IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 08, Issue 10 (October. 2018), ||V (I) || PP 40-46

"Study, Analysis and Refinement in Throughput of Stream Ciphers for Data Security"

Mr. Praneet R shah[1], Dr. Sunil Chavan[2], Dr. Basavaraj Neelgir[3]
[1](Dept. Of ECE, Ph.D. Scholar, VTU RRC, Belagavi.)
[2](Principal, Professor, SIGCOE, Navi Mumbai, Mumbai University, Mumbai.)
[3](Dept. Of ECE, BNMIT, Bangalore. VTU University, Belagavi.)
Corresponding Author: Mr. Praneet R shah

Abstract: Message privacy is the most significant feature of communication but particularly in wireless environment messages are highly insecure and encryption is must in such environment. Over a decades there has been momentous research going towards removing the attacks on different cryptographic algorithms. Aim of proposed research work is to study different stream cipher which includes ZUC, SNOW 3G and RC4 offering dependable security services in Long Term Evolution networks (LTE). The research work will also consider the performance analysis of stream ciphers based on the performance parameter such as weak keys, key vulnerability, risk, different attacks, simplicity, encryption speed, key/IV size, internal state space, performance, memory space, energy consumption. VHDL language is used to design the code and hardware implementation is done using XILINX's Virtex-5 FPGA.

Keywords- Long Term Evolution (LTE) , FPGA, SNOW 3G, RC4, ZUC.

Date of Submission: 29-09-2018 Date of acceptance: 14-10-2018

I. Introduction

Communication has become an crucial part of every-day life. Improvements in computing speed, digital storage capacities, network bandwidth and modern security techniques for the information in the channel are changing our life. Recent years, witness the development of data communication via internet and wireless networks, more information is frequently transmitted in digital forms that includes text, image, audio, video.

Security of the messages is the main concern in many communication applications. Considering the need of message privacy, cryptography concept is being introduced. Basically cryptography is a Greek word for "hidden writing". Cryptography works with problems which are allied with authentication, secrecy and integrity.

WLAN i.e. Wireless Local Area Network technology shows potential for a variety of types of wireless communications. 802.11 is IEEE standard which is one of the most commonly used for wireless communication standards. IEEE 802.11 is standard which not only provide implementation, but also provides the specifications for physical as well as MAC layers. This standard is extensively used in ad-hoc and client/server networks but particular attention should be specified to the security of information in transmission channel. The security of this standard is based on WEP protocol. WEP is having several limitations and also encryption had no provisions for a key rotation users to transmit using same key, which had made cracking the WEP even easier.

The Wireless Fidelity (Wi-Fi) alliance proposed a new security protocol called Wi-Fi Protected Access (WPA), in response to growing corporate concerns on wireless security. In WPA as the security algorithm RC4 stream cipher is also used with new self-motivated key management method, which is known as TKIP (Temporal Key Integrity Protocol). TKIP use message integrity code (MIC) in place of WEP's CRC-32 to ensure the data integrity. WPA is the secured solution for a upgradable equipment of the WEP but doesn't support to WPA2. as much as speed of transmission is concerned to WPA has edge above WPA2.

Advantages of the software implementation of security algorithm include easiness of portability, upgrade, and flexibility. However, a software implementation offers only limited physical security, especially with respect to key storage.

Alternatively, cryptographic algorithms with their connected keys which are actualized on the equipment by means of nature, extra physically secured as they can't exclusive of a stretch be changed by an outside assailant. In case, the algorithm smoothness is required to help the algorithm free conventions i.e. exchanging of encryption algorithms the equal number of as on a for each session premise. The heft of present day security conventions, i.e Secure Sockets Layer (SSL) or Internet Protocol Security (IPsec), permit numerous encryption algorithms. Reconfigurable gadgets, for example, FPGAs are a to a great degree appealing choice for an equipment usage as it give the adaptability of dynamic framework development and the capacity to effectively execute an extensive variety of capacities/algorithms. It has all the earmarks of being particularly applicable to concentrate on high-throughput usage for FPGA-based encryption.

