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

Roll: 1807021 Date: 04/06/2023

Recap: Previously I read and grasped most of the contents of the entire paper. Learnt about proposed cryptosystem in detail to understand the said encryption and decryption process.

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

$$\frac{d\,x(t)}{dt} = a(y - x) \quad \left| \quad \frac{d\,y(t)}{dt} = cx - y - xz \quad \right| \quad \frac{d\,z(t)}{dt} = xy - bz$$

Here a, b and c are the system parameters and x_0, y_0 and z_0 are the initial conditions. Runge-Kutta method is used to solve this equation. It is simulated in MATLAB tool.

- X and Y outputs of random generator are used for permutation and xor blocks.
- These value are converted from float to binary using IEEE754 standard.
- The keys are constructed using the least significant bits (LSBs) of the fractional part of X and Y of the chaotic generator because of their rich dynamics.
- If a generator can produce more than 2^{100} different key combinations, then it is considered unbreakable against brute-force attack.
- Here the generated key depends on 6 values: three initial conditions (x_0, y_0, and z_0) and three parameters (a, b, and c).
- Each value is encoded on 32 bits. Therefore, the key space is $2^{32}\times2^{32}\times2^{32}\times2^{32}\times2^{32}\times2^{32} = 2^{192} \geq 2^{100}$.
- This value is far above the required keyspace making this scheme robust against brute force attacks.

Future Plan: Learn more detail about Lonrenz system and also simulate it in MATLAB tool. Unmodified Lorenz system will be used to be simulated.