Design of Modified Exclusive-128 Bit NLFSR Stream Cipher and Randomness Test

K. Rajam
B.S. AbdurRahman University
Chennai – 600 048
India

I. Raja Mohamed
B.S.AbdurRahman University
Chennai – 600 048
India

K.J. Jegadish Kumar
S.S.N. College of Engineering
Chennai – 603110
India

ABSTRACT
In this paper, we describe modified Exclusive-128 NLFSR stream cipher which generates 128 bit keystreams using only NLFSR element as its main function and XOR operation. It consists of different sizes of NLFSRs both in Fibonacci and Galois configurations which offer better trade off between the algorithm security and hardware capability. Further, using this modified version of Exclusive-128 NLFSR stream cipher, analysis has been done for pseudorandom test to prove that this stream cipher is highly non-linear and truly randomness when all the initial key inputs are either zero and/or one.

Keyword
Cryptography, Stream cipher, NLFSR, Fibonacci configuration, Galois configuration, NIST Randomness Test.

1. INTRODUCTION
Cryptography is a technique that is used to protect information confidentially from unauthorised person and is associated with secrecy, authentication and integrity. Cryptographic systems are classified as secret key (Symmetric) cryptosystems and public key (Asymmetric) cryptosystems. In secret key cryptosystems, a single key is used for both encryption of the plaintext and decryption of the ciphertext. In public key cryptosystem, two different keys are used to transform a message into an unreadable form, decryptable only by using adifferent but matching private key.

Symmetric cryptosystems are further classified as block ciphers and stream ciphers. Block ciphers are memoryless algorithms that permute *N*-bit blocks of plaintext data under the influence of the secret key and generate *N*-bit blocks of encrypted data. Stream ciphers containinternal states of key and a shift register operate serially by generating a pseudorandom bit and bitwise XORed with the data for encryption/decryption. Stream ciphers have no standard model for their construction design, which leads cryptographers to construct various models for stream cipher. It is totally different from block ciphers.

Stream ciphers belong to the family of symmetric key ciphers thatare important in securing streaming information.The stream ciphers are classified into three main categories [1] hardwarebased stream ciphers, softwarebased stream ciphers and hybrid designs of stream ciphers. The hardwarebased stream cipher includes Feedback Carry Shift Register (FCSR) / Non Linear Feedback Shift Register (NLFSR) based stream cipher, Clock Control based stream cipher and Linear Feedback Shift Register(LFSR) [2]based stream ciphers.Stream ciphers do not affectthe error propagation, as in the block ones, because each bit is independently encrypted/decrypted from any other. The stream cipherfeatures have been used for several communication protocols, especially wireless ones, like Bluetooth.

The study of cryptanalysis method in analysing information system (encrypted) is to study the hidden aspects of the system andto finda secret key [3]. The most common cryptanalysis attacks are: (1) Brute force attacks, (2) Algebraic attacks and (3) Linear attacks.Brute force attack is a strategy that involves systematically checking all possible keys until the correct key is found. The key length used in the encryption determines the practical feasibility of performing a brute-force attack, with longer keys are exponentially more difficult to crack than shorter ones.

Table 1.Key size (vs) Brute Force Time estimation

Key Size	Permutations	Brute Force Time
8	2^8	0 milliseconds
40	2^{40}	0.015 milliseconds
56	2^{56}	1 second
64	2^{56}	4 minutes 16 seconds
128	2^{128}	149,745,258,842,898 years

The table 1 shows that the Key size verses Brute Force time estimation of exhaustive key search attack. A key size of 8, 40, 56, 64 bit can be attacked and cracked easily through Brute Force attack cryptanalysis since the number of permutations and also the Brute Force time is considerably very less compared to 128 bit key size[4].

The hardware implementationismainly used in providing the security needed for various cryptographic applications. Some of the stream cipher using NLFSRs to generate random sequences are GRAIN[5] and VEST[6]. Grain stream cipherusestwo types of shift registers, Non Linear Feedback Shift Register (NLFSR)andFeedback with Carry Shift Registers (FCSR).The NLFSRs are generally used to eliminate and destroy the linearity found in LFSRs. The NLFSR design applies a non-linear function in the shift register to ensure the non-linearity in the output values from the corresponding shift register. Several stream cipher designs useNLFSR, and one such stream cipher is the Grain stream cipher. It was developed in 2004 and submitted to eSTREAM project for evaluation in 2005[5]. However, Grain was attacked in 2006 by two different cryptanalysis as reported byMaximov, 2006 and Kucuk,2006.Some method of transforming LFSRs to NLFSR are clock controlled generator and stop and go generators [2].

