– Presented at College of Information Engineering, Shenzhen University –

Analog Chaos-Based Secure Communications: A Survey

Dr. Shujun Li
http://www.hooklee.com
Department of Electronic and Information Engineering
The Hong Kong Polytechnic University
Hung Hom, Kowloon, Hong Kong SAR, China

CIE, SZU
Shenzhen
11 Nov., 2005

Contents

CIE, SZU
Shenzhen
11 Nov., 2005

CIE, SZU
Shenzhen

11 Nov., 2005






1 Chaos

Chaos vs. Cryptography

- Ergodicity vs. Confusion
- Sensitivity to initial conditions vs. Diffusion of a small change in plaintext
- Sensitivity to control parameters vs. Diffusion of a small change in secret key
- Mixing property vs. Diffusion from a small change of one plain-block to the whole plaintext (meaningful for image encryption)
- Deterministic dynamics vs. Deterministic pseudo-randomness
- Structure complexity vs. Attack Complexity

CIE, SZU
Shenzhen

11 Nov., 2005

Chaos vs. Cryptography

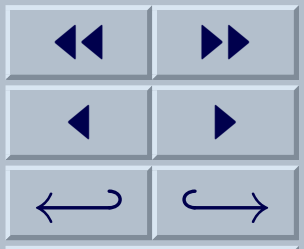
Then, why not use chaos for cryptography?

- 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.

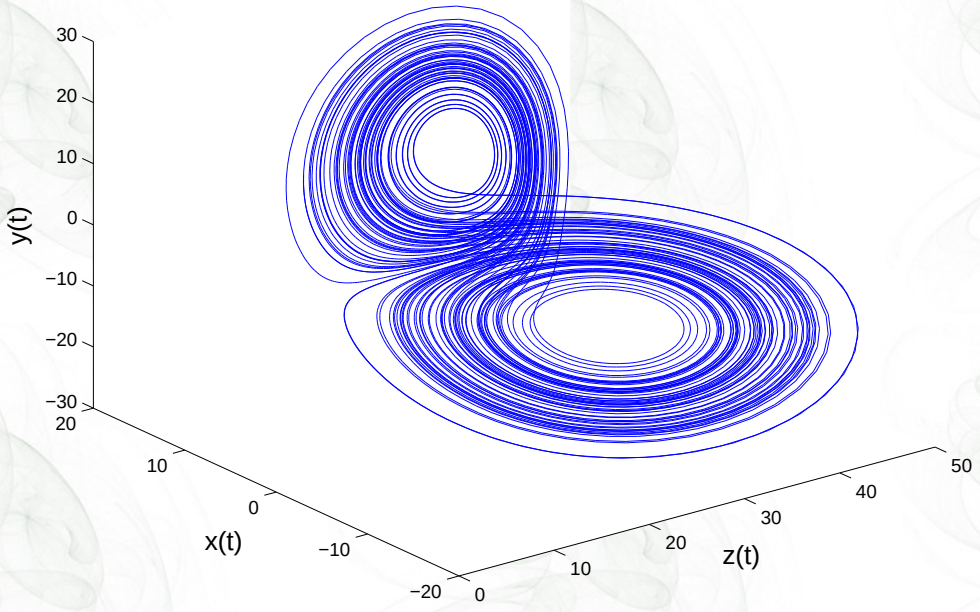
- **Chaotic Cryptography** ...

