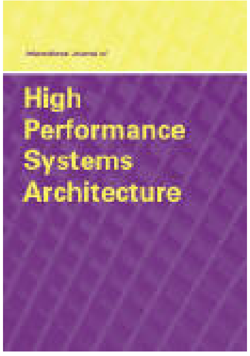


International Journal of High Performance Systems Architecture

ISSN online: 1751-6536 - ISSN print: 1751-6528
https://www.inderscience.com/ijhpsa

Hardware implementations of LBlock and XXTEA lightweight block ciphers for resource-constrained IoT application

Apeksha Kamble, Zeesha Mishra, Bibhudendra Acharya

DOI: 10.1504/IJHPSA.2023.10054395

Article History:

Received:	05 September 2022
Last revised:	06 September 2022
Accepted:	28 October 2022
Published online:	06 April 2023

Hardware implementations of LBlock and XXTEA lightweight block ciphers for resource-constrained IoT application

Apeksha Kamble

Department of Electronics and Communication Engineering,
National Institute of Technology Raipur,
Chhattisgarh – 492010, India
Email: apeksha.kamble.96@gmail.com

Zeesha Mishra

Department of Microelectronics and VLSI, UTD,
Chhattisgarh Swami Vivekananda Technical University,
Bhilai, Chhattisgarh – 491107, India
Email: zmishra.phd2016.etc@nitrr.ac.in

Bibhudendra Acharya*

Department of Electronics and Communication Engineering,
National Institute of Technology Raipur,
Chhattisgarh – 492010, India
Email: bacharya.etc@nitrr.ac.in
*Corresponding author

Abstract: Recent growth in the number of connected Internet of Things (IoT) devices in a network has raised lot of security related issues. Since these devices are mostly battery powered, have low memory and weak computational capability, therefore lightweight ciphers are the most suitable choice for providing security. Among various lightweight ciphers available, we have chosen to implement corrected block TEA (XXTEA) and LBlock ciphers. These lightweight ciphers are feistel based, having simple encryption algorithms. In this work, two different architectures are proposed namely round-based implementation of LBlock cipher and serial implementation of XXTEA cipher with variable length message. Both the architectures are implemented on different field programmable gate array (FPGA) device families and application-specific integrated circuit (ASIC) implementation is performed on 0.18 µm complementary metal-oxide semiconductor (CMOS) technology. By analysing the performance metrics, comparison of the proposed work is done with the existing ciphers. For the proposed LBlock and XXTEA variable length architectures, the percentage improvement obtained with respect to area consumption is 50.92% and 26.04% respectively.

Keywords: IoT; Internet of Things; LWC; lightweight ciphers; LBlock; XXTEA; corrected block TEA; FPGA; field programmable gate array; ASIC; application-specific integrated circuit; block cipher.

Reference to this paper should be made as follows: Kamble, A., Mishra, Z. and Acharya, B. (2023) 'Hardware implementations of LBlock and XXTEA lightweight block ciphers for resource-constrained IoT application', *Int. J. High Performance Systems Architecture*, Vol. 11, No. 3, pp.169–178.

Biographical notes: Apeksha Kamble has received her BE in Electronics and Telecommunication (2018) from Savitribai Phule Pune University, India and has completed her MTech in VLSI and Embedded System (2022) from National Institute of Technology Raipur, India. Her research interest includes lightweight cryptographic ciphers, algorithms and hardware architectures.

Zeesha Mishra has earned her MTech (2015) in VLSI Design from Chhattisgarh Swami Vivekananda Technical University, Bhilai India and PhD in Electronics and Communication Engineering from National Institute of Technology Raipur India. She is currently serving as an Associate Professor in the Microelectronics and VLSI Department, Chhattisgarh Swami Vivekanand Technical University Bhilai, India. She research interests include cryptography,

high-performance architectures, hardware security, and FPGA-based designs. She has more than 18 research publications in national/international journals and conferences.

Bibhudendra Acharya received his MTech in Telematics and Signal Processing from National Institute of Technology Rourkela, India and PhD in Electronics and Communication Engineering from National Institute of Technology Rourkela, India. He is currently serving as an Assistant Professor in the Electronics and Communication Engineering Department, National Institute of Technology Raipur, India. His research interests include cryptography, signal processing, high-performance architectures, hardware security, and FPGA-based designs. He has more than 100 research publications in national/international journals and conferences.

1 Introduction

Recently, Internet of Things (IoT) has become a popular choice because of its wide range of applications in several domains. It involves collecting and transferring of real time data over the network. Deployment of IoT gives rise to many challenges, one of which is the security issue. It is important to preserve the integrity of the information shared over the network. Many applications in IoT have limited resources such as energy, memory, processing power and even physical space. Conventional cryptography could be a solution to guarantee security of data in such devices but due to its high resource requirements it is not a viable choice. In order to secure the real time data, lightweight cryptography is used which is a lighter version of conventional cryptography and it deals with preserving data integrity in such resource constrained devices.

While designing lightweight ciphers (LWC), it is necessary for the designers to consider the trade-off between security, cost and performance. The main aim is to create a balance between these three metrics as it is difficult to improve all at the same time. While designing LWCs for resource constrained devices, the focus is to obtain cost effectiveness through various metrics such as area, speed, power and energy consumption. For example, WSNs require implementation of complex cryptography algorithms for achieving high level security (Biswas et al., 2016). Block ciphers are the most preferred choice in lightweight cryptography as they are simple to implement compared to stream ciphers. Some examples of block ciphers are LED, PRESENT, SIMON, TEA, LiCi etc.

