Chaos, Cryptology, and the Coupled Map Lattice
A Senior Research Project in Mathematics

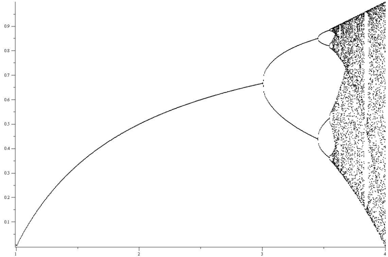
Matthew Weeks

April 22, 2010

Chaos

- Definition
  - Nonperiodicity
  - Sensitivity to initial conditions
- Logistic Map

$$x_{t+1} = \alpha x_t \left(1 - x_t\right)$$



Lyapunov Exponent

- Exponential rate of separation of nearby values
- Chaos when Lyapunov exponent > 0
- For one-dimensional map $x_{n+1} = f(x_n)$

$$\lim_{n\to\infty} \frac{1}{n} \left(\left| f'(x_1) \right| + \left| f'(x_2) \right| + \ldots + \left| f'(x_n) \right| \right)$$

- Lyapunov spectra
    - Extention of Lyapunov exponent
    - For spatially extended systems $x_n = (x_n^1, \ldots, x_n^N)$

$$\lim_{n\to\infty} \frac{1}{n} \ln \left(i\text{th eigenvalue of } J_{n-1} J_{n-2} \ldots J_0 \right)$$

$$(J_n)_{i,j} = \frac{\partial x_{n+1}^i}{\partial x_n^j}$$

Cryptology-Definitions

- Cryptosystem
- Plaintext
- Ciphertext
- Cryptography
- Cryptanalysis
- Cryptology
- PRBSG - Pseudorandom Bit Sequence Generator

Comparison to Chaos

- Similarities
  - Sensitivity to initial conditions/avalanche effect
  - Long-term behavior
  - Pseudo-randomness
- Differences
  - PRBSG's prefer integer formulae and results
  - Chaotic systems usually real numbers, or floating-point approximations

One Time Pad

- Form
- Shannon's proof
- Consequences

OTP example

Ciphertext: AGMROW

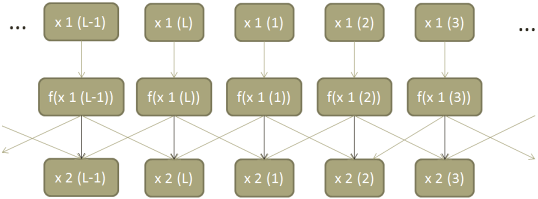
key	plaintext
ANTRMM	ATTACK
XCHNBT	DEFEND

The Coupled Map Lattice-Form

- State at time t held by L lattice elements
- Based on logistic map: $f(x) = \alpha x(1-x)$
- Coupling

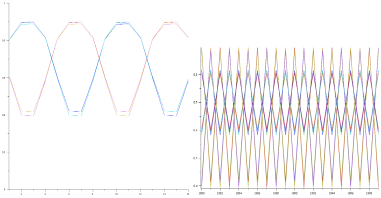
$$x_{t+1}^{i} = (1-\epsilon) f\left(x_t^i\right) + \frac{\epsilon}{2r} \sum_{k=1}^{r} \left(f\left(x_t^{i-k}\right) + f\left(x_t^{i+k}\right) \right)$$

- Visually ($r = 1$):

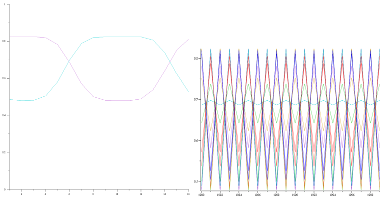


Behavior

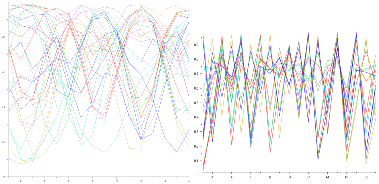
- Researched variations of $L = 16$, $r = 1$, $\alpha = 4$, $\epsilon = 0.5$



