ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 1, Issue 3, July 2016

Design of L Block Lightweight Block Cipher IP Core

[1]Aljazeera.K.R, [2] Nandakumar.R, [3] Ershad.S.B
[1] Student, M.Tech VLSI Design, Nehru College of Engineering & Research Centre, Thrissur,
[2] Scientist/Engineer, NIELIT, [3] Associate Professor, Nehru College of Engineering & Research Centre, Thrissur

***Abstract*: Existing cryptographic algorithms were designed to meet the needs of the desktop computing era and thus require significant resources to implement. Now a day's most of the devices available in the market are resource constrained. Here lightweight cryptography plays a pivotal role. It lends itself to implementation as a block cipher providing a scalable, pipelined architecture. Most importantly, lightweight block ciphers can be implemented with low latency making them ideal for applications in which deterministic performance is required. In this project a detailed study of L Block block cipher is done which is a lightweight cipher in both hardware and 8-bit platforms and an IP core is developed after its implementation. The block size of L Block is 64-bit and the key size is 80-bit and it can achieve competitive hardware and software performances when compared with other known lightweight block ciphers. . L Block cipher is implemented on Xilinx Spartan-6 FPGA (XC6LX16-CS324) and its performance metrics were obtained. It can serve as a benchmark for the hardware design engineers to model devices that utilizes lightweight characteristics.**

Index Terms—Lightweight cryptography, L Block block cipher, Performance metrics, Xilinx

I. INTRODUCTION

The internet, comprised of millions of interconnected computers, allows instantaneous communication and transfer of information, around the world. The perpetual increase of information transmitted electronically has led to an increased reliance on cryptography. Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of adversaries. Cryptography is very important to the continued growth of the internet and electronic commerce. On a new computing environment called "IOT-Internet of Things" or "Smart Objects" networks, a lot of resource constrained devices are connected to the internet. The security of constrained end nodes in such devices is important. It is not easy to implement sufficient cryptographic functions on constrained devices due to limitations of their resources.

Lightweight Cryptography is a cryptographic algorithm or protocol tailored for implementation in constrained environments like RFID tags, sensors, contactless smart cards, health care devices and so on. Lightweight properties described based on target platforms. The main two reasons behind the use of LWC is the efficiency of end to end communication and applicability to lower resource devices. Ciphers targeted for low resource devices are lightweight ciphers. Lightweight block ciphers are practical to use now and has small block size (32, 48, and 64). The key size is also smaller. It simplifies key schedule and performs elementary operations with larger number of rounds. It optimize resource utilization with minimum power and energy consumption, meeting security challenges. In this paper the design and characterization of L Block block cipher is carried out aiming at constrained devices. more than 25% have been reported. This performance deterioration must be taken into account when sizing the array for a multi-year project.

II. L BLOCK BLOCK CIPHER ALGORITHM

L Block (LuBan lock) is a lightweight block cipher proposed by Wenling Wu and Lei Zhang. It ciphers blocks of size 64 bits under keys of size 80 bits using 32 rounds of modified Fiestel network [1]. In the ciphers that uses fiestel structure the block to be encrypted is split into two equal-sized halves. Round function is applied to one half using a subkey and the output is xored with other half. The two halves are then swapped to get the final ciphertext. The specification of L Block consists of three parts, encryption, decryption and key scheduling.

A. Encryption Algorithm

To encrypt the given plaintext using L Block block cipher, the 64-bit plaintext M is divided into two separate sequences of equal length; X1 is the left 32-bit half and X0 is the right 32-bit half. This is denoted as:

M (64-bit) = X1 (32-bit) || X0 (32-bit)

And then the data processing procedure can be expressed as follows

1. For i = 2,3,………33,do

Xi= F (Xi-1, Ki-1) ⊕ (Xi-2<<< 8) (1)

2. Output C = X32 || X33 as the 64-bit cipher text

The encryption procedure for L Block cipher is shown below in figure1.

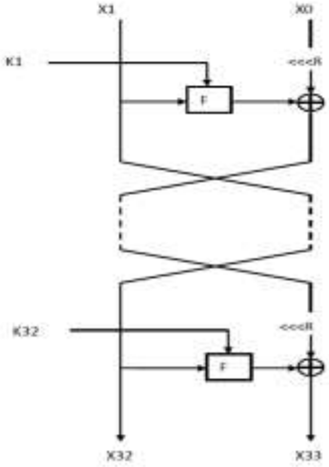


Fig 1: Encryption procedure of L Block

The encryption procedure involves round function, shifting and xor-ing operations. The components used in each round are: Round function-F: The round function F is constructed from two other functions, Confusion function S and Diffusion function P. It is defined as

U = F(X, Ki) = P (S (X⊕ Ki)) (2)

Where U is the output of round function F and Ki denotes the sub key of each round.