1.1 CRYPTOGRAPHIC ALGORITHMS:

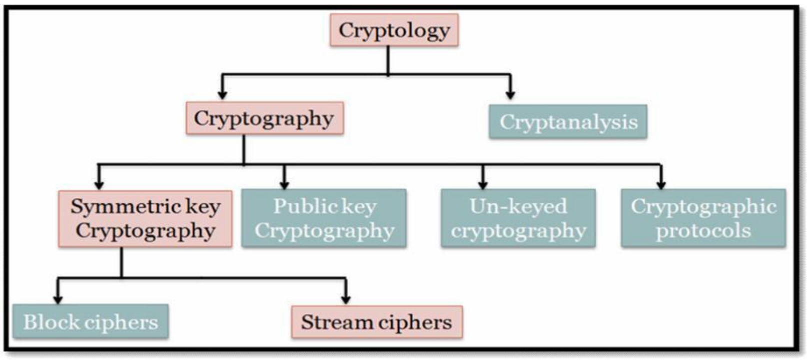


Fig. 1. Types of Cryptology

Cryptology is classified into two principal categories, namely viz. cryptography, the art of developing of new encryption techniques and viz. cryptanalysis, the science of breaking cryptographic tools. Cryptography is classified into four main disciplines: 1) Secret key or symmetric-key cryptography, 2) Public-key/asymmetric-key cryptography, 3) Un-keyed cryptographyand4) Cryptographic protocols. When the encryptions key is same as the decryption key, it is called secret key/symmetric key cryptography and when there exist a private key and a public key, it is called as public-key/asymmetric-key cryptography. The private as well as public key is related mathematically, but we cannot derive private key from a public key within any practical time.

Secret key/symmetric key cryptographic systems can be categorized into either block or stream ciphers. Block ciphers are the memory less algorithms which permutes N-bits of blocks the plaintext data in control of secret key and produce N-bit blocks of the encrypted data. In block ciphers stuffing is required, which decrease the speed of encryption, to overcome such drawback, Ron Rivest designed RC4stream cipher algorithm.

Stream ciphers or key stream generators have been widely used for message security of real time applications such as mobile phones; Global System for Mobile Communications (GSM) network, satellite TV, on line banking and secure military communications. These applications need information which is to be encrypted and decrypted at high speed. Stream ciphers operate serially by creating a stream of pseudorandom key bits and the key stream. Stream cipher does not endure from the error propagation, as in the block ciphers, because each bit is separately encrypted / decrypted from any other. They are usually a lot faster than that of block ciphers.

Block or stream ciphers work on the two basic principles confusion and diffusion. Confusion means attempt to make the connection between the encryption key and the cipher text as difficult as possible. Dispersal is used to front the arithmetical property of the data by spreading it throughout the cipher text.

1.2 STREAMCIPHERS:

Distinctive cryptographic algorithms offer diverse degrees of security. Their decision relies upon the fact that they are so difficult to break. In the event that the cost required to break a algorithm is more prominent than the estimation of the scrambled information, at that point the algorithm should be sheltered. On the off chance that the time required breaking a algorithm is longer than the time that the encoded information must stay mystery, and afterward likewise it is protected. On the off chance that the measure of information scrambled with a solitary key is not as much as the measure of information important to break the algorithm, it should be sheltered.

As a rule, the quality of encryption algorithm relies upon trouble in getting the key, which thusly relies upon both the figure utilized and the length of the key. Encryption quality is regularly portrayed regarding the length of the keys used to play out the encryption, implies the more the length of the key increasingly the quality. Enter length is estimated in bits. For instance, a RC4 symmetric-key figure with key length of 128 bits bolstered by Secure Sockets Layer (SSL) give altogether preferred cryptographic insurance over 40-bit keys for use with a similar figure. It implies 128-piece RC4 encryption is 3 x 1026 times more grounded than 40-bit RC4 encryption. Distinctive encryption algorithms require variable key lengths to accomplish a similar level of encryption quality.

The researchers had considered the factors such as simplicity, encryption speed, key / Initialization Vector (IV) size, performance, memory space, energy consumption, internal state space, output bits for study and development of cryptographic algorithms.7411

Stream ciphers such as SNOW 3G (submitted to the New European Schemes for Signatures, Integrity and Encryption (NESSIE) project), 128-EEA3 (GSM 3G and 4G, for ASIA region) and RC4 (Simplicity, always used in WEP, WPA and http) are considered for study due to their great and/or recent use, simplicity and security.