$\alpha = 3.7$



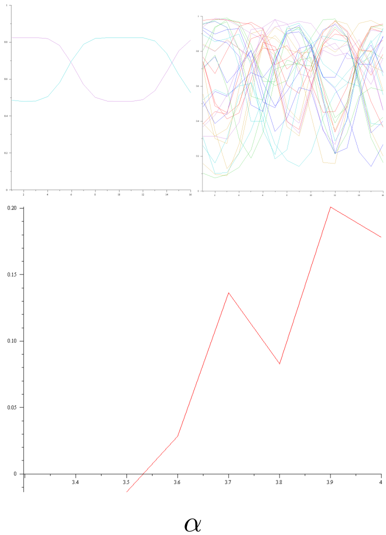
$\alpha = 3.3$



$\alpha = 4.0$

Behavior

Lyapunov Spectra

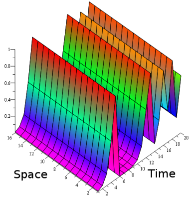


Limits of Lyapunov Spectra

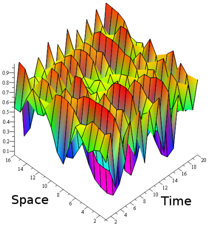
- Willeboordse's Lyapunov spectra capture temporal chaos
- Linear correlation coefficient (ρ) measures spatial

$$\rho = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{(n-1)s_x s_y}$$

  - Lyapunov spectra average s
  - Linear correlation coefficient ρ between $x_n(1)$ and $x_n(2)$



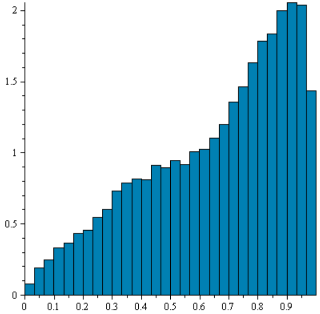
$r = 7$; $s = .5$; $\rho = 1$



$r = 1$; $s = .2$; $\rho = .7$

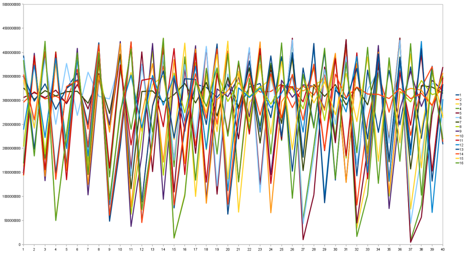
Behavior

Distribution of elements (2000 steps)



Long Term Behavior

- Long-term behavior: Chaotic
- Lyapunov spectra: 0.1-0.3

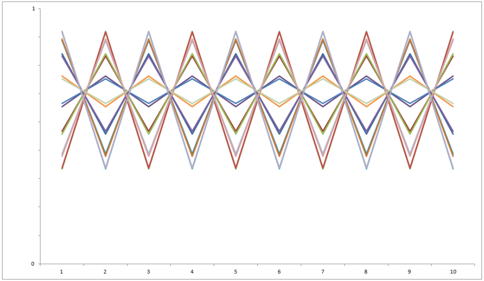


Time

Chaotic behavior at $n = 2000$

Long Term Behavior

- Long-term behavior: ~~Chaotic~~ Periodic
- Lyapunov spectra: $-\infty$

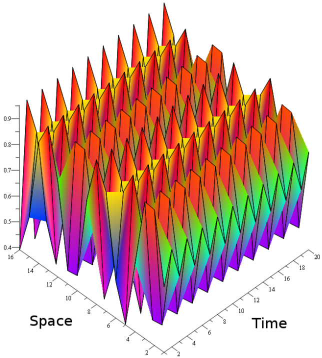


Time

Period-2 behavior at $n = 65530$

Long Term Behavior

- Long-term behavior: ~~Chaotic~~ Periodic
- Lyapunov spectra: $-\infty$



Period-2 behavior at $n = 10000$

Long Term Behavior

- Not all L display periodic behavior
- Long term cycle length dependent on L

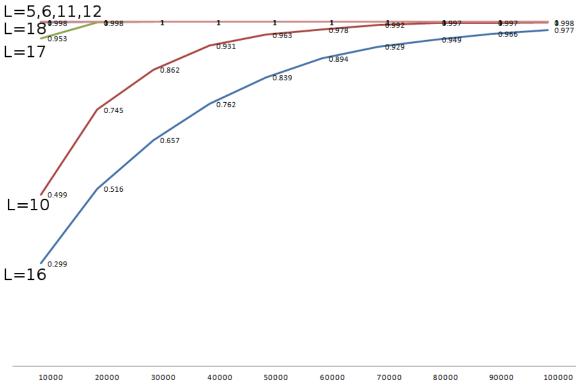
1	2	3	4	5	6	7	8	9	10	11	12	13
-	-	-	-	2	4	-	-	-	2	2	4	-

14	15	16	17	18	19	20	21	22	23	24	25	26
-	-	2	2	4	4	-	-	2	2	4	4	-

"-" = not apparently cyclic after 100000 time steps.