Confusion function-S

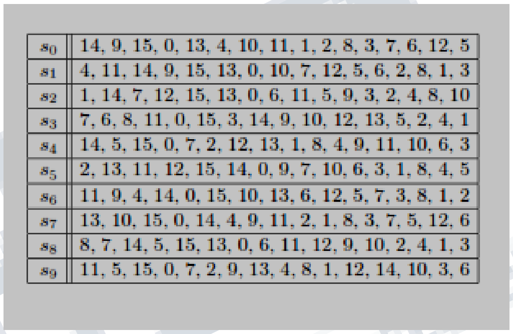
The non-linear layer of the Round Function, F that consists of eight 4 X 4 S-boxes namely s0, s1, s2, s3, s4, s5, s6, s7. The confusion function S defined as

Y=Y7 || Y6 ||Y5 || Y4 || Y3 || Y2 || Y1 || Y0 → Z (3)
Where Y is the input to s box and Z is the output. The output of the s box is defined as Z and it is found as

Z7= s7 (Y7), Z6= s6 (Y6), Z5= s5 Y5), Z4= s4 (Y4),
Z3= s3 (Y3), Z2= s2 (Y2), Z1= s1 (Y1), Z0=s0 (Y0). (4)
Z = Z7 || Z6 || Z5 || Z4 || Z3|| Z2 || Z1 || Z0.

The contents in s box is given below in table I

Table I: Contents of S-boxes used in L Block



s_0	14, 9, 15, 0, 13, 4, 10, 11, 1, 2, 8, 3, 7, 6, 12, 5
s_1	4, 11, 14, 9, 15, 13, 0, 10, 7, 12, 5, 6, 2, 8, 1, 3
s_2	1, 14, 7, 12, 15, 13, 0, 6, 11, 5, 9, 3, 2, 4, 8, 10
s_3	7, 6, 8, 11, 0, 15, 3, 14, 9, 10, 12, 13, 5, 2, 4, 1
s_4	14, 5, 15, 0, 7, 2, 12, 13, 1, 8, 4, 9, 11, 10, 6, 3
s_5	2, 13, 11, 12, 15, 14, 0, 9, 7, 10, 6, 3, 1, 8, 4, 5
s_6	11, 9, 4, 14, 0, 15, 10, 13, 6, 12, 5, 7, 3, 8, 1, 2
s_7	13, 10, 15, 0, 14, 4, 9, 11, 2, 1, 8, 3, 7, 5, 12, 6
s_8	8, 7, 14, 5, 15, 13, 0, 6, 11, 12, 9, 10, 2, 4, 1, 3
s_9	11, 5, 15, 0, 7, 2, 9, 13, 4, 8, 1, 12, 14, 10, 3, 6

Diffusion function-P

Diffusion function P is defined as a permutation of eight 4-bit words, and it can be expressed as the following equations.

Z = Z7 || Z6 || Z5 || Z4 || Z3|| Z2 || Z1 || Z0→ U (5)

The output of round function is U and is obtained as

U7=Z6, U6=Z4, U5=Z7, U4=Z5,
U3=Z2, U2=Z0, U1=Z3, U0=Z1. (6)
U= U7 || U6 || U5 || U4 || U3|| U2|| U1 || U0. (7)

The round function complete operation is shown below in the figure 2.
Fig

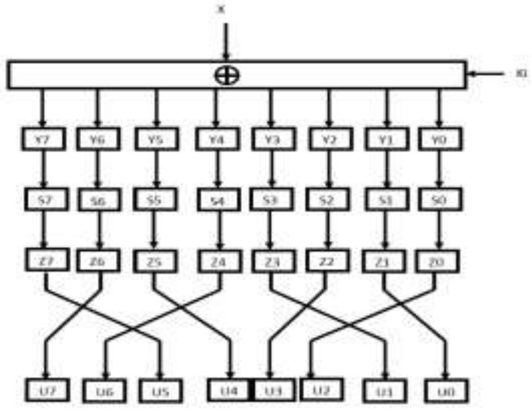


Fig 2: Round function operation

B. Decryption Algorithm

The decryption algorithm of L Block is the inverse of encryption procedure and it consists of a 32-round variant Fiestel structure too. Let C = X32||X33 denotes a 64-bit ciphertext, and then the decryption procedure can be expressed as follows