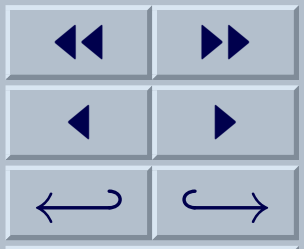


Continuous Chaotic Systems: 3-D Case

The Lorenz system

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



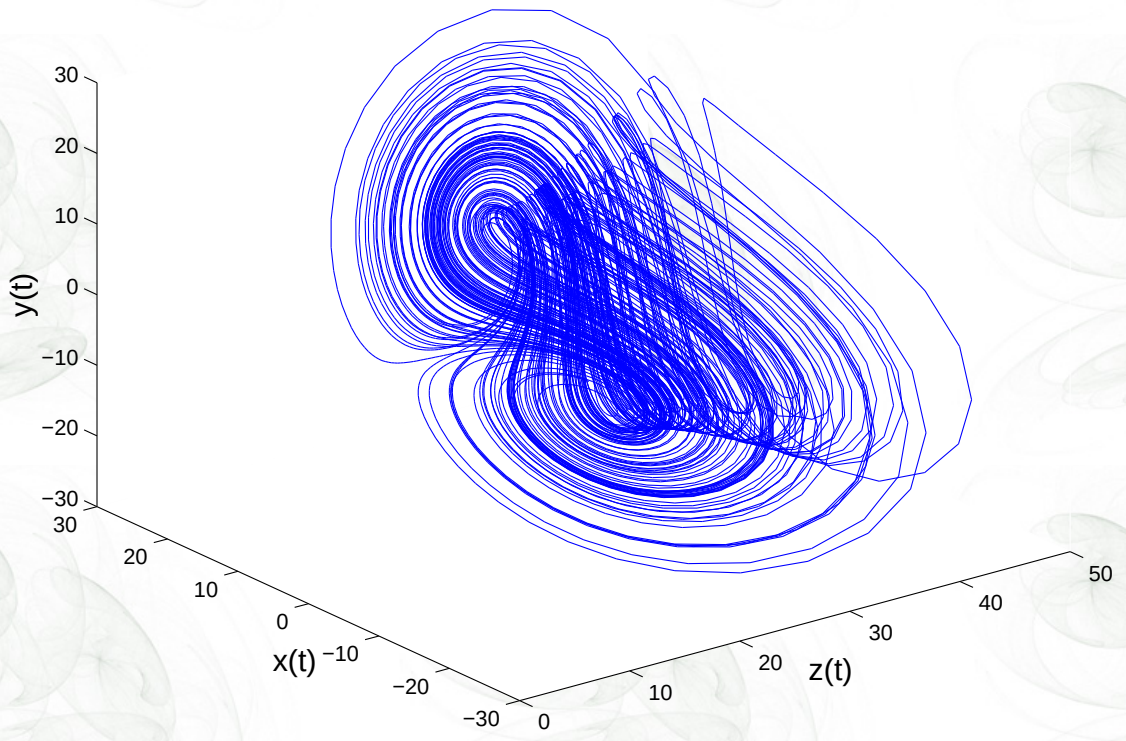


CIE, SZU
Shenzhen

11 Nov., 2005

The Chen system

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

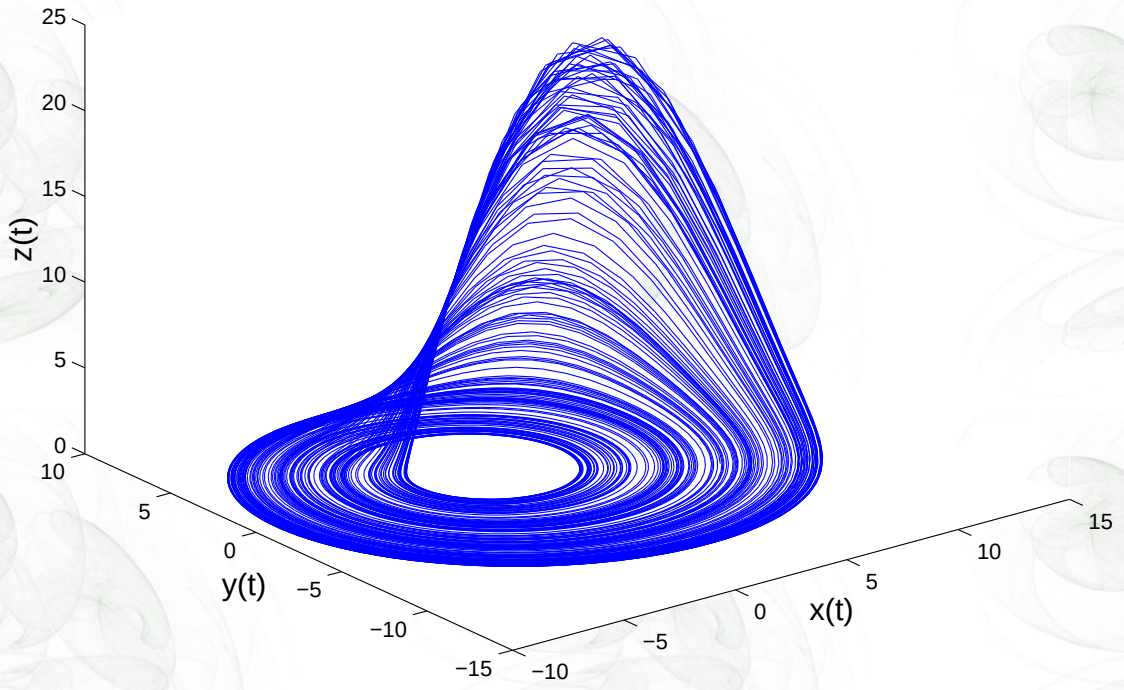


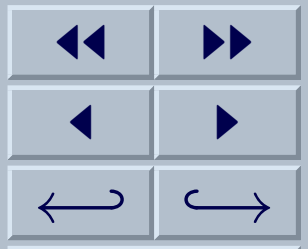
CIE, SZU
Shenzhen

11 Nov., 2005

The Rössler system

$$\begin{cases} \dot{x} = -(y+z) \\ \dot{y} = x + ay \\ \dot{z} = (x-c)z + b \end{cases}$$