The hardware implementations of the LWCs can be performed on various FPGA device families. When compared to the FPGA implementation, ASIC implementation require more manufacturing time and are expensive. Due to the low NRE (Non-recurring engineering) cost, FPGAs are the most suitable choice for hardware implementation (Shrivastava et al., 2020). By using FPGAs, requirement of resource consumption is reduced. It also has built-in BRAM (block random access memory), which is a benefit because it frees up registers that could be used for other purposes in the application (Nedjah and Mourelle, 2007).

LBlock is a lightweight block cipher which was proposed by Wu and Zhang (2011). It operates on 64-bit input block data using a 80-bit key. A security analysis check confirmed that the cipher can withstand many attacks like linear cryptanalysis, differential cryptanalysis, related-key attacks, etc. (Wu and Zhang, 2011). It is known to provide enough security making it a reliable choice in resource constrained devices. Corrected Block TEA (XXTEA) is designed as a modified version of Tiny Encryption Algorithm (TEA) for enhancing the security. It operates on variable length of input block message (multiple of 32-bit) ranging from 32-bit to 256-bit using a 128-bit key. Most of the ciphers adopts a fixed input message length strategy for encryption. In this paper a functionality of accepting variable length of input message is incorporated in the proposed architecture of XXTEA cipher.

The major contributions of this paper are as follows:

- Proposed a round-based architecture of LBlock lightweight block cipher. With this design implementation technique, area optimisation has been achieved.
- Proposed a serial-based architecture of XXTEA lightweight block cipher supporting variable length block size. The variable length functionality incorporated in a single architecture gives the designer flexibility to work on different input block sizes. The serial implementation focuses on achieving area optimisation.
- Both the architectures are implemented on different FPGA device families and ASIC implementation is performed on 0.18 μm CMOS technology. The results obtained are compared and studied with respect to various lightweight ciphers in terms of different metrics.

1.1 Previous work

LBlock is a Feistel cipher which has a simple implementation and performs operation on fixed input data and key size. Wu and Zhang (2011) have performed hardware implementation of LBlock cipher on 0.18 μm CMOS technology. A security evaluation is also done in order to study the response against various known attacks. A software implementation is also presented on a 8-bit micro-controller. According to the authors, 2000 GE is the limitation in RFID applications. The presented design satisfies the limitation by acquiring 1320 GE in 0.18 μm technology. Hasan et al. (2016) have designed functional RTL design of LBlock LWC. The main goal of the work was to evaluate the designs performance on FPGA family devices. The authors have implemented the design on Altera Cyclone II DE1 board. The performance metrics obtained for the design was compared with Hummingbird and XTEA LWC, and it was observed that the presented design occupied less LEs as compared to the existing LWCs. In the paper proposed by (Mishra and Acharya, 2020), pipelined and serial architectures of secure IoT (SIT) algorithm for encryption are proposed for obtaining high speed and low area respectively. Pandey et al. (2019) have presented performance enhanced hardware architectures of PRESENT lightweight block cipher. The PRESENT cipher performs operation on 64-bit input data using 80/128-bit keys. The architectures are designed to execute encryption, decryption and integrated encryption/decryption operations. The designs are developed to target latency critical and area constrained applications. FPGA implementation of the architectures is performed on Virtex-5 device and the overall latency obtained for it is 33 clock cycles. FPGA implementation of the ultra lightweight block cipher Piccolo is presented by Ramu et al. (2020). Piccolo operates on 64-bit input data block and supports two different key sizes of 80-bit and 128-bit. For optimisation of the design three different architectures are described namely loop rolled, parallel round based and pipelined architectures. The presented work is implemented on various FPGA device families. The authors have shown that the design obtained reduction in area and increase in throughput which makes it a suitable choice for low resource devices. (Mishra and Acharya, 2020) have designed round-based architectures of TEA family ciphers for low resource applications. The designed architectures achieved less area and dynamic power consumption making it suitable for RFID applications. The hardware implementation of the work is performed on various FPGA device families.

1.2 Structure of work

This paper presents round-based and serial-based design techniques which are used to implement hardware architectures of LBlock and XXTEA LWCs respectively. The work is organised as follows, Section 2 provides a theoretical description of the LBlock and XXTEA ciphers with an explanation of the algorithm. Section 3 gives an explanation of the implementations of the proposed ciphers. The results and analysis of the work is described in Section 4. Section 5 concludes the work.

2 Theoretical description

2.1 LBlock

The LBlock cipher uses 64-bit input data which is split into two 32-bit data. One half of the 32-bit data is transformed using a round function and on the second half of the data, arithmetic left shift operation is performed. The round function F is composed of Substitution (S) and Permutation (P) layer blocks. The S layer constitutes of 10 S boxes of size 4×4. The S layer and P layer adds confusion and diffusion to the encryption algorithm respectively. The 32-bit W register stores the XORed value of input data X and sub-round Key K_i. The Encryption algorithm uses S0 to S7 boxes whereas key-scheduling algorithm uses S8 and S9 boxes for the operation. Table 1 show the S-boxes used in the process. The final ciphertext is obtained after completing total 32 number of rounds. The encryption algorithm can also be understood from the diagram as shown in Figures 1 and 2.

