ISSN 2347 - 3983
Volume 8. No. 5, May 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter30852020.pdf
https://doi.org/10.30534/ijeter/2020/30852020

Reconfigurable Asymmetric Lightweight Cryptosystem

B. Murali Krishna[1], D. Sai Gopinath[2], M.Kiran[3], Sk.Javid[4]
[1]Assoc Professor, [2,3,4]UG Scholar,
Department of ECE, Koneru Lakshmaiah Education Foundation, K L Deemed to be University, Green Fields, Vaddeswaram, Guntur, AP,India, [1]muralikrishna@kluniversity.in
[2]sai.gopinath9909@gmail.com, [3]kirsnmadanapalli124@gmail.com, [4]skjavid037@gmail.com

ABSTRACT

The tremendous growth in wireless technologies and adapting nature of electronic devices, integrating together gains more popularity in utilization. Day-to-Day millions of these devices communicate in an every minute. Secure channel establishment between cloud and remotely connecting IOT devices for communication is necessity to avoid Cyber Crimes. Cryptography plays a vital rule in cyber theft. Lightweight cryptography gains more significance because of its energy requirements, memory, low cost and high security. Asymmetric lightweight cryptosystem (ALWCS) is designed which reduces the power, area and improves the security. AHLWCS is designed on Artix-7 XC7A35T-1-CPG236 reconfigurable architecture using verilog hardware description language (HDL) which is synthesized, simulated and implemented on Vivado.

Key words: IOT, Reconfigurable Architecture Lightweight Cryptography, Encryption and Decryption.

1. INTRODUCTION

Day-to-Day advancements in Wireless communication the network operators provide unlimited bandwidth to users. Secure communication and network connectivity has become the bottleneck for service providers. Users share information among networks which suffers deficiency in providing data privacy, and authentication. Every information that will be shared to public will be having a chance for cyber-attacks. Modern cryptography algorithms should exhibit high security characteristics to avoid malicious cyber thefts in media. Wireless communication network has become a vital part of various kinds of communication systems. In the present day, users can easily communicate even from rural areas. Due to recent trends in wireless technologies like 3G, 4G,5G, future generations through hand held electronic devices like mobiles, tabs etc. Billions of data is shared among users, where security plays a vital role. Light Weight Cryptography having more advantage than conventional crypto algorithms. Every Wireless Cryptographic Protocol, data confidentiality is the key challenge and encryption algorithms play a significant role for protection in the network. Lightweight cryptography algorithm to be applied in restricted settings such as RFID's, sensor networks, hospitals, twitter, cyber-devices, distribution systems, markers, monitoring systems for human controls, intelligent energy systems, etc where Field Programmable Gate Array (FPGA)and embedded hardware is used for application deployment.

2. LITERATURE SURVEY

In 2019 Reem Jaffal has proposed and implemented the Simon light weight algorithm by intending Communication and Security with various number Rounds [1]. Somasundaram R, has proposed the modified Simon algorithm by cutting down the number of round functions in 2019. which it was implemented for the purpose of power consumption and reduced Secured round function [2].Andreas Bossert has proposed that Comparison of block ciphers with previous algorithms in 2016 stated that the Simon is simple and easily implemented, and this Simon is having high throughput [3].

Masanobu Katagi proposed that the importance of Light weight Cryptography through the security in 2011, efficiency and these are implemented in the networks, lightweight block ciphers are practical to use now [4]. Amrit pal Singh proposed that the longer key will be used for data security which are unable to crack the key and the benefits over using the longer key and compared with DES and RSA in 2018[5].

Bassam J. MOHD proposed a light weight block ciphers for low-resource IoT and presents an energy management algorithm to improve IoT Survivability against Denial of Service in 2018[6].Sowmya Aithal proposeda Partial Reconfiguration technique in 2015 plays an importantrole in the Lightweight Cryptography [7].Michael Appel Proposed that a comparison of seven different Block Ciphers in 2016 with their functionalities along with security of level of the cipher with AES Algorithm [8]. Carlos Andres Lara-Nino Proposed a technique in 2018 that for furnishing integrity and verifying of energy consumption in WSN Cryptography

algorithms in encrypting data under CBCMAC mode [9]. C.T.Thorat proposed that new compact hybrid lightweight encryption in 2018. It uses fastest bit permutation with S-box in PRESENT Algorithm to achieve non-linearity and the results are compared to the PRESENT-GRP block cipher [10].

