Implementation of Chaotic Rossler system in Cryptography

Mahesh Tubaki[1*] & Dr. Rajanna G.S[2]

[1*]Faculty, Government Polytechnic Belgaum, India;

Orcid-ID: 0009-0005-5239-1407; E-mail: maheshtubaki1@gmail.com

[2]Faculty, Srinivas University, Mangalore, India;

Orcid-ID: 0009-0001-4121-0683; E-mail: kgsrajanna@gmail.com

Area/Section: Engineering
Type of the Paper: Regular Paper
Type of Review: Peer Reviewed as per |C|O|P|E| guidance.
Indexed in: OpenAIRE.
DOI: https://doi.org/10.5281/zenodo.15088247
Google Scholar Citation: IJMTS

How to Cite this Paper:

Tubaki, M., & Dr. Rajanna ,G.S., (2025). Implementation of Chaotic Rossler system in Cryptography. *International Journal of Management, Technology, and Social Sciences (IJMTS), 10*(1), 94-104. DOI: https://doi.org/10.5281/zenodo.15088247

International Journal of Management, Technology, and Social Sciences (IJMTS)
A Refereed International Journal of Srinivas University, India.

CrossRef DOI: https://doi.org/10.47992/IJMTS.2581.6012.0374

Received on: 02/03/2024
Published on: 26/03/2025

Implementation of Chaotic Rossler system in Cryptography

Mahesh Tubaki[1*] & Dr. Rajanna G.S[2]

[1*]Faculty, Government Polytechnic Belgaum, India;

Orcid-ID: 0009-0005-5239-1407; E-mail: maheshtubaki1@gmail.com

[2]Faculty, Srinivas University, Mangalore, India;

Orcid-ID: 0009-0001-4121-0683; E-mail: kgsrajanna@gmail.com

ABSTRACT

Security is the major important factor in data communication and networking. Cellular Networks are more vulnerable to security attacks and hence considerable security requirement is required. Hence, to meet up the security requirements in this proposed paper Rossler equation based new cryptographic technique is presented. This paper mainly focuses on encrypting the data transferred between mobile and base stations to ensure high secure environment for transmission of data across cellular networks. In the proposed method, Rossler equations are utilized to produce some numbers and S boxes are generated using random numbers, are required for the encryption of the data. Data is encrypted using KASUMI block cipher, which is the extended version of the MISTY1cipher. The obtained random numbers from Rossler equations are tested on NIST test suite to verify the randomness. Then security of the encrypted data is tested on security parameters like Hamming Distance, Balanced Output and Avalanche effect. The proposed system gives the improved avalanche effect with best randomness result.

Keywords: Cryptography, hamming distance, Cipher, Encryption, Chaotic

1. INTRODUCTION:

Now a day's cellular communication has become significant part of our daily life, besides providing voice communication using mobile phones, it provides internet services, multimedia, e-commerce services, SMS services and in many fields. Even the important confidential matters are sometimes dealing through messages. Transfer of important information through this cellular medium is common today. But in cellular networks these are susceptible to the hackers and eavesdroppers. Nowadays the security problems of the cellular communication system are gaining more attention. Integrity with confidentiality technique protects the messages and prevents message modification. Impersonation attacks can also be prevented from these techniques. Hence protection of information is very significant in the field of communication, specifically in wireless networks. In wireless medium active eavesdropping is relatively simple when compared to wired transmission. The data transferred over the wireless medium can be easily hacked and modified by attackers when there is no integrity and confidentiality protection. While communicating with someone or sending information the data security becomes most important. Due to the fast progress in wireless system, to provide secure and efficient communication to the user's numerous security techniques have been developed.

Cryptography is the security method and it provides authentication, privacy and reliability protection of data which is passing over the insecure medium. Cryptography is emerging and data security mechanisms which protect the data from unauthorized user. It provides significant control over the privacy and authentication. The basic block diagram of the cryptography system is as shown in the Figure 1.

