INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 6.078
(Volume 7, Issue 1)
Available online at: https://www.ijariit.com

A lightweight encryption authentication scheme using rectangle and chaotic logistic map algorithm for smart grid

Arun Kumar
arunkumar28011990@gmail.com
Adesh Institute of Engineering and Technology, Faridkot, Punjab

Puneet Jain
puneetjain988@gmail.com
Adesh Institute of Engineering and Technology, Faridkot, Punjab

ABSTRACT

Smart Grid is the advanced power grid system which combines the renewable energy resources like wind, solar, bio gas with the existing power system. Besides that, it provides a two-way communication using a large number of electronics devices between the customer and providers which is also known as Advanced Metering Infrastructure (AMI). The devices are resource constraint devices and sensitive information is communicating through it. Therefore, in this paper, these constraints are taken under consideration and designed a lightweight encryption authentication scheme for AMI. The lightweight RECTANGLE and chaotic Logistic map algorithms are taken under consideration. These algorithms encrypt the information along with generate authentication tags. These tags are used in the receiver side to verify the authenticity of the data. The algorithm is simulated in the MATLAB and various performance parameter calculated for it. After that it compared with the existing algorithms.

Keywords: *Advanced Metering Infrastructure, RECTANGLE, Chaotic Logistic Map, Encryption Authentication Scheme*

1. INTRODUCTION

Smart Grid constitutes the next generation of electric grid systems, which incorporates different renewable energy resources, automatic and intelligent management of energy, and a more effective and interactive communication with the client [1]. A fundamental component of the Smart Grid is the Advanced Metering Infrastructure (AMI), which results from the integration of advanced sensors, smart meters, monitoring systems, and energy management systems. The AMI enables the bidirectional communications between the Utility and the final users. Overall, Smart grid's communication infrastructure comprise three types of networks: i) Home Area Networks (HAN), which serve as the communication infrastructure for sensors and devices inside homes; ii) Neighborhood Area Networks (NAN), which connect smart meters and data collectors, and correspond to the platform for AMI implementations; and iii) a Wide Area Network (WAN), which communicates data collectors in the AMI with a Utility Control Center [2]. In addition, as valuable data are exchanged among smart grid systems, theft or alteration of this data could violate consumer privacy. In the literature, numerous attacks for the smart grid are defined such as eavesdropping, replay, and jamming attacks [3]. To overcome these attacks, cryptography algorithms are used. These algorithms try to fulfil the security constraints such as confidentiality, integrity, and authentication [4]. Further, based on the key used for encryption and decryption purposes, the cryptography algorithms are classified into symmetric and asymmetric algorithms. In the symmetric algorithms, same key is used for encryption and decryption purposes. However, in the asymmetric algorithm, a key pair (public and private) used. The public key is used for encryption purposes and private key used for decryption purposes [5]. In our work, we have explored the symmetric algorithms used for smart grid. The most preferred cryptography algorithms are Advanced Encryption Standard (AES) [6], ChaCha [7], Blowfish [8], DES [9], and chaotic map algorithm [7,13]. However, these algorithms provide confidentiality not authentication. Also, consumes large resources. Therefore, in our work, we have explored lightweight cryptography algorithms and encryption authentication modes that recommended by the National Institute of Standard & Technology (NIST) [10-11]. In the literature, three encryption authentication modes available: MAC-then-Encrypt, Encrypt-then-MAC, and Encrypt-and-MAC. Out of these, we have used MAC-then-Encrypt mode for our work.

The paper is designed a lightweight encryption authentication scheme for the AMI using the lightweight cryptography RECTANGLE algorithm and chaotic logistic map algorithm. Initially, the private key and message is given to the RECTANGLE algorithm that generates the encrypted data. After that, chaotic map based key generated and XOR operation performed with the message to generate authentication tag. The initial population (X0) for the key generation is determined from the encrypted. The results show that the proposed algorithm provides better results in terms of entropy, Peak Signal to Noise Ratio (PSNR), correlation coefficient, and avalanche effect as compared to the existing algorithms.

The remaining paper is as follow. Section 2 provides the overview of RECTANGLE and Chaotic Logistic map algorithm. Section 3 illustrates the proposed algorithm. Section 4 shows the experimental results performed for the proposed algorithm. Section 5 shows the conclusion.

2. OVERVIEW OF RECTANGLE AND CHAOTIC LOGISTIC MAP ALGORITHMS

In this section, the RECTANGLE and chaotic logistic map algorithm is explained to understand the proposed algorithm.