Sohel Rana proposed an effective lightweight Cryptograpy algorithm in 2018 with a basic concept from genetic algorithm which is used to achieve less data usage and reduced power consumption than the previous cipher [11]. R Shantha Mary Joshitta proposed that JAC-Jo block cipher in 2018 with the use of soft set based key generation algorithm. Soft Key Gen and encrypts 32-bit data using 64-bit key to achieve security in Health care internet of things [12]. In 2019 Arghya Bhattacharjee proposed light weight based authenticated-encryption schemes in two versions parameterized by state and mask size of the permutations [13]. William J.Buchanan proposed a large number of light weight cryptography algorithms in 2017, gives an overview of ultra-light weight cryptography which can be used smart devices like RFID etc [14]. E.Lambooij proposed the differential crypt analysis in 2017 studied the differential transitions occurring in the multiple rounds of a fixed key this will actually impacts on Security of the algorithms [15].

3. CRYPTOGRAPHY

Cryptography gains more popularity information exchange by providing isolation from vulnerable attacks in channel. Cryptography is classified to symmetric and asymmetric.

3.1 Symmetric-Key Cryptography

In this Process both encryption and decryption are done through same key as shown in figure 1, here the transmitter will send the encrypted data along with the key so that receiver will decrypt the message using that key and access the data.

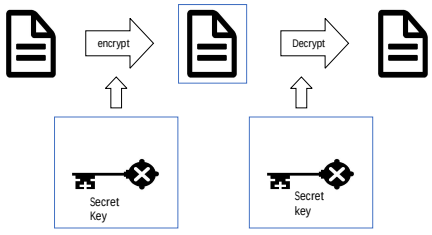

Figure 1: Secret Key Cryptography

3.2 Asymmetric-Key Cryptography

In this Process there will be a Public key and another one is a Private Key. One of these keys will shared to everyone it is called Public key and another key used by only at receiver is Private Key as shown in figure 2. Any key is used to encrypt the data.

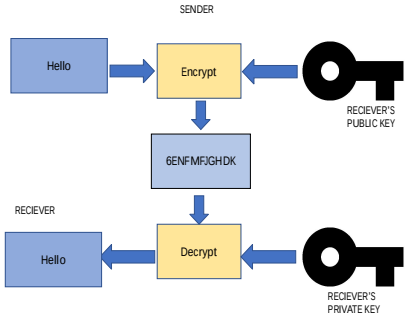

Figure 2: Public Key Cryptography

4. LIGHTWEIGHT CRYPTOGRAPHY

Lightweight cryptography is the minimal footprint and the protection with cryptographic sophistication. The goal is to expand applications of cryptography into restricted systems and obtain their resulting global standardization and direction. Lightweight cryptography gains more popularity in terms of less power consumption, usage of data is less data usage and, high efficiency low cost compared to conventional cryptography. Internet of things (IOT) is one of the present ruling technologies in world. Researchers focus on implementing lightweight design to reduce high-power dissipation and a significant necessity for memory. RFID tag is one of the fastest growing IOT technologies used for many applications for example toll gates uses RFID for fast movement of vehicles with early recharge to avoid excess traffic. A light weight crypto algorithm whose coverage area would be needed to provide protection at RFID level.

4.1 SIMON Algorithm

Simon is a kind of lightweight block which was used in hardware creation since the speck is used in software. In Simon, the whole scheme is based on master key. This algorithm involves a circular feature, key scheduling. Simon's algorithm was initially developed to demonstrate an exponential speed-up over the best conventional algorithm for solving a specific problem. This influenced the quantum algorithm used in the most common quantum algorithm for discrete Fourier Transformation, which is well known as quantum Fourier Transform.

4.1.1 Round Function

In round function message is 2n and the length of the key is m n, suppose if we take 32-bit plain text the key size will be 64. If n=16 the master key will be divided into 4 sub keys. Initially the message is 2n and the key is m n, presume that the value would be 64 if you take a 32-bit plain text. The message will be taken as two sections (16 + 16) in the left and right portion. If n=16 the master keys will be split into four sub keys. The

left portion, is operated with LCS1 and LCS8 circular moves, which are controlled by Logical Bitwise-and& the output is xored with the right part of the single text. XORed with LCS2 and xored with Round Key are now included in the Performance of the previous process shown in figure 3. The performance of the round key shall be moved to the left half and the previous left half shall proceed until the effective cipher has been obtained for the next round task.