2. IMPLEMENTATION OF THE STREAM CIPHER

As discussed in the previous section, a stream cipher is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (keystream). In this stream cipher each plaintext digit is encrypted one at a time with the corresponding digit of the key stream, to give a digit of the ciphertext stream. The pseudorandom key-stream is typically generated serially from a random seed value using digital shift registers. The seed value serves as the cryptographic key for decrypting the ciphertext stream. A stream cipher generates successive elements of the key stream based on an internal state. This state is updated essentially in two ways: either the state changes independently the plaintext or ciphertext messages. By contrast, self-synchronizing stream ciphers update their state based on previous ciphertext digits.

Shift Registers are nothing but a simple register which shifts the values and employs some functions to update its bits. Generally a shift register is a cascade of flip-flops, sharing the same clock, which has the output of anyone but the last flip-flop connected to the "data" input of the next one in the chain, resulting in a circuit that shifts by one position the one-dimensional "bit array" stored in it. The shifting in the data present at its input and shifting out the last bit in the array, is done at the transition of the clock input. Shift registers can have both parallel and serial inputs and outputs. These are often configured as Serial-In Parallel-Out (SIPO) or Parallel-In Serial-Out (PISO). In order to improve the non-linearity of shift registers, a feedback function with a definite feedback polynomial is used. A linear feedback shift register (LFSR) is a shift registerwhose input bit is a linear function of its previous state. Mostly used linear function of single bits is XOR, thus normally it is a shift register whose input bit is driven by XOR of some bits of the overall shift register value. Three methods of implementing NLFSR namely(a) Simple configuration, (b) Fibonacci configuration and (c) Galois configuration are discussed below.

1. In a simple configuration, XNOR gates are used as feedback function.

2. In Fibonacci configuration, feedback is applied only to the last bit.It is a Non-linear combination of taps to produce long periodic states [7] as shown in fig.1.

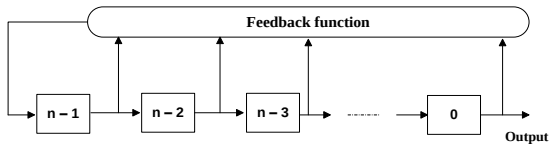

Figure1: Fibonacci configuration

3. In Galois configuration, feedback is applied to each and every bit [7] as shown in fig.2.

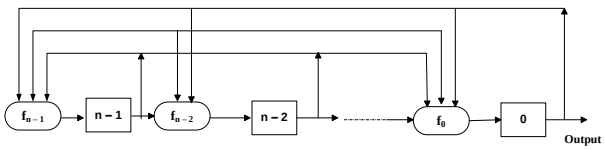

Figure 2: Galois configuration

In the Galois type of NLFSR each bit i isupdated according to its own feedback function.

The circuits in which number ofcomponents required for implementing feedback functions of individual bits is usually smaller than the circuits implementing the feedback function of the Fibonacci NLFSR, and the propagation time can potentially be reduced [8].

This makes Galois NLFSRs attractive for stream cipher applications in which high key stream generation speed is important.

The proposed stream cipher is a 128 bit stream cipher which generates 128 bit key stream. The 128 bit key stream is XORed with the plaintext to produce the ciphertext. The 128 bit key stream is produced using six non-linear feedback shift registers each used in either Fibonacci or Galois configuration. The idea of implementing this new modified stream cipher is adopted from the A5/1 and modified A5/1 stream ciphers [9]. The A5/1 stream cipher is modified by adding a few shift registers to the existing ones and changing the feedback functions so as to make it more secure and less susceptible to attacks. Since our proposed stream cipher is constructed by adding more number of variant sizes of NLFSRs,it is more secure specifically resistant to linear cryptanalysis.

Fig.3 shows internal view of Exclusive-128 bit NLFSR stream cipher.The Exclusive-128 NLFSR stream cipher generates a 128 bit keystream and this string valuesare used as a seed value for each NLFSR shift register. The choice of the feedback function of different lengths 32bit, 31bit, 25 bit, 4 bit NLFSR configuration is based on the function non linearity that generates truly random sequences[2,4].