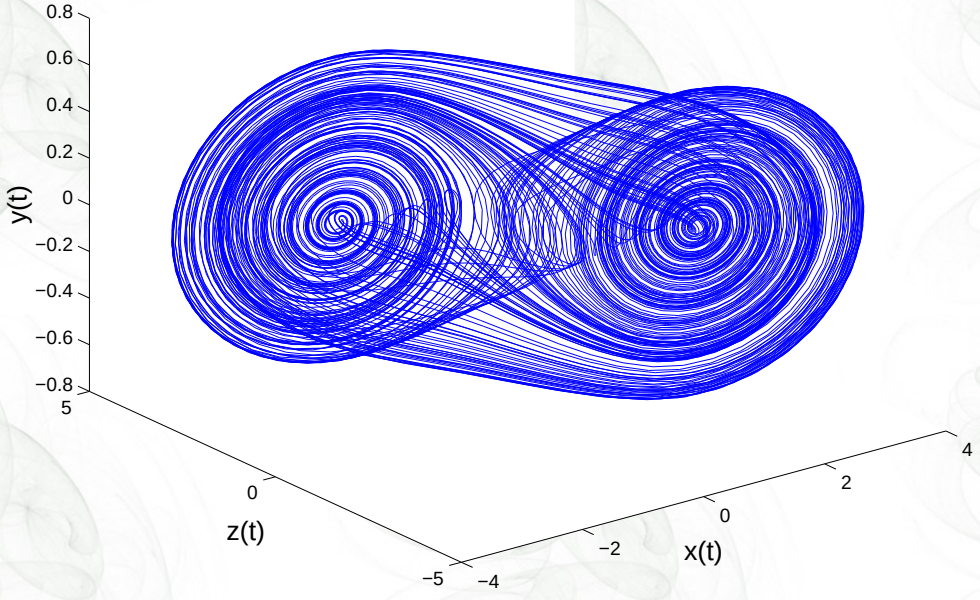


CIE, SZU
Shenzhen

11 Nov., 2005

The Chua system (dimensionless form)

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



CIE, SZU
Shenzhen

11 Nov., 2005

Discrete-Time Chaotic Maps: 1-D Case

- The logistic map:

$$f(x) = rx(1-x)$$

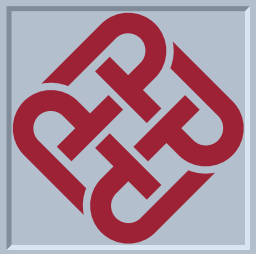
- Piecewise linear chaotic maps (PWLCM)
  - The tent map:

$$f(x) = \begin{cases} rx, & 0 \le x < 0.5 \\ r(1-x), & 0.5 \le x \le 1. \end{cases}$$

  - The skew tent map:

$$f(x) = \begin{cases} x/r, & 0 \le x < r \\ (1-x)/(1-r), & r \le x \le 1. \end{cases}$$

  - The sawtooth (shift) map: $f(x) = rx \bmod 1$ $(r > 1)$.



Discrete-Time Chaotic Maps: 2-D Case

- Hénon map: $f(x,y) = (1 - \alpha x^2 + \beta y, x)$.
- The Baker map:

$$f(x,y) = \left(2x \bmod 1, \frac{\lfloor 2x \rfloor + y}{2}\right)$$

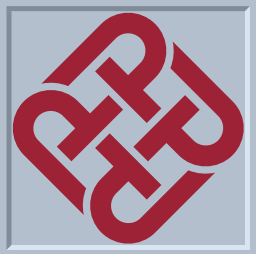
$$= \begin{cases} (2x, y/2), & 0 \le x < 1/2, \\ (2x-1, (y+1)/2), & 1/2 \le x \le 1. \end{cases}$$

- The Arnold Cat map:

$$f(x,y) = (x+y, x+2y) \bmod 1.$$

- The Standard map:

$$f(x,y) = (x+y, y - k\sin(x+y)) \bmod 2\pi.$$



CIE, SZU
Shenzhen

11 Nov., 2005

2 Chaos Synchronization

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 proper way.

- The driving signal may be a function of one or more variables of the driving system.
- The driving and the slave systems may have different structures and even different dimensions.
- Different types: *complete synchronization*, *lag synchronization*, *phase synchronization*, *projective synchronization*, *generalized synchronization*, *noise-induced synchronization*, ...

