

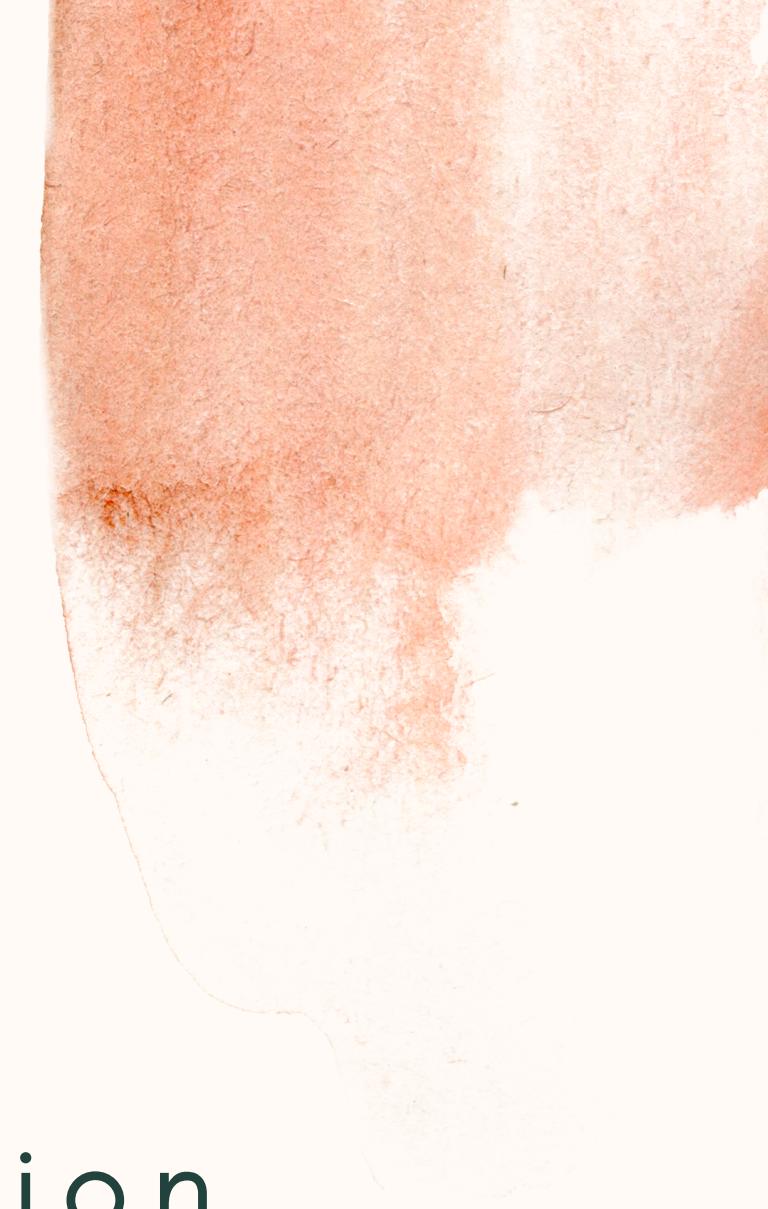
Image Cryptography

Abhinav Kumar
Purnendu Roy
Rushali Sarkar

Contents



1. Introduction
2. Confusion
 - KAA MAP
3. Diffusion
 - Key 1 Generation
 - Key 2 Generation
4. Security Analysis
5. Conclusion



Introduction

- Inspired from Research Paper
- Original Code
- Cryptography
- Random Numbers
- Generators Used

Confusion



Gallilean Transformation

- Symmetric 1D Transformation
- Equation - $r' = r + vt$



Rotational Transformation

- Symmetric 2D Transformation
- Equation -

$$\mathbf{r}' = \mathbf{R}\mathbf{r} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \mathbf{r},$$