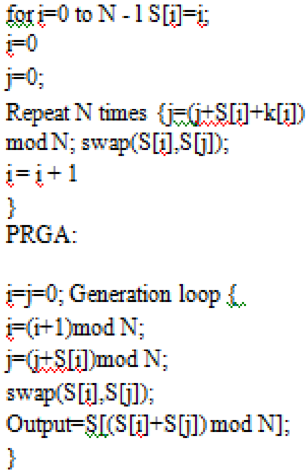
3GPP is a collaborative effort among telecommunications associations to make globally applicable 3rd Generation (3G) and more recently 4 th Generation (4G) mobile phone system specifications. 3GPP specifications are also based on the GSM specification. The groups leading the standardization of 3GPP are the European Telecommunications Standards Institute (ETSI), the Association of Japanese Radio Industries and Businesses/Telecommunication Technology Committee (ARIB/TTC), the China Communications Standards Association, the coalition for Telecommunications Industry Solutions (North America) and Telecommunications Technology Association (South Korea).

Another term 3GPP/LTE is the name given to an undertaking inside 3GPP to enhance the Universal Mobile Telecommunications standard (UMTS). Another arrangement of security algorithms (128-EEA3 and 128-EIA3) is being institutionalized for 3GPP/LTE/LTE-A remote systems worthy for Asian markets. These algorithms depend on the key stream generator ZUC (Named after Zu Chongzhi). The security algorithm 128-EEA3 is a stream figure that is utilized to encode/unscramble pieces of information utilizing a Confidentiality Key CK. The piece of information might be in the vicinity of 1 and 65504 bits in length. The algorithm utilizes ZUC as a key stream generator.

RC4 algorithm was composed by Ron Rivest of RSA Security in 1987; while it is authoritatively named "Rivest Cipher 4", the RC acronym is on the other hand comprehended "Ron's Code". RC4 was at first a prized formula, however in September 1994 a portrayal of it was namelessly presented on the Cipher punk's mailing list so it spilled out in 1994. It was soon posted on the sci.crypt newsgroup, and from that point to many destinations on the web, the algorithm is known to the vast majority of the cryptanalysis, it was not any more a prized formula.

RC4 uses a patchy length key from 1 to 256 bytes to initialize a 256-bytes array and can implemented in hardware and software. The RC4 algorithm works in two phases, Key Setup Algorithm (KSA) and Pseudorandom Generation Algorithm (PRGA). Key setup is the first and most difficult phase of this algorithm. During N-bit key setup (N being your key length), the encryption key is used to generate an encrypting variable using two arrays, state and key, and N-number of mixing operations. This N number of mixing operations of basic RC4 algorithm consists of swapping the bytes depending on KSA and PRGA as shown below.

KSA:



```
for i=0 to N - 1 S[i]=i;
i=0
j=0;
Repeat N times {j=(j+S[i]+k[i])
mod N; swap(S[i],S[j]);
i = i + 1
}
PRGA:

i=j=0; Generation loop {
i=(i+1)mod N;
j=(j+S[i])mod N;
swap(S[i],S[j]);
Output=S[(S[i]+S[j]) mod N];
}
```

Implementations of cryptographic algorithms in hardware usually achieve superior performance because it's encryption speed does not depends on length of a KEY and hacking of KEY is difficult as compared with software based ones as well as it is the growing requirements for high-speed and high-level of secure communications.

II. LITERATURE REVIEW

The environment for network security was evolved during the late 1960's and into the 1970, with the growth of Internet and LAN technologies; there was an increase in the quantity of data transferred. During 1969 when the first model of Internet- Arpanet was developed, most of its users were defence organizations, government companies and educational institutions who were more concerned with discovery rather than on destruction. The real need for network security was realized by the late 1980's with the birth of personal computers followed by Local Area cipher SNOW was proposed. The few attacks discovered, indicating certain weakness in the design. In the year 2003 another version of SNOW, called as SNOW 2.0 was proposed. The new edition of the cipher is more secure and also a bit quicker in software.