Encryption Algorithm for LBlock Cipher:

```
Input : X1 || X0
for i=2 to 33
$X_i = F(X_{i-1}, K_{i-1}) \oplus X_{i-2} <<< 8$
Where, symbol $\oplus$ signifies XOR operator
          symbol <<< signifies left shift operator
Round Function F :
$F(X, K_i) = P(S(X \oplus K_i))$
S Function :
$W(32\text{-bit}) \rightarrow C(32\text{-bit})$
$C_7 = S_7(W_7), C_6 = S_6(W_6), C_5 = S_5(W_5),$
$C_4 = S_4(W_4), C_3 = S_3(W_3), C_2 = S_2(W_2),$
$C_1 = S_1(W_1), C_0 = S_0(W_0)$
P Function:
$C(32\text{-bit}) \rightarrow D(32\text{-bit})$
$D_7 = C_6, D_6 = C_4, D_5 = C_7,$
$D_4 = C_5, D_3 = C_2, D_2 = C_0,$
$D_1 = C_3, D_0 = C_1$
```

Key Scheduling Algorithm:

K denotes the 80-bit input key. Initially the leftmost 32-bit content of K is used as sub-round key K1. Then the operation for further rounds to obtain sub-round key occurs as follows:

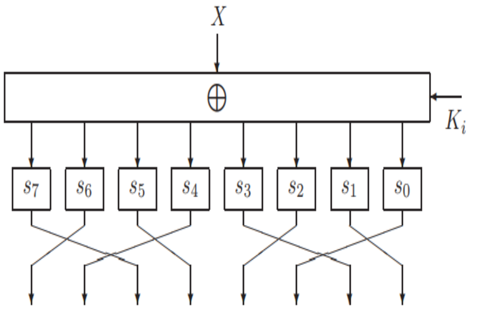
Key Scheduling Algorithm for LBlock Cipher:

```
$K_1 = K[79:48]$
for i = 2 to 31
K<<<29
$[key_{79}\ key_{78}\ key_{77}\ k_{76}] = S9[key_{79}\ key_{78}\ key_{77}\ key_{76}]$
$[key_{75}\ key_{74}\ key_{73}\ key_{72}] = S8[key_{75}\ key_{74}\ key_{73}\ key_{72}]$
$[key_{50}\ key_{49}\ key_{48}\ key_{47}\ key_{46}] = [key_{50}\ key_{49}\ key_{48}\ key_{47}\ key_{46}] \oplus [i]_2$
$K_i = K[79:48]$
```

Table 1 S-boxes used in LBlock encryption and key scheduling algorithms

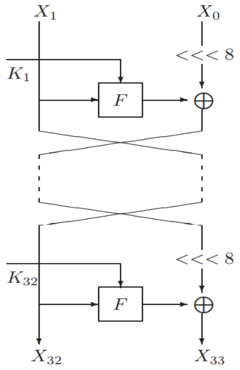
S0	*E*	*9*	*F*	*0*	*D*	*4*	*A*	*B*	*1*	*2*	*8*	*3*	*7*	*6*	*C*	*5*
S1	4	B	E	9	F	D	0	A	7	C	5	6	2	8	1	3
S2	1	E	7	C	F	D	0	6	B	5	9	3	2	4	8	A
S3	7	6	8	B	0	F	3	E	9	A	7	D	5	2	4	1
S4	E	5	F	0	7	2	C	D	1	8	4	9	B	A	6	3
S5	2	D	B	C	F	E	0	9	7	A	6	3	1	8	4	5
S6	B	9	4	E	0	F	A	D	6	C	5	7	3	8	1	2
S7	D	A	F	0	E	4	9	B	2	1	8	3	7	5	C	6
S8	8	7	E	5	F	D	0	6	B	C	9	A	2	4	1	3
S9	B	5	F	0	7	2	9	D	4	8	1	2	E	A	3	6

Figure 1 Block diagram showing combined operation performed by S and P layer blocks (Wu and Zhang, 2011)



Source: Wenling and Lei (2011)

Figure 2 Block diagram of LBlock encryption algorithm (Wu and Zhang, 2011)



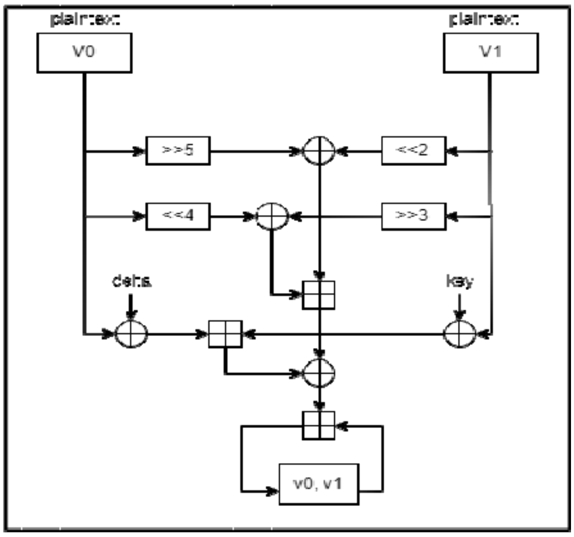
Source: Wenling and Lei (2011)

XXTEA

The corrected block TEA (XXTEA) was designed by Needham and Wheeler (1998). It is a fast and secure encryption method which uses an unbalanced Feistel network. In XXTEA LWC, the length of the input message can vary from minimum 64-bit to maximum.

256-bit. The input message is a multiple of 32-bit. In the encryption algorithm mentioned below, initially the input message is stored in register V and then registers Z and Y are used for storing data obtained in every round operations. The number of rounds required to complete the encryption process is calculated using the length of the input block data to be processed and p denotes the number of sub-rounds required to complete one round of encryption. Figure 3 depicts encryption process of XXTEA cipher.