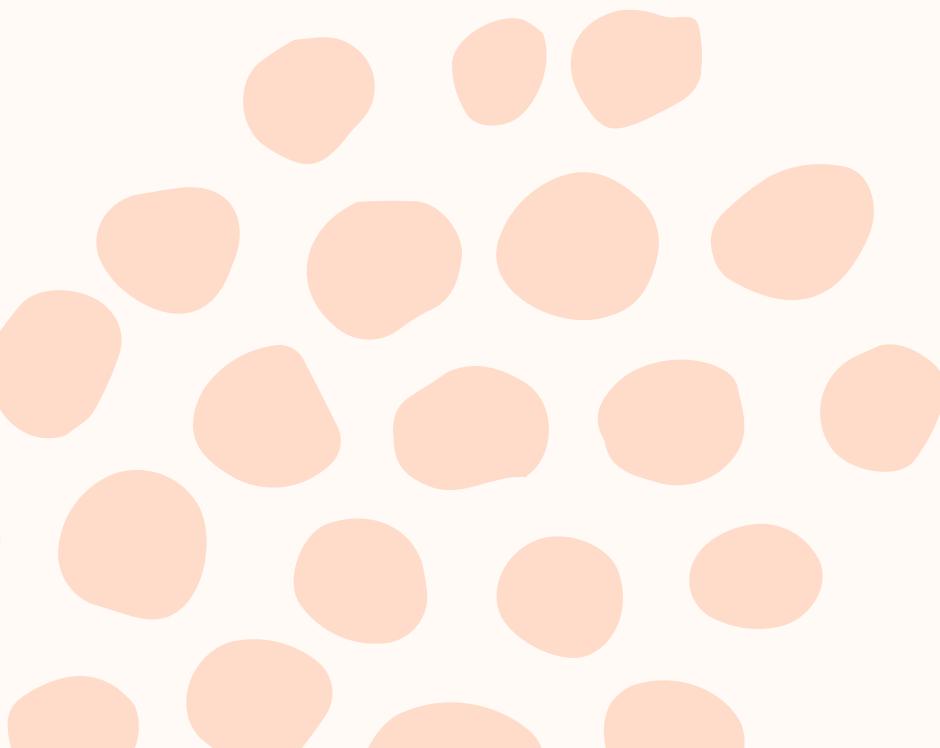
KAA Map

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} V_1 \\ V_2 \end{bmatrix} \times t \quad \text{mod } N,$$