$F(X, Y, K) = (Y \oplus ((S^1x \& S^8x) \oplus S^2x) \oplus K)$

This encryption method relies on the amount rounds through encoding the plain text in cipher code. In encryption, only Left Circular Shift (LCS), changing the left half as right half and varying the right half as left half for every round.

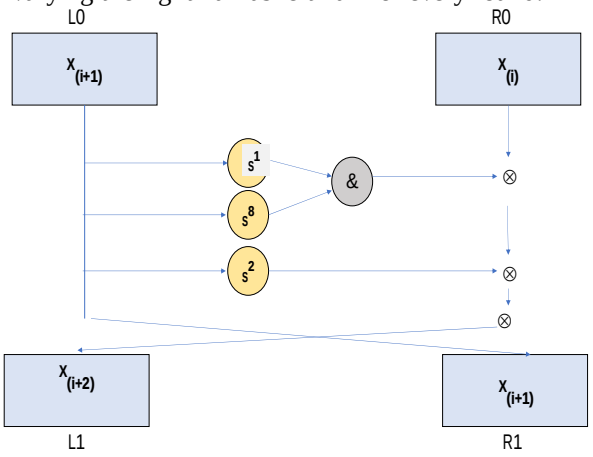

Figure 3: Simon Algorithm

4.2 LEA Algorithm

In order to have protection in lightweight, high-speed computing, such as in mobile apps, etc, the block encryption algorithms are established. The domestic Telecommunications Technology Association (TTA) norm for LEA production and service was created. LEA is the encryption method for 128 bits of plain text, while LEA-128, LEA-192 modes are determined by hidden key frequency shown in figure 4. LEA consists of 24, 28 and 32 rounds, according to each phase. LEA has been designed for lightweight applications; the 32-bit device performs arithmetic processing Addition, Rotation, XOR (ARX). ARX arithmetic operations are made up of Add, Rotation, XOR arithmetic, and were planned for high-speed activities in 32 bit Framework. LEA is the encryption method for 128 bits of plain text, while LEA-128, LEA-192 modes are determined by hidden key frequency shown in figure 4. LEA consists of 24, 28 and 32 rounds, according to each phase. LEA has been designed for lightweight applications; the 32-bit device performs arithmetic processing Addition, Rotation, XOR (ARX). ARX arithmetic operations are made up of Add, Rotation, XOR arithmetic, and were planned for high-speed activities in 32 bit Framework

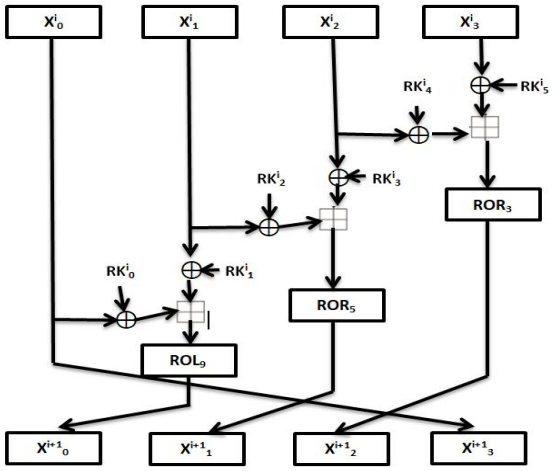

Figure 4: LEA Algorithm

4.3 TEA Algorithm

An especially fast, easy and Feistel-based block cipher, Tiny Encryption Algorithm (TEA) is one of the quickest and one of most efficient encryption algorithm. Plain Text 'P' is used to break into two parts, Left [0] and Right[0], while 'C' is the cipher text (Left[64], Right[64]). P is used for encrypting the second half over 64 processing rounds through half of the plaintext and then is combined together to create the cipher text fragment. TEA sets a 128-bit key to split in four 32-bit main words, with a block size of 64-bit per encoding, in which two 32-bit words will be separated. In its encryption round, TEA involves two Feistel tasks as well as a sequence of additions and bit ways, TEA uses the Feistel method, noted as F.

4.3.1 Round Process

At the beginning of the 64-bit plaintext is separated into two halves (Y and Z).