Figure 3 Encryption process of XXTEA block cipher



Encryption algorithm for proposed XXTEA cipher for variable length block size:

Key: K(128-bit) => (K[0](32-bit)||K[1](32-bit)||K[2](32-bit)||K[3](32-bit))

Constant: Delta(0x9e3779b9)

No. of rounds (N) = (6+52/n) where n is length of the block data

MIX : [(((Z >>5) ^ (Y<<2)) + ((Y>>3) ^(Z<<4))) ^ ((sum^Y) +(K[p&3^e] ^ Z))

Operation :

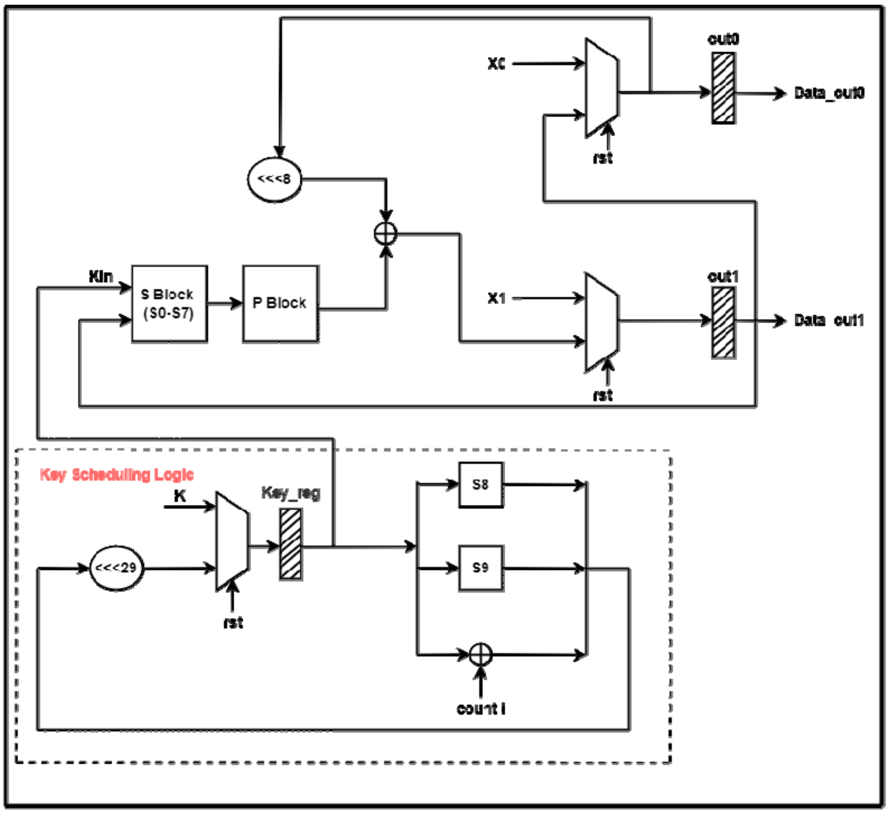
```
Z = V[n-1], Y=V[0]
___________________________________

sum=0
while (N >0) {
sum = sum+delta
for p=0,1 ……n-2
{
Y = V[p+1]
Z = V[p] + MIX
}
Y = V[0]
Z = V[n-1] + MIX
(N -1)          }
Final Ciphertext : Y(32-bit)|| Z(32-bit)
```

3 Hardware implementations of proposed architectures

3.1 Round-Based architecture of LBlock cipher

The proposed work shown in Figure 4 is a round based architecture of LBlock Lightweight Block Cipher. The architecture follows a simple Feistel operation in which the input block data is split into two 32-bit data X0 and X1. Two multiplexers are incorporated in the design for proper selection of input data at each round. When reset (rst) signal is high, the initial input data X0 and X1 are selected for operation. When rst is low the intermediate data is used for operation. Output registers of 32-bit size out0 and out1 are used to store the intermediate round data. The S block shown in the architecture uses 8 S-boxes for operation. It accepts round key and input block data as inputs. In the S block, the inputs are XORed and then XORed value is used to select the appropriate value for substitution from the S-boxes. The S block is responsible for adding confusion in the operation. The P block accepts input from the S block and performs diffusion. The Key Scheduling Logic generates the appropriate sub-round key value. A single multiplexer is used for selection of appropriate input key value based on rst as a select line. A 32-bit Key_reg register is used in the design to store the intermediate sub-round key values. S-boxes S8 and S9 are used in the operation and the count i value which represents the value of round is also used in the operation. For obtaining the final ciphertext, total 32 rounds are required.

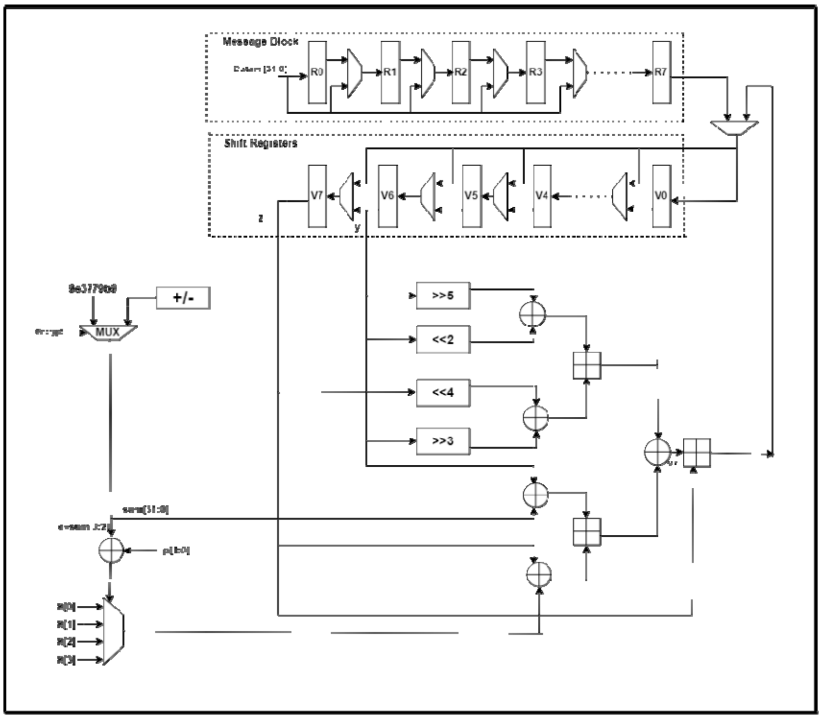
Figure 4 Proposed round-based architecture implementation of LBlock lightweight cipher (see online version for colours)