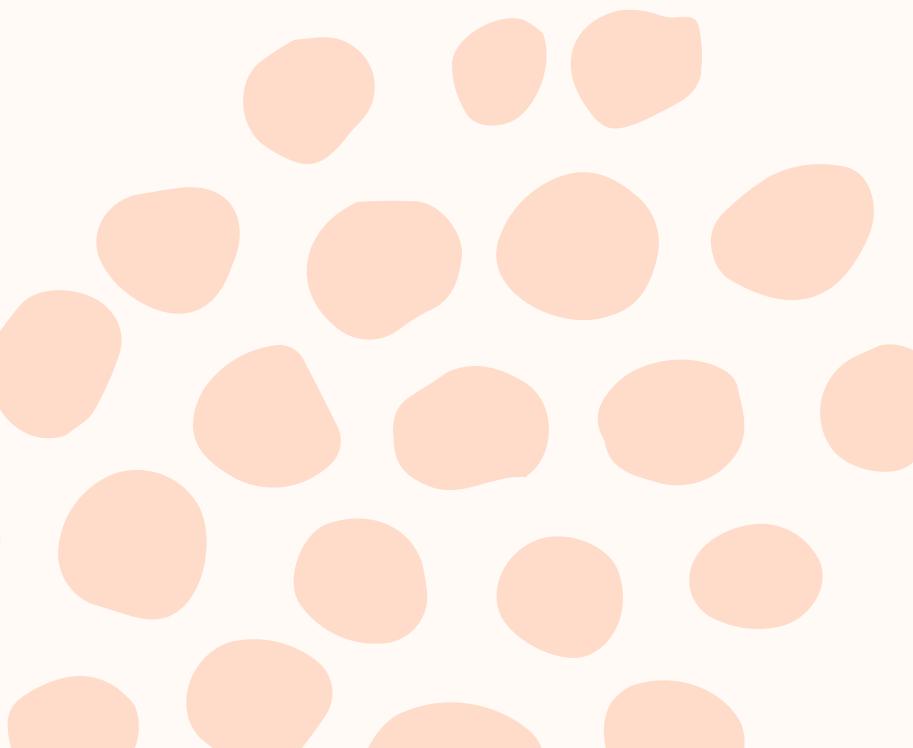
Diffusion

- Key 1 Generation
- Key 2 Generation



Logistic Map

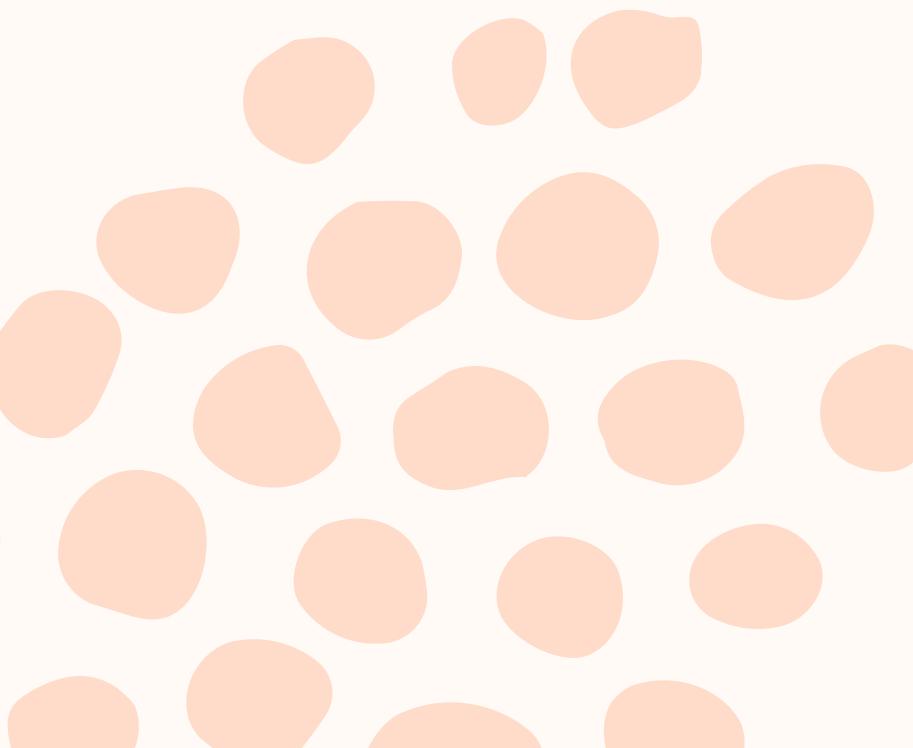
- Discrete-time analog of the logistic equation for population growing
- Equation - $x_{i+1} = p x_i (1 - x_i)$
- When $p \in [0.89, 1]$, Logistic map is chaotic



2D Logistic Map

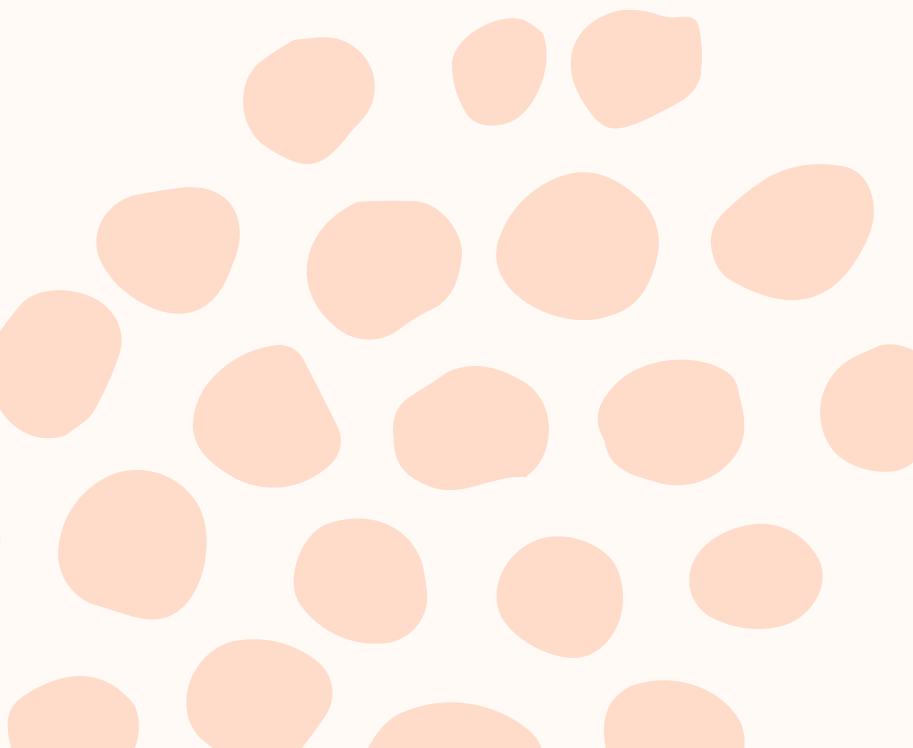
2D Logistic map:

$$\begin{cases} x_{i+1} = r(3y_i + 1)x_i(1 - x_i) \\ y_{i+1} = r(3x_{i+1} + 1)y_i(1 - y_i) \end{cases}$$



Sine Map

- Sine map is derived from sine function by transforming its inputs into $[0, 1]$
- Equation - $x_{i+1} = s \sin(\pi x_i)$
- Sine map is chaotic when $s \in [0.87, 1]$



2D Logistic- Adjusted-Sine Map

$$x_{i+1} = \sin(\pi\mu(y_i + 3)x_i(1 - x_i))$$

$$y_{i+1} = \sin(\pi\mu(x_{i+1} + 3)y_i(1 - y_i))$$

Linear Congruential Generator

- The linear congruential generator (LCG) was first published in 1960 by Thomson and Rotenberg
- Equation - $X_n = (aX_{n-1} + c) \bmod m$

Key 1 Generation

- IEEE-754 Double Presicion Convertor
- 64 bit + 64 bit + 44 bit -> 2D logistic adjusted sine map
- 64 bit + 44 bit -> Linear congruential generator

Bernoulli Map

- The Bernoulli chaotic map is a one-dimensional chaotic map that is defined from the range -A to A
- The Lyapunov exponent of the Bernoulli map is \log_2
- Equation -

$$x_{n+1} = \begin{cases} (B x_{(n)}) - A, & -A \leq x \leq 0, \\ (B x_{(n)}) + A, & 0 \leq x \leq A, \end{cases}$$

Tent Map

- The Tent map is also a chaotic one-dimensional map that displays a good chaotic sequential behavior.
- Similar to the Bernoulli map, it has a Lyapunov exponent of $\log 2$,
- Equation -

$$x_{n+1} = \begin{cases} C(x_{(n)}), & 0 < x < 1/2, \\ C(1 - x_{(n)}), & 1/2 < x < 1, \end{cases}$$

Key 2 Generation

- 32768 bits → Bernoulli Map
- 32768 bits → Tent Map

Security Analysis



Visual And Histogram Analysis



Information Entropy

$$H(m) = \sum_{i=1}^M p(m_i) \log_2 \frac{1}{p(m_i)}$$



Mean Squared Error

$$MSE = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (P_{(i,j)} - E_{(i,j)})^2}{M \times N}$$



