Analog Chaos-based Secure Communications and Cryptanalysis: A Brief Survey

Shujun Li[1*] Gonzalo Alvarez[2] Zhong Li[1] W. A. Halang[1]

[1]FernUniversität in Hagen, Germany

[2]Instituto de Física Aplicada, CSIC, Madrid, Spain

*http://www.hooklee.com

PhysCon 2007, Potsdam

Table of Contents

Table of Contents

Table of Contents

Table of Contents

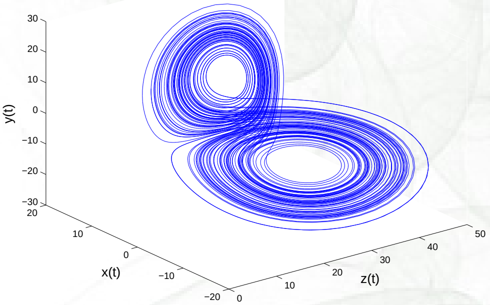
What's next?

Chaos implies

- sensitivity to initial conditions and control parameters;
- ergodicity;
- mixing property;
- complex but deterministic dynamics;
- ...

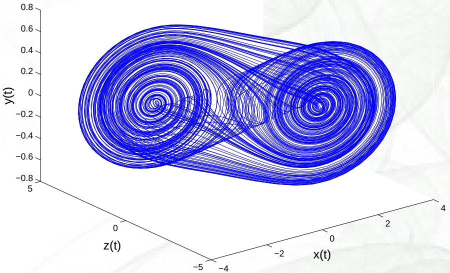
Lorenz system

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = cx - xz - y \\ \dot{z} = xy - bz \end{cases}$$



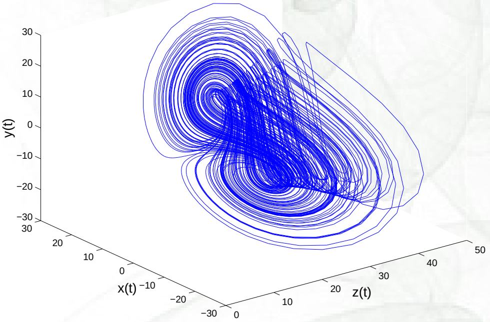
Chua's system (dimensionless form)

$$\begin{cases} \dot{x} = p(-x + y - f(x)) \\ \quad = p\left(-x + y - \left(m_0 x + \frac{(m_1 - m_0)(|x+1| - |x-1|)}{2}\right)\right) \\ \dot{y} = x - y + z \\ \dot{z} = -qy \ (\text{or } \dot{z} = -qy - rz) \end{cases}$$



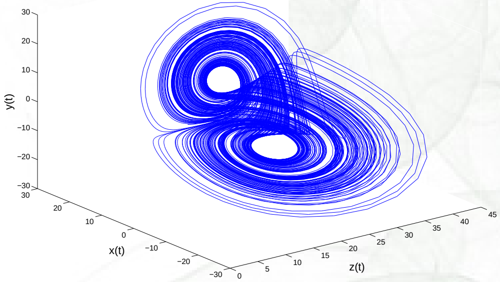
Chen's system

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = (c - a)x - xz + cy \\ \dot{z} = xy - bz \end{cases}$$



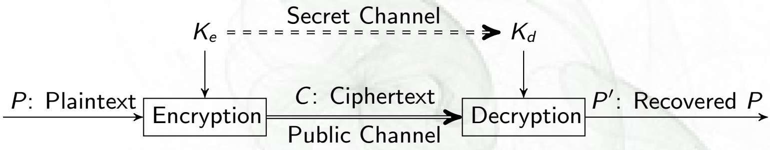
Lü's system

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = cy - xz \\ \dot{z} = xy - bz \end{cases}$$

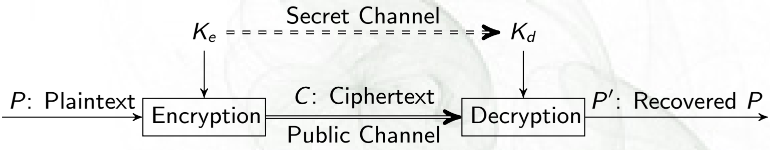


What's next?

Cryptosystem



Cryptanalysis



- Ciphertext-only attack: $C \rightarrow P$ and/or K?
- Known-plaintext attack: (known P) $+ C \rightarrow K$?
- Chose-plaintext attack: (chosen P) $+ C \rightarrow K$?
- Chosen-ciphertext attack: (chosen C) $+ P \rightarrow K$?