3.2 Serial-based architecture of XXTEA variable-length block size

The architecture implementation of XXTEA lightweight cipher with variable message block is shown in Figure 5. The implementation shows usage of several shift registers in order to implement the variable size message block. The incorporated message block accepts input data which is a multiple of 32-bit (ranging from 64-bit to 256-bit) and the operation is performed on 32-bit data in each clock cycle. Once the message is loaded in the registers, the shift registers, serially shift 32-bit data at each clock cycle. Once the design gets the information about the length of the input message block, it uses the necessary number of registers for serial shifting of data. This logic helps in accepting input data of different block sizes. The total number of rounds to obtain the final ciphertext is calculated and accordingly the operation on the data block is performed. The data stored in shift registers is used to calculate the MIX signal. The output from the MIX signal is XORed with the input data and then fed back to the shift registers. The implemented design is taking total 64 clock cycles to generate the final encrypted output for 64-bit block data and 90 clock cycles for 192-bit block data as specified in Table 4.

Figure 5 Proposed serial-based architecture of XXTEA cipher for variable length block size



4 Results and analysis

The proposed work is implemented on FPGA devices using Xilinx ISE and Xilinx Vivado tools. The design is simulated using ModelSim tool. FPGA stands for field programmable gate array. This means that these can be configured on the field by the designers. FPGA devices have many advantages such as low cost, high speed, reconfigurable and shorter time to market. In this work the hardware implementation is performed on various FPGA devices such as Spartan-3, Spartan-6, Virtex-4, Virtex-5, Virtex-6 and Artix-7. The ASIC implementation is performed on 0.18 µm technology using Cadence Genus synthesis tool. The performance metrics are analysed and compared with different ciphers. Some of the metrics which are important to be analysed are area, power and throughput. The total power of the design is sum of its static and dynamic power. The area consumed is determined by the LUT count, slices and the registers occupied. Latency of the device is calculated based on the total count of clock cycles required to conclude the encryption process. Throughput determines the overall speed of the design and it can be calculated as shown in equation (1). The total amount of energy consumed is calculated using equation (2). The main aim is to create a balance between cost, security and performance as it is difficult to improve all at the same time.

$$\text{Throughput} = \frac{\text{Maximum Frequency} \times \text{Block Size}}{\textit{clockcycles}} \tag{1}$$

$$\text{Energy per bit} = \frac{\text{Power} \times \text{Cycle}}{\textit{MaximumFrequency} \times \textit{B.Size}} \tag{2}$$

The performance parameters analysed for the proposed work on different FPGA devices is described in Tables 2 and 3. It can be observed from Tables 2 and 3, that for proposed LBlock and XXTEA among the results obtained for all the devices, Virtex-6 implementation shows stronger results with respect to area and throughput.

Table 2 Performance parameters of the proposed LBlock lightweight cipher on different FPGA device families

Parameter	*Spartan3*	*Spartan6*	*Virtex5*	*Virtex6*	*Artix7*
LUT	223	160	229	171	171
FFs	151	151	151	151	151
Max. Frequency (MHz)	181.760	236.295	453.566	548.140	537.663
Cycle	32	32	32	32	32
Throughput (Mbps)	363.52	472.59	907.132	1096.28	1075.326
Total Power (W)	0.154	0.346	0.837	1.573	0.215
Energy per bit (nJ/bit)	0.423	0.732	0.922	1.434	0.199

For **LBlock cipher**, the total LUT count obtained for the proposed work using Spartan-6 is 160 with a throughput of 472.59Mbps. For Virtex-6 devices a total LUT count of 171 is obtained and a high value throughput of 1096.28 is achieved. Table 4 provides a comparison between proposed work and different existing ciphers in terms of performance metrics. It can be observed that improved results in terms of low area consumption and better throughput values are obtained. The LUT results obtained for the proposed LBlock is better than the results obtained for TEA (Mishra and Acharya, 2021), TEA (Hussain and Badar, 2015), LED

(Rashidi, 2020), SIT (Mishra and Acharya, 2020), QTL (Shrivastava et al., 2020) and Hummingbird (Fan et al., 2010). LBlock (Hasan et al., 2016) is implemented on Cyclone II FPGA device and the LUT count obtained for it is more than the LUT count obtained for the proposed LBlock. The throughput results obtained are also better than LBlock (Hasan et al., 2016). When compared with the ultra-lightweight cipher Hummingbird, the proposed LBlock cipher shows better throughput and less LUT count. Compared to the QTL (Shrivastava et al., 2020) and SIT (Mishra and Acharya, 2020) which are implemented using round-based design technique, proposed work shows improved results. Table 5 provides result obtained for the ASIC implementation along with it, a comparison is performed with different ciphers. The GE obtained is 1364.83 with a low power consumption result of 1.46mW. The GE result obtained for PRESENT (Rashidi, 2020), SIMON (Rashidi, 2020) and XXTEA (Mishra and Acharya, 2021) are more than the GE obtained for the proposed work. However, the GE obtained for the presented work is comparable to LBlock (Wenling and Zhang, 2011; Wu and Zhang, 2011). The results suggests acceptable GE value obtained for the proposed work and suggests that the architecture can be used in resource constrained devices.