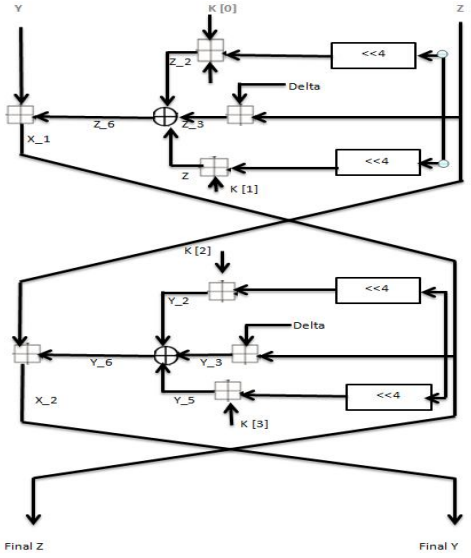

Figure 5: TEA Algorithm

Four passwords can be identified as the user's passcode. Such passwords are often delegated to the TEA system as inputs. The original z input value is first left-shifted with 4 bits and the first K [0] pass key is applied to the output, which is then stored in the z_2 memory. The initial value z is used to add a Golden Ratio constant which is a decimal value of 2654435769 and the values are stored in the z_3 memory. The next move is to replay the original z input value again and then store it in the memory called z_5 shown in figure 5.

4.4 KATAN Algorithm

The algorithm KATAN originally suggested a family of six lightweight block ciphers that were geared towards hardware. Algorithms basically use the same general formula for encryption, but vary in size and timeline. KATAN block sizes are 32, 48 and 64-bit which are given by the KATAN / KTANTAN ciphers. All KATAN ciphers have an 80-bit main. In contrast to software measurements, KATAN ciphers displayed positive performance in hardware architecture indicators that are supposed to exist for hardware. In particular, the KATAN displayed strong output in ground, strength and energy to a lesser extent.

5. ASYMMETRIC LIGHTWEIGHT CRYPTO - SYSTEM

Asymmetric Lightweight Cryptosystem involves encryption and decryption. Utilizing a pair of different keys like public key and a private key generated from prime numbers with correlation to each other. Message is encrypted using public key, so that the intended receiver can only decode the message using recipient private key. Asymmetrical cryptography is used in digital signatures to authenticate records. A digital signature is a cryptographic procedure used to check that a code, device or record has validity and legitimacy. Asymmetric hybrid lightweight crypto system is designed.

5.1 ALWCS Encryption

1. Plain text 64 bits are divided into two halves and apply RCS1 to 1st part and LCS1 to 2nd part.

2. Swapping the values obtained from RCS1 and LCS1 and doing XOR operation. After swapping divide it into left half and right half and perform LCS1 for left half and LCS8 for right half.

3. The obtained text is xored with the key value, again perform LCS2 for the obtained text and xored with the key and perform 1's complement for the obtained text.

4. Consider it as plain text for performing Katan operation divide it into two parts L1and L2,L1 is of 25 bits and L2 is of 39 bits by using formulas
   fa(L1)=L1[X1]⊕L1[X2]⊕(L1[X3].L1[X4])⊕ (L1[X5].IR)⊕Ka
   fb(L2)=L2[Y1]⊕L2[Y2]⊕(L2[Y3].L2[Y4])⊕ (L2[Y5].L2[Y6])⊕Kb
   Where {X1 X2 X3 X4 X5} = 24 15 20 11 9, {Y1 Y2 Y3 Y4 Y5 Y6} = 38 24 33 21 14 9
   Shift operation on any 32 bit part depends on fa and fb values.

5. Consider the obtained text and divide the text into two parts as Xi(0) and Xi(1) and divide the key value into 8 parts and perform xor operation to Xi(0) with key Rk[4] and Xi(1) with key Rk[3].

6. Perform addition operation to the obtained values and after that perform swap forRCS3.

7. The obtained text is again divided into two halves, LCS4 performed to right half and xored with golden ratio constant which is 2654435769 and modified right half combined with left half and xored with key.

8. Obtained text from previous is divided into two halves, now left half is operated with RCS5 and xored with golden ratio constant and modified left half is combined with right half and xored with the key, it will be the final cipher text is shown in figure 6.

5.2 ALWCS Decryption

1. Encrypted cipher is xored with the private key and the obtained text is divided into two 32 bit halves.

2. The first half is xored with golden ratio constant which is 2654435769 and it is undergone with LCS5 and obtained value is xored with private keys $K_1 K_2 K_3 K_4$.

3. The other half is xored with the remaining private keys $K_5 K_6 K_7 K_8$ and the obtained value is again xored with the golden ratio constant and it is undergone RCS4.