2.1 Rectangle Algorithm

RECTANGLE algorithm is a block cipher which is designed based on the substitution permutation network [12]. The block size 64-bit, Key size-80/128-bit, and contains total 25 rounds for encryption. Also, key is updated in each round and updated key is generated based on the previous key and logical function. The 64-bit plaintext is arranged into 4x16 matrix and key into 5x16/8x16 matrix then encryption process is started. The pseudocode for the RECTANGLE cipher is shown in Table 1.

Table 1: Pseudocode for the RECTANGLE Cipher

Encryption Module
Add-Round Key (State, K_i) Sub-Column (State) Shift Rows (State)
Key Scheduling (80-Bit)
1. Apply the S-box to the bits intersected at the 4 uppermost rows and the 4 rightmost columns. 2. Applying a 1 round generalized Feistel Transformation. Row0'=(row0<<8) XOR Row1 Row1'=Row2 Row2'=Row4 Row3'=(Row3<<12) xOR Row4 Row4'=Row0 3. A 5-Bit Round Constant RC[i] is XORed with the 5-bit Key State.

The detail description of the Sub-Column and Shift row is explained below.

- Sub-Column: In this step, the input bits is changed based on the substitution box (S-Box). The S-box is provided bijective mapping. In the RECTANGLE cipher, the matrix each column is extracted and passed through s-box as shown in Fig. 2.1.
- Shift Row: In this step, each row of the matrix circular shifted as shown in Fig. 2.2.

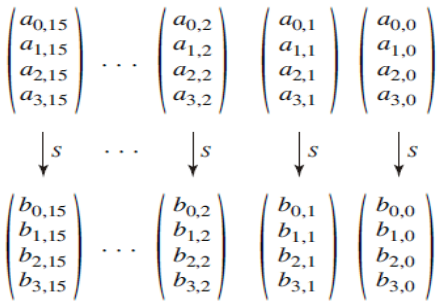

Fig. 2.1: Substitution Step

$$(a_{0,15} \dots a_{0,2}\ a_{0,1}\ a_{0,0}) \xrightarrow{\lll 0} (a_{0,15} \dots a_{0,2}\ a_{0,1}\ a_{0,0})$$
$$(a_{1,15} \dots a_{1,2}\ a_{1,1}\ a_{1,0}) \xrightarrow{\lll 1} (a_{1,14} \dots a_{1,1}\ a_{1,0}\ a_{1,15})$$
$$(a_{2,15} \dots a_{2,2}\ a_{2,1}\ a_{2,0}) \xrightarrow{\lll 12} (a_{2,3}\ \dots a_{2,6}\ a_{2,5}\ a_{2,4})$$
$$(a_{3,15} \dots a_{3,2}\ a_{3,1}\ a_{3,0}) \xrightarrow{\lll 13} (a_{3,2}\ \dots a_{3,5}\ a_{3,4}\ a_{3,3})$$

Fig. 2.2: Shift Row

2.2 Chaotic Logistic Map Algorithm

A chaotic system is a deterministic nonlinear dynamical system whose states change with iterations in a deterministic way [13]. The logistic map is a one-dimensional discrete-time nonlinear system exhibiting quadratic non-linearity. The logistic map is determined using Eq. (1).

$$X_{n+1} = \mu X_n(1 - X_n) \qquad (1)$$

where $X_n \in (0, 1)$ and $\mu \in (0, 4)$. μ is known as the control parameter or bifurcation parameter. Here X_n is the state of the system at time n. X_{n+1} denotes the next state and n denotes the discrete time.

3. PROPOSED ALGORITHM

In this section, the proposed algorithm designed using the RECTANGLE and Chaotic Logistic Map algorithm is explained. The RECTANGLE algorithm is used for generate encrypted data and Chaotic logistic Map algorithm is used for authentication tag. The block diagram of the proposed algorithm is shown in Figure 3.