Table 3 Hardware performance metrics of XXTEA variable length (64-bit) on various FPGA device families

Parameter	*Spartan3*	*Spartan6*	*Virtex4*	*Virtex5*	*Virtex6*
LUT	327	213	426	324	226
FFs	161	163	162	161	163
Max. Frequency (MHz)	97.99	216.305	217.630	247.363	310.516
Cycle	64	64	64	64	64
Throughput (Mbps)	97.99	216.305	217.630	247.363	310.516
Static Power (W) @100 MHz	0.060	0.029	0.236	0.530	1.293
Dynamic Power (W) @100MHz	0.002	0.010	0.011	0.095	0.012
Total Power (W) @100 MHz	0.061	0.039	0.246	0.626	1.293
Energy per bit (nJ/bit)	0.622	0.180	1.130	2.530	4.164

Table 4 Comparison table of lightweight block ciphers based on different performance parameters on FPGA platform

Algorithm	*Device*	*Block size*	*LUTs*	*Max. frequency* (MHz)	*Cycle*	*Throughput* (Mbps)	*Total power* (W)
LBlock (Hasan et al., 2016; Wu and Zhang, 2011)	Cyclone II	64	326	50	–	200	0.124
TEA (Mishra and Acharya, 2021)	Virtex-5	64	234	365.08	–	708.07	–
TEA (Hussain and Badar, 2015)	Spartan 6-xc6slx45	64	447	–	–	55.86	0.228
Hybrid Model (Mishra and Acharya, 2021)	Virtex-5	64	487	253.17	–	491.05	–
LED (Rashidi, 2020)	Spartan3	64	328	207.59	772	17.20	–
PRESENT (Rashidi, 2020)	Spartan-6	64	287	245.6	68	12.76	0.0218
XXTEA (Mishra and Acharya, 2021)	XC7VX330T-2	64	165	591.35	42	1147	0.203
LEA-128 (Mishra et al., 2021)	XC5VLX330T-2	128	360	340	25	1803	3.793
SIT (Mishra and Acharya, 2020)	Virtex-5	64	394	148.35	–	1898.88	0.761
QTL (Shrivastava et al., 2020)	Virtex-5	64	278	173.02	32	346.04	0.562
Hummingbird (Fan et al. 2010)	XCS3200-5	16	473	40.1	4	160.4	–
LBlock-proposed	Spartan-6	64	160	236.295	32	472.59	0.346
LBlock-proposed	Virtex-6	64	171	453.566	32	1096.28	1.573
XXTEA variable length- proposed	Spartan-6	64	213	216.305	64	216.305	0.039
XXTEA variable length- proposed	Virtex-6	64	226	310.516	64	310.516	1.293

Table 5 Comparison table of lightweight block ciphers based on different performance parameters on ASIC platform 0.18 µm technology

Algorithm	*CMOS technology*	*GE*	*Cycle*	*Throughput* (Mbps)	*Total power (mW)*
LBlock (Wenling and Zhang, 2011)	0.18 µm technology	1320	–	200	–
PRESENT (Rashidi, 2020)	0.18 µm technology	4214	32	1492.54	–
SIMON (Rashidi, 2020)	0.18 µm technology	5380	45	1832.76	–
XXTEA (Mishra and Acharya, 2021)	0.18 µm technology	2212	33	193.93	–

Table 5 Comparison table of lightweight block ciphers based on different performance parameters on ASIC platform 0.18 µm technology (continued)

Algorithm	*CMOS technology*	*GE*	*Cycle*	*Throughput* (Mbps)	*Total power (mW)*
Hummingbird-2 (Engels et al., 2012)	0.18 µm technology	3220	4	400	–
Camellia (Aoki et al., 2001)	0.35 µm technology	11350	21	609.5	–
LEA (Mishra et al., 2021)	0.09 µm technology	11080	25	512	–
LBlock-proposed	0.18 µm technology	1364.83	32	715.4	1.461
XXTEA variable length- proposed	0.18 µm technology	2922	64	675.7	3.67

For **XXTEA cipher**, from Table 3 it can be observed that the proposed variable length architecture (**XXTEA-var**) shows that design used less LUTs and Flip-flops. The advantage of incorporating a functionality of accepting variable length message over fixed length message is that it gives the designer a choice of selecting the length of input messages. When compared to the pipelined implementation in XXTEA (Mishra and Acharya, 2021), the LUT count of proposed XXTEA-var is slightly more. This is because the logic used to implement the flexible input message in proposed work required more registers and gates compared to the fixed length architecture presented in XXTEA (Mishra and Acharya, 2021), which increased the total consumption of the proposed XXTEA cipher. Despite of that, the results obtained are quite optimum for resource constrained applications. Hybrid-Model (Mishra and Acharya, 2021) is a hybrid of TEA, XTEA and XXTEA and it is a pipelined architecture implementation designed for high speed applications. When compared to the hybrid-model the proposed XXTEA-var architecture shows better results with respect to LUT count obtained. In LED (Rashidi, 2020), serial architecture implementation is performed and the LUT count obtained for it is more than the presented variable length architecture. Table 5 provides a comparison of the proposed architecture and the existing ciphers on ASIC platform. When compared to PRESENT and SIMON (Rashidi, 2020), hummingbird-2 (Engels et al., 2012), LEA (Mishra et al., 2021) and Camellia (Aoki et al., 2001), the GE value of proposed XXTEA-var architecture is less which suggests area optimisation. However, the GE results of XXTEA-var is more than the proposed LBlock architecture, Lblock (Wenling and Zhang, 2011) and XXTEA (Mishra and Acharya, 2021) as proposed XXTEA-var supports multiple sizes which requires more registers and LUTs. Thus, this increases the overall GE of XXTEA-var.