CIE, SZU
Shenzhen

11 Nov., 2005

Synchronization vs. Communication

- **Q1: What does synchronization mean?**
- **A1: It means that information on initial conditions can be transmitted to reach a remote site in safe. Of course, it is only true in an asymptotical sense.**
- **Q2: Does A1 mean communication?**
- **A2: Yes, it means chaos-based data communication though a noisy channel.**
- **Q3: Then, is it possible to realize secure communication?**
- **A2: Yes, it is possible ☺, but we should be very careful of various attacks ☠☠☠.**

CIE, SZU
Shenzhen

11 Nov., 2005

Chaos Synchronization: Continuous Case

Complete synchronization of two Lorenz systems [Pecora & Carroll, PRL 1990]: $x_2 \to x_1$, $y_2 \to y_1$, $z_2 \to z_1$.

$$\begin{cases} \dot{x}_1 = a(y_1 - x_1) \\ \dot{y}_1 = cx_1 - x_1 z_1 - y_1 \\ \dot{z}_1 = x_1 y_1 - b z_1 \end{cases} \xrightarrow{x_1 \text{ (or } y_1)} \begin{cases} \dot{x}_2 = a(y_2 - x_2) \\ \dot{y}_2 = cx_1 - x_1 z_2 - y_2 \\ \dot{z}_2 = x_1 y_2 - b z_2 \end{cases}$$

Projective synchronization of two Lorenz systems [Mainieri & Rehacek, PRL 1999]: $x_2 \to \alpha x_1$, $y_2 \to \alpha y_1$.

$$\begin{cases} \dot{x}_1 = a(y_1 - x_1) \\ \dot{y}_1 = cx_1 - x_1 z_1 - y_1 \\ \dot{z}_1 = x_1 y_1 - b z_1 \end{cases} \xrightarrow{z_1} \begin{cases} \dot{x}_2 = a(y_2 - x_2) \\ \dot{y}_2 = cx_2 - x_2 z_1 - y_2 \\ \dot{z}_2 = x_2 y_2 - b z_2 \ (z_2 = z_1) \end{cases}$$

CIE, SZU
Shenzhen

11 Nov., 2005

Chaos Synchronization: Continuous Case

Complete synchronization of two Rössler systems [Parlitz et al., PRE 1996]: $x_2 \to x_1$, $y_2 \to y_1$, $z_2 \to z_1$.

$$\begin{cases} \dot{x}_1 = -(y_1 + z_1) = -(x_1 + y_2) + s \\ \dot{y}_1 = x_1 + 0.45 y_1 \\ \dot{z}_1 = 2 + z_1(x_1 - 4) \end{cases}$$

$$\downarrow s = x_1 - z_1$$

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

Using APD (active-passive decomposition) technique, one can design even more complex driving signals, such as $s = x_1 y_1 - 3(y_1 + z_1)$ (see Table 1 in [Parlitz et al., PRE 1996]).

CIE, SZU
Shenzhen

11 Nov., 2005

Chaos Synchronization: Continuous Case

Phase synchronization of two bilaterally-coupled Rössler systems [M.G. Rosenblum et al., PRL 1996]: $\dot{\phi}_1 - \dot{\phi}_2 \to 0$ and $|\phi_1 - \phi_2| <$ constant, where $\phi_i = \arctan(y_i/x_i)$.

$$\begin{cases} \dot{x}_1 = -((1+\Delta\omega)y_1 + z_1) + C(x_2 - x_1) \\ \dot{y}_1 = (1+\Delta\omega)x_1 + 0.15y_1 \\ \dot{z}_1 = 0.2 + z_1(x_1 - 10) \end{cases}$$

$$x_1 \downarrow\uparrow x_2$$

$$\begin{cases} \dot{x}_2 = -((1-\Delta\omega)y_2 + z_2) + C(x_1 - x_2) \\ \dot{y}_2 = (1-\Delta\omega)x_2 + 0.15y_2 \\ \dot{z}_2 = 0.2 + z_2(x_2 - 10) \end{cases}$$

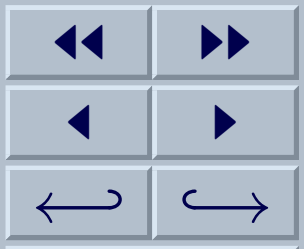
Chaos Synchronization: Continuous Case

Generalized synchronization of two Rössler systems [Rulkov et al., PRE 1995]: $x_2 \to x_1$, $y_2 \to y_1 + az_1 + bz_1^2$, $z_2 \to z_1$.