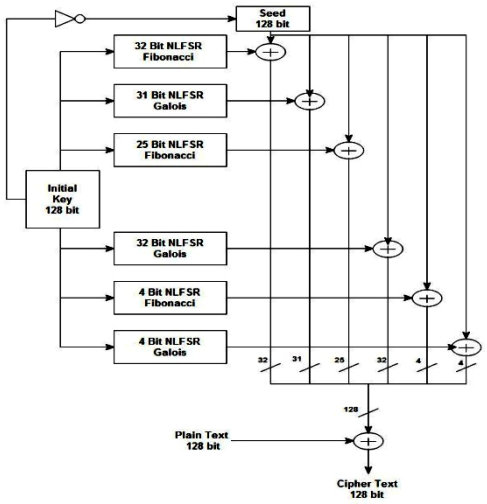

Figure 3: Internal view of Exclusive-128 bit NLFSRstream cipher[2]

The feedback functions of each NLFSR are described as follows. A detailed description can be found in the literature[2,10].

32 bit Fibonacci non-linear feedback function is defined as
$f_{31} = X_0 \oplus X_2 \oplus X_6 \oplus X_7 \oplus X_{12} \oplus X_{17} \oplus X_{20} \oplus X_{27} \oplus X_{30} \oplus X_3X_9 \oplus X_{12}X_{15} \oplus X_4X_5X_{16}$.

The corresponding feedback functions of 32 bit Galois configuration are

$f_{29} = X_{30} \oplus X_0$
$f_{28} = X_{29} \oplus X_0X_6$
$f_{27} = X_{28} \oplus X_0X_1X_{12}$

$f_{25} = X_{26} \oplus X_0$
$f_{24} = X_{25} \oplus X_0$
$f_{19} = X_{20} \oplus X_0 \oplus X_0X_3$
$f_{14} = X_{15} \oplus X_0$
$f_{12} = X_{13} \oplus X_1 \oplus X_8 \oplus X_{11}$

31 bit Galois non-linear feedback function is defined as

$f_{30} = X_0 \oplus X_3 \oplus X_5 \oplus X_7 \oplus X_{10} \oplus X_{16} \oplus X_{17} \oplus X_{18} \oplus X_{19} \oplus X_{20} \oplus X_{21} \oplus X_{24} \oplus X_{30} \oplus X_5 X_{15} \oplus X_{11}X_{18} \oplus X_{16}X_{22} \oplus X_{17}X_{21} \oplus X_1X_2X_{19} \oplus X_1X_{12}X_{14}X_{17} \oplus X_2X_5X_{13}X_{20}$.

The corresponding feedback functions of 31 bit Galois configuration are

$f_{28} = X_{29} \oplus X_0X_3X_{11}X_{18}$
$f_{29} = X_{30} \oplus X_0X_{11}X_{13} \oplus X_0X_1X_{18}$
$f_{27} = X_{28} \oplus X_0$
$f_{25} = X_{26} \oplus X_0X_{10} \oplus X_0$
$f_{23} = X_{24} \oplus X_0$
$f_{20} = X_{21} \oplus X_0$
$f_{19} = X_{20} \oplus X_0X_7$
$f_{18} = X_{19} \oplus X_5X_9 \oplus X_4X_{10} \oplus X_{18} \oplus X_{12} \oplus X_9 \oplus X_8 \oplus X_7 \oplus X_6 \oplus X_5 \oplus X_4$

25 bit Fibonacci non-linear feedback function is defined as

$f_{24} = X_0 \oplus X_1 \oplus X_3 \oplus X_5 \oplus X_6 \oplus X_7 \oplus X_9 \oplus X_{12} \oplus X_{14} \oplus X_{15} \oplus X_{17} \oplus X_{18} \oplus X_{22} \oplus X_1X_6 \oplus X_4X_{13} \oplus X_8X_{16} \oplus X_{12}X_{15} \oplus X_5X_{11}X_{14} \oplus X_1X_4X_{11}X_{15} \oplus X_2X_5X_8X_{10}$

4 bit Fibonacci non-linear feedback function is defined as

$f_3 = X_0 \oplus X_1X_{30}$

4 bit Galois non-linear feedback function is defined as

$f_2 = X_3 \oplus X_0X_2$

The first 32 bits of this string is assigned to the 32 bit non-linear feedback shift register used in Fibonacci configuration and the next 31 bits are given to the 31 bit non-linear feedback shift register used in Fibonacci mode. Similarly the next bits are assigned to each of the other registers used. The stream cipher is implemented in such a way that each configuration is sandwichedbetween the other two configurations either the Fibonacci or the Galois configuration. The variant size of each configuration is 32 bitFibonacci, 31 bit Galois, 25 bit Fibonacci, 32 bit Galois, 4 bit Fibonacci and 4 bit Galois NLFSRs.

