

Design and implementation of a new lightweight chaos-based cryptosystem to secure IoT communications.

Roll: 1807021

Date: 11/06/2023

My Work: Lorenz system is used for random generator part in this paper. Below is the equation:

$$\frac{dx(t)}{dt} = a(y - x) \quad \left| \quad \frac{dy(t)}{dt} = cx - y - xz \quad \left| \quad \frac{dz(t)}{dt} = xy - bz \right.$$

Dynamical System: One or more variables that change over time according to autonomous differential equations.

Phase Space: Cartesian space. Each point in the space is a unique state of the system, and has its own rate of change which can be shown as a vector.

Attractor: Set of points in the phase space which attracts all the trajectories in an area surrounding it – the basin of attraction.

- i) Fixed point attractor
- ii) Limit cycle attractor – Van der pol oscillator.

Strange Attractor: It has a fractal structure. For Lorenz system it is 2.06.

Difference for different initial conditions:

$$D_t = D_0 e^{\lambda t}$$

λ = Lyapunov exponent ;

Positive = Difference between trajectories increases exponentially.

Zero = Difference remains constant

Negative = Difference comes becomes zero eventually.

It is measured by simulation, keeping track of many trajectories.

It provides how chaotic a system is.

For Lorenz system, it is 0.9

Future Plan: Learn more detail about Lorenz system and mathematics related to it.