Inside the security engineering of the 3GPP framework privacy algorithm UEA2 and a trustworthiness algorithm UIA2 are institutionalized algorithms. These algorithms are completely determined in a typical archive. Each of these algorithms depends on the SNOW 3G algorithm. SNOW 3G is a word-situated stream figure that creates an arrangement of 32-bit words under the control of a 128-piece key and a 128-piece instatement variable. These words can be utilized to veil the plaintext. Initial a key introduction is performed, i.e. the figure is timed without delivering yield. At that point with each clocktick it creates a 32-bit expression of yield.

1) Paris Kitsos, Nicolas Sklavos and Athanassios N. Skodras proposed an FPGA implementation of ZUC stream cipher in 2011, but they got very low thoughput (2.08 Gbps) and they implemented it on XilinxVirtex 5.
2) Shadi Traboulsi, Nils Pohl, Josef Hausner, Attila Bilgic and Valerio Frascolla published a article on Power Analysis and Optimization of the ZUC Stream Cipher for LTE-Advanced Mobile Terminals in 2012, in this paper they have achieved the power saving successfully but to achieve this they had compromised on area. The hardware analysis is done using Faraday's 90 nm standard cell.
3) Lingchen Zhang, Luning Xia, Zongbin Liu, Jiwu Jing and Yuan Ma, were proposed optimized Implementations of SNOW3G and ZUC on FPGA in 2012. In this paper, they optimized the implementation of the SNOW 3G and ZUC on FPGA, and also evaluated their performance. Their implementation of SNOW 3G reaches a little higher Throughput than that of the best commercial IP core and optimized implementation of ZUC gives 40% performance improvement.
4) Eyad Taqieddin*, Ola Abu-Rjei, Khaldoon Mhaidat and Raed Bani-Hani, proposed an Efficient FPGA Implementation of the RC4 Stream Cipher using Block RAM and Pipelining in 2015. The main idea of this design is the use of a dual-port block RAM in the FPGA in order to better utilize the available logic and memory resources. Combined with a new pipelined hardware implementation, the new design achieves better performance. The design is described using Verilog HDL and synthesized and implemented using Xilinx ISE suite for different FPGA devices. The proposed design is also more efficient in terms of power consumption.
5) Sourav Sen Gupta, Anupam Chattopadhyay, were proposed High-Performance Hardware Implementation for RC4 Stream Cipher in 2013. In this paper, they presented a systematic study of the hardware implementation of RC4, and propose the fastest known architecture for the cipher. They combined the ideas of hardware pipeline and loop unrolling to design an architecture that produces 2 RC4 keystream bytes per clock cycle. They have optimized and implemented their proposed design using VHDL description.
6) Guang Zeng, Xiaodai Dong, proposed Reconfigurable Feedback Shift Register Based Stream Cipher for Wireless Sensor Networks in 2013 In this paper, they proposed a low complexity and energy efficient reconfigurable feedback shift register (RFSR) stream cipher. The RFSR adds one new dimension, reconfigurable cipher structure, to the existing stream ciphers. The proposed RFSR is then implemented on a field programmable gate array platform. Simulation results show that much lower power consumption, delay and transmission overhead are achieved compared to the existing microprocessor based cipher implementations
7) Poonam Jindal, Brahmjit Singh, were proposed a article on A Survey of RC4 Stream Cipher in 2015. In this paper, a chronological survey of the cryptanalysis on RC4 was presented beginning with its first public appearance to date. They have identified and presented the various weaknesses of RC4 cipher followed by the measure taken by various researchers to improve the security of the cipher.
8) Ghizlane ORHANOU, Said EL HAJJI, Youssef BENTALEB, were proposed SNOW 3G Stream Cipher Operation and Complexity Study in 2010. In this paper, a detailed study of the stream cipher SNOW 3G structure has been carried out and laso they have studied the two interactive modules which constitute the SNOW 3G algorithm and their respective components. The objective is to understand enough SNOW 3G operations and to study its time and space complexity. They found that SNOW 3G has a linear time complexity, which guarantee efficiency and rapidity during the encryption/decryption process.
9) Somnath S.Berad proposed Hardware Implementation of ZUC Stream Cipher in 2014. In this A ZUC high-speed hardware architecture is described, which has been implemented by means of an FPGA device. Experimental results prove that the ZUC implementation is a flexible solution for LTE applications. The implementation on FPGA achieves a throughput of 2.08 Gbps at a 65 MHz clock frequency.
10) Jasbir Kaur, Lalit Sood, proposed Comparison between Various Types of Adder Topologies. In this paper, the design of various adders such as Ripple Carry Adder, Carry Skip Adder, Carry Increment Adder, Carry

Look Ahead Adder, Carry Save Adder, Carry Select Adder, Carry Bypass Adder are discussed and are compared on the basis of their performance parameters such as area, delay and power distribution.