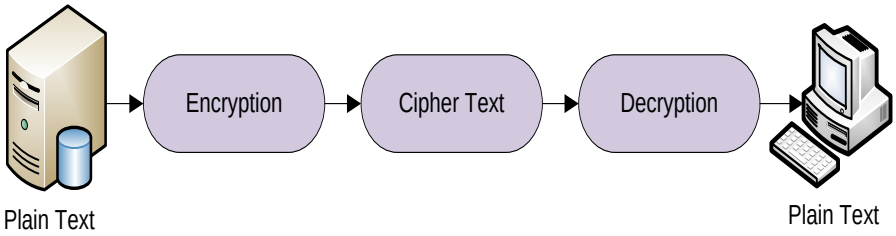

Figure 1: Basic Block Diagram of the Cryptography System

Plain text is the data which can be read and understood by anyone without using any special process. The method of converting readable data i.e. plain text into nonreadable format is called encryption. The output obtained which is unreadable text after encryption of plain text is known as cipher text. Encryption is performed to prevent the unauthorized user access of data. The process of converting back from cipher text into plain text is referred as decryption.

Cellular service customer majorly requires privacy in data, speech etc. Encryption of data in mobile communication plays crucial role to guard the subscriber's data and prevent fraud. Plenty of research works are conducted daily on cryptography. Efficient development of cryptography for secure communication motivated us to develop new cryptosystem. For the encryption of the data, random number generation plays a very significant responsibility in cryptographic system.

Random number generation is the method of creating a sequence of symbols or numbers that cannot be predicted by anyone except authorized users. To test the randomness of a random numbers many statistical test suits are available like ENT, Diehard, Test U 01and NIST. In this proposed work chaotic Rossler equations are used to produce random numbers. Chaotic Rossler equations are also called as Rossler attractor. In three dimensional spaces, Rossler attractor is introduced as chaotic attractor. The random numbers from the proposed system is tested on NIST test suite to verify the randomness. The random numbers produced from the Rossler system is used to generate S-boxes which are used during encryption.

2. MATERIALS AND METHODS :

This section presents the descriptions about the proposed system. Figure 2 presents the pictographic view of the proposed system. In this proposed work new cryptosystem method is designed which is the combination of chaotic Rossler equations and KASUMI block cipher. This proposed system mainly consists of four blocks namely: Random number generator, Creation of S-Boxes (Rossler Generator Key), Encryption and Decryption of the data. Initially in the first block, chaotic Rossler equations are used as random number generator to produce random numbers. Produced random numbers are passed to Rosseler Generator key block to create s-boxes (i.e. s7 and s9). These s-boxes are used in the encryption part to prevent linear structure in data. After creation of s-boxes KASUMI block cipher is considered for encryption of data. KASUMI is an Integration of FL, FO, and FI functions. It uses 64-bit plain data and 128-bit confidential key. In the proposed system 64bit plain data is considered. Eight 16-bit sub keys are created using randomly selected confidential128bit key as per KASUMI. The plain data is converted to binary data. Finally, encryption is performed to binary data using128bit sub keys and s-boxes in encryption block. After encryption 64-bit cipher data will be obtained, which could not be understood by anyone. Similarly, decryption of cipher data is performed by performing reverse operation of encryption to get the plain text.

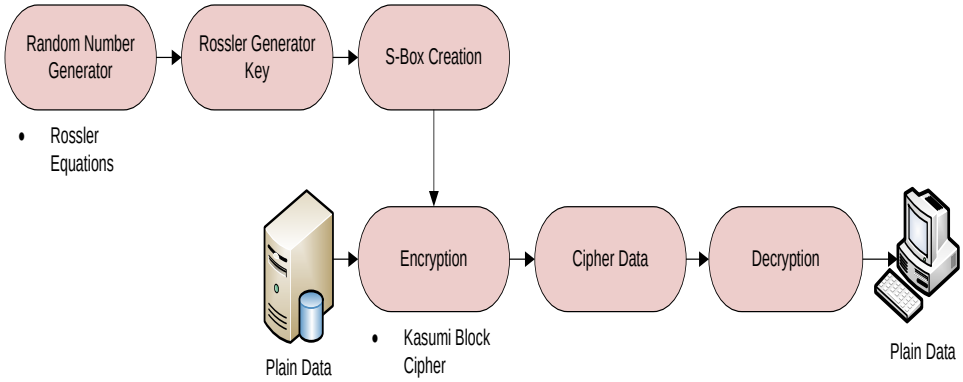

Figure 2: Proposed System Overview Block Diagram

2.1 Chaotic Rossler Equations

Chaos theory examines the dynamics of nonlinear frameworks with generally few sub units of freedom that display random-like, yet exactly deterministic dynamical behaviour and a greater sensitivity to primary conditions [12]. Poincare-Bendixon theorem states that continuous time nonlinear dynamical frameworks with at least three degrees of freedom can show chaotic dynamics. In the design of cryptographic mechanisms, continuous period chaotic frameworks are useful.