A cryptosystem depends on

- confusion;
- diffusion w.r.t small changes in plaintext;
- diffusion w.r.t small changes in secret key;
- pseudo but deterministic randomness;
- ...

What's next?

1. Fundamentals
   - Chaos
   - Cryptography
   - Chaos vs. Cryptography
   - Chaos Synchronization
2. Three Basic Approaches
3. Attacks ☠☠☠
   - Brute-Force Attack
   - Parameter Estimation
   - Estimation of Carrier Signal
   - Direct Extraction of Plaintext
4. New Countermeasures

Chaos vs. Cryptography

Chaos	Cryptography
ergodicity	confusion
sensitivity to initial conditions	diffusion w.r.t. small changes in plaintext
mixing property	
sensitivity to control parameters	diffusion w.r.t. small changes in secret key
complex but Deterministic dynamics	pseudo but deterministic randomness

Chaos + Cryptography

- Shannon's "Chaos" in his classical security paper (1949):
  "Good mixing transformations are often formed by repeated products of two simple non-commuting operations. Hopf has shown, for example, that pastry dough can be mixed by such a sequence of operations. The dough is first rolled out into a thin slab, then folded over, then rolled, and then folded again, etc."
- Digital "Chaos" existing in traditional ciphers:
  $(ax + b) \bmod p$, $x^n \bmod p$, etc.
- **Chaos** + **Cryptography** = **Chaotic Cryptography** ...

What's next?

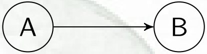
Chaos Synchronization

Definition

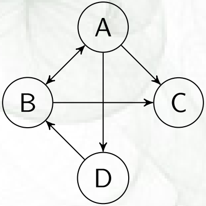
Synchronization of chaos refers to a process wherein two (or many) chaotic systems (either equivalent or nonequivalent) adjust a given property of their motion to a common behavior due to a coupling or to a forcing (periodical or noisy).

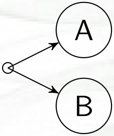
—S. Boccalettia et al. in [*Physics Reports* 366 (2002) 1–101]

Chaos Synchronization: Driving Modes

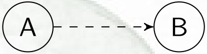
- Internal driving
  - Directional driving: 

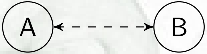
  - Bidirectional driving: 

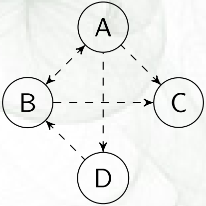
  - Network-like driving: 

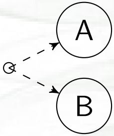
- External driving (forcing): 

Impulsive Driving → Impulsive Synchronization

- Internal driving
  - Directional driving: 

  - Bidirectional driving: 

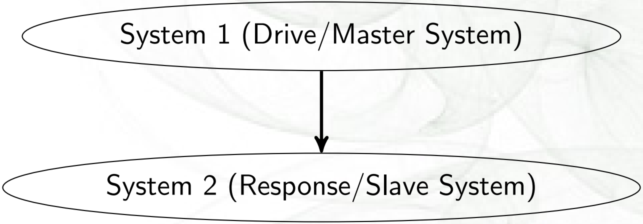
  - Network-like driving: 

- External driving (forcing): 

Chaos Synchronization: Directional Driving Case

Definition

Given two dynamical systems with different initial conditions, under a driving signal from System 1 (called drive system or master system), System 2 (called response system or slave system) asymptotically follows the state of System 1 in a certain sense.



Chaos Synchronization: Directional Driving Case

What does directional synchronization mean?

From information theoretical point of view, the establish of chaos synchronization between two systems means that some information has been successfully transmitted from one side (system 1) to the other (system 2). In other words, this is a communication process!

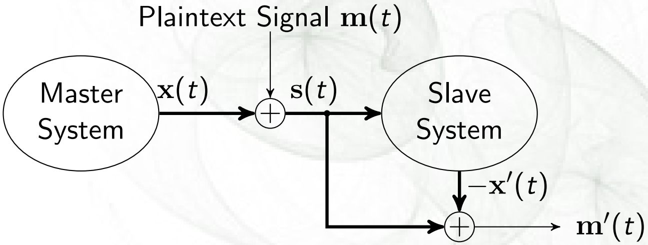
What's next?

$\Rightarrow$ By keeping some part secret, we get a secure communication system!

