International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Cryptographic Strength in Resource-Constrained IoT: XTEA vs. RECTANGLE

Ramya K. V.*[1], Dr. Manjunatha Reddy H. S.[2], Bharathi C.[3], Mamata Dhananjaya[4]

Submitted: 04/10/2023 **Revised**: 23/11/2023 **Accepted**: 04/12/2023

Abstract: This paper introduces two prominent lightweight ciphers: XTEA and RECTANGLE. The exposition provides a detailed elucidation of their respective design principles, security features, and suitability for IoT applications. It is essential to comprehend how these ciphers operate, and this section affords readers a comprehensive insight into their inner workings.

The study takes a pivotal turn as we assess the hardware implementation metrics of both ciphers on an FPGA platform. This assessment reveals the resource efficiency of each cipher, with RECTANGLE emerging as the more resource-friendly choice. Such evaluations are vital in enabling informed decisions when selecting cryptographic solutions for resource-constrained environments.

An indispensable facet of this study revolves around the evaluation of randomness, a paramount factor in cryptographic security. To accomplish this, we employ the NIST Test Suite to scrutinize the randomness exhibited by both XTEA and RECTANGLE. The outcomes of these tests provide valuable insights into the cryptographic strength of each cipher. Notably, XTEA demonstrates superior randomness in certain tests, including the Linear Complexity Test, showcasing its unique attributes.

In conclusion, this paper underscores the pivotal role of lightweight cryptography in fortifying the security of IoT and IoE ecosystems. Through a meticulous comparative analysis of two prominent lightweight ciphers, it offers invaluable insights for researchers and practitioners navigating the complex landscape of interconnected devices and services. The findings of this study contribute significantly to the ongoing discourse surrounding the delicate equilibrium between security imperatives and the resource constraints inherent to IoT environments.

Keywords: *VIVADO, RECTANGLE, XTEA, NIST, Randomness*

1. Introduction

In current society, the human face plays an important function in The Internet of Things (IoT) functions within a virtual domain where physical entities can be located and addressed within a network. These entities possess knowledge of their real-world conditions and could perform independent actions. The notion of IoT has progressed into what is now referred to as the "Internet of Everything" (IoE), which encompasses a diverse array of entities, services, and individuals. IoT is also recognized as Smart Objects Networks, which connect devices that have limited resources. The accessibility to network resources is facilitated through protocols such as IPv6 and 6LoWPAN.

The Internet of Security is an issue of utmost importance in the realm of IoT owing to the possible network-wide consequences that can arise from the compromise of a single device. Nevertheless, IoT devices possess certain limitations including processing power, memory, connectivity, and energy, thereby posing a challenge to the There exist two primary classifications of cryptographic algorithms: symmetric and asymmetric. Symmetric key ciphers are frequently utilized in the context of the Internet of Things (IoT) for the purposes of authentication, confidentiality, and integrity To cryptography has emerged as a viable solution, specifically tailored for resource-constrained environments. This approach to cryptography strikes a balance between security and efficiency.

verification. However, the development of efficient algorithms for IoT devices can pose a challenge due to their limited available resources.

Lightweight cryptography holds particular significance when it comes to ensuring secure communication between interconnected IoT objects. By providing security measures that do not overly strain the constrained resources of these devices, lightweight cryptography guarantees the reliable operation of interconnected devices and services within the ever-evolvi ng realm of the Internet of Everything.

In this paper, we are comparing two lightweight ciphers XTEA and RECTANGLE which have SPN and Feistel structure respectively. First the ciphers are compared on their hardware utilizations factors and then the strength of the ciphers are compared by measuring their randomness.

Paper is organized as follows, section II discusses about SPN and Feistel structures used in lightweight ciphers. In

[1] *Dept of ECE, Global Academy of Technology, Visvesvaraya Institute of Technology, Belagavi 590018*
[2] *Dept of ECE, Global Academy of Technology, Visvesvaraya Institute of Technology, Belagavi 590018*
[3] *Dept of ECE, Global Academy of Technology, Visvesvaraya Institute of Technology, Belagavi 590018*
[4] *Dept of ECE, Global Academy of Technology, Visvesvaraya Institute of Technology, Belagavi 590018*
Corresponding Author: ramya.kv@gat.ac.in
** Corresponding Author Email: ramya.kv@gat.ac.in*

section III the ciphers are implemented using VIvado and few hardware metrics are compared.

