Microprocessors and Microsystems 84 (2021) 104267

Contents lists available at ScienceDirect

Microprocessors and Microsystems

journal homepage: www.elsevier.com/locate/micpro

Design and Implementation of Novel BRISI Lightweight Cipher for Resource Constrained Devices

Kiran Kumar V G *, Shantharama Rai C

Department of Electronics and Communication Engineering, College: A J Institute of Engineering and Technology, Kottara, Mangalore, 575006, India

ARTICLE INFO

Index Terms:
Lightweight cryptography
Internet of Things (IoT)
Low Resource Devices (LRD)
BRIGHT Cipher
SIMON cipher

ABSTRACT

The Internet of Things (IoT) and cyber-physical systems (CPS) has grown exponentially over the recent years, has motivated the development and deployment of the low resource devices for a wide range of applications in the IoT. Many such resource constrained devices are deployed to match the heterogeneous application requirements of IoT and CPS systems, wherein privacy and security have emerged, as the most difficult challenges, as the constrained devices are not been designed to have security features. This paper presents a lightweight cipher, based on ARX (Addition-Modulo, Rotation and XOR) operations, Fiestel structure, an amalgamation of BRIGHT and SIMON structure, hence the name BRISI. The cipher encrypts 32-bit plaintext using 64-bit key. The software implementation is performed using MATLAB tool and it fulfils the Avalanche criterion, Key-sensitivity, correlation coefficient, entropy and histogram. The proposed design is simulated using Xilinx Vivado and is implemented on Nexys-4 DDR Artix-7 and Basys-3 Artix-7 FPGA family and is evaluated for (LUT and register) power and timing

1. Introduction

The proliferation of ubiquitous computing has led to a colossal amount of research in the field, hence there has been an increasing demand for the constrained devices in the application like the IoT (Internet of Things) WSNs (wireless sensor networks), RFIDs (radio-frequency identification), smart cards and so on [1]. These constrained devices for such applications have various constraints like the power and area limitations, increased speed and better performance with reduced cost, but the greatest challenge of all is the privacy and security of the data that are exchanged over these devices [2]. With increase in the requirement of security and confidentiality of the data, the demand for cipher implementations for LRDs is increasing. Considering the constraints of these LRDs an optimized cipher implementation in terms of the parameters Area, power and energy is important. In general, a cryptographic algorithm comprises of three main parts: encryption, decryption, and key-generation/key scheduling [2]. The key generation algorithm generates the number of sub-keys based on the number of rounds and key length required for encryption/decryption. In most ciphers, key expansion is executed once for both decryption and encryption, while in others is executed separately for encryption and decryption such as the case in Advanced Encryption Standard (AES) and RIJNDAEL ciphers [1,2]. Based on the number of keys used on encryption/decryption algorithms, ciphers are categorized as asymmetric (public key) and symmetric (private key) ciphers [1].

Cryptographic Ciphers can be symmetric and asymmetric [3]. Symmetric ciphers use same key for encryption and decryption, Asymmetric ciphers use different keys for encryption and decryption. The ciphers for LRDs are often designed for symmetric ciphers. Based on the number of bits encrypted the ciphers are classified as stream ciphers and block ciphers, the stream ciphers encrypt bit by bit or byte, while, the block ciphers encrypt fixed block size plain-text block (16-bits,32-bits, 48-bits and so on). The block ciphers depend on three parameters the size of the block, size of the key and number of rounds. The block ciphers are can be fiestel structure or SPN (Substitution or Permutation Network) or Lai-Massey [4]. Conventional ciphers cannot be embedded in LRDs hence the term lightweight cryptography is used for design of ciphers for LRDs due to the advantages of like (i) lesser number of gates (Area) (ii) lower power and energy consumption (iii) better performance and security [5]. The lightweight ciphers [6] have simple key scheduling, with lesser rounds and smaller block sizes. Hardware implementations of the ciphers are done in the FPGA due to the flexibility, configurability, efficient utilization of resources, and comparatively lower design costs. FPGA implementation of ciphers also provide many other advantages

* Corresponding author.
E-mail address: kiranvgk@gmail.com (K. Kumar V G).

https://doi.org/10.1016/j.micpro.2021.104267
Received 4 November 2020; Received in revised form 26 February 2021; Accepted 6 April 2021
Available online 8 May 2021

like algorithm agility, algorithm upload, algorithm modification

In this paper, an ultra-lightweight cipher based on ARX operation, the BRIGHT family of cipher fused with SIMON cipher, hence the name BRISI Cipher and a highly optimized novel key generation scheme is designed. The BRISI cipher is based on Addition-Modulo, Rotation and XOR Structure (ARX). the Addition-modulo operation introduces the nonlinearity into the cipher while the diffusion is achieved by Rotation and XOR operations.

The objective of this paper is to design, implement and analyse the novel cipher BRISI, as the structure is similar to the SIMON Cipher [7], but with a modified structure so as to improve security, a novel key scheduling is designed and implemented.

2. Background

In the recent years, the need for the Low resource devices (smart devices) has grown widely hence the research of Lightweight Encryption algorithms has gained tremendous interest [1]. Even though the conventional ciphers approved by NIST can be embedded into the low resource devices, their performance may not be acceptable, to overcome this limitation NIST initiated a lightweight cryptography project [8]. The project mentions about the strategies and issues for developing lightweight cryptography, the requirement like the software and hardware in developing the target devices. The report comprises of the evaluation parameters, considerations for design and development of such lightweight cryptographic primitives.