1. For j=31, 30 ….0, do
XJ= (F (Xj+1, Kj+1) ⊕ Xj+2) >>> 8 (8)
2. Output M=X1||X0 as the 64-bit plaintext.

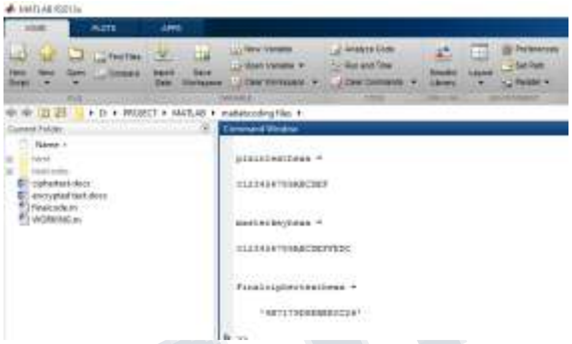
C. Key scheduling

The Key Schedule of L Block block cipher accepts an 80-bit master key, K = k79, k78, k77,…, k1, k0 which is stored in a key register. After 32 rounds of execution, this algorithm will produce 32 round sub keys denoted as Ki.
Step 1: Round sub key, K1 is the leftmost 32 bits of the master key, K.

Step 2: For 1 ≤ i ≤ 31, the key register is updated as follows:-
a) K<<<29
b) [k79, k78, k77, k76] = s9 [k79, k78, k77, k76]
[k75, k74, k73, k72] = s8 [k75, k74, k73, k72]
c) [k50, k49, k48, k47, k46] xor [i] 2.
d) Round sub key, Ki+1 is the leftmost 32 bits of the current key register.

III. SOFTWARE MODEL

Firstly the L Block cipher encryption algorithm is modelled using MATLAB R2013a and calculator is created for the same. Then function table is built for various texts and the output encrypted texts.64-bit plaintext is given as input along with 80-bit master key and 64-bit cipher text is obtained after encryption. The results are shown below:



```
plaintextHexa =

0123456789ABCDEF


masterkeyHexa =

0123456789ABCDEFFEDC


finalciphertextHexa =

    '4B7179D8EBEE0C26'
```

Fig 3: MATLAB Result

The intermediate values are obtained and verified. Here the modeling is carried out in the most direct form. So that the errors are reduced during modeling. The inputs and outputs are expressed in hexadecimal. The function table created for various input values is given below.

Table II: Function table

PLAINTEXT	MASTERKEY	CIPHERTEXT
0000000000000000	00000000000000000000	C218185308E75BCD
0123456789ABCDEF	0123456789ABCDEFFEDC	4B7179D8EBEE0C26
ABADCBE098765432	12345678987654321042	2A076AAB07A8FE49
012A345B678C9DEF	13C3B58789ABCDEFFEDC	1EF60498ACA69A46
1000200030004000	10012002300340045005	8D17319ECAB1C084

IV. PERFORMANCE EVALUATION

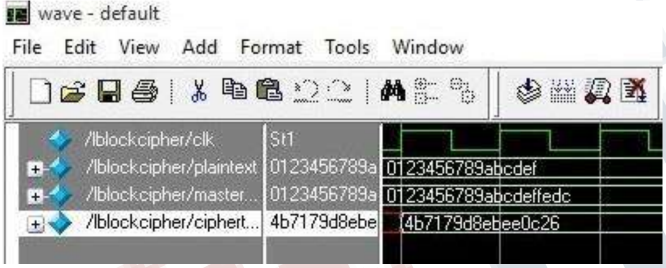
A. Software implementations

For devices of constrained environments, software platform implementations have its own significance. Software implementations method will provide structured approach systematically to integrate a component into the workflow of an organizational structure or an individual end-user. It makes it much easy to build application as it provides all necessary building blocks to implement specific functionalities. Since platform provides readymade functionalities and library, time consumed for software development life cycle is expected to reduce as both development and testing time consumption can be reduced.
Xilinx ISE 14.7 by Xilinx for synthesis and analysis of HDL designs, enabling the developer to synthesize their designs, perform timing analysis, examine RTL diagrams, simulate a design's reaction to different stimuli, and configure the target

device with the programmer is used as a software tool for software platform implementations. Verilog code developed for the algorithm and it is simulated. The following results are obtained.