Section IV checks the strength of the ciphers using NIST TEST Suite for randomness.

2. Lightweight Cipher

Lightweight ciphers make use of various structures such as SPN, Feistel, and ARX. These structures are designed to provide optimal security while minimizing resource usage. SPN (Substitution-Permutation Network) is a type of lightweight block cipher that divides a message into sub-blocks and applies substitution and permutation operations to each sub-block [1]. Feistel networks, on the other hand, divide a message into two sub-blocks and use multiple rounds of operations to achieve diffusion and confusion [2] [3] [4]. ARX (AND-Rotation-XOR) is another structure used in lightweight ciphers, which relies on fundamental binary operations like AND, rotation, and XOR [5]. These structures are chosen based on their ability to provide security while meeting the constraints of low-resource devices.

2.1. XTEA

XTEA-eXtended Tiny Encryption Algorithm is a symmetric block cipher algorithm designed for secure data encryption and decryption. It was developed as an improvement over the original Tiny Encryption Algorithm (TEA) and provides stronger security features. XTEA operates on 64-bit blocks of data and uses a 128-bit key. Structure of XTEA cipher is as shown in Figure1.

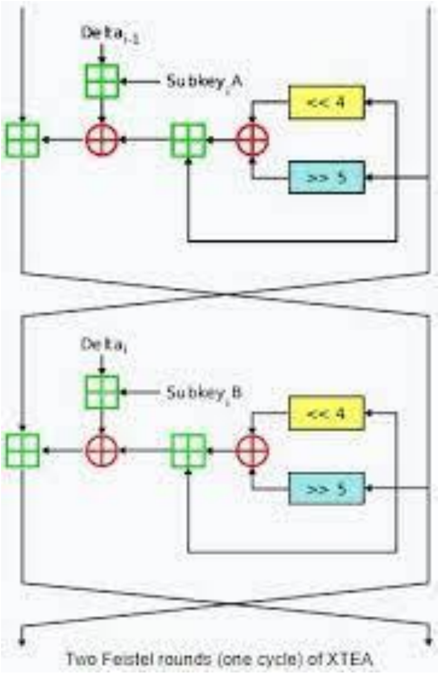

Fig 1 Structure of XTEA cipher

Design Principles:

Block Cipher: XTEA is a block cipher, meaning it operates on fixed-size blocks of data. In the case of XTEA, it processes 64-bit blocks.

Symmetric Key: XTEA employs a symmetric key scheme, thereby implying the utilization of an identical key for both the processes of encryption and decryption.

Feistel Network: XTEA adheres to the Feistel network configuration, a widely employed design methodology in the realm of block ciphers. Within a Feistel network, the data block is partitioned into two halves, with each half undergoing distinct operations during each iteration..

Rounds: XTEA typically uses 64 rounds of processing. This provides a substantial number of iterations to enhance security.

Subkey Generation: The encryption key is used to generate subkeys (delta keys) that are used in each round. These subkeys are derived from the original key in a carefully designed manner.

Security Features:

Strong against Differential Cryptanalysis: XTEA is designed to resist differential cryptanalysis, a common type of attack on block ciphers. The use of multiple rounds and carefully chosen operations provides strong protection against this attack method.

Confusion and Diffusion: XTEA incorporates bitwise operations (XOR), addition, and shifting, which contribute to confusion and diffusion of data. This means that small changes in the plaintext result in significant changes in the ciphertext, making it more resistant to cryptanalysis.

128-Bit Key: XTEA uses a 128-bit key, which provides a reasonably large keyspace, making exhaustive key search attacks computationally infeasible.