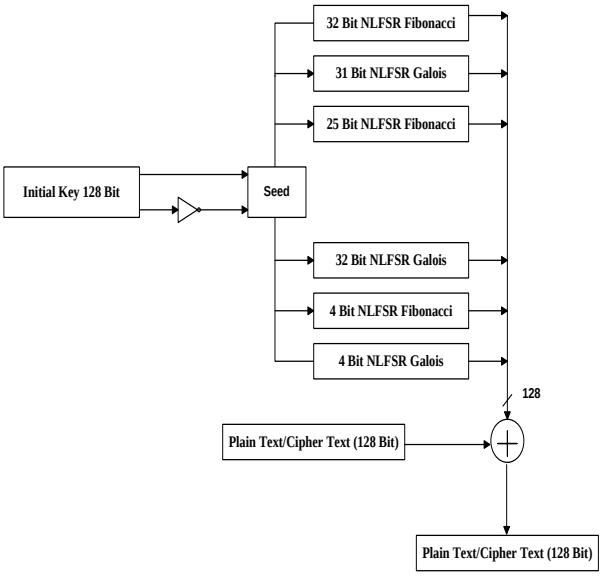

Figure 4: Internal view of modified Exclusive-128 bit NLFSR stream cipher

The architecture of modified Exclusive-128 bit Nonlinear Feedback Shift Register based stream cipher is shown in figure (4),which is to enhance randomness. In this modified stream cipher, each configuration of NLFSR is arranged alternately, and their initial state is the seed value which is the complement of the initial key using an interleaver. An interlever is used to separates the odd and even bits in a given binary sequence.

3. RANDOM NUMBER TESTING

In this section, we discuss the analysis of randomness test for the pseudorandom number generators. In many cryptographic applications,generators are used to generate random sequences and may need to meet stronger than for other applications. These generators are classified as random number generators(RNG) and pseudorandom number generators (PRNG), both these produce a stream of zeros and ones that may be divided into substreams or blocks of random numbers. The outputs of such generators may be used to determine whether or not a generator is suitable for a particular cryptographic application. However, no set of statistical tests can absolutely certify a generator as appropriate for usage in a particular application, i.e., statistical testing cannot serve as a substitute for cryptanalysis.

Therefore, a pseudorandom number generator (PRNG) is required as an alternative to RNG but a PRNG requires a RNG as a companion.A pseudorandom number generator (PRNG) inputs are called seeds and outputs are typically deterministic functions of the seed; i.e., all true randomness is confined to seed generation. It should obtain its seeds from the outputs of a RNG.

The National Institute of Standard Technology (NIST) Test Suitewas developed to test the randomness of arbitrarily long binary sequences produced by either hardware or software based cryptographic algorithm or pseudorandom number generators. These NIST tests [11] focus on a variety of different types of a randomness that could exist in a sequence. Some tests are decomposable into a variety of subtests. The tests are: (1) The Frequency (Monobit) Test, (2) Frequency Test within a Block, (3) The Runs Test and (4) Discrete Fourier Transform(DFT) Test.Frequency Mono-bit

Testfocuseson the number of zeroes and ones for the entire sequence. The purpose of this test is to determine whether the number of ones and zeros in the sequence are approximately the same as would be expected for a truly random sequence. Frequency Test within a Block determines the proportion of ones within the M-bit block is approximately M/2, as would be expected under an assumption of randomness. The purpose of Run test is to determine whether the number of runs of ones and zeros of various lengths is expected for a truly random sequence. Discrete Fourier Transform Test focuses on the peak heights in the Discrete Fourier Transform of the sequence and the purpose of this test is to detect periodic features in the tested sequence that would indicate a deviation from the assumption of randomness. Using this test, if the P-value is ≥ 0.01, then the sequence is random, otherwise the sequence is non random[11].