In the proposed method Rossler three Differential equations are considered when creating random numbers.
.Otto Rossler is a person who studied about Rossler equations. These Rossler systems get emerged from his work in the chemical kinetics field. Rossler system is presented by a framework of three nonlinear ordinary differential equations [10] as in Eq. (1), (2) and (3):

$$\frac{dx}{dt} = -y - z \quad (1)$$

$$\frac{dy}{dt} = x + a\,y \quad (2)$$

$$\frac{dz}{dt} = b + z\,(x - c) \quad (3)$$

Where x, y, z creates system state and a, b, c are the constant terms. Nonlinear equations are quite challenging
to solve systematically. These equations required to be resolve using numerical mechanisms. The simple form of the three differential equations is presented in the proposed work using Euler's technique.
The equation mentioned in Eq. (1), (2) and (3) are cannot be resolved by computer. Hence Euler's modified formula for these equations is presented in Eq. (4), (5) and (6):

$$Xn + 1 = Xn - h(Yn + Xn) \quad (4)$$

$$Yn + 1 = Yn + h(Xn + aYn) \quad (5)$$

$$Zn + 1 = Zn + h(b + ZnXn - cZn) \quad (6)$$

Here a, b, c are constant terms and h = step size. True random numbers are produced using Eq. (4), (5) and (6). The generated random numbers are used as Rossler generator key to generate S-Boxes which are used in encryption. The main purpose of these S-Boxes is to prevent linear structure. The steps involved in the process are presented in Algorithm-1.

Algorithm 1: Random Number Generation Algorithm

Input: $X(0) = Y(0) = Z(0) = 0.1, h = 0.01$, *a, b and c are constant terms.*
Output: R= Random Numbers.
Step.1. Initialize the input parameters X, Y, Z, h, a, b, c *and output parameter R.*
Step.2. Consider three ordinary differential equations of chaotic Rossler System.
Step.3. Convert considered Rossler differential equations into Euler's modified formula.
Step.4. Set the range of Random numbers required to generate.
Step.5. Apply inputs to the Rossler Equations and generate random numbers.
Step.6. Store the generated random numbers (R) in a variable and create two s-boxes i.e. $s7, s9$.
End Algorithm

2.2 Encryption:

It is the mechanism of encoding of information from readable format into unreadable format to avoid unauthorized user access of data. Encryption plays vital role in data security. In the proposed system KASUMI, block cipher is used for the encryption of data.

2.2.1 KASUMI Block Cipher :

KASUMI mechanism is a 64-bit block cipher. It mainly consists of two parts namely: Key generation part and encryption part. The outcome of the key generation part is used in encryption section to encrypt the data. KASUMI cipher modifies the 64bit plain data using 128-bit confidential key and gives 64-bit cipher data. KASUMI consists of repeated Feistel structure and it is extended from MISTY1 cipher. KASUMI cipher has 8 Feistel rounds. The pictographic representation of KASUMI cipher and KASUMI functions are presented in Figure 3.

In the proposed system as per KASUMI 8 feistel rounds are considered for encryption. Each round consists of two F functions namely: FL function and FO function. Function FL mixes a 32-bit plain data with 32-bit sub keys in a linear form. Function FO is a three round 32-bit feistel structure. Order of FO and FL function depends on the round type: If round is even FL function is applied first and then FO functions are applied. If round is odd FO function is applied first then FL functions. FO Function contains one sub function which is FI and it is a four round 16-bit feistel structure. FI Function utilizes two S-boxes i.e. $s7$ and $s9$. $s7$ is a 7 bit to 7-bit permutation and $s9$ is a 9 bit to 9-bit permutation. These S-boxes are created from numbers which are obtained using Rossler system of proposed system. Apart from S-boxes, FI function uses 16-bit sub key which is mixed with 16-bit data. In each round FO functions accept 96-bit sub keys and in this 96-bit key 48-bit sub keys will be used for FI functions and 48-bit sub keys are used in the key mixed stage inside the FO function. The FL function receives the 32-bit input and two 16-bit sub keys. One key affects the plain data using OR operation and other one affects the data using AND operation.

The Key generation part of KASUMI is simple compared to MISTY key schedule. In this eight 16-bit keys are derived linearly from the 128-bit confidential key. First 128-bit confidential key is considered and then 128-bit round key (K) is separated into eight 16-bit values i.e. $K = K1||K2||K3||K4||K5||K6||K7|K8$. Using this divided key eight 16-bit sub keys are produced and it is presented in Table 1. Different small keys are generated for each round of KASUMI. Sub keys which are used in KASUMI are not same for all the rounds; they differ for each round. In Table 1 we presented a key generation details of KASUMI.