Peak Signal to Noise Ratio

$$PSNR = 10 \log \left(\frac{I_{max}^2}{MSE} \right)$$

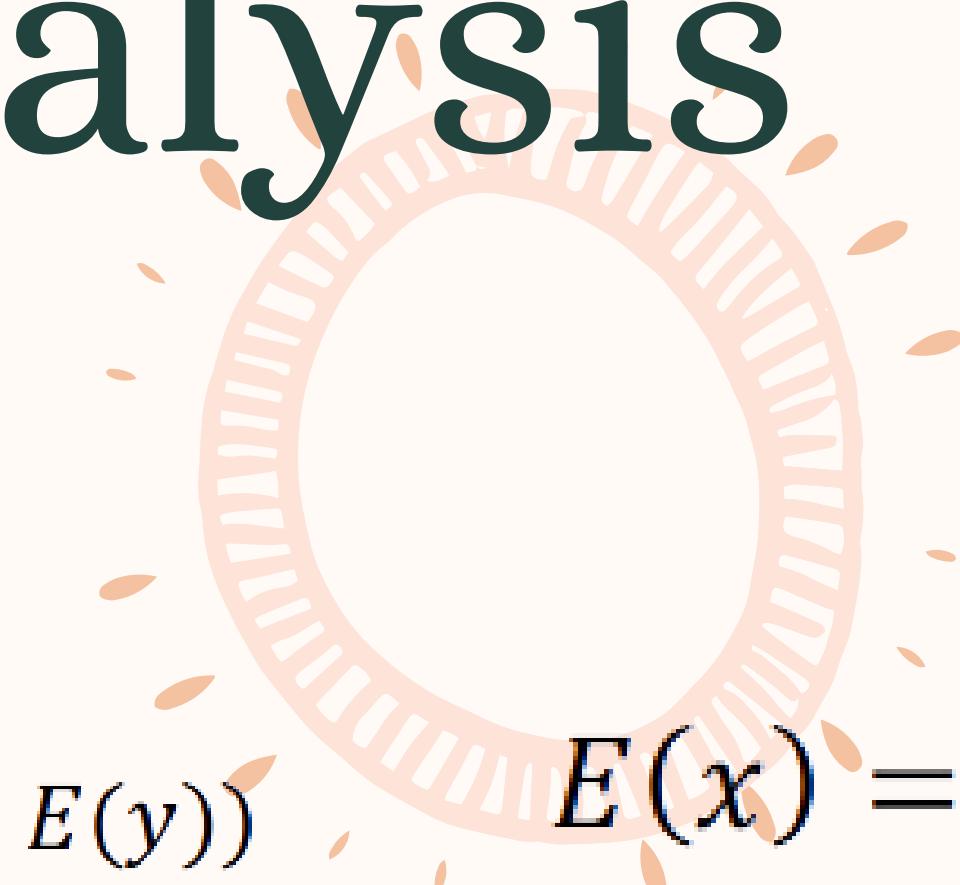


Correlation Coefficient Analysis

$$r_{xy} = \frac{cov(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

$$cov(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y))$$

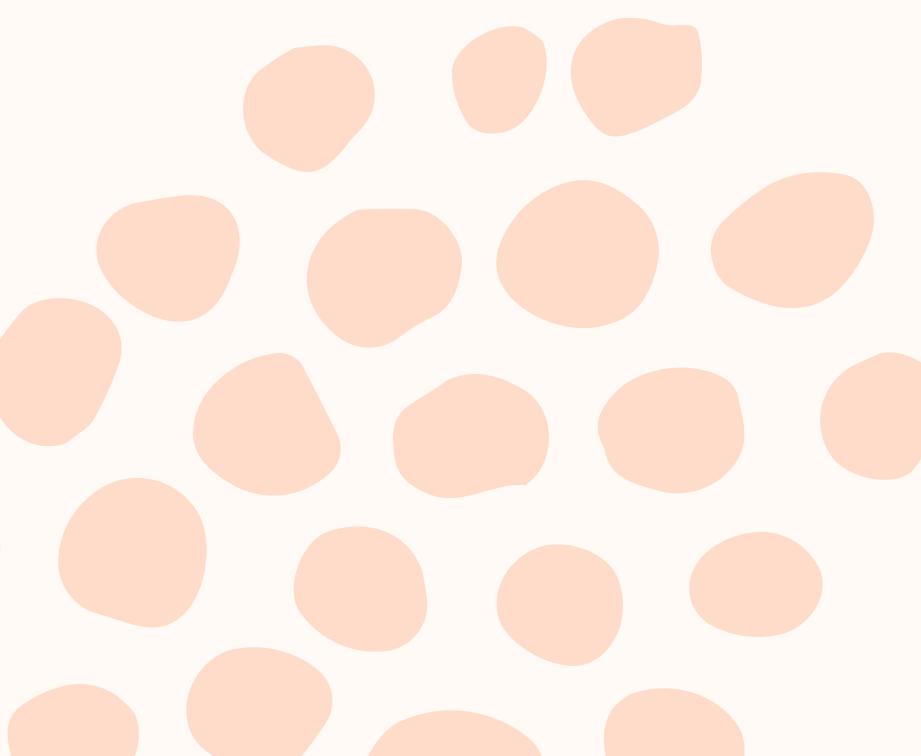
$$D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2$$



$$E(x) = \frac{1}{N} \sum_{i=1}^N (x_i)$$

Conclusion

- Efficiency and Reliability
- Challenges Faced





Thank
you