III. AIM, OBJECTIVES AND SCOPE

3.1 AIM:

Message privacy is one of most important feature of communication but especially in wireless communication messages are highly insecure and encryption is important in such environment. Over a last decade research directed has been significant towards removing the attacks on different cryptographic algorithms. Aim of proposed research work is to study different stream ciphers which includes SNOW 3G, 128-EEA3, and RC4. The research work will also consider the performance analysis of stream ciphers based on the performance parameter such as weak keys, key vulnerability, risk, different attacks, simplicity, encryption speed, key/IV size, internal state space, performance, memory space, energy consumption.

3.2. OBJECTIVE:

The key objective of the research is to analyze different cryptographic algorithms such as SNOW 3G, 128-EEA3, and RC4 and suggest the suitable stream cipher as per the requirement of application.

3.3. SCOPE:

Main scope of the research includes the implementation stream cipher. The system will be realized and the performance analysis of the system will be studied by defining proper performance indices. The study will evolve the technique that will offer proper refined stream cipher as per the requirement of network application. The algorithm may be validated by appropriate system modeling using a suitable platform, the algorithm will be used for message encryption and the scheme will be compare with conventional encryption method.

IV. METHODOLOGY

4.1 SNOW 3G:

SNOW 3G is a word-oriented stream cipher that generates a sequence of 32-bit words under the control of a 128-bit key and a 128-bit initialization variable[4]. First a key initialization is performed and the cipher is clocked without producing output[1]. Then the cipher operates in key-generation mode and it produces a 32-bit cipher text / plaintext word output in every clock cycle[1].

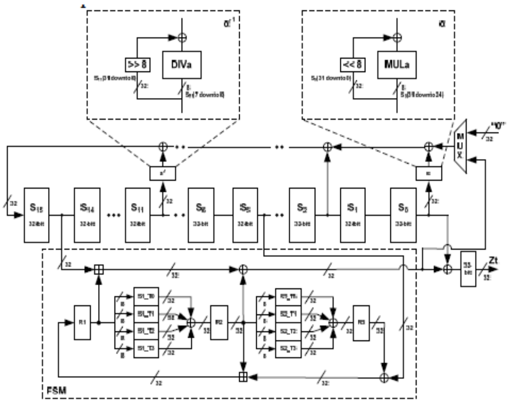


Figure 4.1: Block Diagram of SNOW 3G Stream Cipher.

4.2 ZUC:

ZUC is a word-oriented stream cipher [8] that takes a 128-bit Key and a 128-bit Initial Vector (IV) as input, and outputs a key stream of 32-bit words. ZUC has three logical layers[1]. The top layer is a Linear Feedback Shift Register (LFSR) of 16 stages, the middle layer is for bit reorganization (BR), and the bottom layer is a nonlinear function F[12]. The LFSR has 16 of 31-bit cells (s0 , s1 , , s15). This LFSR has two stages operations: the initialization stage and the working stage[1]. In the initialization, the LFSR receives a 31-bit input word u, which is obtained by removing the rightmost bit from the 32-bit output W of the nonlinear function[1] F The bit-reorganization layer extracts 128-bit 16 from the cells of the LFSR and forms 4 of 32-bit words, where the first three will be used by the nonlinear function[1] F in the bottom layer, and the last word will be involved in producing the key stream[14]. For the cipher operation firstly the key loading procedure expands the initial key and the initial vector into 16 of 31-bit integers as the initial state of the LFSR and then two stages are executed; initialization stage and working stage[1]. In the first stage, a Key/IV initialization is performed and the cipher is clocked without producing output[17]. The second stage is a working stage in which every clock cycle produces a 32- bit word of output[17].