Abed S et al. [9] presented a lightweight SIMON cipher, this cipher emphasizes on the design metrics-power and energy. The SIMON2n/mn, where n-bits and m – key-length. pipelined and scalar implementation of SIMON cipher is implemented. The pipelined implementation has a better throughput by a factor of 12 compared to scalar design. The scalar design consumes 39% lesser power than pipelined design. A 64-bit data path PRESENT block cipher is proposed by Jai Gopal Pandey et al. [10]. The proposed cipher is implemented for 80-bit and 128-bit key length and is area efficient and has better throughput with high MHz clock and consumes 16mW power for a 2000 input vector. The implementation, for an 80-bit key consumes 12.6% lesser FPGA slices and 9.7% lower slices for 128-bit key length than the state of the art benchmarked designs. Saranya Karunamurthi et al [11] presented a cipher based on the reversible logic named RLCD-LFSR (Reversible-logic Cryptography Design-Linear Feedback Shift Register). RLCD logic is used to design both the encryption and decryption units. The cipher is designed using reversible logic gates like Feynman, Fredkin, Toffoli and SCL gates. 128 $\times$ 128 image input-plaintext image is converted into a text-file to binary using MATLAB coding. Key generation is implemented using LFSR. Histogram analysis was performed for security analysis. The hardware implementation was carried out with ASIC 180nm technology using CADENCE tool. The implementation resulted in 7.97% reduction in area, a power reduction of 2.32% and the reduction in delay by 26.4%, the 45nm technology resulted in 9.61% area reduction, and 8.33% of power reduction and 20.46% delay reduction compared with the state of the art implementations. UBRIGHT or ULTRABRIGHT, presented by Deepti Sehrawat et al [12] is an ultralight weight cipher, the key features of the cipher are key whitening, enhanced security, better diffusion, optimized register usage. The algorithm is based on fiestel structure. The algorithm is implemented in four layers (i) key whitening (ii) ARX operation (iii) permutation (iv) final key whitening. The algorithm is executed on an Intel (R) processor Core (TM) i5-2430M CPU @ 2.20 GHz. The algorithm obeys Strict Avalanche Criteria with 50% diffusion. The key sensitivity is achieved. The algorithm also passes all the Randomness tests. The algorithm requires a Memory utilization of 477 bytes and 479 bytes for encryption and decryption respectively, the execution time required is 52.21 Mb/s. GRANULE a new ultra-light cipher, designed by Gaurav Bansod et al [13], based on Fiestel network. the algorithm encrypts 64-bit plaintext using 80/128-bit key in 32 rounds. The cipher has proved resistance for linear and differential cryptanalysis. The GRANULE cipher shows better resistance against various kinds of attacks performed on the cipher. It has good resistance against linear and differential cryptanalysis. GRANULE 2104 bytes of Flash memory1256 bytes of a RAM Memory when implemented in C. The cipher is implemented in FPGA consumes 1288 for 80-bit key encryption and 1577 for 128-bit key encryption thus consumes lesser power by 12-79% when compared to available algorithms literature. Hence making it suitable for low resource devices. VAYU, a lightweight cipher presented by Gaurav Bansod [13], uses 80/128-bit key to encrypt 64-bit plaintext in 31 rounds. The cipher is implemented in ARM-7 LPC2129 processor the proposed cipher requires lesser memory, GE compared to PRESENT, CLEFIA, AES and LED cipher. An improved advanced encryption standard (IAES) is proposed by Celestine Iwendi et. al.[14] In this method both the user and the data in the IoT network provides improved privacy preservation strategies. In this research IoT devices and the 5G architecture issues are addressed by the PDS (PRIVACY DATABASE STRUCTURE). The proposed algorithm is compared with AES and DES algorithms. The proposed algorithm performs better than the AES and DES in terms of the performance parameters like the throughput and execution time for encryption. A lightweight selective encryption scheme presented by Amna Shifa et.al [15] proposes an ESR-validated encryption scheme. Two entropy encoders for the H.264/AVC codec like CABAC and AVLC are examined for Internet of Multimedia Things devices. The Encryption space ratio is determined by applying the proposed Selective Encryption with the proposed cipher to encrypt the selected syntax elements. The proposed method has an ESR percentage of 14.14% for CABAC scheme while 31.23% is achieved for CAVLC scheme. the novel cipher EXPer which is based on permutation and EXOR operations using 128-bit key found to perform well on absolute values of syntax elements like the dQP. The bitrate and decoder remains unchanged. The proposed EXPer algorithm is compared with the state of the art implementation, the confidentiality of the algorithm is similar to that of AES-CFB while the computational cost is similar to XOR, thus ensuring it a suitable for real-time video communication for IoT devices

3. The proposed BRISI cipher

A software-based block cipher implementation benchmarking frame work termed as FELICS (FAIR EVALUATION OF LIGHTWEIGHT CRYPTOGRAPHIC SYSTEMS) was held by The University of Luxembourg in 2015 [24]. This framework aims at implementing the algorithms in low-resource devices like the IoT applications [30–36]. LEA, HIGHT [25] and SIMON [29] were some of the top ranked ciphers of the competition. These ciphers are based on ARX (ADDITION, ROTATION AND EX-OR) operations. Compared to SPN (SUBSTITUTION AND PERMUTATION NETWORKS) based structure, ARX based structure has better performance and are comparatively faster and consumes lesser area and power [28]. The software implementations are also comparatively cheaper. The ARX structure offers better confusion and diffusion property and hence resistant to timing attacks.

The proposed BRISI cipher is a ARX based balanced Feistel Structure, symmetric key block cipher. It encrypts the plain-text of block size 32-bits using an initial key of 64-bits length and consists of 5 rounds. Lesser number of rounds are chosen so as to improve efficiency; the number of rounds can be increased so as to improve security. The 16-bit round key ki required for encryption is extracted from a novel key generation scheme which is consists of a 64-bit initial key.

For the proposed cipher the following notations are used

PT - input plaintext of block size 32-bits.

CT - output cipher-text block size 32-bits.

Ri, Li - Right half and left half bits.

K - initial Input-Key 64-bits. ki - sub-keys of 16-bits each for one round.

$\oplus$ - Bitwise exclusive-OR operation

$\boxplus$ - Addition-modulo n

⊗ - Multiplication-modulo n
<<< - p-bits Left Circular shift
|| - Concatenation of bits/registers

3.1. Round function

The one round encryption process for the proposed ARX based BRISI cipher comprises of following operations

- Addition-Modulo-n
- Rotation/Left-circular shift, (Si by i bits)
- Bitwise-EXOR

Figure 1 shows the one-round function of the proposed BRISI cipher, the plain text input block is 2n and its split into two halves of n-bit each as Left n-bits Li and Right n-bits Ri. In each round function, three circular shifts to the lefts (shift-left one, shift-left eight, and shift-left two) and bitwise-XOR and Addition-modulo operation with Key are performed on the plain-text.

The ARX based BRISI round encryption function, F, is represented in Equation (1).

$$F(R,L,k) = ((Ls1 \oplus Ls8) \oplus R0) \oplus Ls2) \boxplus Ki) \parallel L0 \quad (1)$$

where Ki is the round key, L0 is the leftmost bits of the plaintext block, and R0 is the rightmost bits.

Steps: In this paper a 32-bit plain-text is encrypted using a 64-bit initial-key

The 32-bit input plain-text is partitioned into two blocks of 16-bits each, With Left half bits L0 and right half bits as R0

1 The left half bits are shifted by 1-bit (Ls1) and eight-bits (Ls8) and XORing is performed the result is Ls18.
2 Ls18 is XORed with R0 and the output is R01.
3 Left half bits are shifted by 2 bits (Ls2) and XORed with R01 the output is R02.
4 Then R02 is XORed with the round Key Ki with output as RR0.
5 The Left half and right half are swapped.

The proposed BRISI cipher is based on ARX operations and thus the cipher can be implemented in parallel, more efficiently compared to other type of operations so that the diffusion may be performed faster.

