A New Lightweight Chaos Based Cryptosystem For IoT Devices

Presented By:
Partho Choudhury Shoumya
Roll: 1807021

Supervised By:
Dr. Kazi Md. Rokibul Alam
Professor

Department of Computer Science & Engineering
Khulna University of Engineering & Technology
Khulna -9203, Bangladesh

8/24/2023

Outline

- Motivation
- Introduction
- Related Works
- Objectives
- Methodology
- Progress
- Discussion & Conclusion
- References

Motivation

- Data communication between IoT devices are increasing rapidly
- Techniques are required to keep transmitted data safe from outsiders
- Some existing algorithms are no longer reliable and some of the other requires more amount of resources than IoT devices may offer
- To deal with these issues, a dedicated cryptosystem is required to ensure efficient and secure IoT communication

Introduction

Why IoT?

- With growing amount of population, number of cities are also increasing
- Cities face problems such as pollution, traffic congestion and waste management.
- Experts suggest to connect these systems to internet to maintain them easily and efficiently.
- This leads to the concept of Internet of Things (IoT)

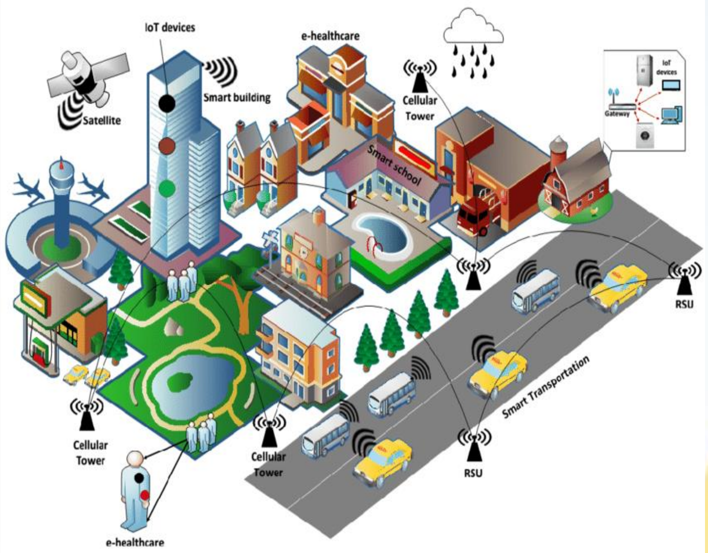


Fig 1: IoT network in a city

Introduction (Contd.)

Some Existing Algorithms

- Some well known cryptographic techniques such AES, DES, RSA etc. are being used to secure IoT communications

Limitations

- Not suited for constrained devices with limited resources

Lightweight Cryptosystems

- Huge emphasis is being put into developing lightweight cryptosystems adapted to these constrained devices

Introduction (Contd.)

Why Chaos Based Cryptosystem

- Chaotic systems have good cryptographic features such as unpredictability, aperiodicity, nonlinearity and high sensitivity to control parameters.
- Implementation requires fewer resources than conventional approaches
- Thus making it lightweight and attractive for providing strong and efficient cryptography for resource constrained nodes.

Related Works

Table 1: Comparison of related works

Author	Approach	Problem
Nguyen et al. [1]	Low power circuit	Hardware solution
Nesa and Banerjee [2]	Chaos based encryption algorithm built upon a quadratic sinusoidal map	No decryption process. No implementation result
Akgul et al. [3]	Uses three different chaos generators	Only text data can be encrypted

Objectives

- **Dedicated cryptographic algorithm:** To design a technique that can be used by nodes having limited memory, CPU capability, power resource etc.
- **Ensuring security:** The lightweight technique must ensure security in communication between the nodes
- **Covering all types of data:** The algorithm must work for all types of data such as text, image, voice etc.