$$\begin{cases} \dot{x}_1 = -(y_1 + z_1) \\ \dot{y}_1 = x_1 + 0.2y_1 \\ \dot{z}_1 = 0.2 + z_1(x_1 - 5.7) \end{cases}$$

$$\downarrow x_1$$

$$\begin{cases} \dot{x}_2 = -(y_2 + (1-a)z_2 - bz_2^2) - g(x_2 - x_1) \\ \dot{y}_2 = x_2 + 0.2(y_2 - az_2 - bz_2^2) \\ \qquad\quad +(a + 2bz_2)(0.2 + z_2(x_2 - 5.7)) \\ \dot{z}_2 = 0.2 + z_2(x_2 - 5.7) \end{cases}$$



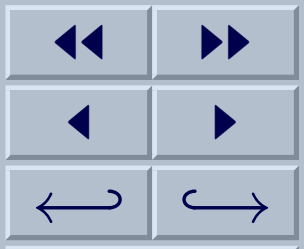
Chaos Synchronization: Continuous Case

Lag synchronization of two hyperchaotic Rössler systems [Chuandong Li et al., CSF 2005]: $y_{1,2,3,4}(t) \longrightarrow x_{1,2,3,4}(t-\tau)$.

$$\begin{cases} \dot{x}_1 = -x_2 - x_3 \\ \dot{x}_2 = x_1 - \alpha x_2 + x_4 \\ \dot{x}_3 = x_1 x_3 + \beta \\ \dot{x}_4 = -0.5 x_3 + 0.05 x_4 \end{cases}$$

$$\downarrow s(t) = x_1(t-\tau)x_3(t-\tau) + \sum_{i=1}^{4} k_i x_i(t-\tau)$$

$$\begin{cases} \dot{y}_1 = -y_2 - y_3 \\ \dot{y}_2 = y_1 - \alpha y_2 + y_4 \\ \dot{y}_3 = y_1 y_3 + \beta + \left(s(t) - \sum_{i=1}^{4} k_i y_i \right) \\ \dot{y}_4 = -0.5 y_3 + 0.05 y_4 \end{cases}$$



Chaos Synchronization: Discrete-Time Case

Impulsive complete synchronization of two Chua's systems [Yang, IJCC 2004]: $x_2 \to x_1$, $y_2 \to y_1$, $z_2 \to z_1$.

$$\begin{cases} \dot{x}_1 = p(-x_1 + y_1 - f(x_1)) \\ \dot{y}_1 = x_1 - y_1 + z_1 \\ \dot{z}_1 = -qy_1 - rz_1 \end{cases}$$

$$\downarrow \{x_1(t_i), y_1(t_i), z_1(t_i)\}$$

$$\begin{cases} \dot{x}_2 = p(-x_2 + y_2 - f(x_2)), & t \neq t_i \\ \dot{y}_2 = x_2 - y_2 + z_2, & t \neq t_i \\ \dot{z}_2 = -qy_2 - rz_2, & t \neq t_i \\ \begin{bmatrix} \Delta x_2 \\ \Delta y_2 \\ \Delta z_2 \end{bmatrix} = -\mathbf{B} \begin{bmatrix} x_1 - x_2 \\ y_1 - y_2 \\ z_1 - z_2 \end{bmatrix}, & t = t_i \end{cases}$$

Chaos Synchronization: Discrete-Time Case

Complete synchronization of two Hénon maps [Feki et al., CSF 2003] ($m(k)$ is an external signal): $x_2 \to x_1$, $y_2 \to y_1$.

$$\begin{cases} x_1(k+1) = 1 - \alpha \left(s(k) - \left\lfloor \frac{s(k)+P}{2P} \right\rfloor 2P \right)^2 + y_1(k) \\ y_1(k+1) = \beta x_1(k) + 0.05 x_1(k)(m(k)-1) \end{cases}$$

$$\downarrow s(k) = x_1(k) m(k)$$

$$\begin{cases} x_2(k+1) = 1 - \alpha \left(s(k) - \left\lfloor \frac{s(k)+P}{2P} \right\rfloor 2P \right)^2 + y_2(k) \\ y_2(k+1) = \beta x_2(k) + 0.05(s(k) - x_2(k)) \end{cases}$$

CIE, SZU
Shenzhen

11 Nov., 2005

Chaos Synchronization: Discrete-Time Case

Noise-induced complete synchronization of two intermittently-chaotic maps via a common random driving signal [Minai & Pandian, PRE/Chaos 1998]: $|x_2 - x_1| \to 0$.

$$u(k) \in \{A, B\} \rightrightarrows \begin{cases} x_1(k+1) = F(x_1(k), u(k)), \\ x_2(k+1) = F(x_2(k), u(k)), \end{cases}$$

where $F(x, u(k)) = \tanh(\mu(ax + u(k))) - \tanh(\mu bx)$.