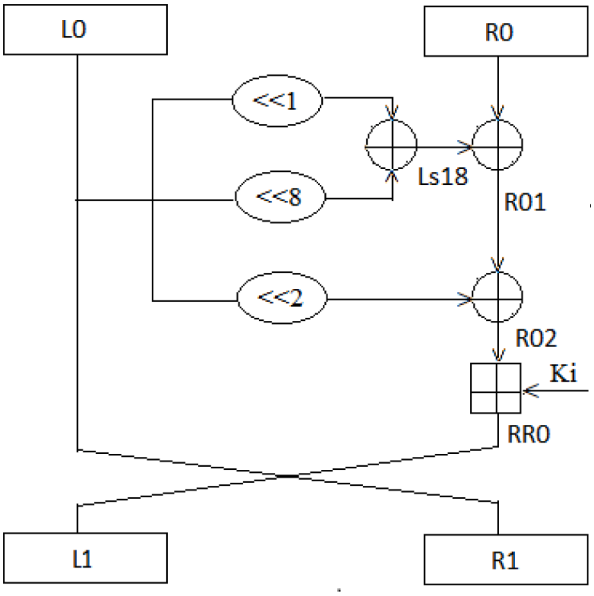


Fig. 1.. The BRISI one round function.

The addition-modulo operation using key, provides the non-linear operation on the cipher-text. The shift operation or permutation of bits and the swapping operation also provides the diffusion thus the Shannon's property of confusion and diffusion has been implemented for the cipher making the encryption scheme more secured [3].

3.2. Key scheduling

The design of a Key generation scheme is the most vital part of any cipher system. The information is rendered secure if an intelligible the key is generation scheme is designed [26,27]. If an adversary predicts the key, the encryption system would be rendered useless.

Since the algorithm requires five keys of 16-bit each from a 64-bit initial input key. A novel key generation key scheme shown in figure 2, inspired from the Simple Encryption scheme for Internet of Things [17,18] is implemented. The key expansion unit comprises of Permutation, Shift, XOR operations so as to create confusion and diffusion in the input key which makes it more secure so as to prevent from attacks.

3.3. Key expansion steps

1 The initial input key is split up into 4-bit each segment. (ki1,ki2, ki3…..,ki16).
2 Initial permutation of bits input bits

(ie kp1=ki1||ki5||ki9||ki13)
(ie kp2=ki2||ki6||ki10||ki14)
(ie kp3=ki3||ki7||ki11||ki15)
(ie kp4=ki4||ki8||ki12||ki16)

1 Left shift by i bits (kx1 = kp1<<5, kx2 = kp2<<3 kx3 = kp3<<5, kx4=kp4<<3);
2 Perform an XOR operation to get the round keys

k1 = kp1⊕kx1, k2 = kp2⊕kx2, k3 = kp3⊕kx3, k4 = kp4⊕kx4 and k5 = k1⊕k2⊕k3⊕k4.

4. Hardware and software implementation and results

The proposed BRISI Cipher has been implemented both in software and hardware [37,38] to evaluate the cipher the following criteria are considered.

4.1. Key generation

For the proposed key generation scheme, 10^6 bit streams were generated and the NIST randomness tests [43] were run with a significance level $P \geq 0.01$ on the sequences of the generated output to accept the sequences as random. The table 1 shows the results of the P value for the NIST randomness tests, it is found that all the P values are greater than 0.01 hence the generated bits are random in nature.

4.2. Software implementation of the BRISI cipher

The software implementation [39–42] of the proposed cipher is performed in MATLAB tool

4.2.1. Histogram analysis

To visualize the security strength of a cryptographic algorithm histogram analysis is performed. The randomness of the encrypted image is measured. The encryption is performed on the images shown in figure 3a, 3b, 3c concludes that the calculated histogram is uniform hence the algorithm is secured.

4.2.2. Correlation coefficient

is a technique to measure the strength of a cryptographic algorithm.

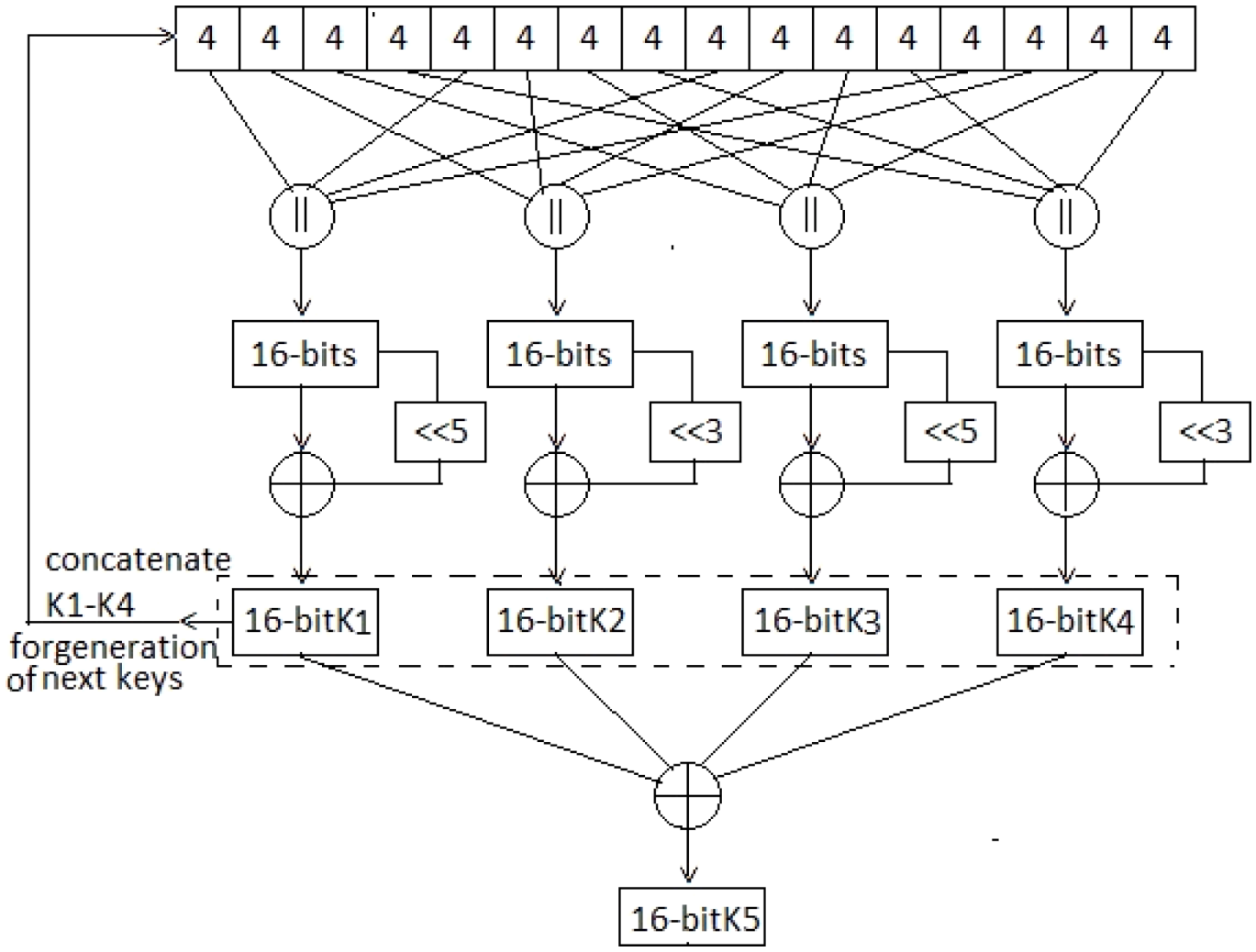


Fig. 2.. Key generation process.