Figures 6 and 7 shows graphical representation of the LUT count obtained on different FPGA device families for proposed LBlock and XXTEA variable length respectively. It can be observed that the LUT count results are better on Spartan-6 and Virtex-6 device families. The throughput results obtained are also optimum. LEA (Mishra et al., 2021) shows better throughput result than proposed work, as its architecture is pipelined based which improves the operating frequency which in turn increases the overall throughput. Figure 8 shows graphical representation of the optimised area results for proposed LBlock and XXTEA-var when compared with different ciphers on different FPGA devices. Figure 9 shows a graphical representation of the GE obtained for the proposed architectures compared with different architectures on ASIC platform.

Figure 6 Graphical representation of comparison of LUT count obtained for proposed LBlock on different FPGA device families

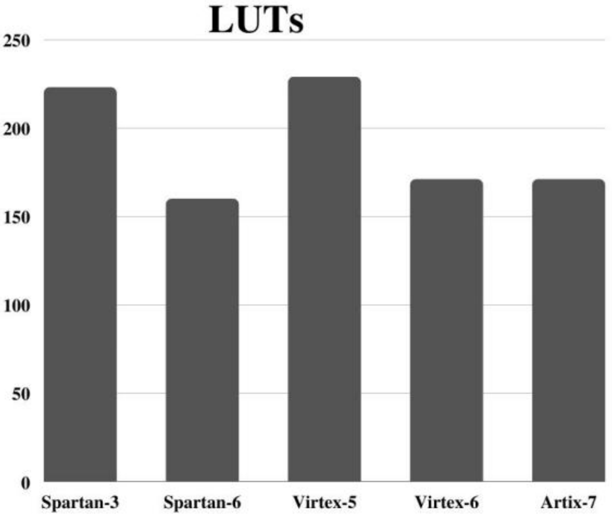


Figure 7 Graphical representation of comparison of LUT count obtained for proposed XXTEA variable length on different FPGA device families

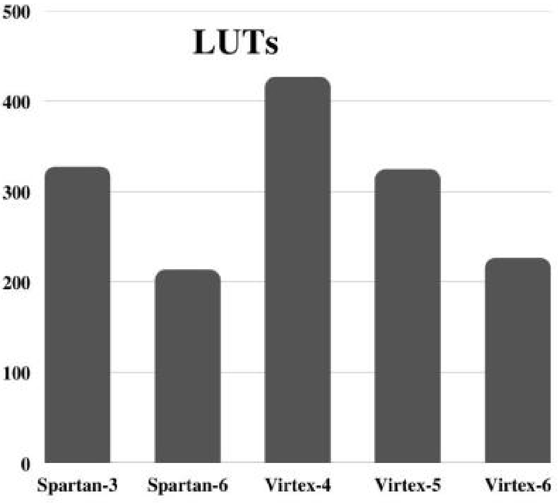


Figure 8 Graphical representation of comparison of LUT count obtained for proposed LBlock and proposed XXTEA variable length with existing ciphers

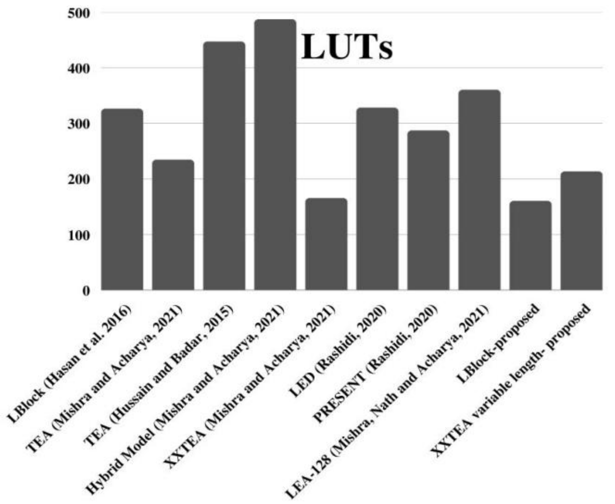
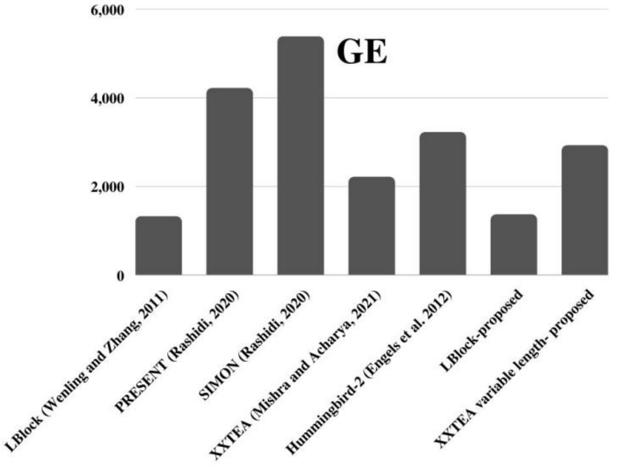


Figure 9 Graphical representation of comparison of GE obtained for the proposed LBlock and XXTEA variable length with different ciphers on ASIC platform