CIE, SZU
Shenzhen

11 Nov., 2005

A Classification

- Chaotic Masking
- Chaotic Switching (Chaotic Shifting Key = CSK)
- Chaotic Modulation
- Chaotic Inverse System
- Chaos Control

★ Hyperchaos (including Time-Delay Chaos)

★ Chaos + Encryption (Yang's 3rd Generation)

★ Impulsive Synchronization (Yang's 4th Generation)

★ Projective Synchronization

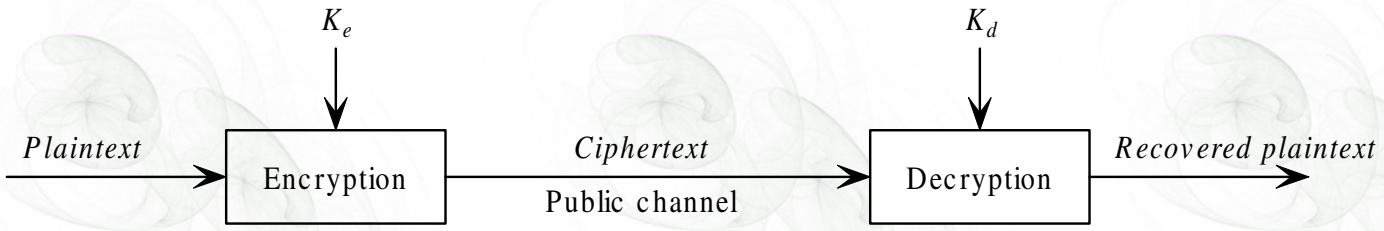
★ Re-Modulation

CIE, SZU
Shenzhen

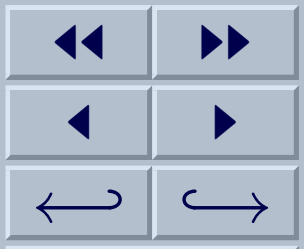
11 Nov., 2005

3 Cryptology

- Cryptography = how to design ciphers, secure protocols and systems
- Cryptanalysis = how to break ciphers, secure protocols and systems



- Ciphertext-only attack
- Known-plaintext attack
- Chose-plaintext attack
- Chosen-ciphertext attack



4 Chaotic Masking

Assume that the plaintext signal is $m(t)$, the transmitted ciphertext signal is $s(t)$, and the recovered plaintext signal is $\tilde{m}(t)$.

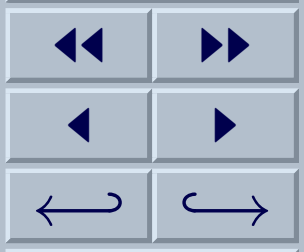
$$\begin{cases} \dot{x}_1 = a(y_1 - x_1) \\ \dot{y}_1 = cx_1 - x_1 z_1 - y_1 \\ \dot{z}_1 = x_1 y_1 - bz_1 \end{cases}$$

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

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

$$\Downarrow$$

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

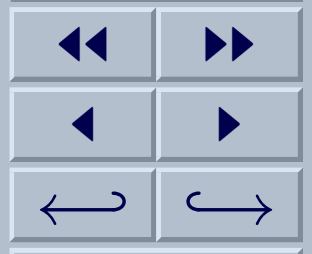


CIE, SZU
Shenzhen

11 Nov., 2005

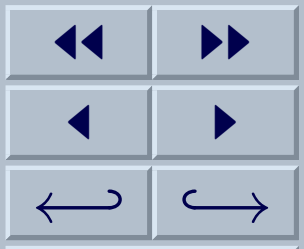
Advantages

- The encryption structure is very simple.
- The plaintext signal is independent of the sender system.
- The plaintext can be either analog or digital.
- Any more advantages?



Disadvantages

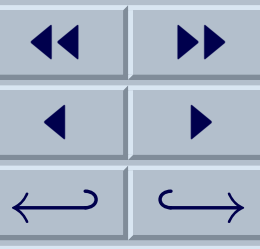
- The amplitude of the plaintext signal has to be much smaller than the carrier signal.
- The plaintext signal cannot be exactly recovered, due to two reasons:
  - the plaintext signal perturbs the synchronization at all times;
  - even without the perturbation of $m(t)$, the synchronization error approaches to zero as $t \to \infty$.
- The plaintext signal has to be band limited to the spectrum of the carrier signal.



Disadvantages: Security Problems

- A tradeoff exits between the robustness and the sensitivity to parameter mismatch (i.e., the security against the brute-force attack).
- It is essentially (structurally) insecure against many kinds of attacks, such as Short's NLD forecasting attack, filtering attack, return-map attack, etc.