Fig 4: Xilinx Result

Also the L Block encryption algorithm is simulated using ModelSim SE 6.2c and the results are compared and verified with the previous ones.



```
/lblockcipher/clk         St1
/lblockcipher/plaintext   0123456789a   0123456789abcdef
/lblockcipher/master...   0123456789a   0123456789abcdeffedc
/lblockcipher/ciphert...  4b7179d8ebe   4b7179d8ebee0c26
```

Fig 5: Model Sim Result

B. Hardware platform implementation and metrics

In hardware designs area, timing, energy, power and efficiency metrics are the basic performance metrics. Based on the type and completeness of the implementation, design area utilized will be different. Hardware designs are typically implemented using full-custom design, ASIC or FPGA technology. ASIC designs are based on automated design flows to lessen the design time. In case of ASIC implementation, the area is expressed in µm2, is given by physical design tools [2]. For pre-layout design area is expressed in the number of gate equivalent (GE).The throughput is a function of design frequency [2]. Power and energy are essential performance metrics for ciphers targeted for energy constrained low-resource devices. Power is also dependent on clock frequency similar to throughput. The average power dissipation indicates the rate of energy consumption.

The input-output diagram gives the black box representation of a design. The overall idea of the design can be easily obtained from it. It should be compact and easy to understand. The design has three inputs: plaintext, master key and clock. The plaintext is 64 bit wide and master key is 80 bit wide. The output is the cipher text which is 64 bit wide. The input-output diagram is given below.

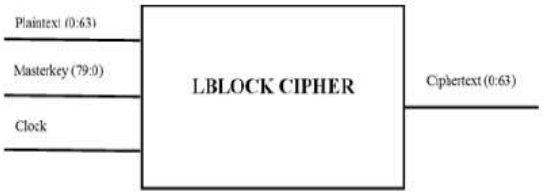


Fig 6: Input-output diagram for L Block encryption

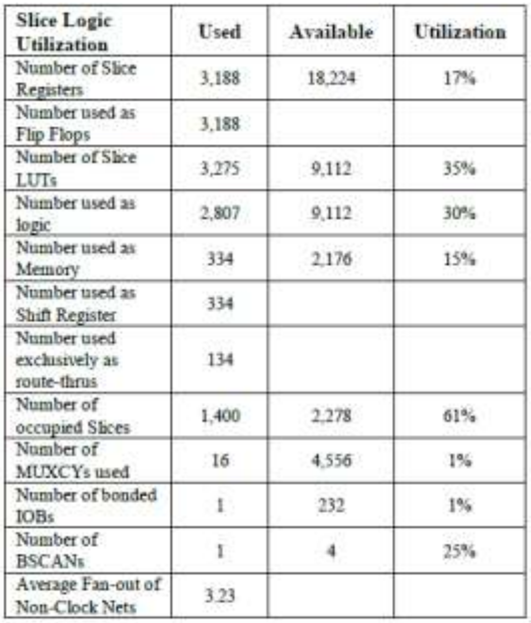
Compared with ASIC designs and full-custom design, FPGA designs provide advantages such as reduced development cost, shorter time to market and flexibility. The other benefits include algorithm agility, upgrading device by new algorithm uploading and algorithm modification. The following list of results will give the hardware performance metrics for the L Block block cipher algorithm.

1) Synthesis result

The L Block encryption is implemented in Verilog and synthesized it on Xilinx Spartan-6 (XC6LX16-CS324) FPGA Kit to check for its hardware performance. Xilinx ISE 14.7 is used as FPGA development environment during the implementation process (i.e., synthesis, map and place& route).

The table below shows the overall resource utilized during implementation process.

Table III: Resource utilization summary



Slice Logic Utilization	Used	Available	Utilization
Number of Slice Registers	3,188	18,224	17%
Number used as Flip Flops	3,188		
Number of Slice LUTs	3,275	9,112	35%
Number used as logic	2,807	9,112	30%
Number used as Memory	334	2,176	15%
Number used as Shift Register	334		
Number used exclusively as route-thrus	134		
Number of occupied Slices	1,400	2,278	61%
Number of MUXCYs used	16	4,556	1%
Number of bonded IOBs	1	232	1%
Number of BSCANs	1	4	25%
Average Fan-out of Non-Clock Nets	3.23		

2) Power utilization summary

FPGAs are widely used in many applications due to its advantages over others. FPGAs can provide huge benefits to the system design by reducing the power consumption. The power analysis for L Block cipher is done using XPower Analyzer (XPA) tool on Spartan-6 FPGA. Xilinx Power tool performs power estimation and analysis for the design given. The result obtained after running XPA is 0.021 W.