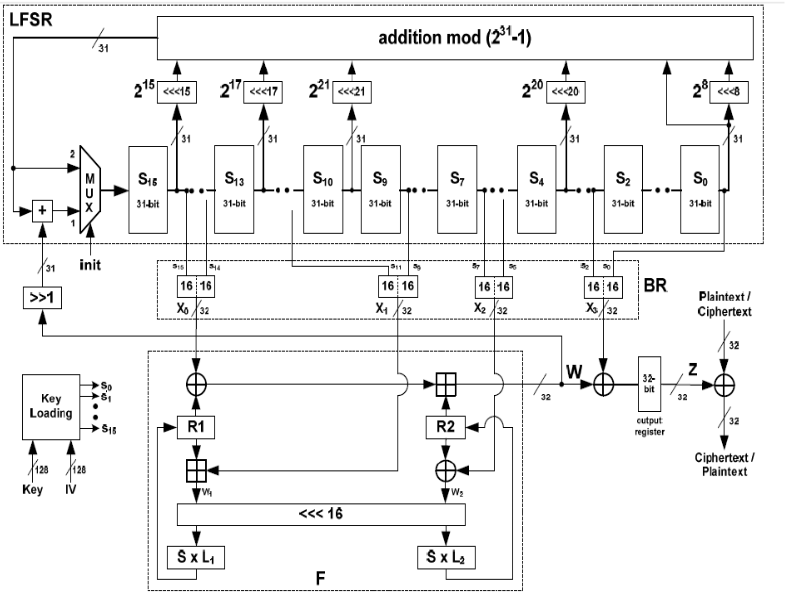


Figure 4.2: Block Diagram ZUC stream cipher.

4.3 RC4:

RC4 follows the design strategy used in stream ciphers. To extract the pseudorandom data bytes from a pseudorandom permutation is the basic design principle of RC4 stream cipher. RC4 has two working modules: first there is a KSA with key K as input (with typical size of 40-256 bits), and second is PRGA which generates a pseudo-random output sequence. The pseudo code for RC4. Fig 4.3 presents the complete working of RC4 encryption algorithm. KSA generates the 256 byte initial state vector S, by scrambling input state vector with a random key *K*. The expanded key is generated in the manner such that if secret key *k* is of length *l* bytes, the expanded key will be K[i] = *k* [*i* mod *l*] for $0 \leq i \leq N\text{-}1$. [16]Further *S* pairs are swapped and an initial state SN-1 is achieved at the end which is the input to the second module PRGA. [16]It generates the key-stream of words and is further XORed with the plaintext to produce a cipher text.

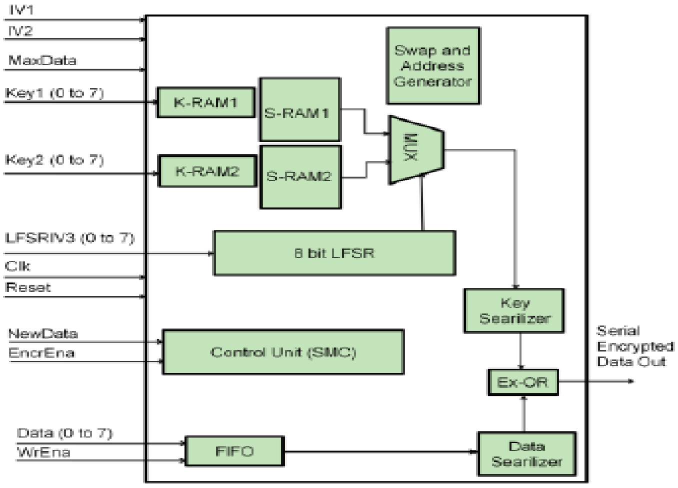


Figure 4.3: Block Diagram of RC4 Stream Cipher

REFERENCES

[1]. Paris Kitsos, Nicolas Sklavos, and Athanassios N. Skodras, **IEEE standard:** "An FPGA Implementation of ZUC Stream Cipher". 2011 14th Euromicro Conference on Digital System Design. pp. 814-817.

[2]. Traboulsi, S.; Pohl, N.; Hausner, J.; Bilgic, A.; Frascolla, V., **IEEE standard :** "Power analysis and optimization of the ZUC stream cipher for LTE-Advanced mobile terminals". Circuits and Systems (LASCAS), 2012 IEEE Third Latin American Symposium.

[3]. Lingchen Zhang, Luning Xia, Zongbin Liu, Jiwu Jing and Yuan Ma, **IEEE Standard:** "Evaluating the Optimized Implementations of SNOW3G and ZUC on FPGA". 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications. Pp. 436 -442.

[4]. Ghizlane Orhanou, Said El Hajji, Abdelmajid Lakbabi, Youssef BENTALEB, **IEEE Standard:** "Analytical Evaluation of the stream cipher ZUC". 2012.

[5]. Eyad Taqieddin*, Ola Abu-Rjei, Khaldoon Mhaidat, Raed Bani-Hani, **Science Direct:** "Efficient FPGA Implementation of the RC4 Stream Cipher using Block RAM and Pipelining". The 6th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2015).pp. 8-15.

[6]. Poonam Jindal*, Brahmjit Singh, **Science Direct:** "RC4 Encryption-A Literature Survey". International Conference on Information and Communication Technologies (ICICT 2014). Pp. 697 – 705.

[7]. Sourav Sen Gupta, Anupam Chattopadhyay, **IEEE Standard:** "High-Performance Hardware Implementation for RC4 Stream Cipher". IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 4, APRIL 2013. Pp. 730- 743.

[8]. Debrup Chakraborty, Cuauhtemoc Mancillas-L_opez, and Palash Sarkar, **IEEE Standard:** "STES: A Stream Cipher Based Low Cost Scheme for Securing Stored Data". IEEE TRANSACTIONS ON COMPUTERS, VOL. 64, NO. 9, SEPTEMBER 2015. Pp. 2691 – 2707.

[9]. Guang Zeng, Xiaodai Dong, Senior Member, IEEE, and Jens Bornemann, Fellow, IEEE Standard: "Reconfigurable Feedback Shift Register Based Stream Cipher for Wireless Sensor Networks". IEEE WIRELESS COMMUNICATIONS LETTERS, VOL. 2, NO. 5, OCTOBER 2013. Pp. 559 – 562.

[10]. Prerana Choudhari, Vikas Kaul, S K Narayankhedkar, International Journal of Applied Information Systems (IJAIS), "Security Enhancement Algorithms for Data Transmission in 4G Networks". ICWAC 2014. Pp. 25 -30.

[11]. Poonam Jindal, Brahmjit Singh,I.J. Computer Network and Information Security, " A Survey on RC4 Stream Cipher". 2015. pp. 37-45.

[12]. Ghizlane ORHANOU, Said EL HAJJI, Youssef BENTALEB, Contemporary Engineering Sciences, "SNOW 3G Stream Cipher Operation and Complexity Study". Vol. 3, 2010, no. 3. Pp. 97 – 111.

[13]. Mr. Berad S. S., Prof. Rahane S.B., International Journal of Engineering Research & Technology (IJERT), "An FPGA Implementation of ZUC Stream Cipher". Vol. 2 Issue 12, December – 2013. Pp. 2256 – 2260.

[14]. Somnath S.Berad, International Journal of Innovative Research in Science, Engineering and Technology, "Hardware Implementation of ZUC Stream Cipher". Volume 3, Special Issue 4, April 2014. Pp. 440 - 446.

[15]. Jasbir Kaur, Lalit Sood, International Journal of Computer Science And Technology, "Comparison Between Various Types of Adder Topologies". Vol. 6, Iss ue 1, Jan - March 2015. Pp. 62 – 66.

[16]. Parul Rajoriya, Nilesh Mohota (Professor) " Fpga Implementation of Image Encryption and Decryption Using Aes Algorithm Along With Key Encryption" IOSR Journal of Electronics and Communication Engineering (IOSR-JECE), e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 12, Issue 3, Ver. II (May - June 2017), PP 40-50

[17]. A.Vijaya Bhaskar, C.Ravi Shankar Hanuman, International Journal of Engineering Science and Technology (IJEST), "ZUC Stream Cipher Using Feedback Carry Shift Register" Vol. 4 No.06 June 2012, ISSN : 0975-5462

IOSR Journal of Engineering (IOSRJEN) is UGC approved Journal with Sl. No. 3240, Journal no. 48995.

Mr. Praneet R shah" "Study, Analysis and Refinement in Throughput of Stream Ciphers for Data Security" IOSR Journal of Engineering (IOSRJEN), vol. 08, no. 10 , 2018, pp. 40-46.