My opinion: pessimistic.



5 Chaotic Switching (Chaotic Shift Keying – CSK)

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

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

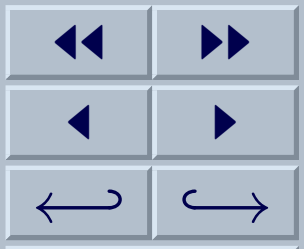
$$\begin{cases} \dot{x}_2 = a^{(0)}(y_2 - x_2) \\ \dot{y}_2 = c^{(0)}s(t) - s(t)z_2 - y_2 \\ \dot{z}_2 = s(t)y_2 - b^{(0)}z_2 \end{cases}$$

$$\Downarrow$$

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

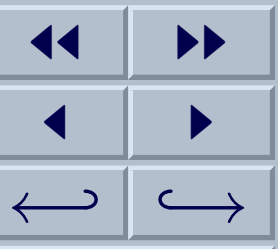
Features and Advantages

- Only binary signal can be used as the plaintext, i.e., $m(t) \in \{0,1\}$.
- The plaintext signal can be exactly recovered (better than chaotic masking).
- The plaintext signal is independent of the sender systems.
- It is robust to channel noise (better than chaotic masking).
- It is possible to use two completely different sender systems.



Disadvantages

- The bit rate of the plaintext is relatively low.
- The sender part is more (double) complex than that in chaotic masking scheme.
- A tradeoff exits between the robustness and the sensitivity to parameter mismatch (i.e., the security against the brute-force attack).
- It is also insecure against many kinds of attacks, such as return-map attack, GS-based attack, power energy attack, short-time period attack, etc.

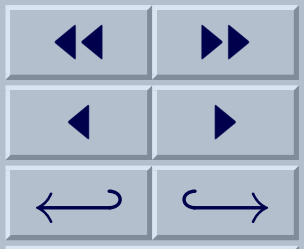


Some Improved CSK Schemes

Differential CSK (DCSK) [Parlitz & Ergezinger, PLA 1994]

- Replace the two analog chaotic systems with a discrete-time logistic map $x(n+1) = 1 - a(x(n))^2$, where $a \approx 2$.
- For the plaintext signal $m(k) \in \{-1, 1\}$, the transmitted ciphertext signal is $s(n) = m\left(\left\lfloor \frac{n}{N} \right\rfloor\right) x(n)$.
- The recovery of the plaintext signal is achieved via correlation detection:

$$m'(k) = \text{sign}\left(\sum_{n=(k-1)N+1}^{kN} s(n)x'(n) \right).$$

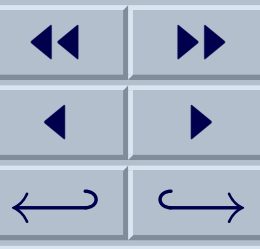


CIE, SZU
Shenzhen

11 Nov., 2005

DCSK: Advantages and Disadvantages

- Different from CSK, DCSK is actually a digital system robust to channel noises, without using chaos synchronization. The synchronization between the sender and the receiver systems are achieved by sharing the same initial condition and control parameter.
- It is insecure against a return-map attack and a correlation attack [Zhou & Chen, PLA 1997].
- Actually, it is a digital CDMA communication system, not a secure communication system.

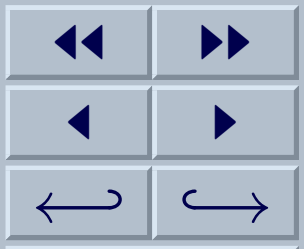


Multiple-Step CSK with Alternative Driving (MS-CSK) [Palaniyandi & Lakshmanan, IJBC 2001]

- **Multiple-Step Modulation (Switching)**: using $2n$ different chaotic systems to enhance the security.
- **Alternative Driving**: using $x_1^{(0,1)}$ and $y_1^{(0,1)}$ alternatively to replace the single driving variables.

* The two countermeasures were proposed to resist the return-map attack.

$$m(t) \rightarrow \begin{cases} CS_1^{(0)} \\ \vdots \\ CS_n^{(0)} \\ CS_1^{(1)} \\ \vdots \\ CS_n^{(1)} \end{cases} \rightarrow s(t) \longrightarrow \begin{cases} CS_{1,x}^{(0)} \\ \vdots \\ CS_{n,x}^{(0)} \\ CS_{1,y}^{(0)} \\ \vdots \\ CS_{n,y}^{(0)} \end{cases} \rightarrow \tilde{m}(t) \approx m(t)$$



CIE, SZU
Shenzhen

11 Nov., 2005

Problems of MS-CSK [Shujun Li et al., 2004]

- To resist the brute-force attack with a complexity 2^{100}, $n \geq 50$, which is too large for a practical cryptosystem.
- It is insecure against known/chosen-plaintext attacks based on return map cryptanalysis. The average number of required known/chosen plain-bits is only $3n$.
- It is easy to detect the switching times between the two driving modes, then it is possible to separately break the two sub-systems with the return-map attack.