Long Term Behavior

- Depends on L, initial conditions



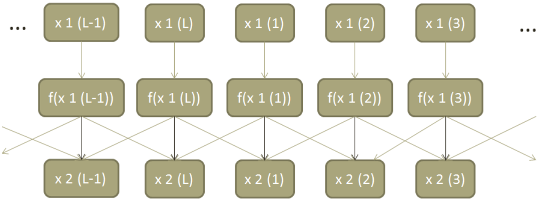
Probability of periodic behavior - threshold $2^{-6} = 0.015625$

Nanjing Cryptosystem

- Mao, Cao, and Liu (2006)
- Nanjing University of Science & Technology
- Basic idea - Pseudorandom Number Generator for OTP
- Parameters
    - $\epsilon = 0.5$, $r = 1$
    - $L = 16$ lattice elements
    - $M = 32$ (each $x_n(i)$ is 32 bits long)
    - $V = 16$ (lower 16 bits of each $x_n(i)$ used as output)
    - Holds $LM = (16)(32) = 512$ bits of internal state
    - Gives $LV = (16)(16) = 256$ bits of output for each block (each time n)
- Hardware implementation
- Bit extraction

Nanjing Cryptanalysis

- Impact of known plaintext
  - V/M of the key visible with known plaintext over one block
- Coupling weaknesses



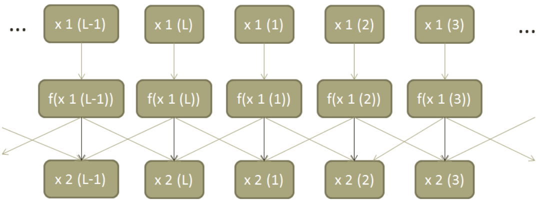
  - $x_n(i)$ not sensitive to initial conditions of most elements of x_{n-1}
  - Fails avalanche criterion (single bit change in input changes approximately half the output bits) and bit independence criterion (change in one bit affects bits j and k independently)
  - Takes $L/2$ steps for one lattice to affect all the others

Known Plaintext Attack

	$\mathbf{X}_1$	$\mathbf{X}_2$	$\mathbf{X}_3$	$\mathbf{X}_4$
$\mathbf{X}_n$	0.1234	0.8745	0.1936	0.6590
Output (K)	34	45	36	90
Plaintext (P)	72	73	84	88
	MESSAGE	START	SECRET	STUFF
Ciphertext (C, $C_i \equiv K_i + P_i$)	06	18	10	78
Known Plaintext	72	73		
	MESSAGE	START	?	?
Known Output ($K_i \equiv C_i - P_i$)	34	45		
Known $\mathbf{X}_n$	0.XX34	0.XX45	0.XXXX	0.XXXX

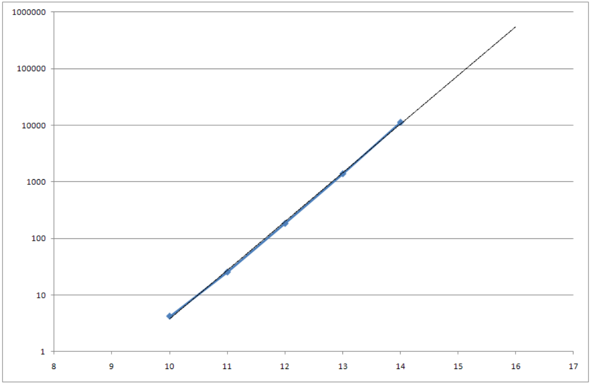
Nanjing Piecewise Attack

- Known 32 byte (256 bit) plaintext block gives lower 16 bits of each $x_n(i)$ with recommended $L = 16$ $M = 32$ $V = 16$
- Attack with at least two known-plaintext blocks starting at $n = 1$:
- Brute-force upper 16 bits of $x_1(1)$, $x_1(2)$, $x_1(3)$, that is, $x_1(1-3)$ checking against lower 16 bits of $x_2(2)$ to reduce the possibilities of those three (only about 1 in each $2^{16} = 65536$ remains)
- Find reduced set of possible $x_1(2-3)$, then $x_1(3-5)$, then $x_1(1-5)$