Table 1: Key Schedule of KASUMI

Round	KLi1	KLi2	KOi1	KOi2	KOi3	KIi1	KIi2	KIi3
1	K1<<<1	K3'	K2<<<5	K6<<<8	K7<<<13	K5'	K4'	K8'
2	K2<<<1	K4'	K3<<<5	K7<<<8	K8<<<13	K6'	K5'	K1'
3	K3<<<1	K5'	K4<<<5	K8<<<8	K1<<<13	K7'	K6'	K2'
4	K4<<<1	K6'	K5<<<5	K1<<<8	K2<<<13	K8'	K7'	K3'
5	K5<<<1	K7'	K6<<<5	K2<<<8	K3<<<13	K1'	K8'	K4'
6	K6<<<1	K8'	K7<<<5	K3<<<8	K4<<<13	K2'	K1'	K5'
7	K7<<<1	K1'	K8<<<5	K4<<<8	K5<<<13	K3'	K2'	K6'
8	K8<<<1	K2'	K1<<<5	K5<<<8	K6<<<13	K4'	K3'	K7'

2.3 Decryption :

Decryption is the method of decoding unreadable format data into readable format. After receiving the data from authorized sender, receiver decrypts the data by performing decryption. Before decrypting the data, receiver must know about the keys will be used during encryption. How encryption is important for secure transmitting of data in the similar manner decryption of data is also very important at authorized receiver side to decrypt and understand the information.

In the proposed system, decryption of cipher data is like encryption. Encryption of data is performed by performing two operations. In the first case functions which are used in the encryption part are interchanged. In the next case sub keys are reversed to get plain data from cipher data i.e. first key used in the encryption must be the last key in the decryption.

Main purpose of our proposed work is to develop efficient cryptosystem for data security. Overall Functional flow of the proposed system is presented in the Figure 4.