Efficiency: XTEA is known for its efficiency in terms of both computation and memory requirements. This makes it suitable for resource-constrained devices and applications.

Balanced Security and Efficiency: XTEA strikes a balance between security and performance. While it may not offer the same level of security as some more advanced ciphers, it is often sufficient for many practical use cases.

Open Design: XTEA is an open and publicly available cipher, which allows for transparency and scrutiny by the cryptographic community.

2.2 RECTANGLE cipher

The RECTANGLE cipher is a lightweight symmetric-key block cipher designed for efficient hardware implementations, particularly in resource-constrained environments. It was introduced as a part of the CAESAR competition, which sought to develop cryptographic algorithms suitable for lightweight and constrained platforms. The structure of RECTANGLE cipher is as shown in Figure2.

Design Principles:

i. Hardware Efficiency: RECTANGLE is primarily designed for hardware implementations, making it well-suited for applications like IoT devices and embedded systems where hardware acceleration can be leveraged for cryptographic operations.

ii. Lightweight: The cipher aims to strike a balance between security and efficiency, with a focus on minimizing resource utilization while maintaining strong cryptographic properties.

iii. Block Size and Key Size: RECTANGLE uses a block size of 64 bits and supports key sizes of 80, 128, or 192 bits, allowing users to choose the level of security according to their requirements.

iv. Substitution-Permutation Network (SPN): The RECTANGLE cipher employs a Substitution-Permutation Network structure, a common design approach in modern symmetric-key ciphers. It consists of multiple rounds, each of which involves substitution and permutation operations on the data.

Security Features:

i. Resistance to Cryptanalysis: RECTANGLE is designed to resist known cryptanalytic attacks, such as differential and linear cryptanalysis, which are common techniques for breaking cryptographic algorithms.

ii. Key Schedule: The cipher employs a robust key schedule algorithm to derive round keys from the user-provided key, enhancing the overall security of the encryption process.

iii. Confusion and Diffusion: RECTANGLE ensures a good balance between confusion (making the relationship between the key and ciphertext complex) and diffusion (spreading changes in plaintext across the ciphertext), which are essential properties for cryptographic strength.

iv. Efficient Avalanche Effect: The cipher exhibits a rapid avalanche effect, meaning that a small change in the input (plaintext or key) results in significant changes throughout the ciphertext, making it resistant to plaintext or key differences

v. Efficient Implementation: RECTANGLE's design prioritizes ardware efficiency, making it a practical choice for constrained devices. It optimizes the use of hardware resources, including gates, memory, and power.

3. Implementation

Implementation and Tools Used:

The implementation of the RECTANGLE and XTEA algorithms was executed on an Artix-7 FPGA (xc7a100t2fgg484-2L). For the design phase, we employed Vivado 2019 as the primary tool for RTL (Register-Transfer Level) design. Additionally, ModelSim 10.7 played a pivotal role in conducting both functional and timing simulations.

Top-Level Design Overview:

Figure 3 and Figure 4 depict the top-level design of the XTEA and RECTANGLE algorithm modules, respectively.

Fundamental Components of FPGA:

The core elements within a Field-Programmable Gate Array (FPGA) consist of flip-flops and lookup tables (LUTs), forming the building blocks of FPGA architecture. These integral components are seamlessly integrated to form logic blocks, which, in turn, facilitate interconnections among themselves and with external entities through programmable interconnects

Table 1 indicates that RECTANGLE cipher uses much lesser LUT and FF as compared to XTEA cipher.

Table 1 Utilization of FPGA

Name of the cipher	LUT	FF
RECTANGLE	168	149
XTEA	482	305

4. Randomness Measurement is Critical in Lightweight Ciphers:

In the realm of cryptography, the assessment of randomness holds paramount significance, serving as a linchpin for ensuring the security and efficacy of cryptographic systems. The quality of randomness inherent in the encryption process plays a pivotal role in determining the robustness of cryptographic applications [6]. To gauge the quality of random numbers in cryptography, an array of randomness testing techniques comes into play. These techniques are instrumental in scrutinizing the randomness of sequences generated by cryptographic algorithms. Various standards and test requisites have been introduced, accompanied by corresponding test toolkits. These tests are indispensable in guaranteeing that the sequences generated by cryptographic algorithms possess the essential attributes of being random, unpredictable, and independent. Statistical assessments, such as the NIST randomness tests, are widely employed to ascertain the randomness of these sequences. The pursuit of randomness in cryptographic algorithms constitutes a foundational concern in their design, as it exerts a direct influence on their security characteristics [7] - [11].