4. The obtained text that is combined again divided into two different halves i.e, L_2 and R_2.The L_2 part is done with LCS3 and R_2 part xored with $K_4$and both the values are swapped and the value is xored with K_2.The obtained value and the R_2 are combined.

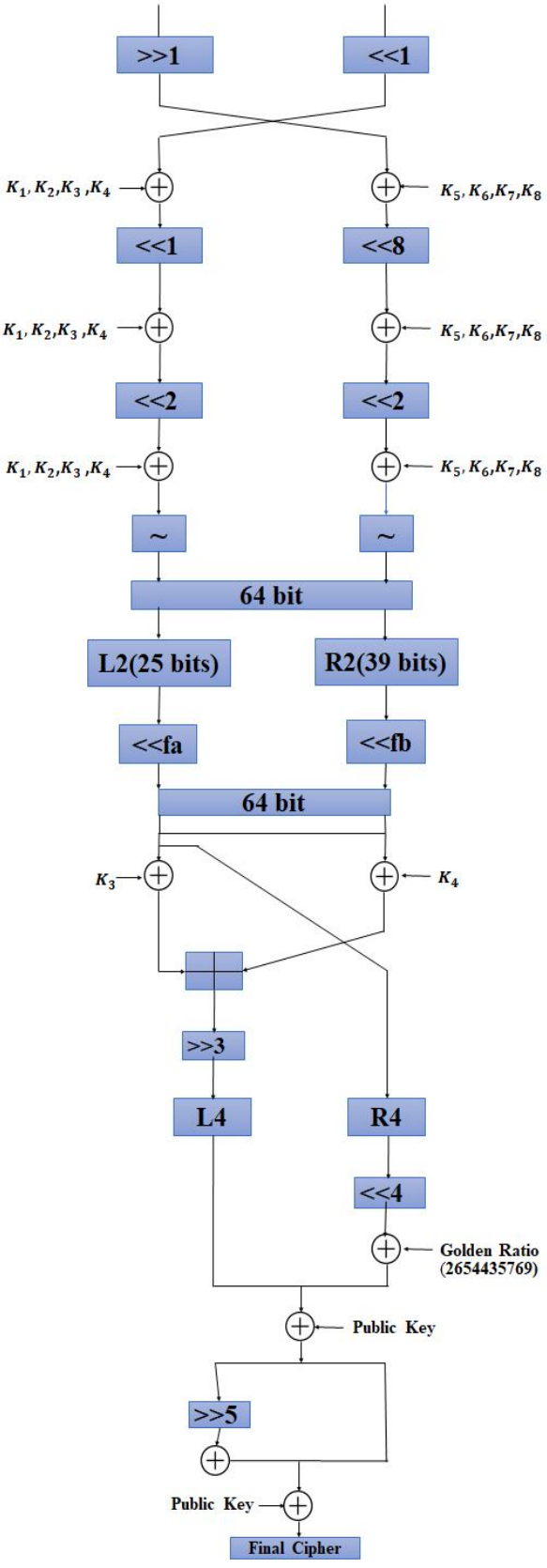

Figure 6: ALWCS Encryption

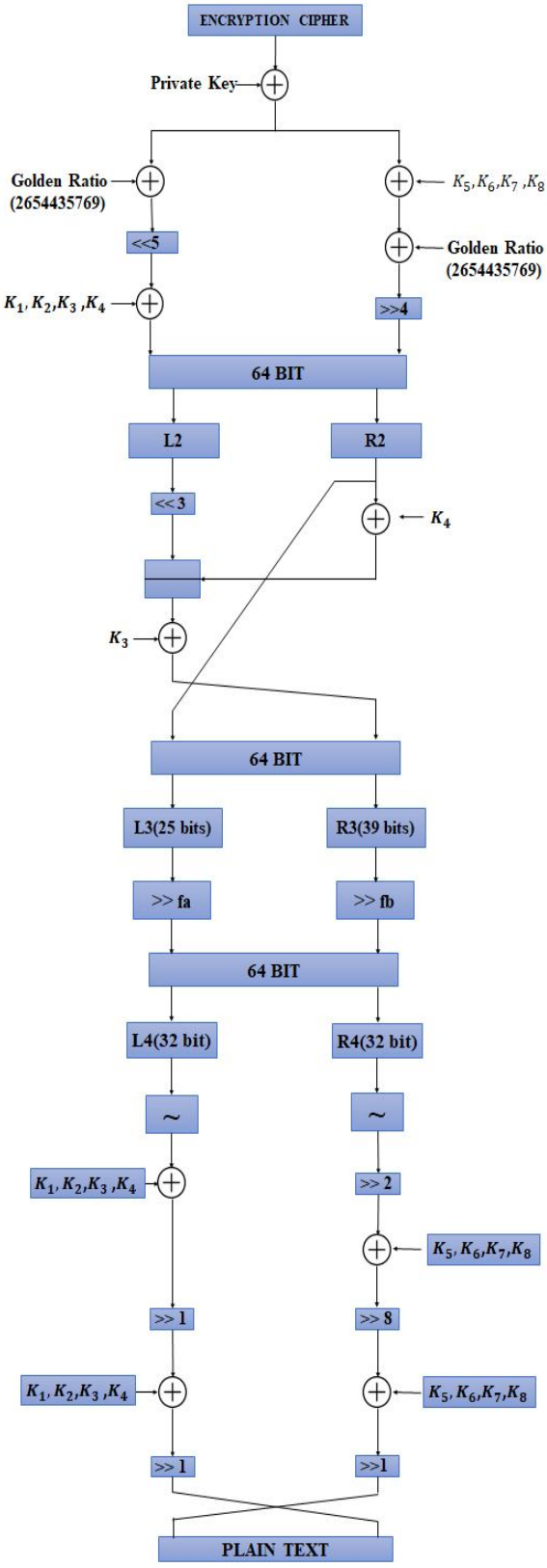

Figure 7: ALWCS Decryption

5. The obtained text is again divided into two different halves L_3 of 25 bits and $R_2$of 39 bits. Perform right shift for both parts with fa and fb.

6. Combine both parts and again divide it into two equal halves the left part is xored with $K_1K_2K_3K_4$and the right part is undergone with RCS2 and it is xored with $K_5K_6K_7K_8$and both are performed with RCS1 and RCS8 and both are again xored with the keys.

7. Obtained both parts are undergone with RCS1 and the values are combined it is decrypted plain text as shown in figure 7.

6. RESULTS

Figure.8 represents RTL schematic of encryption and decryption of ALWCS.