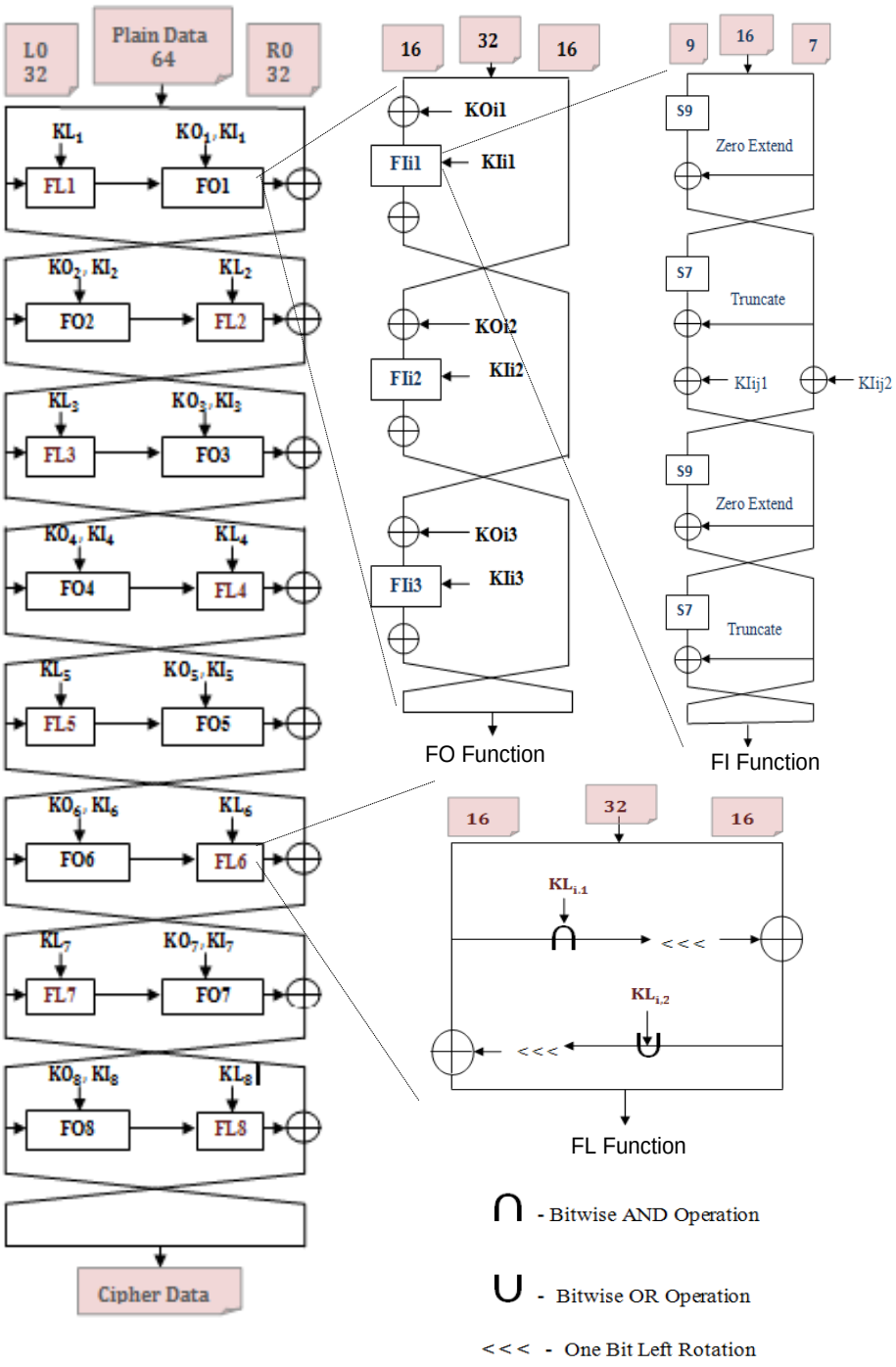

Figure 3: Architecture of KASUMI

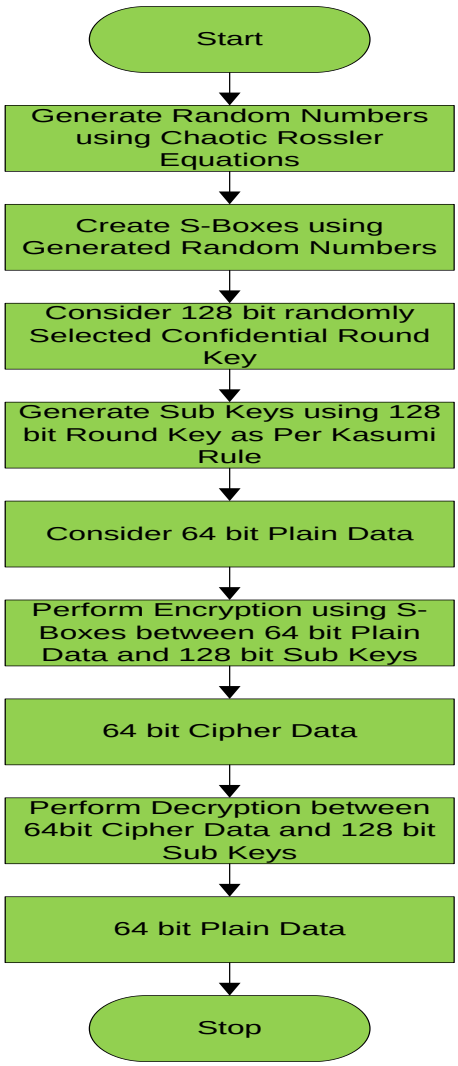

Figure 4: Functional Flow of the Proposed Scheme

3. RESULTS AND DISCUSSIONS :

This section provides the experimental results and security investigation of the proposed work and comparison of proposed technique with our old developed method. To check the output quality which is obtained from the proposed method, four security parameters are considered namely: Randomness Test, Hamming Distance, Balanced Output and Avalanche Effect.

3.1 Randomness Test

Randomness test is a test to check the randomness of generated random numbers to state how efficient it is to use for further security system. In the proposed scheme Rossler equations based random numbers are generated. Generated random numbers are passed to NIST statistical test to validate the randomness. National institute of Standards Technology (NIST) is a statistical test suite used to verify the randomness. The randomness outcome of the proposed scheme is presented in below tables. Output of seven-randomness test of all the seven tests satisfies the NIST randomness criteria.