Methodology

- An overview of the proposed methodology is as follows:

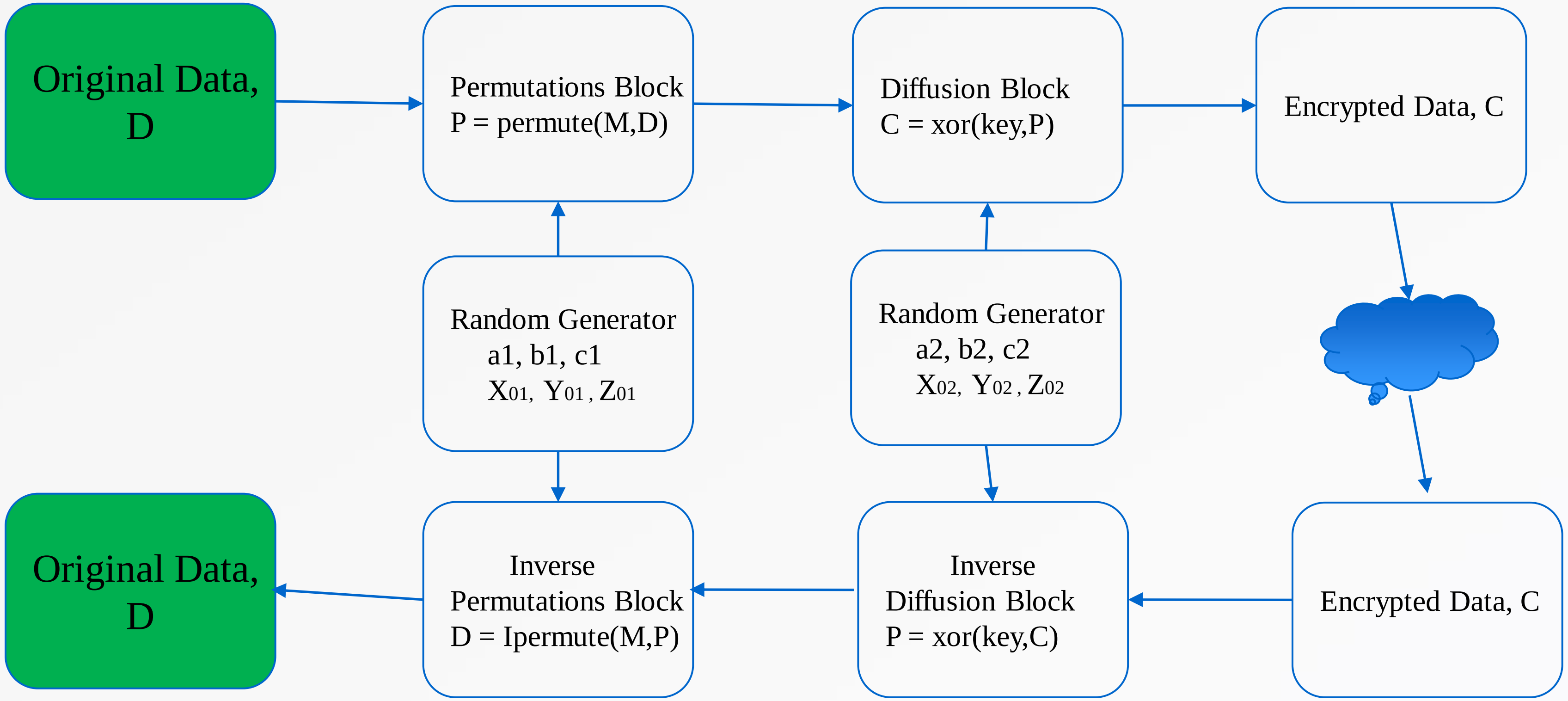


Fig 2: Overview of the proposed methodology

Methodology (Contd.)