Nanjing Break

- Implementation details
  - Optimized implementation
  - Distributed computation
- Performance:



  - About 8 hours on 100-200 cores for full break

Nanjing Reverse Breaking

- Can obtain previous blocks given one known block
  - Solve linear system of equations with Gaussian elimination:

$$\frac{1}{2}f_n(i) + \frac{1}{4}f_n(i-1) + \frac{1}{4}f_n(i+1) = x_{n+1}(i)$$

$$\frac{1}{2}f_n(i+1) + \frac{1}{4}f_n(i) + \frac{1}{4}f_n(i+2) = x_{n+1}(i+1)$$

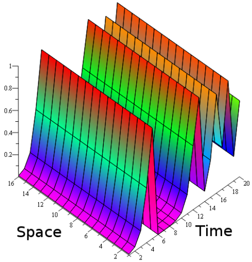
  ... (L equations, L variables)
  - Might not be invertible, but will reduce search space
- Find each $x_n(i)$ from $f_n(i)$

$$f^{-1}(x) = (4 \pm \sqrt{16 - 16x})/2x$$

- Two solutions - must check both

Alternatives

- Increase L to increase internal state size
  - Piecewise attack still succeeds
  - Only putting together possibilities for first three and first five is slow
- Increase r to stop piecewise attack
  - Causes excessive synchronization of lattice elements
  - $x_n(1) \approx x_n(2)$...



Synchronization. Long term behavior with $r = 7$, $L = 16$.

Alternatives

- Iterate $L/2$ times between extracting bits
  - 8x slower
  - Still has distribution problems, and linear correlation issues
  - Long term behavior still not chaotic
    - Reduces to XOR cryptosystem
    - Defeated by frequency analysis
- Use $L = 7$ or another value that does not become cyclic
  - Still has distribution problems, and linear correlation issues
  - Long term still fails

Tianjin Cryptosystem

- Hui, Kai-En, and Tian-Lun (2006)
- Institute of Physics, Nankai University, Tianjin, China
- Also PRBSG for OTP
- Parameters
  - $\epsilon = 0.2$, $r = 1$
  - $L = 64$ lattice elements
  - No detailed calculation information (bit sizes)
- Bit extraction
  - Reseed lattice for each block with key and separate PRBSG
  - Iterate lattice 116 times
  - Extract 1 bit from each element (most significant)

Tianjin Cryptosystem Analysis

- Strengths
  - Designed so brute-force attacker must try more than 100 possibilities for each lattice element
  - 100^{64} is secure
- Weaknesses
  - But (116)(64)(20) $\approx$ 128000 operations to encrypt/decrypt each block of 64 bits is unrealistic
  - Each key creates PRBSG with period of $2^{64} \approx 10^{19}$
  - Not suitable for long term use - 64 bit RC5 key brute forced in 2002

Further Research

- Long term behavior
  - Larger values of L, longer time steps for apparently chaotic values of L
  - What is the pattern that defines which values of L become periodic?
  - What about other values of r and ϵ?
- New ideas for cryptographically secure PRBSG's

Summary

- Coupled Map Lattices
- Coupling can synchronize and stabilize
- Not easy to make a practical, secure cryptosystem
- Still plenty of research to be done

Works consulted:

- Yaobin Mao, Liu Cao, and Wenbo Liu. Design and FPGA Implementation of a Pseudo-Random Bit Sequence Generator Using Spatiotemoral Chaos. In Communications, Circuits and Systems Proceedings, 2006 International Conference on.
- MA Hui, ZHU Kai-En, and CHEN Tian-Lun. A Cryptographic Scheme Based on Spatiotemporal Chaos of Coupled Map Lattices. Communications in Theoretical Physics, 45(3):477?482, 2006.
- F. H. Willeboordse. The Spatial Logistic Map as a Simple Prototype for Spatiotemporal Chaos. Chaos, 13, 2003.
- Distributed.net. Distributed.net completes rc5-64 project. (list announcement) 2002.