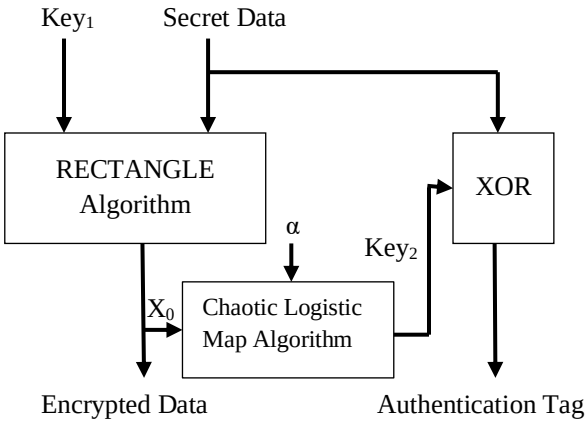

Fig. 1: Blossck Diagram of the Proposed Algorithm

Initially, the secret data and key_1 is read and given to the RECTANGLE algorithm. The RECTANGLE algorithm scrambles the secret data and gives the encrypted data. After that, the encrypted data correlation determined with respect to secret data and the absolute correlation value works as an initial population (X_0). Next, the X_0 and α given to the chaotic map algorithm that generates a 64-bit key. In the last, the 64-bit key and secret data XOR operation performed which gives the authentication tag in the output. The advantages of the proposed algorithm are given below.

1.The chaotic Logistic map algorithm generates different key for different secret data.

2. The proposed algorithm provides confidentiality and authentication.

4. EXPERIMENTAL RESULTS

In this section, the experimental results are shown that performed for the proposed algorithm. The secret data is randomly generated. The algorithm is simulated in MATLAB and various performance metrics calculated for it.

4.1 Different Key Generation using the Chaotic Logistic Map Algorithm

The chaotic Logistic map algorithm generates the random key for the authentication tag. The initial population (X_0) for it is determined using the encrypted data. Table 1 shows the generated X_0 for different secret data. The results show that the generated initial population is different.

Table 1: Correlation for the Different Encrypted Data

S no.	Secret Data	X_0
1	File1	0.0036
2	File2	0.0008
3	File3	0.0019
4	File4	0.0126
5	File5	0.0024

4.2 Peak Signal to Noise Ratio

The Peak-Signal-to-Noise Ratio (PSNR) can be used to assess the quality of the data. A good encryption method is expected to produce encrypted data with a low value of PSNR [14]. Mathematically, PSNR is calculated using Eq. (2).

$$PSNR = 10 \log_{10} \left(\frac{Peak^2}{MSE} \right) \qquad (2)$$

where peak denotes the maximum value of the secret message and MSE denotes the mean square error and it is calculated using the Eq. (3).

$$MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(P_{ij} - E_{ij} \right)^2 \qquad (3)$$

where mn denotes the row and column of the data. P and E denotes the secret and encrypted data. In the last, ij denotes the subscripted variables. Table 2 shows the PSNR for chaotic map and proposed algorithm. The PSNR value of proposed algorithm is lesser than chaotic map algorithm.

Table 2: PSNR for the Chaotic Map Algorithm and Proposed Algorithm

Sr No.	Secret Data	Chaotic Logistic Map Algorithm [7]	Proposed Algorithm
1	File1	12.96	12.61

2	File2	14.56	13.83
3	File3	13.28	12.90
4	File4	13.28	12.34
5	File5	12.88	12.45

4.3 Correlation Coefficient

This parameter measures the demographic changes between original and encrypted data [14]. The CC is varies -1 to 1. The 1 value represents the original and encrypted data is same and -1 value represents the original and encrypted data are complement to each other. It is determined using Eq. (6)

$$CC = \frac{\sum_{m=1}^{J}\sum_{n=1}^{K}(A_{mn}-A_{mean})(B_{mn}-B_{mean})}{\sqrt{\sum_{m=1}^{J}\sum_{n=1}^{K}((A_{mn}-A_{mean})^2)\sum_{m=1}^{J}\sum_{n=1}^{K}(B_{mn}-B_{mean})^2}} \quad (6)$$

whereas, AB denotes the original and encrypted data. JK represents the row and column of the data. In the last, mn denotes the subscripted variables. Table 3 shows the minimum correlation between secret data and encrypted data. Besides that, the proposed algorithm provides lesser correlation as compared to chaotic map algorithm.