The Significance of Randomness Measurement in Lightweight Ciphers: Within the domain of lightweight ciphers, the importance of evaluating randomness is underscored by several critical factors:

Safeguarding Security: In the context of lightweight ciphers, the security of a cryptographic system hinges on the degree of randomness exhibited by the cipher's operations. Predictable or non-random behavior in a cipher can expose vulnerabilities, potentially compromising the entire system's security. The infusion of randomness into the encryption process ensures that ciphertext patterns remain devoid of any discernible relationship with the plaintext or the encryption methodology. Consequently, this makes it substantially more challenging for potential attackers to exploit patterns or biases and mount successful attacks.

Resisting Differential and Linear Cryptanalysis: Differential and linear cryptanalysis represent formidable techniques employed by adversaries to scrutinize the behavior of ciphers. Randomness and diffusion within the operations of the cipher stand as potent bulwarks against these analytical methodologies. By introducing randomness into the cipher's operations, it becomes exceedingly arduous for attackers to predict or deduce the intricate relationships that exist among plaintext, ciphertext, and encryption keys. This inherent complexity fortifies the cipher's resistance to differential and linear cryptanalysis, enhancing its security posture.

Non-reproducibility: The introduction of randomness in a lightweight cipher guarantees that encrypting identical plaintext with the same key on multiple occasions produces distinct ciphertexts. This lack of reproducibility is crucial for security as it thwarts attackers from capitalizing on potential patterns that may arise when encrypting the same data repeatedly

Key Derivation: In many cryptographic applications, randomness is used to derive cryptographic keys, such as session keys or initialization vectors (IVs). Ensuring that these keys are unpredictable and have high entropy is essential for the overall security of the system.

Counteracting Side-Channel Attacks: Lightweight ciphers are often used in devices where side-channel attacks (e.g., timing attacks, power analysis) are a concern. A non-randomness in the cipher's operations can make it easier for attackers to exploit side-channel leakages. Randomness can help introduce noise into the side-channel data, making it more challenging for attackers to extract meaningful information.

Compliance with Cryptographic Standards: Many cryptographic standards and protocols require the use of ciphers with specific randomness properties. Ensuring that a lightweight cipher meets these requirements is essential for interoperability and compliance with security standards.

Advances: The field of cryptography is constantly evolving, and new cryptanalysis techniques and computing power advances may expose vulnerabilities in ciphers that were once considered secure. Randomness helps future-proof a cipher by making it more resilient to emerging threats.

In some applications, lightweight ciphers are used to protect user data and privacy. Randomness ensures that the encrypted data does not leak information about the original data, helping to preserve user privacy.

The NIST test suite is a collection of statistical tests used to measure the randomness of sequences. It consists of 15 different