Table 1.
NIST test results of proposed Key generation scheme.

Test	P-value	Result
Frequency	0.534146	Passed
Block Frequency	0.739918	Passed
Cumulative Sums(forward)	0.534146	Passed
Cumulative Sums(inverse)	0.035174	Passed
Runs	0.534146	Passed
LongestRun	0.911413	Passed
Rank	0.937229	Passed
FFT	0.350485	Passed
Non-Overlapping Template	0.017912	Passed
Overlapping Template	0.213309	Passed
Universal	0.350485	Passed
Approximate Entropy	0.739918	Passed
Random Excursions	0.035174	Passed
Random Excursions Variant	0.739918	Passed
Serial	0.911413	Passed
Linear Complexity	0.534146	Passed

it is the dependency between two values.

The correlation coefficient between any two adjacent pixel pairs can be calculated as

$$cov(p,q) = \frac{1}{N}\sum_{i=1}^{N}(p_i - E(p))(q_i - E(q))$$

$$r_{pq} = \frac{cov(p,q)}{\sqrt{D(p)}\sqrt{D(q)}}$$

here p and q are the values of two adjacent image pixels.

$$E(p) = \frac{1}{N}\sum_{i=1}^{N} p_i$$

$$D(p) = \frac{1}{N}\sum_{i=1}^{N}(p_i - E(p))^2$$

The figures 3a, 3b and 3c concludes that the encrypted images highly correlated, hence the algorithm is secured.

4.2.3. *Image entropy*

Entropy refers to the amount of data to be coded by a cipher.
It is calculated using the formula

$$\textbf{\textit{Entropy}} = \sum \boldsymbol{p}_i(\boldsymbol{i})\log_2\left(\frac{1}{\boldsymbol{p}_i(\boldsymbol{i})}\right)$$

Where pi denotes the probability of the ith pixel value of the image
The table 2 lists the correlation coefficient and entropy, it is found that correlation of the encrypted images is nearer to zero, and the information entropy of the encrypted images $7.9 < E < 8$. Thus infers that attacks are infeasible and the plaintext is secured.

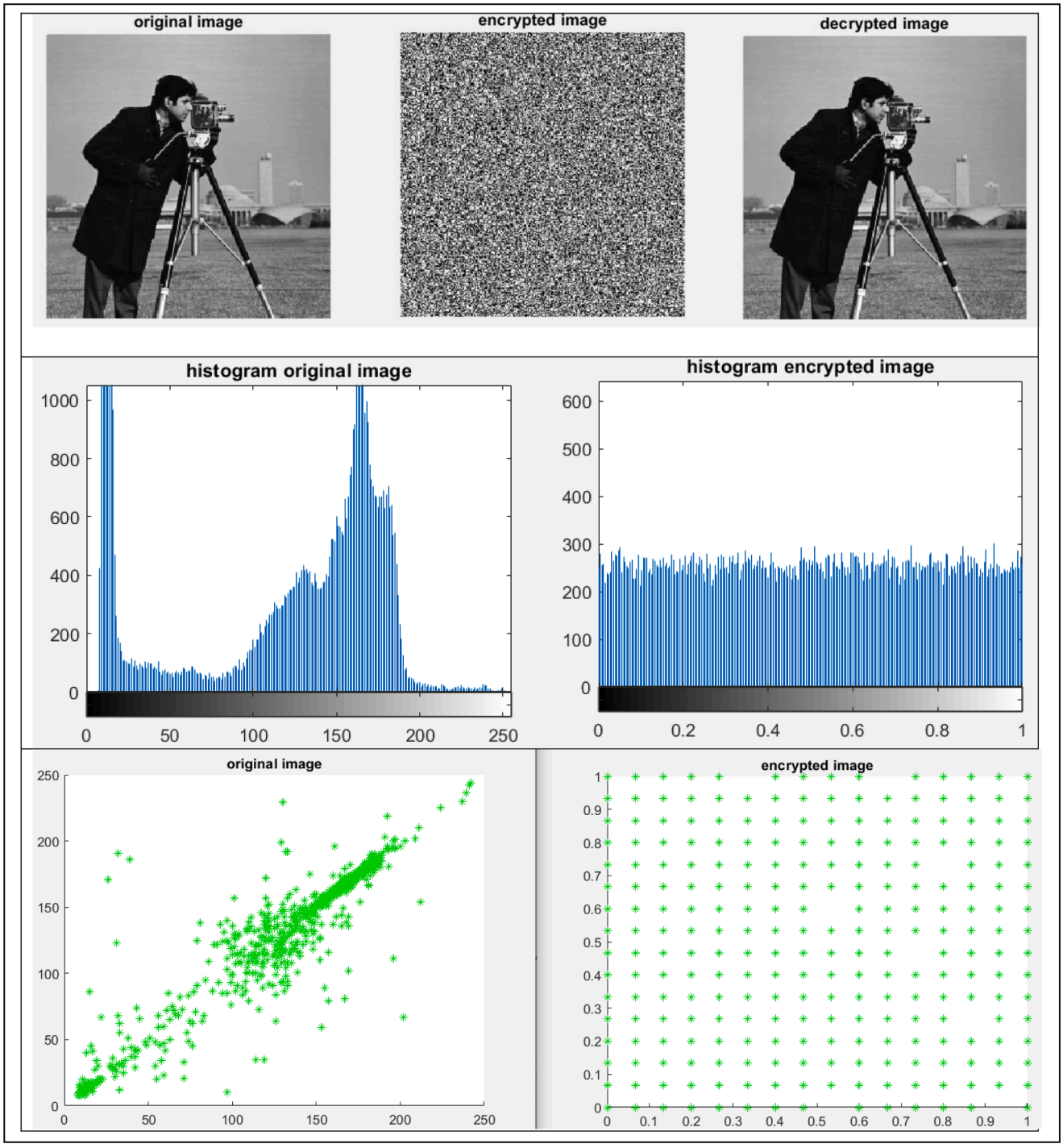


Fig. 3a. Image Encryption, Histogram and correlation coefficient of Cameraman Image.

4.2.4. *Avalanche effect*

Avalanche effect is one of the desirable property in cryptography. A one-bit change in the input (plain-text or key) causes a considerable change in the output cipher-text as depicted in figure 4 and 5. A one-bit change in the plaintext with key constant causes a considerable change in cipher-text, figure 4a shows both the input and output in binary while figure 4b shows the input and output data in hexadecimal.