5 Conclusion

Several embedded devices are integrated in the ubiquitous computing environment to enable ambient intelligence applications. Securing these devices against various security breach becomes significantly important. With the proper selection of lightweight ciphers for specific applications can help in improving the security level. These resource constrained devices have a requirement of low memory footprint, power consumption and cost. The proposed work is based on designing a simple feistel based lightweight cipher called LBlock and XXTEA for low resource devices. A round based design of LBlock is employed in the architecture to obtain low area. The hardware implementations are performed on Spartan-3, Spartan-6, Virtex-5, Virtex-6 and Artix-7 FPGA devices and 0.18 µm technology ASIC platform. LUT count of 160 and GE of 1364.83 are obtained for proposed LBlock. A serial architecture of XXTEA for variable length message is also designed and implemented on various FPGA devices. The total LUT count obtained for the work in Spartan-6 device is 213 and the throughput obtained is 216.305 Mbps. ASIC implementation on 0.18 µm technology of proposed XXTEA cipher achieved GE value of 2922. The results obtained for both the proposed architectures on FPGA and ASIC platforms, shows reduction of area consumption when compared to different lightweight ciphers. Therefore it can be concluded that the proposed architectures has been optimised in terms of area. The proposed LBlock and XXTEA architectures can be used in devices having limited resources such as WSNs, smart wearable, healthcare applications and many more.

References

Aoki, K., Ichikawa, T., Kanda, M. *et al.* (2001) 'Camellia: a 128-bit block cipher suitable for multiple platforms – design and analysis', in Stinson, D.R. and Tavares, S. (Eds.): *Selected Areas in Cryptography*, Springer, Berlin, Heidelberg, Vol. 2012, pp.39–56.

Biswas, K., Muthukkumarasamy, V., Wu, X.W. and Singh, K. (2016) 'Performance evaluation of block ciphers for wireless sensor networks', in Choudhary, R., Mandal, J., Auluck, N. and Nagarajaram, H. (Eds.): *Advanced Computing and Communication Technologies. Advances in Intelligent Systems and Computing*, Springer, Singapore, Vol. 452, pp.443–452.

Engels, D., Saarinen, M.J.O., Schweitzer, P. and Smith, E.M. (2012) 'The hummingbird-2 lightweight authenticated encryption algorithm', in Juels, A. and Paar, C. (Eds.): *RFID. Security and Privacy*, Springer, Berlin, Heidelberg, Vol. 7055, pp.19–31.

Fan, X., Gong, G., Lauffenburger, K. and Hicks, T. (2010) 'FPGA implementations of the hummingbird cryptographic algorithm', *IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, Anaheim, CA, USA, pp.48–51.

Hasan, M.N., Hasan, M.T., Toma, R.N. and Maniruzzaman, M. (2016) 'FPGA implementation of LBlock lightweight block cipher', *3rd International Conference on Electrical Engineering and Information Communication Technology (ICEEICT)*, Dhaka, Bangladesh, pp.1–4.

Hussain, M.A. and Badar, R. (2015) 'FPGA based implementation scenarios of TEA block cipher', *13th International Conference on Frontiers of Information Technology (FIT)*, Islamabad, Pakistan, pp.283–286.

Mishra, Z. and Acharya, B. (2020) 'High throughput and low area architecture of secure IoT algorithm for medical image encryption', *Journal of Information Security and Applications*, Vol. 53, p.102533.

Mishra, Z. and Acharya, B. (2021) 'Efficient hardware implementation of TEA, XTEA and XXTEA ciphers for low resource IoT applications', *International Journal of High Performance Systems Architecture*, Vol. 10, No. 2, pp.80–88.

Mishra, Z. and Acharya, B. (2021) 'High throughput novel architectures of TEA family for high speed IoT and RFID applications', *Journal of Information Security and Applications*, Vol. 61, p.102906.

Mishra, Z., Mishra, S. and Acharya, B. (2020) 'LEA: 128 high frequency architecture with image analysis', *International Conference for Emerging Technology (INCET)*, Belgaum, India, pp.1–5.

Mishra, Z., Nath, P. and Acharya, B. (2021) 'High throughput unified architecture of LEA algorithm for image encryption', *Microprocessors and Microsystems*, Vol. 85, p.104309.

Nedjah, N. and Mourelle, L.D.M. (2007) 'Parallel computation of modular exponentiation for fast cryptography', *Int. J. of High Performance Systems Architecture*, Vol. 1, pp.44–49.

Pandey, J., Goel, T. and Karmakar, A. (2019) 'Hardware architectures for PRESENT block cipher and their FPGA implementations', *IET Circuits Devices & Systems*, Vol. 13, No. 7, pp.958–969.

Ramu, G., Mishra, Z., Singh, P. and Acharya, B. (2020) 'Performance optimised architectures of piccolo block cipher for low resource IoT applications', *International Journal of High Performance Systems Architecture*, Vol. 9, No. 1, pp.49–57.

Rashidi, B. (2020) 'Flexible structures of lightweight block ciphers PRESENT, SIMON and LED', *IET Circuits Devices Syst.*, Vol. 14, No. 3, pp.369–380.

Shrivastava, N. and Acharya, B. (2019) 'FPGA implementation of RECTANGLE block cipher architectures', *International Journal of Innovative Technology and Exploring Engineering*, Vol. 8, No. 10, pp.2382–2391.

Shrivastava, N., Singh, P. and Acharya, B. (2020) 'Efficient hardware implementations of QTL cipher for RFID applications', *International Journal of High Performance Systems Architecture*, Vol. 9, pp.1–10.

Wu, W. and Zhang, L. (2011) 'LBlock: A lightweight block cipher', in Lopez, J. and Tsudik, G. (Eds.): *Applied Cryptography and Network Security*, Vol. 6715, Springer, Berlin, Heidelberg.