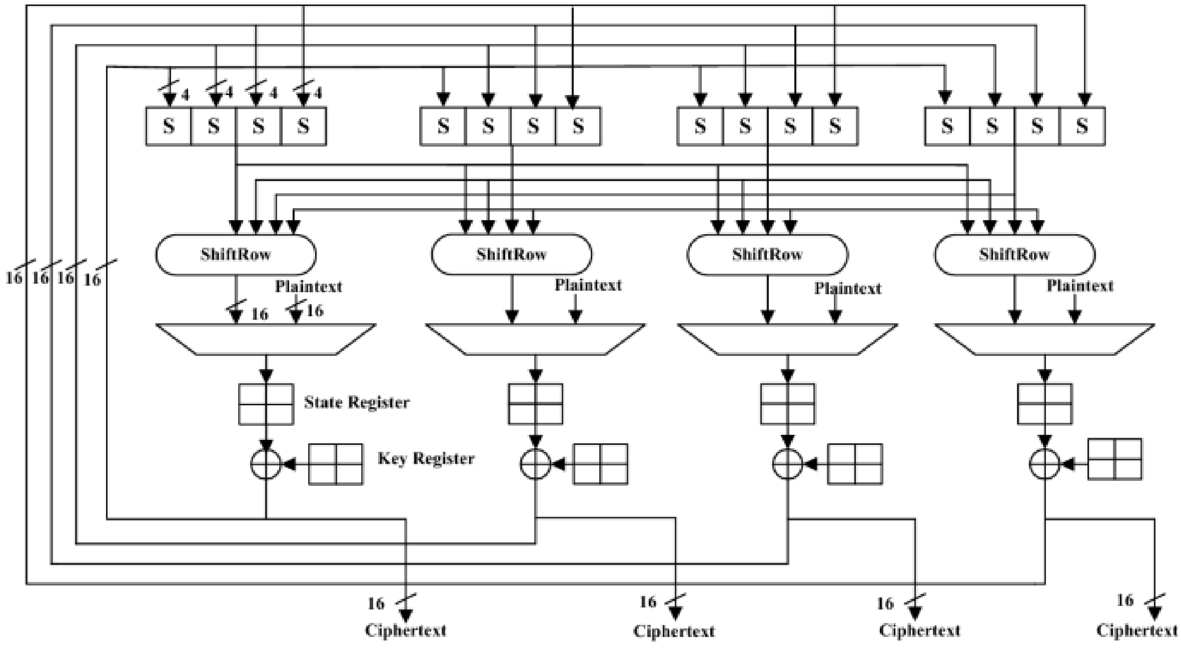

Fig 2 structure of Rectangular cipher

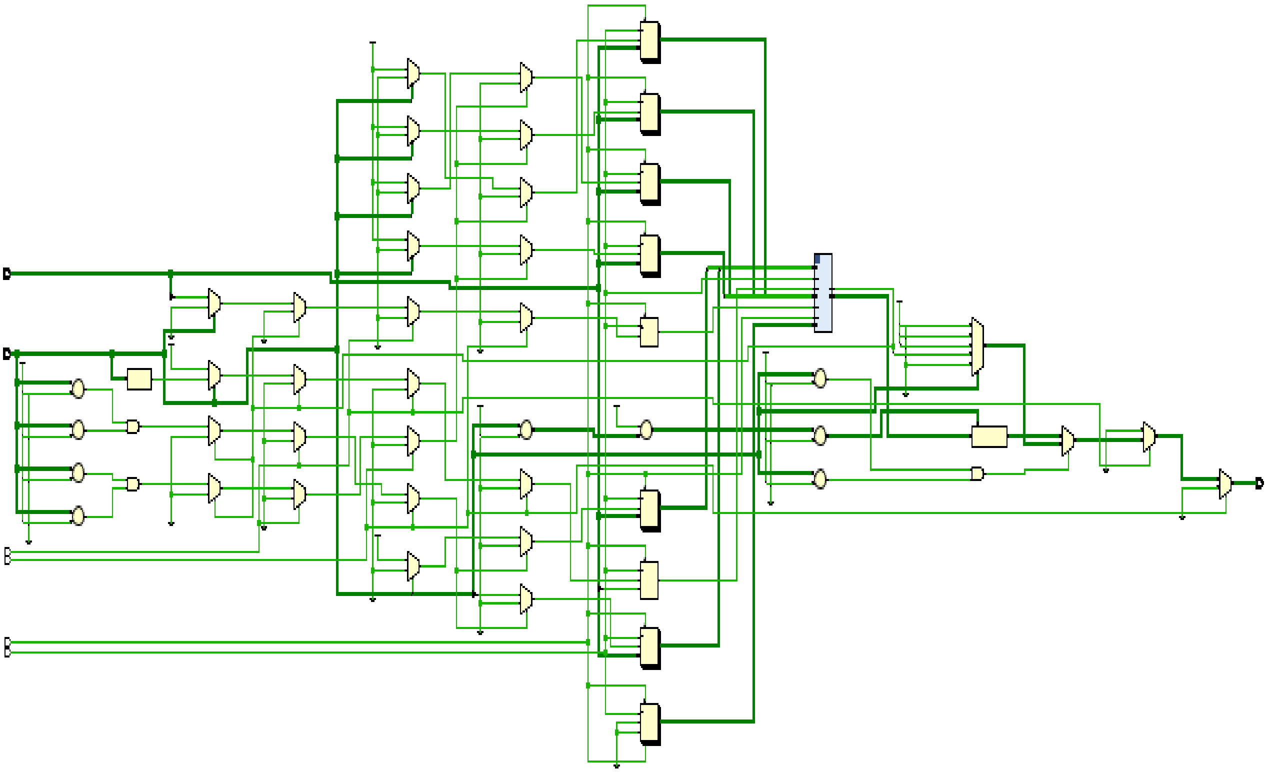

Fig 3 Schematic diagram of XTEA cipher

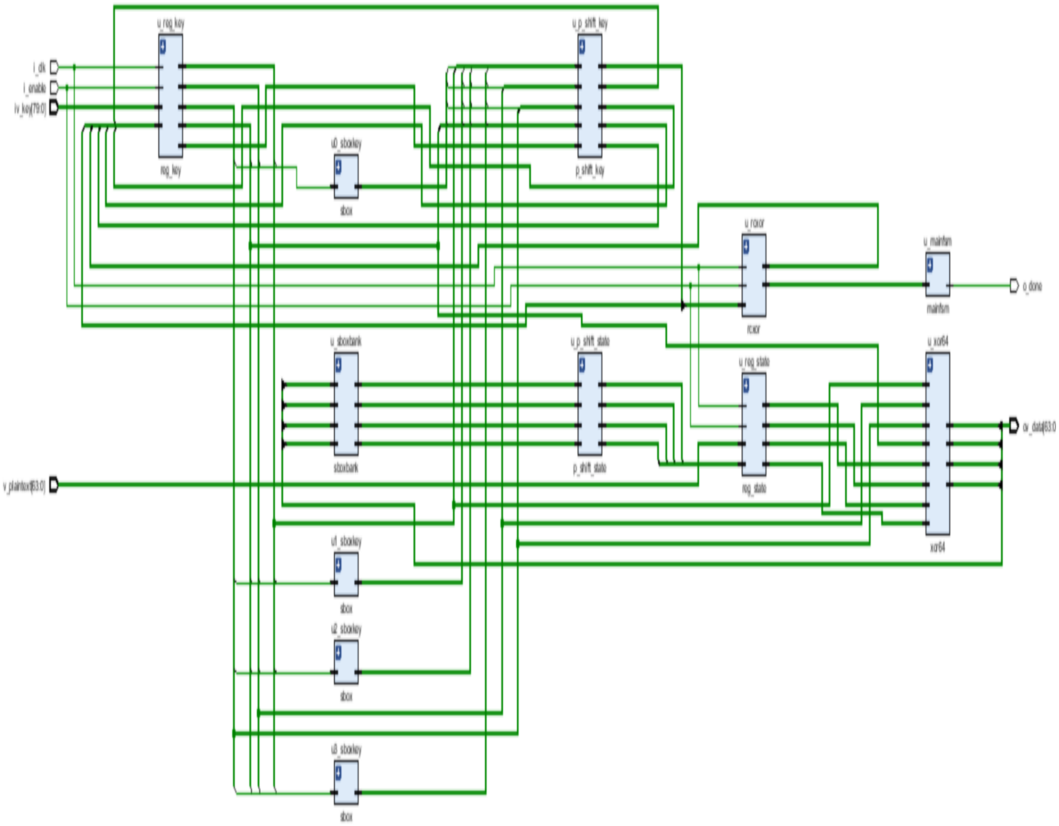

Fig 4 Schematic diagram of Rectangular cipher

tests that output p-values for each sequence tested. Additional hypothesis tests, such as the proportion test and the uniformity test, are performed on the multiple p-values to judge the randomness of the sequences [13] [14]. The suite aims to detect nonrandom characteristics in sequences and is commonly used in the evaluation of random numbers and sequences for cryptographic algorithms [15]. The tests in the suite analyze various statistical parameters and deviations to assess the randomness property of the sequences [16]. The suite provides a comprehensive approach to evaluating the randomness of data, considering multiple statistical measures obtained from different tests [17].