4.2.5. *Key sensitivity*

For a one-bit change in the key with plaintext constant there is a considerable change in the cipher-text shown in figure 5a both plaintext and cipher text in binary form while figure 5b the plaintext and cipher text is in hexadecimal form. A radical change in cipher-text is observed with single bit change in key or the plaintext as seen above for a robust block cipher design. if the block cipher does not show the avalanche effect then such a block cipher is said to have a poor randomization [16]. From the figures 4 and 5 it is found that a single bit change in the input (plain-text or key) results in change of 50% cipher text *i.e.*, more than half of the bits of cipher-text is changed.

4.3. *Hardware implementation of the BRISI cipher*

The proposed BRISI cipher is simulated using Xilinx Vivado and verified on the Nexys-4 Artix-7 and Basys-3 Artix-7 FPGA.

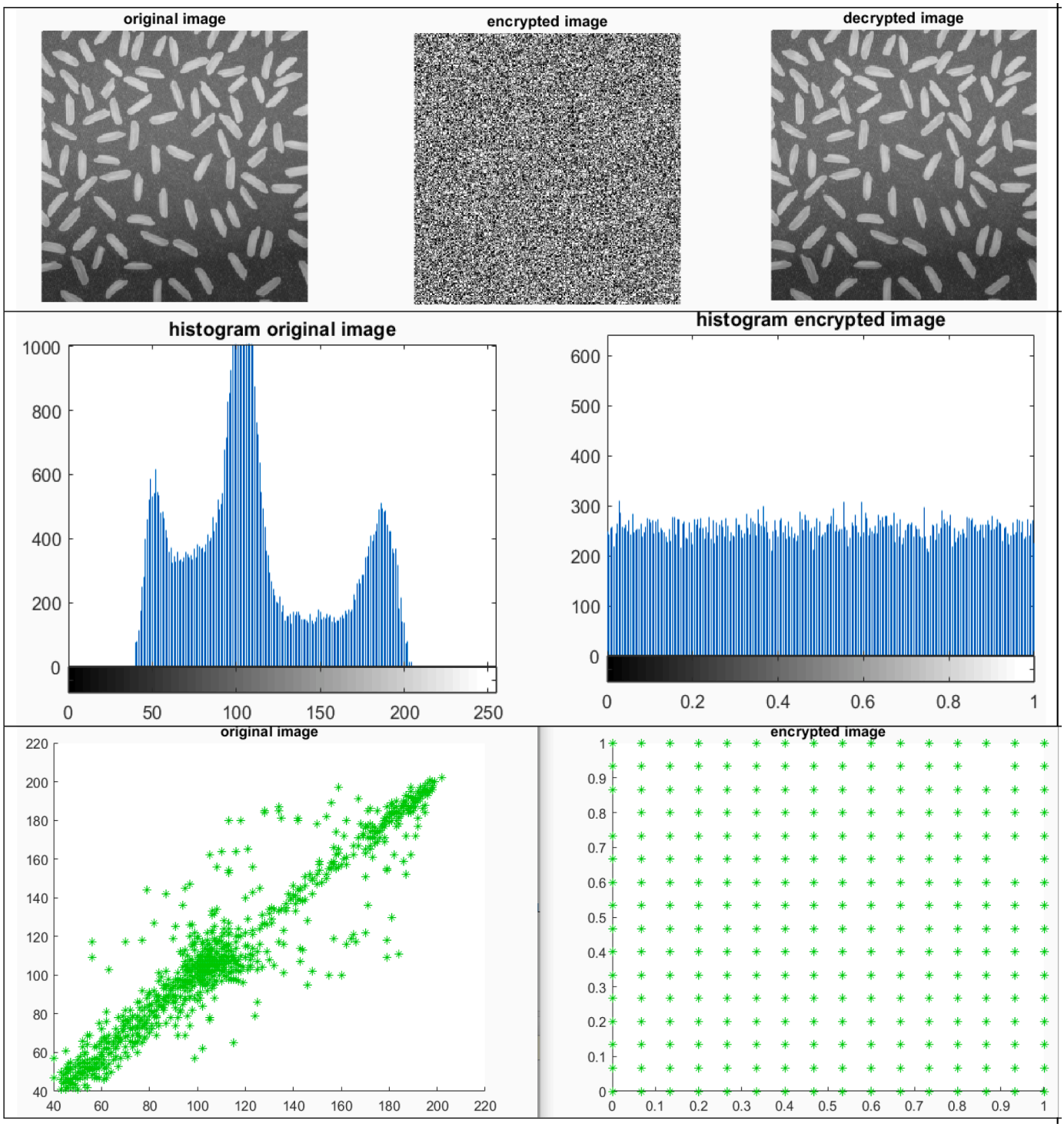


Fig. 3b. Image Encryption, Histogram and correlation coefficient of rice Image.

Figure 6 shows the RTL schematic for one round encryption process of BRISI Cipher.

Table 3 shows the FPGA implementation of the proposed ciphers in terms of LUTs, IOBs.

The comparative analysis of the Proposed BRISI encryption algorithm with the State of the art implemented algorithms is shown in table 4 and figure 7 the comparison chart

5. Conclusion and future work

The implementation of cryptographic algorithms in the Low resource devices will play a dominant role and will be a major challenge in the near future. This paper proposes a simple ARX based BRISI cipher for low resource devices and the proposed cipher has been analysed for Entropy, Correlation coefficients Histogram, Strict Avalanche Criterion and Key Sensitivity. It thus fulfils all the criteria for proving the security of the proposed algorithm. The hardware implementation of the cipher is analysed for area, power and timing, it infers that it is efficient when