Table 2: Results of the NIST Statistical Randomness Tests

Statistical Test	P-value	Result
Frequency	**288.000000**	**Passed**
Block Frequency (m = 128)	**0.082403**	**Passed**

Longest Runs of Ones	**0.170482**	**Passed**
FFT	**0.232884**	**Passed**
Non-overlapping Templates (m = 9, B = 000000001)	**0.779952**	**Passed**
Overlapping Templates (m = 9)	**0.349672**	**Passed**
Linear Complexity (M = 500)	**0.743824**	**Passed**

3.2 Security Analysis

After encrypting the data, security analysis of the encrypted data is very important to check the quality of encrypted data. The sanctity of the proposed system is analysed by considering three security parameters namely: Hamming Distance, Balanced Output and Avalanche effect.

3.3 Hamming Distance

Hamming distance is a distance in which numbers of bits which are changed between two binary strings. This distance is used to find out the dissimilarity between two binary strings.

Example 1: Plain Data = Security = 01010011011001010110001101110101011100100110100101110100 01 111001

Cipher Data = ÝNµÂ£q = 1101110101001110101101011100001000011011101000110111000110000000

In the Example 1, hamming distance between plain data and cipher data is 35. Out of 64 bits 35 bits are different between cipher data and plain data. Higher hamming distance shows good performance. In first example more than 50% bits are different. Hence, we can say that this hamming distance is good. Table 2 presents the output obtained from the proposed system. In Table 2, 5 samples are giving good hamming distance out of 8 samples.

3.4 Balanced Output

Balanced output is the binary string output which contains approximately equal number of zeros and ones [15]. If number of zeros and ones are approximately equal, then it shows that the encrypted data is good. In Example 1 number of one's equal to 31 and number of zeros equal to 33. These zeros and ones are approximately equal. Hence example one is giving best balanced output. In Table 2, 6 samples are giving good balanced output out of 8 samples.

3.5 Strict Avalanche Criterion

Avalanche effect is desirable security property of cryptographic system. SAC get satisfied when the probability of the changes in output is more than 50% if one bit changed in input. Avalanche effect can be computed using Eq. (7).

$$Avalanche\ effect = \frac{Number\ of\ changed\ bits\ in\ the\ ciphered\ texts}{Total\ Number\ of\ bits\ present\ in\ the\ ciphered\ text} \times 100\% \quad (7)$$

As shown in Table 2 in three cases we getting more than 50% avalanche effect out of 8 samples and average avalanche effect is 48.63%. Compare to [13] and [14], we getting good improved avalanche effect. Avalanche effect comparison with existing methods is presented in Table 3.

Table 3: Parameters of Proposed System

Sl. No	Plain Data	Encrypted Data	Balanced Output		Hamming Distance	Avalanche Effect %
			No. of 1's	No. of 0's		
1	Security	ÝNµÂ£q	31	33	35	53.1250
2	Networks	æÔÆÔÔ	29	35	33	46.8750

3	RJ45JACK	°ÆbH • /¾	27	37	28	46.8750
4	FUNCTION	|vãc%$	29	35	28	43.7500
5	FRAGMENT	>ËgøÄñßí	41	23	33	42.1875
6	ZXQRASPK	AÒqåtªD	28	36	29	53.1250
7	INVERTER	Ö¹b • T	31	33	23	59.3750
8	ELECTRON	×º.¿UvDa	36	28	31	43.7500

Table 4: SAC checking with Existing Methods

Encryption Methods	Avalanche Effect
Piotr Mroczkowski et.al [13]	**48**
K. Kazlauskas et.al [14]	**48.22**
Projected Method	**48.63**

Our research work is to develop different cryptosystems i.e. Lorenz and Rossler equation-based cryptosystem and compare between them to provide efficient cryptosystem. In paper we had designed Lorenz equations based new cryptosystem and in this proposed work new chaotic Rossler system based new cryptosystem is presented. Comparison between these two cryptosystems is performed to provide efficient security system in cellular networks. Comparison between our previously developed Lorenz based crypto method and proposed method of hamming distance is presented in Table 4. In Table 4 compare to proposed method our previously developed method [] giving good hamming distance in almost all the cases hence we can say that method is best compared to the proposed system.
Table 4 shows that comparison of SAC of proposed method with method. As observed in Table 5 our previously developed cryptosystem giving more SAC than proposed method. From the Table 4 and Table 5 observation we can state that previously developed method is best and efficient. The SAC performance analysis graph between proposed method and method is presented in Figure 3.