Result of NIST Test Suite shown in Table2 indicates that lightweight cipher do not satisfy all the test for randomness. RECTANGLE and XTEA cipher satisfy the following tests:

Table 2 Tests listed in NIST Randomness TEST Suite

Type of Test	XTEA	RECTANGLE
Frequency Test (Monobit)	NO	NO
Frequency Test within a Block	NO	NO
Run Test	NO	NO
Longest Run of Ones in a Block	NO	NO
Binary Matrix Rank Test	NO	NO
Discrete Fourier Transform (Spectral) Test	NO	NO
Non-Overlapping Template Matching Test	YES	YES
Overlapping Template Matching Test	YES	YES
Maurer's Universal Statistical test	NO	NO
Linear Complexity Test	YES	NO
Serial test:	NO	NO
Approximate Entropy Test	NO	NO
Cummulative Sums (Forward) Test	NO	NO
Cummulative Sums (Reverse) Test	NO	NO
Random Excursions Test:	YES	YES
Random Excursions Variant Test:	YES	YES

Random -YES Non-Random-NO

Non-Overlapping Template Matching Test: This particular examination is crafted to evaluate the frequency of predefined target string occurrences within a sequence generated by a random number generator. The main goal is to pinpoint generators that exhibit an unusually high frequency of a specific non-repeating pattern.

Overlapping Template Matching Test: Similar to the Non-Overlapping Template Matching test, this assessment focuses on tallying the occurrences of predefined target strings within a sequence produced by a random number generator.

Random Excursions Test: The central focus of this test involves quantifying the instances where a cumulative sum random walk precisely reaches K visits within cycles. The cumulative sum random walk is created by accumulating partial sums after transforming the (0,1) sequence into the corresponding (-1, +1) sequence. In this context, a cycle in a random walk is defined by a sequence of randomly taken unit-length steps starting from the origin and returning to it. The main objective of this test is to determine whether the number of visits to a specific state within a cycle deviates from what would be anticipated in a genuinely random sequence.

Random Excursions Variant Test:

In this test, the primary emphasis is on the overall tally of occurrences or visits to a particular state during a cumulative sum random walk. The overarching goal is to identify any deviations from the expected number of visits to different states within the random walk.

Linear Complexity Test: It's crucial to highlight that this specific test is specifically designed for the XTEA cipher. The essence of this evaluation revolves around assessing the length of a linear feedback shift register (LFSR). The ultimate objective is to ascertain whether the examined sequence demonstrates a level of complexity that qualifies it as a truly random sequence.

5. Conclusion:

In resource-constrained environments, the preference is for lightweight block ciphers to safeguard data. Two ciphers namely RECTANGLE and XTEA ciphers were selected for implementation. RECTANGLE has SPN structure and XTEA cipher has FEISTEL structure. Both the ciphers were implemented on ARTIX7 Zynq board. Simulation results were observed and then synthesized; synthesized results indicated that RECTANGLE cipher consumed less area than XTEA cipher. Further the encryption strength was measured using NIST Randomness TEST suite. The test suite has 15 tests, among which only 4 tests was random for both the ciphers. Additionally, XTEA cipher passed Linear complexity test. So, there is trade-off between RECTANGLE and XTEA ciphers, as XTEA cipher passes additional test but RECTANGLE cipher consumes less memory.