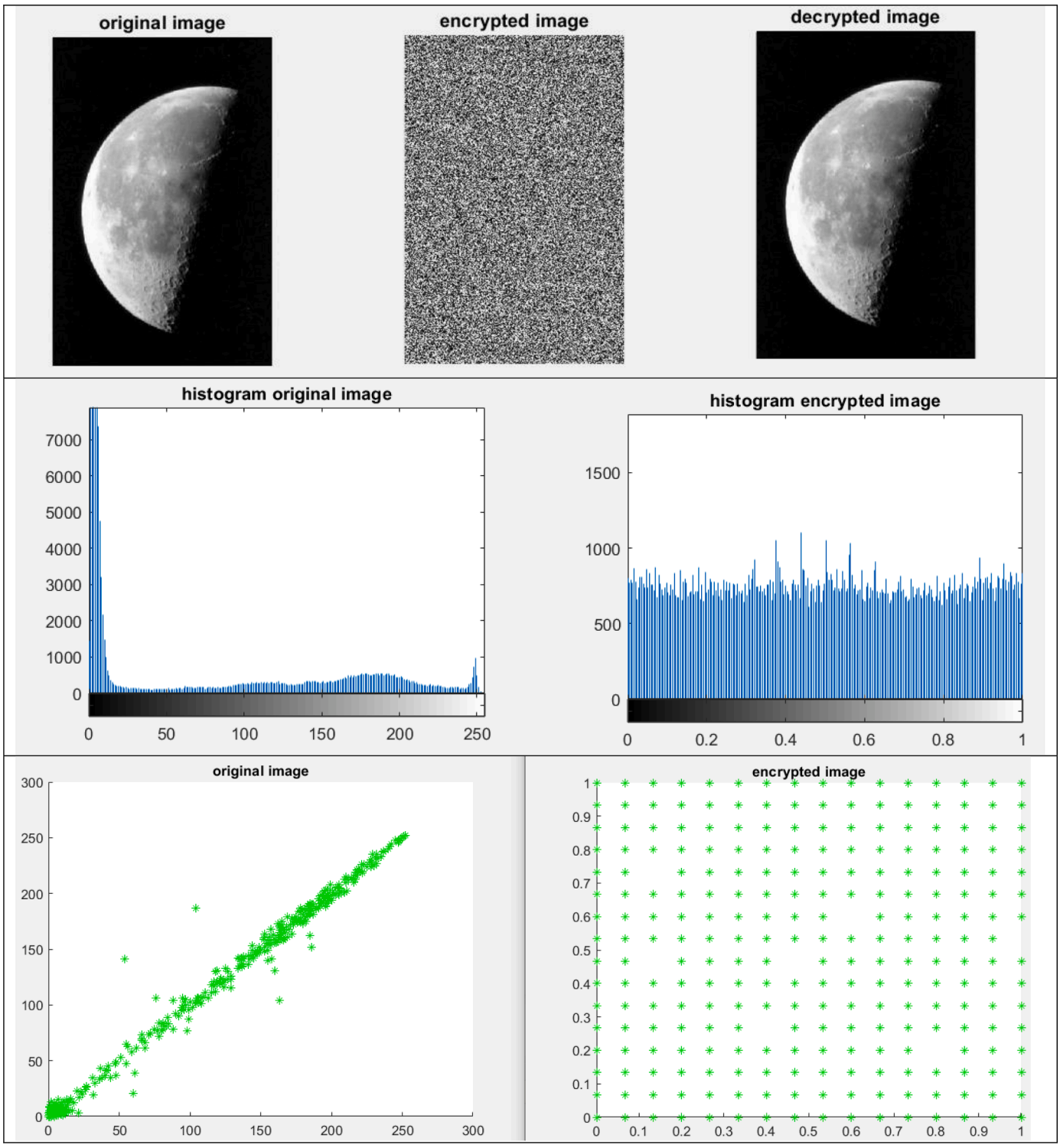


Fig. 3c. Image Encryption, Histogram and correlation coefficient of moon Image.

Table 2
Correlation and entropy of the test images.

Test Image	Correlation coefficient		Information Entropy	
	Original	Encrypted	Original	Encrypted
Cameraman	0.9840	-0.0374	7.0098	7.9967
Coins	0.9687	-0.0089	6.3162	7.9966
Moon	0.9983	0.0281	5.5128	7.9932
Rice	0.9227	-0.0023	7.0116	7.9964

compared to the state of the art implementations, thus the proposed algorithm can be suited for the Low resource devices. In this paper a 32-bit cipher using 64-bit key using 5 rounds is implemented, the future work, the number of rounds can be increased so as to strengthen the security and also input plain-text and keys can be increased. Also the attacks can also be performed.

Fig. 4a. One-bit change in plain-text in binary format.

Fig. 4b. One-bit change in plain-text in hexadecimal format.

Fig. 5a. One-bit change in input key in binary format.

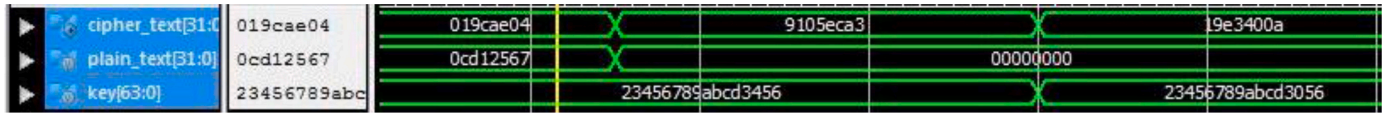
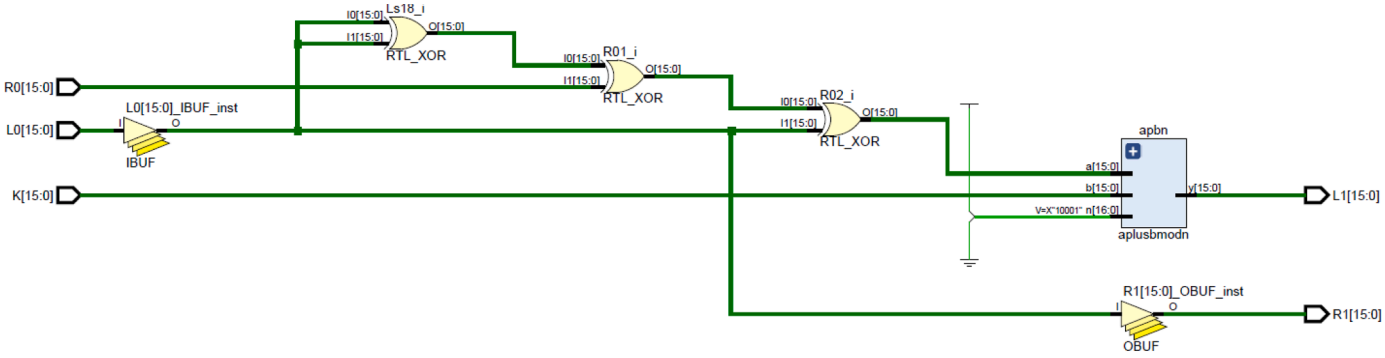


Fig. 5b. One-bit change in input key in hexadecimal format.



One round Encryption of BRISI Cipher.

Fig. 6. One round Encryption of BRISI Cipher.

Table 3
FPGA implementation of the proposed BRISI encryption algorithm.

FPGA Family	Slice LUTs+ Registers	IOBs	Power(W)	Timing(ns)
Nexus-4 DDR Artix-7	45+15	80	21.164	13.068
Basys- 3 Artix-7	45+15	80	21.164	13.068

Power and timing.

Table 4
Comparative analysis of the BRISI encryption algorithm.