4. RESULT AND DISCUSSION

The analysis of modified exclusive-128 bitNLFSRhas been donefor the fourstandard types of pseudorandom test like frequency Mono-Bit, Frequency Test within a Block, Run Test and Discrete Fourier Transform Testand the results are shown in Table2, Table3 and Table4. P-values are calculatedfor proposed stream cipher and it is observed that all P-values are the much greater than 0.01. Hence our stream cipheris highly random. As, the number of permutations to crack a 128 bit key is quite larger equal to 2^{128} and even the time devoted for brute force attack is also larger, our proposed stream cipher is a secure one.The tables2,3 and 4 below describe the various test conducted to determine the Randomness and strength of the proposed algorithm against linear cryptanalysis.In the following, we describe with examples how to determine the randomness using the above mentioned tests for different initial keys.

Example 1:Initial Key is expressed in Hexadecimal as:

"8997C67B596354C619E5C6C2B9E376C6"

The initial key is applied to the conventional Exclusive 128 bit NLFSR stream cipher and also the modified one. In table 2, for the Frequency Monobit Test on both the stream ciphers, the P-value of Exclusive-128 bit NLFSR stream cipher is 0.5959 while for modified Exclusive -128 bit NLFSR stream cipher is 0.8597.For Frequency Test within a Block on both the stream ciphers, the P-value of Exclusive-128 bit NLFSR stream cipher is 0.9981 while for modified Exclusive -128 bit NLFSR stream cipher is 0.9862.For Run Test on both the stream ciphers, the P-value of Exclusive-128 bit NLFSR stream cipher is 0.2766 while for modified Exclusive -128 bit NLFSR stream cipher is 0.5164.For DFT test on both the stream ciphers, the P-value of Exclusive-128 bit NLFSR stream cipher is 0.0744 while for modified Exclusive-128 bit NLFSR stream cipher is 0.8575. Hence, the table 2clearly states that the modified stream cipher generates highly random sequence. But, the key streams generated by the modified stream cipher claims to be highly random.The table 2 shows the test analysis for the initial key vector "8997C67B596354C619E5C6C2B9E376C6"

Table 2.Random Test Results

Random Test	Exclusive 128 bit NLFSR Stream cipher	Modified exclusive 128 bit NLFSR Stream cipher
Frequency Monobit	Test Passed (0.5959)	Test Passed (0.8597)
Frequency within a Block	Test Passed (0.9981)	Test Passed (0.9862)
Run	Test Passed (0.2766)	Test Passed (0.5164)
DFT	Test Passed (0.0744)	Test Passed (0.8575)

Example 2:Initial Key is expressed in Hexadecimal as:

"00000000000000000000000000000000"

The initial key of all 'zeros' is applied to the conventional Exclusive 128 bit NLFSR stream cipher and also the modified one. In table 3, for the Frequency Monobit Test on both the stream ciphers, the P-value of Exclusive-128 bit NLFSR stream cipher is << 0.01 while for modified Exclusive -128 bit NLFSR stream cipher is 0.7237. For Frequency Test within a Block on both the stream ciphers, the P-value of Exclusive-128 bit NLFSR stream cipher is << 0.01 while for modified Exclusive -128 bit NLFSR stream cipher is 0.9994. For Run Test on both the stream ciphers, the P-value of Exclusive-128 bit NLFSR stream cipher is <<< 0.01 while for modified Exclusive-128 bit NLFSR stream cipher is <<0.01. For DFT test on both the stream ciphers, the P-value of Exclusive-128 bit NLFSR stream cipher is 0.0744 while for modified Exclusive-128 bit NLFSR stream cipher is 0.0541. Hence, the table 3 clearly states that the generated sequence by the modified Exclusive 128 bit stream cipher is highly random. The table 3shows the test analysis for the initial key vector"00000000000000000000000000000000".