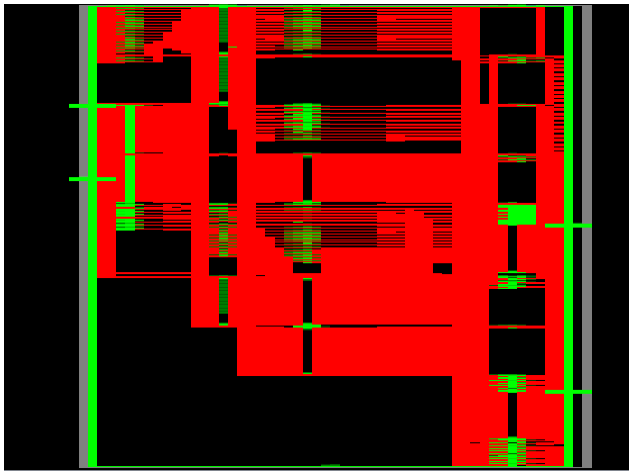

Figure 8: RTL Schematic of ALWCS

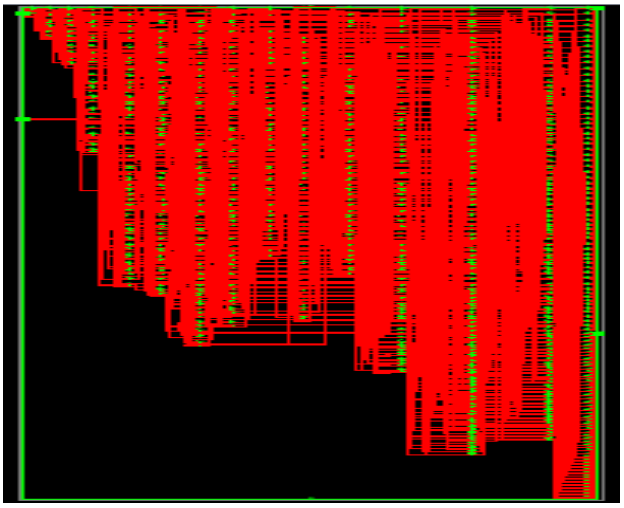

Figure 9: Technology Schematic of ALWCS

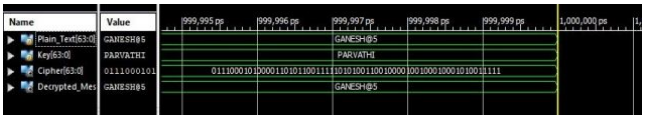

Figure 10: Simulation Result of ALWCS

RTL schematic exhibits the design internal structure created by components like general basic gates like AND, OR, adders, multipliers and so on. Whereas Figure.9 signifies the Technology schematic of ALWCS. Technology schematic is used to represent the design at a higher level by replacing the basic elements with Slices, LUT's, Flip-Flops, Multiplexers, buffers etc which are mapped in accordance to target architecture. Simulation output of ALWCS encryption and decryption is shown in figure.10

7. CONCLUSION

Energy is one of the most typical constraints in IoT applications. Research tailored on optimizing area, power and enhancing the security of asymmetric lightweight cryptosystem system for handling to improve battery life even under extreme energy usage and power assaults or cloud based applications. To reduce cyber crimes and vulnerability attacks in channel algorithm can be extended by introducing Partial Reconfiguration with Light Weight Cryptography Algorithm. Dissimilar permutations can be configured in runtime using dynamic partial reconfiguration which results a change in parameters like speed, storage and efficiency by using these Light Weight Cryptography Algorithm.

REFERENCES

1. Saed Abed, Jaffal R, Mohd BJ, Alshayeji M,"**FPGA Modelling and Optimization of a Simon Light Weight Block Cipher**", NCBI,2017.
2. Somasundaram R, Mythili Thirugnanam, "**Energy Optimized Simon Light Weight Security Algorithm for Internet of Medical Things (IoMT)**", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-8 June, 2019.
3. Andreas Bossert, Steven Cooper, Alexander Wiesmaier, "**A comparison of block ciphers Simon, Speck, and Katan**", Sematic Scholar, 2016.