Algorithm	Year	Slice LUT	Slice Registers	Timing (nS)	FPGA
Saranya K et al [11] LFSR +Rev Logic	2019	25	11	1.314	Virtex-7
A. Alkamil et al [19] SIMON cipher	2019	570	594	13.65	Virtex -6
Korobeynikov [20] Kuznyechik cipher	2019	2713	-	3.03	Arria-10
Um e Rabab et al [21] SIT	2018	711	796	12.11	Cyclone-II
Sruthi.N et al [22] HIGHT	2016	2689	2409	8.34	Spartan-6
Zeesha Mishra LEA [23]	2019	360	382	4.44	Virtex-5
Proposed BRISI	2020	45	15	13.068	Artix-7

Declaration of Competing Interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:

(i) Mr Kiran Kumar V G, Assistant Professor Department of Electronics and Communication, A J Institute of Engineering and Technology Mangaluru India

(ii) Dr Shantharama Rai C, Professor Department of Electronics and

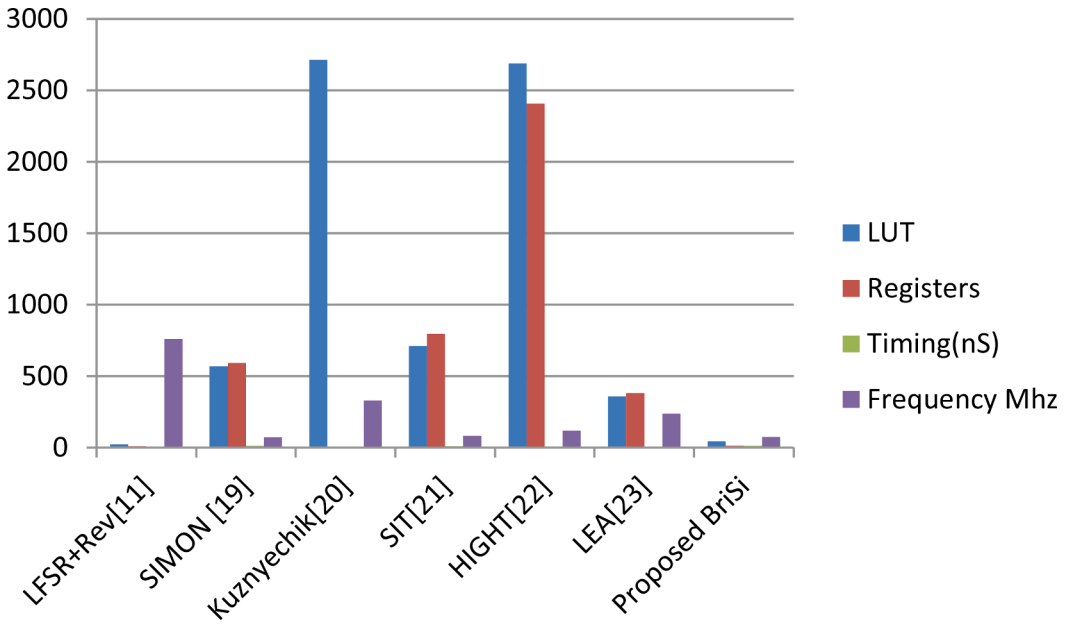


Fig. 7. Comparison of the various cipher with the proposed ciphers.

Communication, A J Institute of Engineering and Technology Mangaluru India.

Acknowledgements

The authors would like to thank the Department of Electronics and Communication and Engineering, Canara Engineering College Mangalore and Visvesvaraya Technological University, Belagavi for the support for carrying out the research work.

References

[1] B.J. Mohd, T. Hayajneh, A.V. Vasilakos, A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues, J. Netw. Comput. Appl. 58 (2015) 73–93.
[2] S. Li, H. Song, M. Iqbal, Privacy and Security for Resource-Constrained IoT Devices and Networks: Research Challenges and Opportunities, Sensors 19 (2019) 1935.
[3] W. Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall, Inc., Upper Saddle River, New Jersey, 2005.
[4] X. Fan, K. Mandal, G. Gong, Wg-8: A lightweight stream cipher for resource-constrained smart devices, in: International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, 115, Springer, Berlin/Heidelberg, Germany, 2013, pp. 617–632.
[5] G. Hatzivasilis, K. Fysarakis, I. Papaefstathiou, et al., A review of lightweight block ciphers, J Cryptogr Eng 8 (2018) 141–184, https://doi.org/10.1007/s13389-017-0160-y.
[6] M. Cazorla, K. Marquet, M. Minier, Survey and benchmark of lightweight block ciphers for wireless sensor networks, in: Proceedings of the 2013 International Conference on Security and Cryptography (SECRYPT), Reykjavik, Iceland, 2013, pp. 1–6, 29–31 July.
[7] S. Abed, R. Jaffal, B.J. Mohd, M. Alshayeji, FPGA Modeling and Optimization of a SIMON Lightweight Block Cipher, Sensors 19 (2019) 913.
[8] Kerry A. McKay, Marry Bassham, Meltem Sönmez Turan, Nicky Mouha, DRAFT NISTIR 8114 Report on Lightweight Cryptography", National Institute of Standards and Technology Internal Report 8114 (2016). August.
[9] S Abed, R Jaffal, BJ Mohd, M. Alshayeji, FPGA Modeling and Optimization of a SIMON Lightweight Block Cipher, Sensors (Basel) 19 (4) (2019) 913, https://doi.org/10.3390/s19040913. Published 2019 Feb 21.
[10] J.G. Pandey, T. Goel, A. Karmakar, A High-Performance and Area-Efficient VLSI Architecture for the PRESENT Lightweight Cipher, in: 2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID), Pune, 2018, pp. 392–397, https://doi.org/10.1109/VLSID.2018.96.
[11] Karunamurthi Saranya, Vijeyakumar Krishnasamy Natarajan, VLSI implementation of reversible logic gates cryptography with LFSR key, Microprocess. Microsyst. 69 (2019) 68–78.
[12] Deepti Sehrawat, Nasib Gill, Ultra BRIGHT: A Tiny and Fast Ultra Lightweight Block Cipher For IoT, International Journal of Scientific & Technology Research 9 (2020) 1063.
[13] Gaurav Bansod, Abhijit Patil, Narayan Pisharoty, GRANULE: An Ultra lightweight cipher design for embedded security, IACR Cryptol. ePrint Arch. 2018 (2018) 600.
[14] J.H. Anajemba, C. Iwendi, M. Mittal, T. Yue, Improved Advance Encryption Standard with a Privacy Database Structure for IoT Nodes, in: 2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT), Gwalior, India, 2020, pp. 201–206, https://doi.org/10.1109/CSNT48778.2020.9115741.
[15] A. Shifa, M.N. Asghar, S. Noor, N. Gohar, M. Fleury, Lightweight Cipher for H.264 Videos in the Internet of Multimedia Things with Encryption Space Ratio Diagnostics, Sensors 19 (2019) 1228, https://doi.org/10.3390/s19051228.
[16] G. Bansod, A new lightweight encryption design at node level, International Journal of Security and Its Applications 10 (12) (2016) 111–128 (2016).
[17] Sohel Rana, Saddam Hossain, Hasan Imam Shoun, Dr.Mohammod Abul Kashem, An Effective Lightweight Cryptographic Algorithm to Secure Resource-Constrained Devices, International Journal of Advanced Computer Science and Applications (IJACSA) 9 (11) (2018), https://doi.org/10.14569/IJACSA.2018.091137.
[18] M Usman, I Ahmed, MI Aslam, S Khan, UA Shah, SIT: a lightweight encryption algorithm for secure internet of things, 2017 arXiv preprint arXiv:1704.08688.
[19] Alkamil, D.G. Perera, Efficient FPGA-Based Reconfigurable Accelerators for SIMON Cryptographic Algorithm on Embedded Platforms, in: 2019 International Conference on ReConFigurable Computing and FPGAs (ReConFig), Cancun, Mexico, 2019, pp. 1–8, https://doi.org/10.1109/ReConFig48160.2019.8994803.
[20] A. Korobeynikov, Effective Implementation of "Kuznyechik" Block Cipher on FPGA with OpenCL Platform, in: 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 2019, pp. 1683–1686.
[21] U.E. Rabab, I.U. Ahmed, M.I. Aslam, M. Usman, FPGA Implementation of Secure Internet of Things (SIT) Algorithm for High Throughput Area Ratio, International Journal of Future Generation Communication and Networking Vol. 11 (5) (2018) 63–72.
[22] N. Sruthi, R. Nandakumar, P. Rajkumar, ***Design and characterization of HIGHT cryptocore***, in: 2016 *International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)*, Paralakhemundi, 2016, pp. 205–209.
[23] Z. Mishra, G. Ramu, B. Acharya, Hight Speed Low Area VLSI Architecture for LEA Encryption Algorithm, in: V. Nath, J. Mandal (Eds.), Proceedings of the Third International Conference on Microelectronics, Computing and Communication Systems. Lecture Notes in Electrical Engineering 556, Springer, Singapore, 2019, https://doi.org/10.1007/978-981-13-7091-5_14.
[24] R Gupta, A Pandey, RK Baghel, FPGA implementation of chaos-based high-speed true random number generator, Int J Numer Model 32 (2019) e2604, https://doi.org/10.1002/jnm.2604.
[25] Bohun Kim, Junghoon Cho, Byungjun Choi, Jongsun Park, Hwajeong Seo, Compact Implementations of HIGHT Block Cipher on IoT Platforms, Security and Communication Networks (2019), https://doi.org/10.1155/2019/5323578. Article ID 532357810 pages, 2019.
[26] Wu Xufan, Li Shuguo, A new digital true random number generator based on delay chain feedback loop, in: IEEE conference, 2017, 978-1-4673-6853-7/17/$31.00.
[27] P Choi, M-K Lee, DK Kim, Fast compact true random number generator based on multiple sampling, Electron. Lett. 53 (13) (2017) 841–843.
[28] V.G Kiran Kumar, C. Shantharama Rai, FPGA Implementation of Simple Encryption Scheme for Resource-Constrained Devices, International Journal of Advanced Trends in Computer Science and Engineering 9 (4) (2020), https://doi.org/10.30534/ijatcse/2020/213942020. July – August.