Chaos Synchronization: Synchronization Modes

- Complete synchronization: $\mathbf{x}_2(t) \to \mathbf{x}_1(t)$
- Phase synchronization: $\phi_2(t) \to \phi_1(t)$
- Projective synchronization: $\mathbf{x}_2(t) \to \alpha\mathbf{x}_1(t)$
- Time-delay synchronization: $\mathbf{x}_2(t) \to \mathbf{x}_1(t-\tau)$
- Generalized synchronization: $\mathbf{x}_2(t) \to \mathbf{h}(\mathbf{x}_1(t))$
- ...

Chaotic Masking



Chaotic Masking: An Example

$$\begin{cases} \dot{x}_1 = a(y_1 - x_1) \\ \dot{y}_1 = cx_1 - x_1 z_1 - y_1 \\ \dot{z}_1 = x_1 y_1 - bz_1 \end{cases}$$

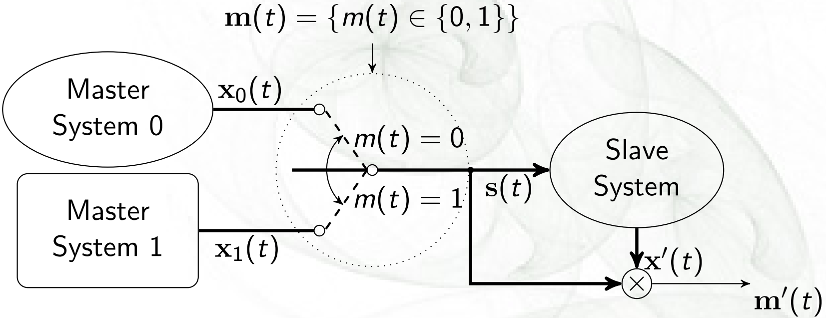
$$\downarrow s(t) = x_1(t) + m(t)$$

$$\begin{cases} \dot{x}_2 = a(y_2 - x_2) \\ \dot{y}_2 = cs(t) - s(t) z_2 - y_2 \\ \dot{z}_2 = s(t) y_2 - bz_2 \end{cases}$$

$$\Downarrow$$

$$\tilde{m}(t) = s(t) - x_2(t) \rightsquigarrow m(t)$$

Chaotic Switching (Chaotic Shift Keying = CSK)



Chaotic Switching: An Example

$$\begin{cases} \dot{x}_1^{(0)} = a^{(0)}(y_1^{(0)} - x_1^{(0)}) \\ \dot{y}_1^{(0)} = c^{(0)}x_1^{(0)} - x_1^{(0)}z_1^{(0)} - y_1^{(0)} \\ \dot{z}_1^{(0)} = x_1^{(0)}y_1^{(0)} - b^{(0)}z_1^{(0)} \end{cases} \quad \begin{cases} \dot{x}_1^{(1)} = a^{(1)}(y_1^{(1)} - x_1^{(1)}) \\ \dot{y}_1^{(1)} = c^{(1)}x_1^{(1)} - x_1^{(1)}z_1^{(1)} - y_1^{(1)} \\ \dot{z}_1^{(1)} = x_1^{(1)}y_1^{(1)} - b^{(1)}z_1^{(1)} \end{cases}$$

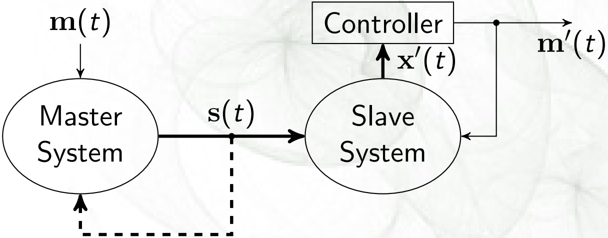
$$\downarrow s(t) = x_1^{(m(t))}(t)$$

$$\begin{cases} \dot{x}_2 = a^{(0)}(y_2 - x_2) \\ \dot{y}_2 = c^{(0)}s(t) - s(t)z_2 - y_2 \\ \dot{z}_2 = s(t)y_2 - b^{(0)}z_2 \end{cases}$$

$$\Downarrow$$

$$\tilde{m}(t) = \begin{cases} 0, & \int_{\Delta t} |x_2 - s(t)| \leq \varepsilon \\ 1, & \int_{\Delta t} |x_2 - s(t)| > \varepsilon \end{cases} = m(t)$$

