Chaotic Cryptography: Applications of Chaos Theory to Cryptography

Nathan Holt

What is Chaos Theory?

- Loosely speaking, the study of dynamical systems that are sensitive to initial conditions.

- In mathematically rigorous terms:
  - Sensitive to initial conditions
  - Topologically mixing
  - Dense periodic orbits

- In the words of Lorenz, “Chaos: When the present determines the future, but the approximate present does not approximately determine the future.”

Why is This Appealing For Cryptography?

- The sensitivity to initial conditions means that the slightest change to the start state will drastically alter the future orbit of the chaotic map.

- In cryptographic terms, imagine the “start state” as the key, and the orbit of the chaotic map as an output of cipher text. This means that the slightest change to the key (1 bit) will drastically change the encrypted ciphertext.

- This creates seeming randomness from deterministic processes. Thus, this is also called deterministic chaos.

What Work Has Been Done in The Field?

- Gutowitz first proposed dynamical systems-based cryptography in 1996 in his paper "Cryptography with Dynamical Systems" published in *Cellular Automata*.
- Baptista proposed the first cryptosystem based on Chaos Theory in 1998.
- The topic died off for several years, but was brought back in 2008 in a paper posted to Arxiv called "On the Inadequacy of the Logistic Map for Cryptographic Applications."
- Since then, multiple papers have been published regarding chaotic cryptography.
- Two papers in particular, "Modified Logistic Maps for Cryptographic Application" and "2-Step Logistic Map Chaotic Cryptography Using Dynamic Look-up Table" were published in 2015 in *Applied Mathematics* and *International Journal of Computer Applications* respectively. These papers are the focus of my research.

What Are the Proposed Cryptographic Processes?

Based on the Logistic Map:

$$X_{n+1} = r \cdot X_n \cdot (1 - X_n)$$

- Most cryptosystems are based on the Logistic Map, or variants thereof.

- In “Modified Maps for Cryptographic Application”, a modified Logistic Map is proposed which increases sensitivity to the initial condition and the chaotic range of the map, meaning an increase in the keyspace.

- In “2-Step Logistic Map Chaotic Cryptographic Using Dynamic Look-up Table,” an encryption scheme is proposed that uses subkeys and a dynamic lookup table.

Modified Logistic Map

- $X_{n+1} = \begin{cases} g(x) = r \cdot X_n \cdot (1 - X_n), & X_n < 0.5 \\ h(x) = r \cdot X_n \cdot (X_n - 1) + \frac{r}{4}, & X_n \geq 0.5 \end{cases}$

- This increases the chaotic range of the parameter r to [2,4], whereas in the original Logistic Map, the chaotic range is [3.56995,4] (excluding islands of stability).

- This alteration increases the chaotic range of the logistic map fivefold times, increasing the potential keyspace for cryptographic protocols that implement this.

Proposed Encryption Scheme

- Based on Baptista's original Logistic Map Encryption Scheme (1998)
- New encryption scheme uses a 2-Step Logistic Map variant proposed in 2008, which we will modify further using the Cryptographic Logistic Map variant.
- Encryption is a stream cipher that utilizes a dynamic lookup table.
- Encryption has a key size of 160 bits.

NIST Statistical Test Suite

- NIST created a suite of tools in C to test binary bits for apparent randomness.
- These are based on statistical tests, and are no way a definitive test for randomness.
- For example, looking at small samples of pi or e will fail some of the NIST Statistical Tests, whereas taking larger sample sizes will pass.

- I will be implementing the proposed cryptographic encryption from the *International Journal of Computer Applications* with the alteration of the logistic map proposed in *Applied Mathematics*.
- The output of which will be tested for randomness via the NIST Suite.

Objectives

- Implementing the 2-Step Logistic Map Encryption with Dynamic Lookup Table using the modified Cryptographic Logistic Map
- Performing statistical analysis on the output of the logistic map encryption
- Measuring runtime and efficiency of the algorithm
- Discussion of brute force attacks against this encryption scheme
- Determining future improvements or other conclusions