Table 3: Correlation Coefficient between Secret Data and Encrypted Data for Chaotic Map and Proposed Algorithm

Sr No.	Secret Data	Chaotic Logistic Map Algorithm [7]	Proposed Algorithm
1	File1	-0.0548	0.0036
2	File2	-0.0489	0.0008
3	File3	-0.0657	0.0019
4	File4	-0.0697	0.0126
5	File5	-0.0681	0.0024

4.4 Avalanche Effect

Avalanche effect is desired security parameter of the cryptography. It measures the number of bits in the encrypted data change if 1-bit change is done in key or plaintext [15]. It is calculated using Eq. (5). In the ideal case, 50% bit changed required.

$$Avalanche\ Effect = \frac{No.of\ Bits\ Change\ in\ the\ Encrypted\ Data}{Block\ Size} X100 \quad (5)$$

Table 4 shows the avalanche effect for chaotic logistic map and proposed algorithm (RECTANGLE) algorithm. The results indicate that the proposed algorithm provides better avalanche effect as compared to chaotic map algorithm.

Table 4: Avalanche Effect for the Different Algorithms

S no.	Secret Data	Chaotic Logistic Map Algorithm [7]	Proposed Algorithm
1	File1	4%	48%

5. CONCLUSION

Advanced Metering Infrastructure (AMI) provides the two-way communication in the smart grid. The data is prone to attacks when communicated over the network. In the literature, various cryptography algorithm used for security purposes. However, these algorithms provide encryption not authentication of the data. Thus, in this paper, a lightweight encryption-authentication scheme is designed for the AMI using the RECTANGLE and Chaotic map algorithm. The proposed algorithm consumes lesser memory, generates different key, better security. Thus, the proposed algorithm is efficient, it is deployed for the real time security for smart grid.

6. REFERENCES

[1] Ramirez, D. F., Céspedes, S., Becerra, C., & Lazo, C. (2015, May). Performance evaluation of future AMI applications in smart grid neighborhood area networks. In *IEEE Colombian Conference on Communication and Computing (IEEE COLCOM 2015)* (pp. 1-6). IEEE.

[2] Kuzlu, M., Pipattanasomporn, M., & Rahman, S. (2014). Communication network requirements for major smart grid applications in HAN, NAN and WAN. *Computer Networks*, *67*, 74-88.

[3] El Mrabet, Z., Kaabouch, N., El Ghazi, H., & El Ghazi, H. (2018). Cyber-security in smart grid: Survey and challenges. *Computers & Electrical Engineering*, *67*, 469-482.

[4] Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer Networks*, *169*, 107094.

[5] Joseph, D. P., Krishna, M., & Arun, K. (2015). Cognitive analytics and comparison of symmetric and asymmetric cryptography algorithms. *International Journal of Advanced Research in Computer Science*, *6*(3).

[6] Arab, A., Rostami, M. J., & Ghavami, B. (2019). An image encryption method based on chaos system and AES algorithm. *The Journal of Supercomputing*, *75*(10), 6663-6682.

[7] Reza, S. S., Ayob, A., Arifeen, M. M., Amin, N., Saad, M. H. M., & Hussain, A. (2020). A lightweight security scheme for advanced metering infrastructures in smart grid. *Bulletin of Electrical Engineering and Informatics*, *9*(2), 777-784.

[8] Menon, D. M., & Radhika, N. (2015). Design of a secure architecture for last mile communication in smart grid systems. *Procedia Technology*, *21*, 125-131.

[9] Abood, O. G., Elsadd, M. A., & Guirguis, S. K. (2017, December). Investigation of cryptography algorithms used for security and privacy protection in smart grid. In *2017 Nineteenth International Middle East Power Systems Conference (MEPCON)* (pp. 644-649). IEEE.
[10] Chakraborti, A., Datta, N., Jha, A., & Nandi, M. Structural Classification of Authenticated Encryption Schemes.
[11] McKay, K., Bassham, L., Sönmez Turan, M., & Mouha, N. (2016). *Report on lightweight cryptography* (No. NIST Internal or Interagency Report (NISTIR) 8114 (Draft)). National Institute of Standards and Technology.
[12] Zhang, W., Bao, Z., Lin, D., Rijmen, V., Yang, B., & Verbauwhede, I. (2015). RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms. *Science China Information Sciences*, *58*(12), 1-15.
[13] Patel, S., & Muthu, R. K. (2020). Image encryption decryption using chaotic logistic mapping and dna encoding. *arXiv preprint arXiv:2003.06616*.
[14] Ramasamy, P., Ranganathan, V., Kadry, S., Damaševičius, R., & Blažauskas, T. (2019). An image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced logistic—Tent map. *Entropy*, *21*(7), 656.
[15] Bansod, G., Pisharoty, N., & Patil, A. (2017). BORON: an ultra-lightweight and low power encryption design for pervasive computing. *Frontiers of Information Technology & Electronic Engineering*, *18*(3),

