

Subramanian, Srivatsan et al; "Reliable Hardware Architectures for Cryptographic Block Ciphers LED and HIGHT", *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,* vol. 36, no. 10, pp. 1750-1758, 2017.

Li, Lang et al; "SFN: A new lightweight block cipher", *Microprocessors and Microsystems,* vol. 60, pp. 138-150, 2018.

Li, Lang; Liu, Botao; Wang, Hui; "QTL: A new ultra-lightweight block cipher", *Microprocessors and Microsystems,* vol. 45, pp. 45-55, 2016.

Bansod, Gaurav; Pisharoty, Narayan; Patil, Abhijit; "BORON: an ultra-lightweight and low power encryption design for pervasive computing", *Frontiers of Information Technology & Electronic Engineering,* vol. 18, no. 3, pp. 317-331, 2017.

Lara-Nino, Carlos; Diaz-Perez, Arturo; Morales-Sandoval, Miguel; "Lightweight Hardware Architectures for the Present Cipher in FPGA", *IEEE Transactions on Circuits and Systems I: Regular Papers,* 64(9), 2544-2555, 2017.

Chen, Hao et al; "Stealthy Hardware Trojan Based Algebraic Fault Analysis of HIGHT Block Cipher", *Security and Communication Networks,* 2017, 1-15, 2017.

Thorat, C.G.; Inamdar, V.S.; "Implementation of New Hybrid Lightweight Block Cipher", *Applied Computing and Informatics,* 2018.

Bhoyar, Prachin; Dhok, Sanjay; Deshmukh, Raghavendra; "Hardware implementation of secure and lightweight Simeck32/64 cipher for IEEE 802.15.4 transceiver", *AEU - International Journal of Electronics and Communications,* vol. 90, pp. 147-154, 2018.

Järvinen, Kimmo; Roy, Sujoy; Verbauwhede, Ingrid; "Arithmetic of τ-adic expansions for lightweight Koblitz curve cryptography", *Journal of Cryptographic Engineering,* 2018.

Dalmasso, Loic et al; "Evaluation of SPN-Based Lightweight Crypto-Ciphers," in *IEEE Access, 7,* 10559-10567, 2019.