4. Masanobu Katagi and Shiho Moriai**,"Light Weight Cryptography for the Internet of Things"**, IAB-uploads,2011.
5. Mohit Marwaha, Rajeev Kumar Bedi, Amritpal Singh, **"Comparative Analysis of Cryptographic Algorithms"**, Research Gate, 2013.

6. BASSAM J.MOHD, THAIER HAYAJNEH, **"Lightweight Block Ciphers for IoT: Energy Optimization and Survivability Techniques"**, IEEE, 2018.
7. Sowmya Aithal, **"A survey on Partial Reconfiguration Techniques"** ,International Journal of Science and Research (IJSR), 2319-7064, 2015. https://doi.org/10.18535/ijecs/v5i5.47
8. Michael Appel, Andreas Bossert, Steven Cooper, Tobias Kußmaul, Johannes L¨offler, Christof Pauer, and Alexander Wiesmaier**, "Block Ciphers for the IoT-Simon , Speck, Katan, LED, TEA, PRESENT, and SEA compared"**, semanticscholar,2016.
9. Carlos Andres Lara-Nino, Arturo Diaz-Perez, Miguel Morales-Sandoval' **"Energy and Area Costs of Lightweight Cryptographic Algorithms for Authenticated Encryption in WSN"**,ID 5087065, 2018. https://doi.org/10.1155/2018/5087065
10. C.T.Thorat, V.S.Inamdar, **"Implementation of new hybrid Light Weight cryptosystem"**, ScienceDirect, 2018. https://doi.org/10.1016/j.aci.2018.05.001
11. 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(IJCSA), Vol. 9, No. 11, 2018. https://doi.org/10.14569/IJACSA.2018.091137
12. R Shantha Mary Joshitta, L Arockiam**"A novel block cipher for enhancing data security in healthcare internet of things"**, Journal of Physics, Volume 1142,2018. https://doi.org/10.1088/1742-6596/1142/1/012002
13. ArghyaBhattacharjee, Eik List, Cuauhtemoc Mancillas Lópezand Mridul Nandi, **"The Oribatida Family of Lightweight Authenticated Encryption Schemes"**, isical, 2019.
14. William J.Buchanan, Shancang Li, Rameez Asif, **"Lightweight cryptography methods"** Journal of Cyber Security Technology, 2017. https://doi.org/10.1080/23742917.2017.1384917
15. E.Lambooij **"Cryptanalysis of Simon"**, cryptanalysis of lightweight symmetric ciphers, 31 Aug 2017.