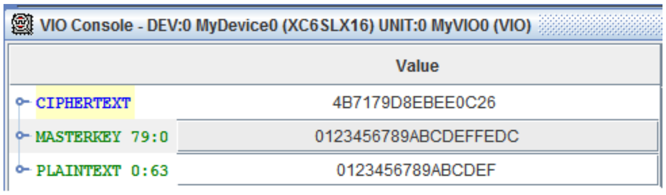
3) Timing analysis

Timing analysis is done by considering the architecture of the FPGA device and the logic implemented. Throughput is calculated using the timing analysis report. Throughput can be defined as the data processed by a design within a fixed amount of time. It depends on block size of the algorithm, frequency and latency of the hardware design. From the timing report the clock frequency is found as 120.174 MHz with a clock period of 8.321 ns. The block size is 64 in this case and latency is 8 cycles. The throughput obtained at frequency 120.174 MHz is 924.304289 Mbps.

4) Area and Power

The design was implemented on ASIC platform and the area, power, timing details were obtained .The area consumed was found to be 416286 (μm2) cell area for instances 13346 and total power consumed, leakage and dynamic power consumed are obtained.

5) On chip debugging result



VIO Console - DEV:0 MyDevice0 (XC6SLX16) UNIT:0 MyVIO0 (VIO)

	Value
CIPHERTEXT	4B7179D8EBEE0C26
MASTERKEY 79:0	0123456789ABCDEFFEDC
PLAINTEXT 0:63	0123456789ABCDEF

Fig 7: On chip debugging result.

V. CONCLUSION

A detailed study on L Block block cipher was done and carried out its algorithm validation. L Block block cipher is a lightweight block cipher of block size 64 bit and key size 80 bit targeted to provide cryptographic security for resource constrained applications e.g. RFID, sensor networks etc. The behavioral description of the design is written in Verilog HDL and simulated using XilinxISE 14.7 and ModelSim 6.2 c software platforms. Then the design is successfully implemented on Xilinx Spartan6 FPGA (XC6LX16-CS324). Design verification is performed with chip scope tool of Xilinx. Test result is compared with MATLAB results and found to be right. Power utilization is analyzed using Xilinx Power Analyzer (XPA) and noted that it took only 0.021W. It can serve as reference for hardware design engineers who wants to provide cryptographic security in constrained environments. The decryption of L Block cipher has to be carried out and as an extension the study and test should be done to check the possibility of its application in PUF (Physically Unclonable Function). PUF are usually implemented in integrated circuits and are used in applications with high security requirements.

REFERENCES

[1] Wenling Wu, Lei Zhang “L Block: A Lightweight Block Cipher” *Springer*, 2011.

[2] Bassam J.Mohd, Thaier Hayajneh, Athanasios V.Vasilakos, “A survey of lightweight block ciphers for low-resource devices-Comparative studies and open issues,” *Journal of Network and Computer Application “*, September 2015.

[3] Mickael Cazorla, Kevin Marquet and Marine Minier, “Survey and Benchmark of Lightweight Block Ciphers for Wireless Sensor Networks,” *Security and Communication Networks*, Volume 8, Issue 18, pages 3564–3579, December 2015.

[4] Sufyan Salim Mahmood AlDabbagh ,Imad Fakhri Taha Al Shaikhli, “Improving the Security of L Block Lightweight Algorithm using Bit Permutation,” *IEEE* , Dec 2013 DOI:10.1109/ACSAT.2013.65

[5] Hideki Yoshikawa, Masahiro Kaminaga, Arimitsu Shikoda, Toshinori Suzuki, “Secret Key Reconstruction Method using Round Addition DFA on Lightweight Block Cipher L Block,” *IEEE*, Oct 2014, pp.493 – 496.

[6] Jinyong Shan1, Lei Hu1, and Siwei Sun, “Security of L Block-s against Related-Key Differential Attack,” *IEEE*, Feb. 2015, pp 1278 – 1283.

[7] Panasayya Yalla and Jens-Peter Kaps, “Lightweight Cryptographys for FPGA,” *International Conference on Reconfigurable Computing and FPGAs*, IEEE, Dec 2009, pp. 225–230.