[29] R. Beaulieu, S. Treatman-Clark, D. Shors, B. Weeks, J. Smith, L. Wingers, The SIMON and SPECK lightweight block ciphers, in: 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, CA, 2015, pp. 1–6, https://doi.org/10.1145/2744769.2747946.
[30] W. Zhang, Z. Bao, D. Lin, et al., RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms, Sci. China Inf. Sci. 58 (2015) 1–15, https://doi.org/10.1007/s11432-015-5459-7.
[31] C.O. Iwendi, A.R. Allen, Enhanced security technique for wireless sensor network nodes, in: IET Conference on Wireless Sensor Systems (WSS 2012), London, 2012, pp. 1–5, https://doi.org/10.1049/cp.2012.0610.
[32] Wajih El Hadj Youssef, Ali Abdelli, Fethi Dridi, Mohsen Machhout, Hardware Implementation of Secure Lightweight Cryptographic Designs for IoT Applications, in: Security and Communication Networks 2020, 2020, p. 13 pages, https://doi.org/10.1155/2020/8860598. Article ID 8860598.
[33] Pei Li, Shihao Zhou, Bingqing Ren, Shuman Tang, Ting Li, Chang Xu, Jiageng Chen, Efficient implementation of lightweight block ciphers on volta and pascal architecture, Journal of Information Security and Applications 47 (2019) 235–245, https://doi.org/10.1016/j.jisa.2019.04.006. ISSN 2214-2126.
[34] Sandip Dutta Nayancy, Soubhik Chakraborty, A survey on implementation of lightweight block ciphers for resource constraints devices, Journal of Discrete Mathematical Sciences and Cryptography (2020), https://doi.org/10.1080/09720502.2020.1766764.
[35] Jamil Mohd Bassam, Thaier Hayajneh, Khalil M.Ahmad Yousef, Zaid Abu Khalaf, Md Zakirul Alam Bhuiyan, Hardware design and modeling of lightweight block ciphers for secure communications, Future Generation Computer Systems 83 (2018) 510–521, https://doi.org/10.1016/j.future.2017.03.025. ISSN 0167-739X.
[36] D. Sehrawat, N.S. Gill, M. Devi, Comparative Analysis of Lightweight Block Ciphers in IoT-Enabled Smart Environment, in: 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), 2019, pp. 915–920, https://doi.org/10.1109/SPIN.2019.8711697. Noida, India.
[37] W Gong, P Choi, DK Kim, Hardware implementation of lightweight block ciphers for IoT sensors, Journal of Semiconductor Technology and Science 20 (4) (2020) 381–389, https://doi.org/10.5573/JSTS.2020.20.4.381.
[38] M.S. Rohmad, A. Saparon, H. Amaran, N. Arif, H. Hashim, Lightweight block cipher on VHDL, in: 2017 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), Langkawi, 2017, pp. 87–90, https://doi.org/10.1109/ISCAIE.2017.8074955.
[39] P.K.R. Maddikunta, T.R. Gadekallu, R. Kaluri, G. Srivastava, R.M. Parizi, M. S. Khan, Green communication in IoT networks using a hybrid optimization algorithm, Comput. Commun. 159 (2020) 97–107.
[40] M. Henriques, N. Vernekar, Using symmetric and asymmetric cryptography to secure communication between devices in IoT, in: 2017 IEEE International Conference on IoT and Application (ICIOT), Nagapattinam, India, June 2017.
[41] Ankit Shah, M. Engineer, A survey of lightweight cryptographic algorithms for IoT-based applications, Advances in Intelligent Systems and Computing 851 (2019) 283–293.
[42] R. Benadjila, J. Guo, V. Lomné, T. Peyrin, Implementing lightweight block ciphers on x86 architectures, in: Proceedings of the Selected Areas in Cryptography (SAC), Lecture Notes in Computer Science 8282, Springer, Berlin, Heidelberg, August 2013.
[43] E.B. Smid, S. Leigh, M. Levenson, M. Vangel, A.David Banks, S.James Dray, A statistical test suite for random and pseudorandom number generators for cryptographic applications, 2010 [online] Available: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf.