ISSN No:-2456-2165

Literature Review of Stream Cipher Techniques

Rojasree. V
Department of Computer Science,
Rajah Serfoji Govt. College(A),
(Affiliated to Bharathidasan University),
Thanjavur-613005, Tamilnadu, India.

Dr. J. Gnana Jayanthi
Department of Computer Science,
Rajah Serfoji Govt. College(A),
(Affiliated to Bharathidasan University),
Thanjavur-613005, Tamilnadu, India.

Abstract:- Nowadays data plays a very important role in all the business and corporate industries. It has become necessary to secure the data. Many methodologies are followed in order to keep the confidentiality, integrity and availability of valuable data. Here in this survey we consider the Symmetric cryptography algorithms and their reviews, innovations done in the perspective of multiple authors. The survey includes the analysis of the design architecture, code flexibility, system reliability, information and data security and also the limitations of the chosen symmetric cryptography through any medium of communication.

Keywords:- *Stream cipher, DES, AES, EDES, Triple DES, Blowfish, Two fish.*

I. INTRODUCTION

Modern cryptography is classified into two, (i) Private key (Symmetric) Cryptography and (ii) Public key (Asymmetric) Cryptography based on the key sharing between the sender and the receiver (Sr-Rr) [1, 2]. This paper presents a literature review done specifically to concentrate on the research aspects of symmetric cryptography.

Private Key cryptography is a mechanism in which same secret key is shared between Sr-Rr. The communication message is called the *plaintext* (M). M is to be encrypted into a *ciphertext* (C) a meaningless text using the secret key on Sr side before sending it to Rr. When this C reaches Rr, the same secret key is used to decrypt C to the meaningful information sent from Sr [3]. The functioning of symmetric cryptography is as shown in figure, FIGURE-1, below.

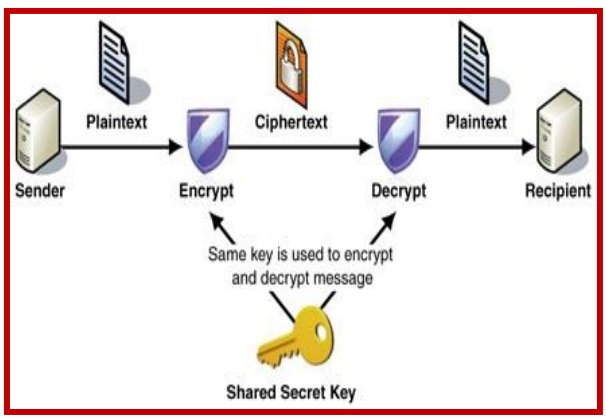

Fig 1: Symmetric key cryptography

Modern symmetric key cryptography, (both block cipher and stream cipher) uses a short secret bit stream that is divided into two parts a secret key and an Initialization Vector (IV) and performs two operations (i) generation of long key stream based on the input stream and (ii) a bit-by-bit encryption (XOR concatenation) of M with the key stream generated. Stream ciphers use secret key and IV with a fixed length for key stream generator [4]. The stream generators can be designed either using hardware (electronical circuits) or software and some of the wide used generators are presented.

Linear Feedback Shift Registers (LFSRs) are the common building blocks that have several statistical properties similar to the statistical properties of truly random strings. As the generation of new symbols are linear, few additional building blocks are needed to remove the linearity. The non-linearity in the key stream are removed by Irregular clocking, non-linear filters and decimation algorithms. Other remarkable electronical key stream generators are Feedback with Carry Shift Registers (FCSRs) that uses a feedback input and Non-Linear Feedback Shift Registers (NLFSRs) which uses a non-linear input [5]. The software programmed key generators are T-functions and lookup tables. These are used to generate pseudo random number streams for encryption in block and stream ciphers. Encrypt Stream Cipher Project (eSTREAM), the authorizing body for the random streams selected seven efficient and secure stream ciphers as follows RC-128, RABBIT, Salsa 20/12, SOSEMANUK and remaining hardware oriented Grain v1, MICKEY and Trivium [6].

Symmetric key cryptography is classified into two types namely (i) Block Ciphers and (ii) Stream Ciphers, based on how the encryption is performed. Block ciphers are the one in which, the encryption is done on chunks of bits at a time. Stream ciphers are the one in which, the encryption is done bit by bit as a stream of bits getting converted to cipher text [7, 8].

A literature study is carried out in stream ciphers. There are plenty of methods covered in the literature and this paper briefs most of the methods / algorithms, including the merits and demerits of stream ciphers [9].

The researchers have worked, analyzed these methods and algorithms; explored the loopholes or flaws; and projected their ideas and findings to provide better methods and algorithms. In spite of many proposals on stream ciphers they are not used widely, as they are used to encrypt only text

of limited length and not suitable for lengthy messages. Still stream cipher is used profoundly in Internet of Things (IoTs) and some smart devices where small text or word is to be validated and authenticated. Therefore this paper is targeted to survey the advancements in stream cipher algorithms till date, by various researchers to know what has happened so far in the research perspective and what different authors proposed and listed in their research.

The major objective of this paper is to open an eye on the reason for the development of various new symmetric stream cipher methods and thus highlighting the prospective design directions of symmetric stream ciphers. A concise report of the literature study on stream ciphers is presented in section-II. Section III summarizes the outcome of the literature. Section IV concludes the paper with our further research focus.

II. REVIEW OF LITERATURE SURVEY

Symmetric cipher system which is well known for its advantages in speed and scale of hardware implementation, symmetric cipher has a major part. It has always been an ever open research topic as it is used to for massive data transfers and resource constraints. With the advancement of Internet and communication technology, the requirement of the cipher algorithms has also increased rapidly as it plays a crucial role in securing the information in the digital world.

At the same time the environment where the cryptography algorithms are used, is also becoming complex day-by-day, thus imposing a necessity for a novel suitable design. To satisfy this requirement and provide a better cipher system to suite the need of the society a thorough review of the standardized cryptographic algorithms and improvement in the existing cryptographic techniques are required. The major principles of various symmetric stream cipher methods are reviewed, classified and summarized as follows.

James (1986) in his paper focused on two goals secrecy and/or authenticity and the security of two kinds, theoretical or practical security. The author considered the various attacks and has presented various examples and implementing a mathematical proving method on cryptographic algorithms to check for its secrecy and authenticity. *The paper gives a light on the detailed analysis of the security and authenticity of various algorithms mathematically thus paving a way of analyzing the latest algorithms in the similar mathematical approach* [10].

Martin *et al.* (2003) proposed a synchronous stream cipher called rabbit cipher. The rabbit stream cipher takes 128 bits secret key and 64 bits IV as input and the process done in four iterations. In all iteration the inner state of 513 bits are combined with the output of every 128 bits for which pseudo random binary digits are generated. These inner state bits are split into 8 state variables and 8 counter variables each of length 32 bits and a carry-bit. It is infeasible for an attacker to break these output blocks that generates a real random number combination of 2128 keys [11].

Sadkhn (2004) studied on cryptographic mechanisms from the era of Julius Ceasar till modern cryptography. The author also concentrated on the Arabic industrial status academic efforts in the field of cryptography in a search for new evolutionary methods for the security of data and information [12].

Hongjun (2004) proposed software efficient stream cipher called HC-256 with key stream and an initialization vector of length 256-bits to generate a key stream of maximum length 2^{128} bits. The HC-256 uses two secret tables used as S-Boxes out of which one is updated at each step and the other is used for 32-bit output. In the encryption process the key stream is XORed with the plaintext to get the cipher text and in the decryption process the cipher text is XORed with the key stream to get back the plaintext [13].

Bernstein (2005) proposed Salsa20, a successor AES, is a stream cipher with a hash function that works on the key in the counter mode. Salsa20 takes both input and output of 64byte. The author expanded the key size from 256-bit into 264 randomly accessible streams where each stream consists of 64byte blocks. The encryption is performed in three simple steps (i) hashing plain text with the key, (ii) breaking the result into 4-byte words and (ii) XORing the result with the plaintext. The salsa20 family also contains reduced round ciphers namely (i) Salsa 20/20, if there are 20 rounds, (ii) Salsa20/12, if there are 12 rounds and (iii) Salsa 20/8, if there are 8 rounds. The rounds are reduced to speedup the encryption / decryption process [14].

Martin *et al.* (2006) proposed a new stream cipher called Grain-128 which supported a key size of 128 bits and an Initialization vector of size 96 bits. The Grain-128 used very small hardware with limited number of gates to implement on any edge device used on Internet of Things [15].

Martin *et al.* (2006) after Grain-128 Martin et. al. proposed a family of stream ciphers, named Grain family, which includes Grain (with 80 bits) and GRAIN 128 (with 128 bits) specifically designed for areas where small size, power consumption and lesser cost. The functioning of Grain can be varied by making small variations in the hardware gates. The initial version of Grain called Grain-0 had many flaws which was rectified by the addition of a few variables into the design [16].

Christophe (2006) proposed a new stream cipher by replacing the building blocks of block cipher with an equivalent stream cipher element. Trivium is a simple stream cipher that takes a key and an IV of 80-bits each to produce 264 bits key stream. Trivium is a participant in eSTREAM final portfolio. Even though simple it is believed by author to survive devastating attacks [17, 18].

Chong *et al.* (2007) proposed a chaos-based stream cipher algorithm to enhance the security. The main stream generator is developed by three one dimensional chaotic maps and their non-linear transform. As this cipher algorithm uses three chaotic maps and so the enlarges the key space. [19]

Hongjun (2008) proposed a refined version of HC-256 named it HC-128 to secure 128-bit message stream. Similar to HC-256, HC128 also has two tables that is continuously changed at every 1024 steps. Every step generates a 32-bit output from a non-linear output filtering function. This is designed to suite super scalar microprocessor. The key generated in this is secure as it is an exhaustive search to recover the key [20].

Bernstein (2008) presented a successor of Salsa20 called ChaCha8 is a 256-bit stream cipher that is 8-round cipher. Similar to Salsa20, ChaCha8 follows 3 steps (i) 4 additions, (ii) 4 XORs and (iii) 4 rotations to invertible revise four 32-bit state words where as in Salsa20 the 3 steps affect only 4 words at a time. But the difference is that ChaCha applies the operations to update each word twice rather than once as in Salsa20. The diffusion rate is quicker in ChaCha as it allows the input word to change the output word at every quarter round. [21].

Berbain *et al.* (2008) proposed Sosemanuk that uses the base principles of Snow 2.0 and few transformations from SERPENT block cipher. Sosemanuk is a new synchronous software oriented stream cipher that is designed to improve the security and the efficiency of the stream cipher. Sosemanuk is considered a fastest algorithm on quite a few platforms for the reason that the data mapping design is good and exhibits low data cache pressure [22].

Babbage *et al.* (2008) proposed Mutual Irregular Clocking KEY stream generator called MICKEY Stream Ciphers, specifically designed for low resource platforms with high level of security. They implemented using two shift registers, R and S, for providing different modes of clocking for a selected control bit. MICKEY has two variants MICKEY-80 and MICKEY-128 representing the key size. R register works as Galois-stepping feedback field register and S register works as non-linear clock in two different ways. The statistical properties and protection against attacks of MICKEY was good and is guaranteed by the two shift registers R and S [23].

Yong *et al.* (2009) have proposed Nearest-neighbouring Coupled-Map Lattices (NCML) to generate pseudorandom number generator for stream cipher, using spatiotemporal chaotic system. In stream cipher if the sequence of key stream is maintained the same, it becomes easier for the intruder to identify the forth coming stream of message, hence in stream ciphers the key stream is made chaotic so as to generate random bit streams to encrypt the message. The concept of Chaos creation in stream cipher attracted number of researchers to create different methods in securing stream ciphers [24].

Jian *et al.* (2010) proposed an improved RC4 stream cipher which is used in TLS / SSL networking protocol in order to eradicate most of the weaknesses of the RC4 algorithm. The improved RC4s output is more random and fast as it uses a pseudo-random bit generator in RC4 and by increasing the number of internal states [25].

David *et al.* (2011) proposed a hardware-oriented stream cipher A2U2 that uses ideology from stream cipher and implementation methods form block cipher design with the help of less than 300 gates. A2U2 uses four building blocks "a counter, a combination of two nonlinear registers, an irregular change in the feedback function through a key-bit mixing mechanism and a filter function" as it has become an important need with the emerging Radio Frequency Identification (RFID) tags [26].

Bokhari *et al.* (2012) proposed a stream cipher BOKHARI using NLFSR and NLF function with secret key of length 128bits. The authors have discussed about several attacks on BOKHARI stream cipher but did not claim any mathematical proof of security [27].

El-Razouk *et al.* (2013) proposed two new hardware based stream cipher designs of the Welch-Gong transformations which prove cryptographic properties. They are (i) multiple outputs WG (MOWG) version and (ii) single output version based on normal representation. WG cipher works on keys of length 80, 96, 112 and 128 bits along with a suitable IV. It is apt to use the same size of key length and IV size to increase the strength of the cipher [28].

Igor *et al.* (2015) proposed a fuzzy synchronous stream cipher system using NLFSR to obtain a pseudorandom noise instead of pseudorandom number. This stream cipher is used for ciphering in telecommunication. The fuzzy logic and the LFSRs are used to generate random sequence. Four LFSRs are used to produce pseudo-random sequences to make the system strong against cryptanalysis [29].

Kuznetsov *et al.* (2016) proposed STRUMOK a word based stream cipher by using basic design principles of SNOW2.0, where a word of 64bits is chosen. The author specified that STRUMOK uses a productive key stream generation procedure. The functioning of STRUMOK is good in a 32bit computing system also [30].

Ahmed *et al.* (2017) have proposed a security algorithm based on Lorenz Stream cipher [31] with the help of two FPGA boards. For data encryption they used two Lorenz generators in main generator in the chaotic region and an auxiliary Lorenz generator. The data transferred is received and recovered at the receiver [32].

Patrik *et al.* (2018) proposed a series of SNOW ciphers called SNOW-V in an idea to meet the virtualization environment relevant for the 5G industrial environment. The general FSM and LFSR are previous version of SNOW 3.0 / SNOW 2. In order to provide confidentiality and integrity at the same time, they introduced Authenticated Encryption with Associated Data (AEAD) operational mode. By increasing the key length from 32-bits to 128-bits in the new model makes it easy for SNOW-V to make authentication framework in Galois Message Authentication Code (GMAC) [33].

Prathima *et al.* (2019) proposed a Rabbit algorithm that uses a pipelined methodology for any forms of data. This

architecture is introduced with pipelined approach to reduce the critical path delay and thereby increase speed [35].

Alexander *et al.* (2019) proposed a nonlinear quarter round function QR which applies ChaCha stream cipher similar to the salsa family of stream ciphers. They designed this algorithm as nonlinear Quarter round function with QR(a, b, c, d) where two rows of Matrix V to be processed at a time. They designed QR function based on four additions in F_2^{32}, which is done by four XORs and four rotations on the 32-bit input words *a, b, c* and *d*. The QR changes each input word twice thus affecting the next word. By these processes the authors introduced the detection of any odd-weight error on input, output and intermediate signals [36].

Anna *et al.* (2019) proposed "All-Optical Layered encryption" by generating an optical stream cipher using an Field Programmable Gate Array (FPGA) on an AES circuit to create a stream of bit that are created by the optical interference. The authors generated a long optical key stream using optical light source [37].

Khafagy *et al.* (2020) proposed a hybrid-key stream cipher mechanism (HKSCM) to minimize the time taken for encryption and decryption. HKSCM included a One-Time Pad (OTP) encryption algorithm and AES algorithm. The OTP key is encrypted using AES algorithm and is included in the encrypted file. HKSCM is mainly designed to secure the fragmented data of the HADOOP environment [38].

Yevgeniy *et al.* (2012) introduced "Key-Insulated Symmetric Key Cryptography and Mitigating Attacks against Cryptographic Cloud Software" to lessen the effect of various attacks on symmetric key cryptographic algorithm. They also created a kernel virtual machine code so that also proved to be an implementation of mitigating the attacks into the operating system [39].

Varol *et al.* (2017) studied on safeguarding some text and speech using symmetric encryption by converting the content to be sent is first encrypted and then encapsulated so that it cannot be understood by any cipher algorithm [40].

Ximin *et al.* (2018) designed an algorithm for invocation mechanism Free to Add (FTA) to be used in IPsec. *This algorithm proved to solve the impacts of IPsec on the network applications and to resolve the unnecessary consumption of time and memory caused by traditional IPsec processes.* The contributions of this paper are software defined invocation of Free-to-Add (FTA) routine to IPsec so that the etire process becomes software controlled. The block diagram is as in figure below. The average processing rate under a full-load CPU for these algorithms is as given in the table below [41].

Shashank *et al.* (2018) has designed strong and intuitive game-based ideas that are easy to understand using Distributer symmetric key encryption with new notions of correctness, privacy and authenticity in the presence of hackers and attackers. All the base mathematical concepts at every level of distributed symmetric key encryption are implemented with well defined algorithms [42].

Shweta (2018) has designed a new protocol for key generation and key sharing using symmetric key cryptography. The authors state that the protocol is secure as they use symmetric keys. They also add on that "the protocol could be used in varied number of applications where simplicity and security are major requirement" [43]. The validity of the statement of the author is yet to be proved.

III. INFERENCES OF THE LITERATURE REVIEW

It is clear from the above papers that all the symmetric stream key cryptography mechanisms had it own pros and cons. Among all the issues addressed by different researchers it is obvious that the single secret key shared between the sender and the receiver is to be shared through some means such that the key is not known to any other third party. Moreover there are number of papers addressing on the performance of the mechanisms used in encryption and decryption which shows that the performance behavior and efficiency of each and every crypto mechanism creates a serious issue in implementing a cryptography mechanism. The space occupied by the source encryption or decryption program, the space occupied by the key space and the strength of the keys (how tough it is to guess the secret key used) all together decides the success of symmetric cryptographic mechanism. Few authors have tried to overcome the negative issues of an existing encryption program they tried to combine two or three cryptography mechanisms or they combined the symmetric mechanism with steganography (method of hiding in an image or wave) so that at least the data stored could me recovered. Almost all the algorithms prove this by showing at least one drawback in each method of symmetric key cryptography.

To specify, the rabbit stream cipher is prone to key stream bias with a complexity of 2^{158}, the finding of this bias is critical and could not be neglected while using. The Julius Ceasar cryptography is considered a good and simple encrypt method, but the vulnerability is due to the small key size that allows the attacker to perform brute force attack. The smaller key size is itself a drawback for the Julius Ceasar cipher to avoid this when key size is increased the storage also increases that is not desirable as it increases the hardware cost. The key generated in HC-256 is assumed to be secured as it is an exhaustive search to recover the key. Chacha8 is designed from Salsa20 in order to increase the speed of performance with the same security level as that of salsa20. In ChaCha the resistance towards attacks is achieved by diffusion per round at the same time preserving the time-period. The use of registers is also reducing in ChaCha when compared to Salsa20. To our knowledge, Grain-128 has smaller gate count in hardware. When differential fault analysis was applied on Trivium it disclosed the private key after approximately 43 fault injections using a chosen cipher text attack scenario. The HC-128 a successor to HC-256 passed 3 rounds of ECRYPT stream cipher project when exposed to differential fault analysis it broke in about 7968 faults. While SOSEMANUK is a well known fast cipher but its implementation uses a lookup table with state-dependent address thus very prone to side channel attacks, this is a very big threat to us the SOSEMANUK with as safety lock for the lookup table. Mickey uses less power and lesser gates so

could be used in situation where power and space is crutial. The system is put into 16 various tests suggested by US NIST to check for the efficiency of the randomness and strength. NCML creates the pseudorandom bit streams to cipher the message randomly and assures that the algorithm is strong and fast enough to randomly generate the cipher stream. NCML generates a good stream cipher for e-commerce applications. There are several attacks on BOKHARI stream cipher but did not claim any mathematical proof of security. WG Stream cipher has all the cryptographic properties of WG transformation sequences, is resistant to Time/Memory/Data trade off attacks, algebraic attacks and correlation attacks, and can also be implemented in hardware. Many researchers have proved that WG stream cipher is not secure as it is prone to algebraic attack, Key recover attack and distinguishing attack, therefore it is not recommended. The fuzzy logic LFSR passed the 16 randomness test from NIST Test suite and is considered to be strong enough to withstand all kinds of cryptanalysis. The nonlinear quarter round QR function is also a derivative of Salsa with the same architecture. In optical layered encryption of stream cipher the optical XOR and optical LFSR are available only in experimental area and remain difficult to deploy. The implementation of signal re-modulation and encryption-decryption of optical signals requires further learning. A synchronization delay can occur if the circulator for key and data are not synchronized and a system designed and implemented without considering these factors is likely to fail.

IV. CONCLUSION

From the survey of all the scholarly papers it is clear that almost all the symmetric key cryptosystems work absolutely excellent until and unless the single secure key is maintained as a secret between the sender and the receiver. Once the key is broken or published, anyone could find out the message shared between the sender and the receiver. From budding researchers point of view the survey puts a spark on developing a new algorithm that works with all the goodies of the symmetric key algorithms at the same time avoids the vulnerability of the commonly shared key. A new algorithm that replaces overcomes the weaker common private key method could be designed.

ACKNOWLEDGEMENT

A sincere thanks and gratitude is expressed by the authors to the Tamil Nadu State Council for Higher Education (TNSCHE) and Department of Science and Technology (DST), India, for sponsoring this research works.

REFERENCES

[1]. Evolution of Cryptography. @url: https://sherpasoftware.com/blog/the-evolution-of-cryptography/ Last visited on 21-03-2020.
[2]. Mohd Zaid Waqiyuddin Mohd Zulkifli, “Evolution of Cryptography”, 17 January 2007 @url http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.698.2641&rank=190.
[3]. S. Vollala, V. Varadhan, K. Geetha, N. Ramasubramanian, "Efficient modular multiplication algorithms for public key cryptography", In the Proceedings of the IEEE International Advance Computing Conference (IACC), E-ISBN: 978-1-4799-2572-8, PP:74-78, 2014, Gurgaon, @IEEEXplore, DOI: 10.1109/IAdCC.2014.6779297.
[4]. A. Engelmann, A. Jukan, "Toward All-Optical Layered Encryption: A Feasibility Analysis of Optical Stream Cipher”, In the IEEE Transactions on Information Forensics and Security”, ISSN: 1556-6013, Vol. 14, No. 10, PP: 2689-2704, Oct. 2019, DOI: 10.1109/TIFS.2019.2904793.
[5]. E. B. Barker, J. M. Kelsey, “Recommendation for Random Number Generation using Deterministic Random Bit Generators”, In the Special Publication of National Institute of Standards and Technology, Supersedes Published 800-90A Revision 1, National Institute of. Standard Technology, 109 pages (June 2015) CODEN: NSPUE2, http://dx.doi.org/10.6028/NIST.SP.800-90Ar1.
[6]. “eStream,” 2012. [Online]. Visited on 12.08.2019, Available @URL: http://www.ecrypt.eu.org/stream/
[7]. “AES: The Advanced Encryption Standard”, Last visited on 21-Mar-2018, @url: https://competitions.cr.yp.to/aes.html
[8]. Joan Daemen, Vincent Rijmen, “AES submission document on Rijndael”, Rijndael AES Proposal. Website: http//:www.csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael-ammended.pdf (1999).
[9]. Chowdhury, Z. J., Pishva, D., Nishantha, G. G. D, “AES and Confidentiality from the Inside Out”, In the Proceedings of the 12th International Conference on Advanced Communication Technology (ICACT, 7-10 February 2010), ISBN: 978-1-4244-5427-3, PP:1587-1591, 2010, South Korea, @IEEEXplore
[10]. Massey, J. L. "Cryptography, A Selective Survey”, In the Proceedings of the Second Tirrenia International Workshop on Digital Communications", PP: 3-25, 1986.
[11]. Boesgaard, Martin, et al. "Rabbit: A New High-Performance Stream Cipher." In The Proceedings of the International Workshop on Fast Software Encryption, ISSN 0302-9743, PP: 307-329 Springer, Berlin, Heidelberg, 2003.
[12]. S. B. Sadkhan, "Cryptography : Current Status and Future Trends", In the Proceedings of the International Conference on Information and Communication Technologies: From Theory to Applications, ISBN: 0-7803-8482-2, PP:417-418, 2004, DOI:10.1109/ICTTA.2004.1307809.
[13]. Wu, Hongjun. "A New Stream Cipher HC-256", In the Proceedings of the International Workshop on Fast Software Encryption (FSE), Lecture Notes in Computer Science, vol 3017, PP: 226-244, 2004, Springer, Berlin, and Heidelberg. https://DOI.org/10.1007/978-3-540-25937-4_15
[14]. Bernstein, Daniel J. "Salsa20 specification", eSTREAM Project algorithm description, http://www. ecrypt. eu. org/stream/salsa20pf. html (2005).

[15]. Hell, M, Johansson, T, Maximov, A & Meier, "A Stream Cipher Proposal: Grain-128", In the Proceedings of the IEEE International Symposium on Information Theory, ISBN 1-4244-0504-1, PP. 1614-1618, 2006, Seattle, WA, United States, 2006/07/09. https://doi.org/10.1109/ISIT.2006.261549.

[16]. Hell, Martin, et al. "The Grain family of stream ciphers - New Stream Cipher Designs", In Lecture Notes in Computer Science, ISBN978-3-540-68350-6, Vol 4986 PP: 179-190, Springer, Berlin, Heidelberg, https://doi.org/10.1007/978-3-540-68351-3_14.

[17]. De Cannière, Christophe. "Trivium: A Stream Cipher Construction Inspired By Block Cipher Design Principles", In the Proceedings of the International Conference on Information Security, ISBN:978-3-540-38341-3, Vol 4176. PP: 171-186, 2006, Springer, Berlin, Heidelberg. https://doi.org/10.1007/11836810_13.

[18]. De Cannière Christophe, Bart Preneel. "Trivium." New Stream Cipher Designs - The ESTREAM Finalists, ISBN: 9783540683506 Springer, Berlin, Heidelberg, PP: 244-266, https://doi.org/10.1007/978-3-540-68351-3_18, 2008.

[19]. Fu, Chong, Fang-fang Zhang. "A Novel Stream Cipher Algorithm Based On Chaotic Maps", In the Proceedings of the IEEE Conference on TENCON-2007, ISBN: 978-1-4244-1271-6, 2007, DOI: 10.1109/TENCON.2007.4429127.

[20]. Wu, Hongjun. "The Stream Cipher HC-128", In the Publication of New stream cipher designs. New Stream Cipher Designs, ISBN : 978-3-540-68350-6, Vol. 4986, PP: 39-47, Springer, Berlin, Heidelberg, 2008, DOI: 10.1007/978-3-540-68351-3_4.

[21]. Bernstein D, "ChaCha, A Variant of Salsa20", January 2008, http://cr.yp.to/chacha/chacha-20080128.pdf.

[22]. Berbain, Côme, et al. Côme Berbain, Olivier Billet, Anne Canteaut, Nicolas Courtois, Henri Gilbert, Louis Goubin, Aline Gouget, Louis Granboulan, Cédric Lauradoux, Marine Minier,Thomas Pornin,Hervé Sibert, "Sosemanuk, A Fast Software-Oriented Stream Cipher", In the Publications of Lecture Notes in Computer Science book series- New stream cipher designs. Vol: 4986, PP:98-118, DOI:10.1007/978-3-540-68351-3_9.

[23]. Babbage, S., Dodd, M. "The MICKEY Stream Ciphers, New Stream Cipher Designs", The eSTREAM Finalists, Lecture Notes in Computer Science. In: Robshaw, M., Billet, O. (eds.), ISBN: 9783540683506, Vol. 4986, PP. 191–209. Springer, Berlin (2008), https://doi.org/10.1007/978-3-540-68351-3_15.

[24]. Longyan Luo, Qing Xie, Haijiang, Tian, Huaqian Yang, "A Fast Stream Cipher Based On Spatiotemporal Chaos", In the Proceedings of the IEEE International Symposium on Information Engineering and Electronic Commerce, ISBN : 978-0-7695-3686-6/09,PP:418-422, 2009, DOI 10.1109/IEEC.2009.93

[25]. Xie, Jian, Xiaozhong Pan, "An Improved RC4 stream cipher", In the IEEE Proceedings of the International Conference on Computer Application and System Modeling (ICCASM 2010), ISSN: 2161-9069, Vol. 7, PP: 156-159, DOI: 10.1109/ICCASM.2010.5620800, 2010.

[26]. David, Mathieu, Damith C. Ranasinghe, and Torben Larsen. "A2U2: A Stream Cipher For Printed Electronics RFID Tags", ISBN: 978-1-4244-9607-5, DOI: 10.1109/RFID.2011.5764619. 2011

[27]. Bokhari, M. U., and Faheem Masoodi. "BOKHARI: A New Software Oriented Stream Cipher: A Proposal", In the IEEE Proceedings of the World Congress on Information and Communication Technologies, ISBN: 978-1-4673-4805-8, PP: 128-131, DOI: 10.1109/WICT.2012.6409062, 2012.

[28]. El-Razouk, Hayssam, Arash Reyhani-Masoleh, and Guang Gong. "New implementations of the WG stream cipher", In the IEEE Transactions on Very Large Scale Integration (VLSI) Systems, ISBN: 978-1-4799-7103-9. Vol 22.9 (2013): PP: 1865-1878, DOI:1109/TVLSI.2013.228009.

[29]. Anikin, Igor V., and Khaled Alnajjar, "Fuzzy Stream Cipher System", In the Proceedings of the International Siberian Conference on Control and Communications (SIBCON), ISBN: 978-1-4799-7103-9, IEEE, 2015.

[30]. Kuznetsov, Olexandr, Mariya Lutsenko, and Dmytro Ivanenko, "Strumok Stream Cipher: Specification and Basic Properties", In the Proceedings of the IEEE Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), ISBN: 978-1-5090-5715-3, 2016. 10.1109/INFOCOMMST.2016.7905335.

[31]. Alshammari, Ahmed S., Mohamed I. Sobhy, and Peter Lee. "Secure digital communication based on Lorenz stream cipher", In the Proceedings of the 30th IEEE International System-on-Chip Conference (SOCC), ISBN: 978-1-5386-4035-7, 2017, DOI: 10.1109/SOCC.2017.8225999.

[32]. "Lorenz cipher" @ URL: https://www.codesandciphers.org.uk/lorenz/fish.htm Last Visited on 17-Sep-2020.

[33]. Ekdahl P, Johansson T, Maximov A, et al. "A new SNOW stream cipher called SNOW-V" 2018. https://eprint.iacr. org/2018/1143.pdf, Vol.2019, Issue:3, PP: 1-42. https://doi.org/10.13154/tosc.v2019.i3

[34]. Prathima N,Chetan S, Syed M Rehman, "ASIC Implementation of Rabbit Stream Cipher Encryption for Data", In the Proceedings of the 5th IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE) ISBN : 978-1-7281-4499-3/19, PP:1-4,2019, DOI: 10.1109/WIECON-ECE48653.2019.9019903.

[35]. Alexander Zeh, Manuela Meier and Viola Rieger, "Parity-Based Concurrent Error Detection Schemes for the ChaCha Stream Cipher", In the Proceedings of the IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), ISBN:978-1-7281-2260-1/19 , pp. 1-4, 2019, Netherlands, DOI: 10.1109/DFT.2019.8875478.

[36]. A. Engelmann and A. Jukan, "Toward All-Optical Layered Encryption: A Feasibility Analysis of Optical Stream Cipher", In IEEE Transactions on Information Forensics and Security, Vol. 14, No. 10, PP: 2689-2704, Oct. 2019, DOI: 10.1109/TIFS.2019.2904793.

[37]. Khafagy, Omar Helmy, Mohamed Hasan Ibrahim, Fatma A. Omara. "Hybrid-Key Stream Cipher Mechanism for Hadoop Distributed File System Security", In the Proceedings of the IEEE International Conference on Innovative Trends in Communication and Computer Engineering (ITCE), ISBN: 978-1-7281-4801-4, PP: 39-43, 2020, DOI: 10.1109/ITCE48509.2020.9047775.

[38]. Yevgeniy Dodis, Weiliang Luo, Shouhuai Xu, Moti Yung, "Key-Insulated Symmetric Key Cryptography and Mitigating Attacks Against Cryptographic Cloud Software", In the Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security (ASIACCS '12), ISBN: 978-1-4503-0564-8/11/03, PP:57–58, 2012, Korea, DOI: 10.1145/2414456.2414489.

[39]. N. Varol, F. Aydoğan, A. Varol, "Cyber Attacks Targetting Android Cellphones", In the Proceedings of the 5th International Symposium on Digital Forensics and Security (ISDFS 2017), ISBN: 978-1-5090-5835-8, PP: 1-5, Tirgu Mures, 2017, DOI: 10.1109/ISDFS.2017.7916511.

[40]. Ximin Yang, Deqiang Wang, Wei Feng, Jingjing Wu, Wan Tang, "Cryptographic Algorithm Invocation Based on Software-Defined Everything in IPsec", Wireless Communications and Mobile Computing, Vol. 2018, Article ID 8728424, 11 Pages, 2018. https://doi.org/10.1155/2018/8728424.

[41]. Shashank Agrawal, Pratyay Mukherjee, Peter Rindal, "Dise: Distributed Symmetric-Key Encryption", In the Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, PP: 1993–2010, January 2018, https://doi.org/10.1145/3243734.3243774

[42]. Arora, Shweta, Muzzammil Hussain, "Secure Session Key Sharing using Symmetric Key Cryptography", In the Proceedings of the IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI), PP: 850-855, 2018, DOI: 10.1109/ICACCI.2018.8554553.