Table 5: Hamming Distance Comparison between Method and Proposed Method

Data	Hamming Distance of Lorenz based Cryptosystem	Hamming Distance of Proposed Method
Data1	21	35
Data2	33	33
Data3	32	28
Data4	27	28
Data5	38	33
Data6	36	29
Data7	35	23
Data8	35	31

Table 6: SAC comparison with Method

Encryption Methods	Avalanche Effect
Lorenz based Method	**56.054**
Projected Method	**48.63**

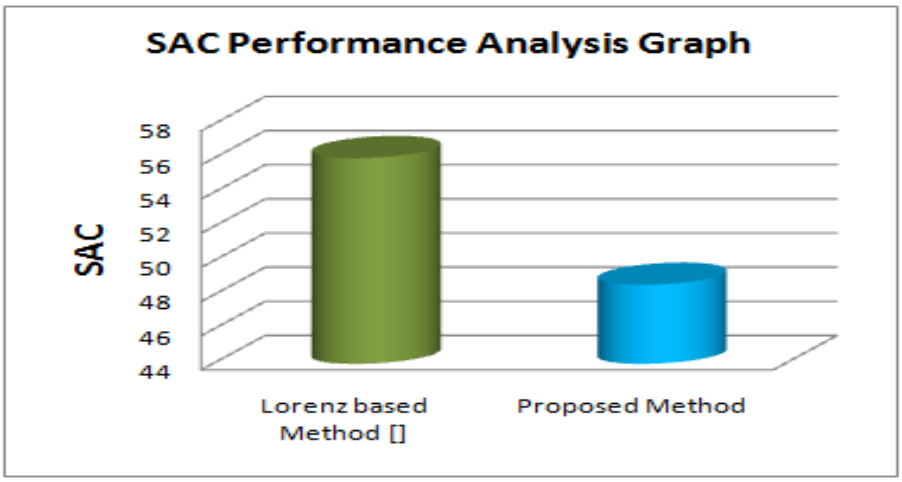

Figure 5: SAC Comparison Graph

4. CONCLUSION :

Here chaotic Rossler system, based new cryptosystem is proposed to provide enhanced security for data in cellular networks. The main aim of this proposed work is to encrypt the data to protect it from unauthorized user access. In the proposed system chaotic Rossler equations are used to generate random numbers. Generated random numbers from Rossler equations are passed to statistical test to test the randomness sequence of generated random numbers. S-boxes are created which are required for encryption by making use of random numbers. KASUMI block cipher is considered for data encryption. The proposed method is compared with existing methods resulting in improved avalanche effect. To provide efficient cryptosystem for data security we have compared proposed method with our previously developed Lorenz based cryptosystem. Compare to proposed method our method giving good hamming distance with improved avalanche effect. Hence, our previous Lorenz based cryptosystem is efficient tool and it can be implemented in cellular networks.

REFERENCES :

[1] Shushan Zhao, Akshai Aggarwal, Richard Frost and Xiaole Bai (2012). *A Survey of Applications of Identity-Based Cryptography in Mobile ad-hoc Networks*, 14(2), 380-400. Google Scholar↗
[2] Alpesh R. Sankaliya, V. Mishra and Abhilash Mandloi (2011), Implementation of Cryptographic Algorithm for GSM and UMTS Systems, *International Journal of Network Security & Its Applications*, 3(6), 81-85. Google Scholar↗
[3] Gaurav Sharma, Suman Bala and Anil K. Verma (2012), "Security Frameworks for Wireless Sensor Networks-Review", *Elsevier*, 6(1), 978-987. Google Scholar↗
[4] Iftikhar Rasheed, Asjad Amin, Mahwish Chaudhary, Sadaf Bukhari, Muhammad Rizwan and Kashif Ali (2013), "Analysing the Security Techniques used in LTE Advanced and their Evaluation", *In Digital Information Management (ICDIM) IEEE*, 3(1), 11-13. Google Scholar↗
[5] Mona Dara and Kooroush Manochehri (2013), "A Novel Method for Designing S-Boxes Based on Chaotic Logistic Maps Using Cipher Key", *World Applied Sciences Journal*, 28(12), 2003-2009. Google Scholar↗
[6] Ihsan Cicek, Ali Emre Pusane, and Gunhan Dundar (2014). "A Novel Design Method for Discrete Time Chaos based True Random Number Generators", *Elsevier*, 47(1), 38-47.Google Scholar↗