Chaotic Modulation



Example 1: Chaotic Parameter Modulation

$$\begin{cases} \dot{x}_1 = \frac{1}{C_1}(Gm(t)(-x_1 + y_1) - f(x_1)) \\ \dot{y}_1 = \frac{1}{C_2}(Gm(t)(x_1 - y_1) + z_1) \\ \dot{z}_1 = \frac{1}{L}(-y_1 - R_0 z_1) \end{cases}$$

$$\downarrow x_1$$

$$\begin{cases} \dot{x}_2 = \frac{1}{C_1}(G\tilde{m}(t)(-x_2 + y_2) - f(x_2) + K_1(x_1 - x_2)) \\ \dot{y}_2 = \frac{1}{C_2}(G\tilde{m}(t)(x_2 - y_2) + z_2 + K_1(x_1 - x_2)) \\ \dot{z}_2 = \frac{1}{L}(-y_2 - R_0 z_2 + K_1(x_1 - x_2)) \\ \dot{\tilde{m}}(t) = k_1 \mathrm{sign}\left(\frac{1}{C_1}G(y_2 - x_2)\right)(x_1 - x_2) \end{cases}$$

$$\Downarrow$$

$$\tilde{m}(t) \rightsquigarrow m(t)$$

Example 2: Chaotic Direct (Non-Autonomous) Modulation

$$\begin{cases} \dot{x}_1 = -(y_1 + z_1) = -(x_1 + y_1) + s \\ \dot{y}_1 = x_1 + 0.45y_1 \\ \dot{z}_1 = 2 + z_1(x_1 - 4) + m(t) \end{cases}$$

$$\downarrow s = x_1 - z_1$$

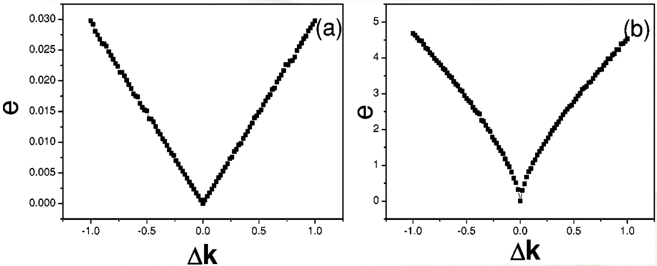
$$\begin{cases} \dot{x}_2 = -(x_2 + y_2) + s \\ \dot{y}_2 = x_2 + 0.45y_2 \\ \dot{z}_2 = 2 + z_2(x_2 - 4) + \tilde{m} \\ \dot{\tilde{m}} = a((x_2 - z_2) - s) = a(\tilde{s} - s) \end{cases}$$

$$\Downarrow$$

$$\tilde{m}(t) \rightsquigarrow m(t) \text{ when } a > 4$$

What's next?

Low Sensitivity to Parameter Mismatch



Source

Xingang Wang et al., "Error function attack of chaos synchronization based encryption schemes," *Chaos*, 14(1):128-137, 2004

What's next?

Parameter Estimation

- Adaptive synchronization (online)
- Direct parameter estimation (offline)
- Return-map method
- Chosen-ciphertext attack
- DAC (divide-and-conquer) attack

What's next?

Estimation of Carrier Signal

- Valid when $s(t) = m(t) + x(t)$ (chaotic masking and some modulation schemes).
- Short's NLD (Nonlinear dynamic) forecasting technique [IJBC 1994].
- One of most well-known cryptanalysis tool.

What's next?

Direct Extraction of Plaintext

- Return-Map Attack (one of most well-known cryptanalysis tool)
- Power Spectral (Filtering) Analysis
- Estimating Short-Time Period
- Generalized Synchronization Method
- Power Energy Analysis
- Switching Detection

New Countermeasures

- Using More Complex Chaotic Systems
  - Hyperchaos ✗
  - Time-delay Chaos ✗
  - ...
- Using more Complex Synchronization Modes
  - Impulsive Synchronization ✗
  - Projective Synchronization ✗
  - Phase Synchronization ✗
- Combining Heterogeneous Structures
  - Chaotic Masking + Chaotic Modulation ✗
  - Chaotic Switching + Chaotic Modulation ✗
  - ...

New Countermeasures (Continued)

- Pre-Encryption ✗
- Post-Modulation ✗
- Double-Channel Approach ✗
- Modified CSK Schemes
  - Multiple Chaotic Systems ✗
  - Alternative Driving ✗
  - False Switching Events

A Reference

Some Rules

Gonzalo Álvarez and Shujun Li, "Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 8, pp. 2129-2151, 2006

Questions and Answers

Thanks for your attentions!