References

[1] Hatzivasilis, George & Fysarakis, Konstantinos & Papaefstathiou, Ioannis & Manifavas, Harry. (2018). A review of lightweight block ciphers. Journal of Cryptographic Engineering. 8. 1-44. 10.1007/s13389-017-0160-y.

[2] Thakor, M. Razzaque, and M. Khandaker, “Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities,” *IEEE Access*, vol. 9, 2021

[3] M. Jangra and &amp; Buddha Singh, “Performance analysis of CLEFIA and PRESENT lightweight block ciphers,” *Journal of Discrete Mathe- matical Sciences and Cryptography*, vol. 22, no. 8, pp. 1489–1499, 2019.

[4] Manjushree B Somasagar , Dr. Kiran Bailey, 2020, CLEFIA- A Encryption Algorithm using Novel S-Box Architecture, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 09, Issue 07 (July 2020),

[5] T. Cihangir, Ali, and S. Aydın, “Improved improbable differential attacks on ISO standard CLEFIA,” *Information Processing Letters*, pp. 136–143, 2016

[6] Z. Guo, W. Wu, and S. Gao, “Constructing Lightweight Optimal Diffusion Primitives with Feistel Structure,” *Selected Areas in Cryp- tography - SAC 2015*. vol. 9566, 2016.

[7] Rashidi, Bahram. (2020). Efficient and Flexible Hardware Structures of the 128-bit CLEFIA Block Cipher. IET Computers & Digital Techniques. 14. 10.1049/iet-cdt.2019.0157..

[8] K. He, X. Zhang, S. Ren, and J. Sun, “Deep Residual Learning for Image Recognition,” 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 770–778, 2016.

[9] Cheng, Xin & Zhu, Haowen & Xu, Yixuan & Zhang, Yongqiang & Xiao, Hao & Zhang, Zhang. (2021). A reconfigurable and compact hardware architecture of CLEFIA block cipher with multi-configuration. Microelectronics Journal. 114. 105144. 10.1016/j.mejo.2021.105144.

[10] M. Imdad, S. N. Ramli, and H. Mahdin, “An Enhanced Key Schedule Algorithm of PRESENT-128 Block Cipher for Random and Non-Random Secret Keys,” *Symmetry*, vol. 14, no. 3, p. 604, Mar. 2022, doi: 10.3390/sym14030604.

[11] A. Poojary, V. G. K. Kumar, and H. R. Nagesh, “FPGA implementation novel lightweight MBRISI cipher,” J Ambient Intell Human Comput, vol. 14, pp. 11 625–11 637, 2023.

[12] “FPGA implementation novel lightweight MBRISI cipher,” *J Ambient Intell Human Comput*, vol. 14, pp. 11 625–11 637 k Cipher for Random and Non-Random Secret Keys. , 2023

[13] V. A. Thakor, M. A. Razzaque, and M. Khandaker, “Lightweight cryptography algorithms for resource-constrained IoT devices: a re- view, comparison and research opportunities,” *IEEE Access*, vol. 9, pp. 28 177–28 193, 2021

[14] Y. -T. Teng, W. -L. Chin, D. -K. Chang, P. -Y. Chen and P. -W. Chen, "VLSI Architecture of S-Box With High Area Efficiency Based on Composite Field Arithmetic," in IEEE Access, vol. 10, pp. 2721-2728, 2022, doi: 10.1109/ACCESS.2021.3139040.

[15] I. N. Mohammad Shah, E. S. Ismail, F. Samat, and N. Nek Abd Rahman, “Modified Generalized Feistel Network Block Cipher for the Internet of Things,” Symmetry, vol. 15, no. 4, p. 900, Apr. 2023, doi: 10.3390/sym15040900. [Online]. Available: http://dx.doi.org/10.3390/sym15040900

[16] Rourab, Paul., Hemanta, Dey., Amlan, Chakrabrti., Ranjan, Ghosh. "NIST Statistical Test Suite." arXiv: Applications, undefined (2016).

[17] Atsushi, Iwasaki. "The relation between Proportion test and Uniformity test in NIST SP800-22." undefined (2020). doi: 10.34385/PROC.65.C01-8