Table 3.Random Test Results

Random Test	Exclusive 128 bit NLFSR Stream cipher	Modified exclusive 128 bit NLFSR Stream cipher
Frequency Monobit	Test Failed ($1.1224\ e^{-29}$)	Test Passed (0.7237)
Frequency within a Block	Test Failed ($1.3294\ e^{-05}$)	Test Passed (0.9994)
Run	Test Failed ------	Test Failed ($1.5388\ e^{-15}$)
DFT	Test Passed (0.0744)	Test Passed (0.0541)

Example 3:Initial Key is expressed in Hexadecimal as:

"FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF"

The initial key of all 'ones' is applied to the conventional Exclusive 128 bit NLFSR stream cipher and also the modified one.In table 4, for the Frequency Monobit Test on both the

stream ciphers, the P-value of Exclusive-128 bit NLFSR stream cipher is << 0.01 while for modified Exclusive -128 bit NLFSR stream cipher is 0.8597. For Frequency Test within a Block on both the stream ciphers, the P-value of Exclusive-128 bit NLFSR stream cipher is << 0.01 while for modified Exclusive-128 bit NLFSR stream cipher is 0.9932. For Run Test on both the stream ciphers, the P-value of Exclusive-128 bit NLFSR stream cipher is <<< 0.01 while for modified Exclusive-128 bit NLFSR stream cipher is << 0.01. For DFT test on both the stream ciphers, the P-value of Exclusive-128 bit NLFSR stream cipher is 0.0744 while for modified Exclusive -128 bit NLFSR stream cipher is 0.0744. The table 4 clearly states that the generated sequence by the modified cipher is highly random. The table4shows the test analysis for the initial key vector"FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF".

Table4.Random Test Results

Random Test	Exclusive 128 bit NLFSR Stream cipher	Modified exclusive 128 bit NLFSR Stream cipher
Frequency Monobit	Test Failed ($1.7920\ e^{-15}$)	Test Passed (0.8597)
Frequency within a Block	Test Failed ($2.5625\ e^{-05}$)	Test Passed (0.9932)
Run	Test Failed ------	Test Failed ($5.2889\ e^{-09}$)
DFT	Test Passed (0.0744)	Test Passed (0.0744)

5. CONCLUSION

We proposed a Modified Exclusive-128 Non Linear Feedback Shift Register (NLFSR) based stream cipher which is a simple architecture with basic elements likes shift register, flipflop and XOR. The tables 2, 3 and 4 show that calculated P-valuefor using various Initial key lengths and in this modified stream cipher, tests have been done to prove that the stream cipher is highly non-linear with full pseudo randomness.The implementation of FPGA and various attacks models based studies are to be made as future works.

6. REFERENCES

[1] KhaledSuwais, AzmanSamsudin, 2010 "NewClassification of Exiting Stream Ciphers," In Book: Computational Intelligence and Modern Heuristics, ISBN: 978-953-7619-28-2.

[2] Jegadish Kumar, K.J. et.al., 2013 "Exclusive-128 Bit NLFSR Stream Cipher for Wireless Sensor Network Applications," International Journal of Engineering and Technology (IJET), pp:3668 – 3675.

[3] Maximov, A.2006"Some Words on Cryptanalysis of Stream Ciphers", Ph.D. Thesis, Lund University.

[4] Elena Dubrova,2010"Finding Matching Initial States for Equivalent NLFSRs in the Fibonacci and the Galois Configurations", IEEE transactions on information theory, vol. 56, no. 6.

[5] Hell,M. Johansson,T. and Meier,W. "Grain - a stream cipher for constrained environments," citeseer.ist.psu.edu/732342.html.

[6] Gittins,B. Landman, H. A. O'Neil, S. andKelson,R. 2005 "A presentation on VEST hardware performance, chip area measurements, power consumption estimates and benchmarking in relation to the AES, SHA-256 and SHA-512." Cryptology ePrint Archive, Report 2005/415.Http://eprint.iacr.org/.

[7] Elena Dubrova,2009"ATransformation From the Fibonacci to the Galois NLFSRs", *IEEE transactions on information theory*, vol.55,(November 2009) no.11,pp. 5263-527.

[8] Dubrova.E, 2009 "How to speed up your NLFSR based stream cipher," Design, Automation and test in Europe Conference and Exhibition,pp: 878 – 881.

[9] NurHafizaZakaria, KamaruzzamanSeman and Ismail Abdullah, 2011 "Modified A5/1 Based Stream Cipher For Secured GSM Communication", IJCSNS International Journal of Computer Science and Network Security, vol.11 No.2.

[10] Tarannikov,Y.2001 "New constructions of resilient Boolean function with maximum nonlinearity", Lecture Notes in Computer Science, vol. 2355, pp. 66–77.

[11] Andrew Rukhin, Juan Soto, 2010 "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", National Institute of Standards and Technology (NIST), US department of Commerce, (April 2010).