[7] Kazys Kazlauskas, Gytis Vaicekauskas and Robertas Smaliukas (2015). "An Algorithm for Key-Dependent S-Box Generation in Block Cipher System", *Informatica*, 26(1), 51-65. Google Scholar↗
[8] Shyam Nandan Kumar (2015), "Review on Network Security and Cryptography", *International Transaction of Electrical and Computer Engineers System*, 3(1), 1-11. Google Scholar↗
[9] Wentan Yi and Shaozhen Chen (2016), "Multidimensional zero-correlation linear cryptanalysis of the block cipher KASUMI", *IET Information Security*, 10(4), 215-221. Google Scholar↗
[10] Biham, E., Dunkelman. O, & Keller, N. (2005). A Related-Key Rectangle Attack on the Full KASUMI. *ASIACRYPT 2005*, *[SpringerLink](https://link.springer.com)*, 443-465. Google Scholar↗
[11] Blunden, M., & Escott, A. (2002). Related Key Attacks on Reduced Round KASUMI. *FSE 2001*, *[SpringerLink](https://link.springer.com)*, 277-285. Google Scholar↗
[12] Dunkelman, O., Keller, N, & Shamir, A. (2010). A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony. *CRYPTO 2010*, 393–410. Google Scholar↗
[13] Kühn, U. (2001). Cryptanalysis of Reduced-Round MISTY. *EUROCRYPT 2001*, *[SpringerLink](https://link.springer.com)*, 325–339. Google Scholar↗
[14] Sugio, N., Aono, H., Hongo, S., & Kaneko, T. (2006). A Study on Integral-Interpolation Attack of MISTY1 and KASUMI. *Computer Security Symposium 2006*, 173–178. Google Scholar↗
[15] Sugio, N., Tanaka, H., & Kaneko, T. (2007). A Study on Higher Order Differential Attack of KASUMI. *IEICE Transactions*, 14–21. Google Scholar↗
[16] 3GPP (2001), Technical Specification Group Services and System Aspects, 3G Security, Specification of the 3GPP Confidentiality and Integrity Algorithms, *Document 2: KASUMI Specification. [ETSI](https://www.3gpp.org).* Google Scholar↗
[17] 3GPP (2002). Technical Specification Group Services and System Aspects, 3G Security, Specification of the A5/3 Encryption Algorithms for GSM. *[ETSI](https://www.3gpp.org).* Google Scholar↗
[18] Blunden, M., & Escott, A. (2002). A Related-Key Attack on KASUMI in GSM Systems. *FSE 2002*, 61–75. *[SpringerLink](https://link.springer.com).* Google Scholar↗
[19] Dunkelman.O, & Keller, N. (2007). Higher-Order Differential Attack on KASUMI. *CRYPTO*.Google Scholar↗
[20] KASUMI Algorithm Specification, Version 3.1.1. (2001). 3rd Generation Partnership Project. *[Wikipedia](https://en.wikipedia.org/wiki/KASUMI)*. Google Scholar↗
[21] Biham, E., & Dunkelman, O. (2000). The MISTY Cryptosystem and its Application in GSM Networks. *FSE 2000*.Google Scholar↗
[22] Keller, N., & Matsui, M. (2001). Security Analysis of the MISTY1 and KASUMI Algorithms. *Journal of Cryptology*.Google Scholar↗
[23] A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM. (2010). *IACR*Google Scholar↗
[24] KASUMI. (n.d.). *Wikipedia*. *[KASUMI Wikipedia] (https://en.wikipedia.org/wiki/KASUMI).* Google Scholar↗
[25] Dunkelman, O., & Keller, N. (2007). Higher-Order Differential Attack on KASUMI. *CRYPTO*.Google Scholar↗
[26] Sugio, N., Tanaka, H., & Kaneko, T. (2007). A Study on Higher Order Differential Attack of KASUMI. *IEICE Transactions*, 14–21. Google Scholar↗
[27] Wentan Yi and Shaozhen Chen (2016), "Multidimensional zero-correlation linear cryptanalysis of the block cipher KASUMI", *IET Information Security*, 10(4), 215-221. Google Scholar↗
[28] Ihsan Cicek, Ali Emre Pusane, and Gunhan Dundar (2014). "A Novel Design Method for Discrete Time Chaos based True Random Number Generators", *Elsevier*, 47(1), 38-47.Google Scholar↗
[29] Alpesh R. Sankaliya, V. Mishra and Abhilash Mandloi (2011), "Implementation of Cryptographic Algorithm for GSM and UMTS Systems", *International Journal of Network Security & Its Applications*, 3(6), 81-85. Google Scholar↗
[30] Shyam Nandan Kumar (2015), "Review on Network Security and Cryptography", *International Transaction of Electrical and Computer Engineers System*, 13(1), 1-11 Google Scholar↗