- For random generator Lorenz System has been choosen.
- The equations are as below:

$$\frac{d\,x(t)}{dt} = a(y - x)$$

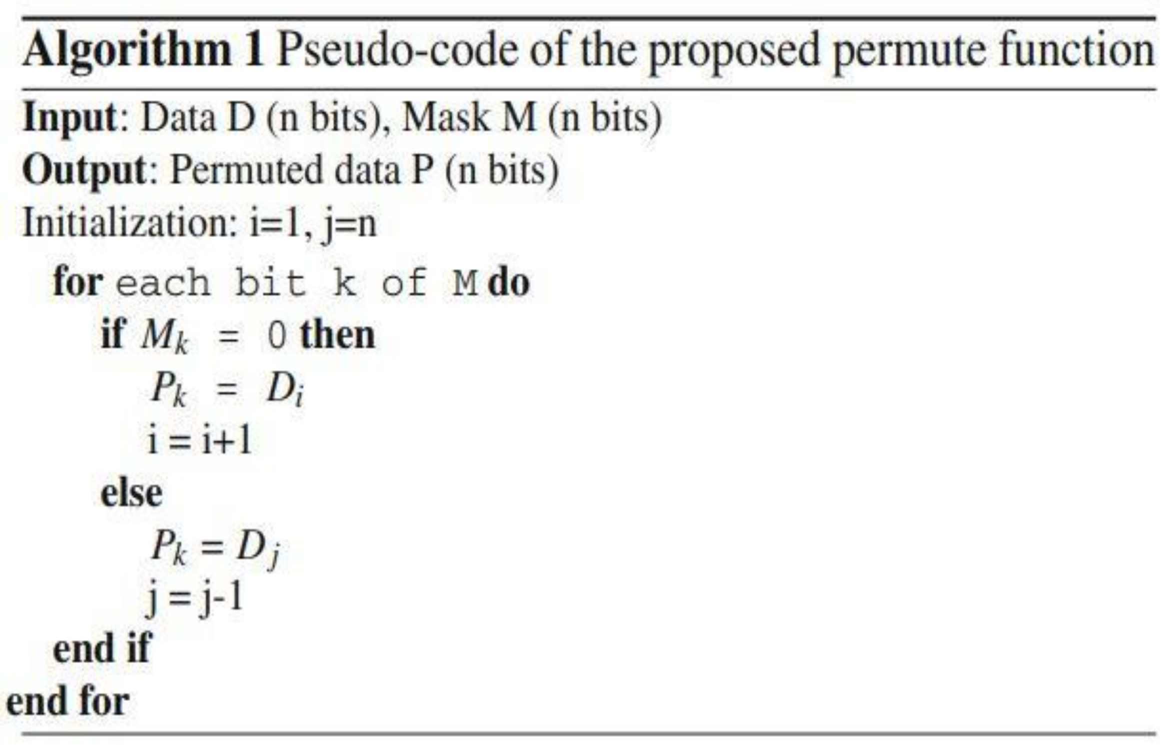
$$\frac{d\,y(t)}{dt} = cx - y - xz$$

$$\frac{d\,z(t)}{dt} = xy\ - bz$$

- Here a, b, c are system parameters and x, y, z are initial conditions
- Runge-Kutta method could be used to solve this

Methodology (Contd.)

- Primarily the below algorithm is designed to perform encryption process:

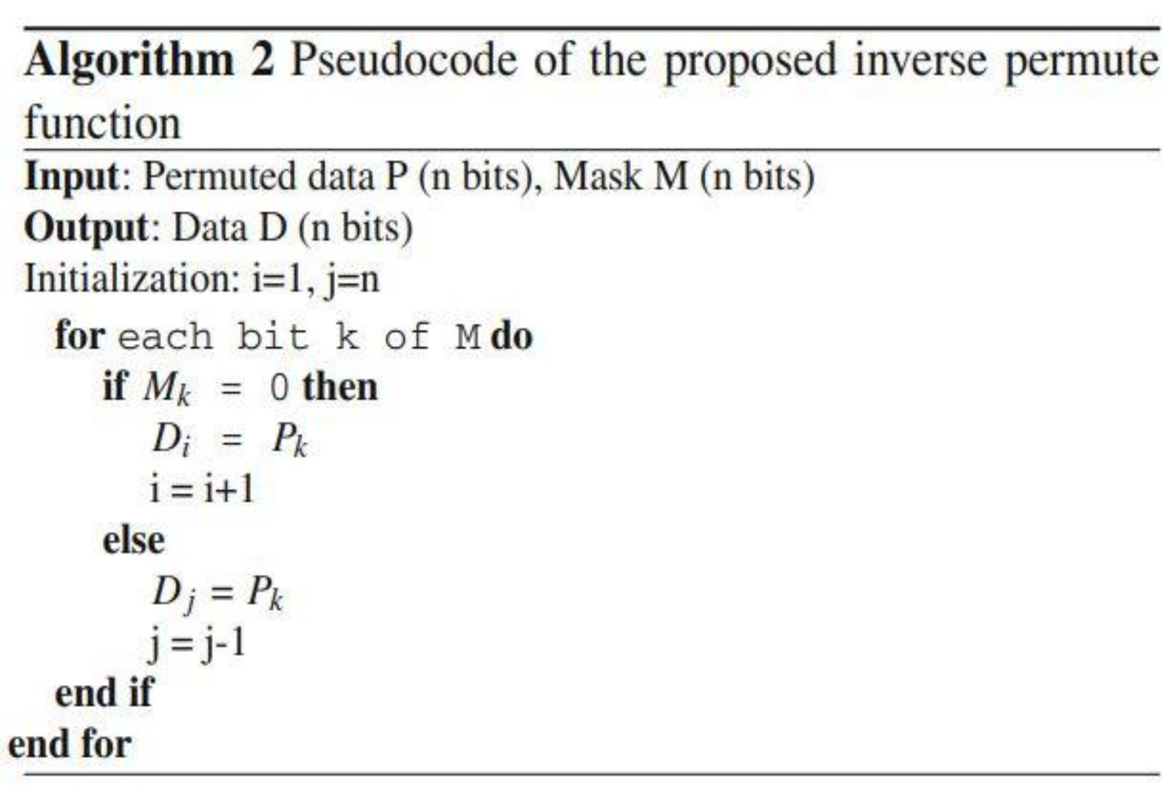


Algorithm 1 Pseudo-code of the proposed permute function

```
Input: Data D (n bits), Mask M (n bits)
Output: Permuted data P (n bits)
Initialization: i=1, j=n
  for each bit k of M do
    if $M_k = 0$ then
      $P_k = D_i$
      i = i+1
    else
      $P_k = D_j$
      j = j-1
  end if
end for
```

Methodology (Contd.)

- Primarily the below algorithm is designed to perform decryption process:

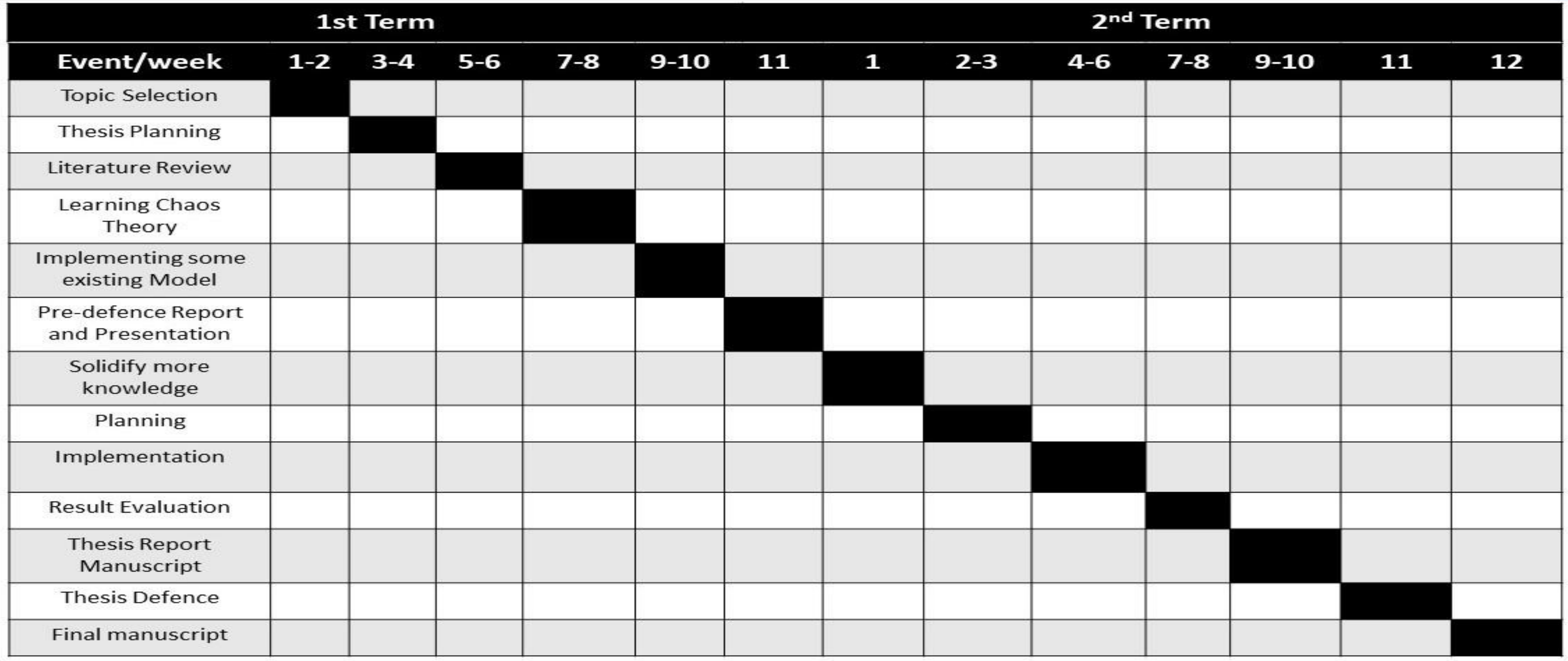


Algorithm 2 Pseudocode of the proposed inverse permute function

```
Input: Permuted data P (n bits), Mask M (n bits)
Output: Data D (n bits)
Initialization: i=1, j=n
  for each bit k of M do
    if $M_k = 0$ then
      $D_i = P_k$
      i = i+1
    else
      $D_j = P_k$
      j = j-1
  end if
end for
```

Progress

Fig 2: Gantt chart depicting thesis progress



	1st Term						2nd Term						
Event/week	**1-2**	**3-4**	**5-6**	**7-8**	**9-10**	**11**	**1**	**2-3**	**4-6**	**7-8**	**9-10**	**11**	**12**
Topic Selection	■												
Thesis Planning		■											
Literature Review			■										
Learning Chaos Theory				■									
Implementing some existing Model					■								
Pre-defence Report and Presentation						■							
Solidify more knowledge							■						
Planning								■					
Implementation									■				
Result Evaluation										■			
Thesis Report Manuscript											■		
Thesis Defence												■	
Final manuscript													■

Discussion & Conclusion

Key features:

1. Have 3 essential components: Lorenz based random generator, Chaotic permutation XOR operation
2. Provides enough powerful protection against brute-force attack
3. Suitable to use in resource constrained IoT nodes

Future Work:

1. Develop a key sharing mechanism
2. A lightweight security protocol that involves authentication of deployed IoT devices

References

- [1] Nguyen, N., Pham-Nguyen, L., Nguyen, M.B., Kaddoum, G.: A low power circuit design for chaos-key based data encryption. IEEE Access 8, 104432–104444 (2020)
- [2] Nesa, N., Banerjee, I.: A lightweight security protocol for iot using Merkle hash tree and chaotic cryptography. In: Advanced Comput ing and Systems for Security, pp. 3–16. Springer (2020). https://doi.org/10.1007/978-981-13-8969-6_1
- [3] Akgül, A., Kaçar, S., Aricıo ˘glu, B., Pehlivan, I.: Text encryption by using one-dimensional chaos generators and nonlinear equations. In: 2013 8th International Conference on Electrical and Electronics Engineering (ELECO), pp. 320–323. IEEE (2013). https://doi.org/10.1109/ELECO.2013.6713853

Thank you

QUESTIONS?