Pseudo-Random False Switching [Xu & Chee, IJBC 2004]

- One system parameter is switched by the plaintext signal, and another system parameter is dynamically switched according to the values of one or more state variables (false switching events).
- The bit rate of the plaintext is even (much?) lower, since (much?) more transient time is needed for the receiver system to achieve synchronization with the sender system.
- Security (still under study): It seems secure against all known attacks. Another merit is the key space is much larger than other CSK schemes. The sensitivity to parameter mismatch is not clear at present.

6 Chaotic Modulation

Chaotic Parameter Modulation $\supset$ CSK

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

$$\downarrow x_1$$

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

$$\Downarrow$$

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

CIE, SZU
Shenzhen

11 Nov., 2005

Chaotic Direct (Non-Autonomous) Modulation

Example 1 : A Simple Case (Chua's) [Wu & Chua, IJBC 1993]

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

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

$$\begin{cases} \dot{x}_2 = \frac{1}{C_1}(G(-x_2 + y_2) - f(s(t))) \\ \dot{y}_2 = \frac{1}{C_2}(G(x_2 - y_2) + z_2) \\ \dot{z}_2 = \frac{1}{L}(-y_2 - R_0 z_2) \end{cases}$$

$$\Downarrow$$

$$\tilde{m}(t) = s(t) - x_1(t) \rightsquigarrow m(t)$$

CIE, SZU
Shenzhen

11 Nov., 2005

Chaotic Direct (Non-Autonomous) Modulation

Example 2: The APD Case (Rössler) [Parlitz et al., PRE 1996]

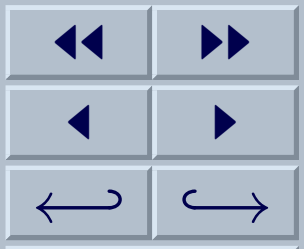
$$\begin{cases} \dot{x}_1 = -(y_1 + z_1) = -(x_1 + y_1) + s \\ \dot{y}_1 = x_1 + 0.45 y_1 \\ \dot{z}_1 = 2 + z_1(x_1 - 4) + m(t) \end{cases}$$

$$\downarrow s = x_1 - z_1$$

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

$$\Downarrow$$

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



CIE, SZU
Shenzhen

11 Nov., 2005

Chaotic-Masking-Like "Chaotic Modulation"

Some researchers call the following enhanced chaotic masking scheme *chaotic modulation*, due to the multiplication between the plaintext signal and the carrier signal.

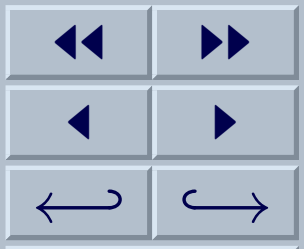
$$\begin{cases} \dot{x}_1 = a(y_1 - x_1) \\ \dot{y}_1 = cx_1 - x_1 z_1 - y_1 \\ \dot{z}_1 = x_1 y_1 - b z_1 \end{cases}$$

$$\downarrow s(t) = x_1(t)(1 + \varepsilon m(t))$$

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

$$\Downarrow$$

When $x_2(t) \neq 0$, $\tilde{m}(t) = \frac{s(t)/x_2(t) - 1}{\varepsilon} \rightsquigarrow m(t)$

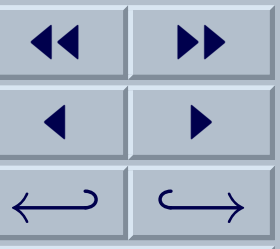


CIE, SZU
Shenzhen

11 Nov., 2005

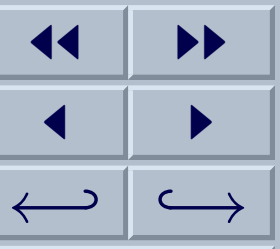
Features

- Both binary and analog plaintext signals can be transmitted.
- The bit rate of transmission can be (not much) higher than that of CSK.
- The plaintext signal influences the evolution of the chaotic systems, so the recovery of the plaintext signal has to be achieved via an adaptive controller, which is different for different chaotic systems and modulated parameters.
- It is possible to transmit multiple plaintext signals by modulating multiple parameter simultaneously, though the recovery accuracy will be compromised.

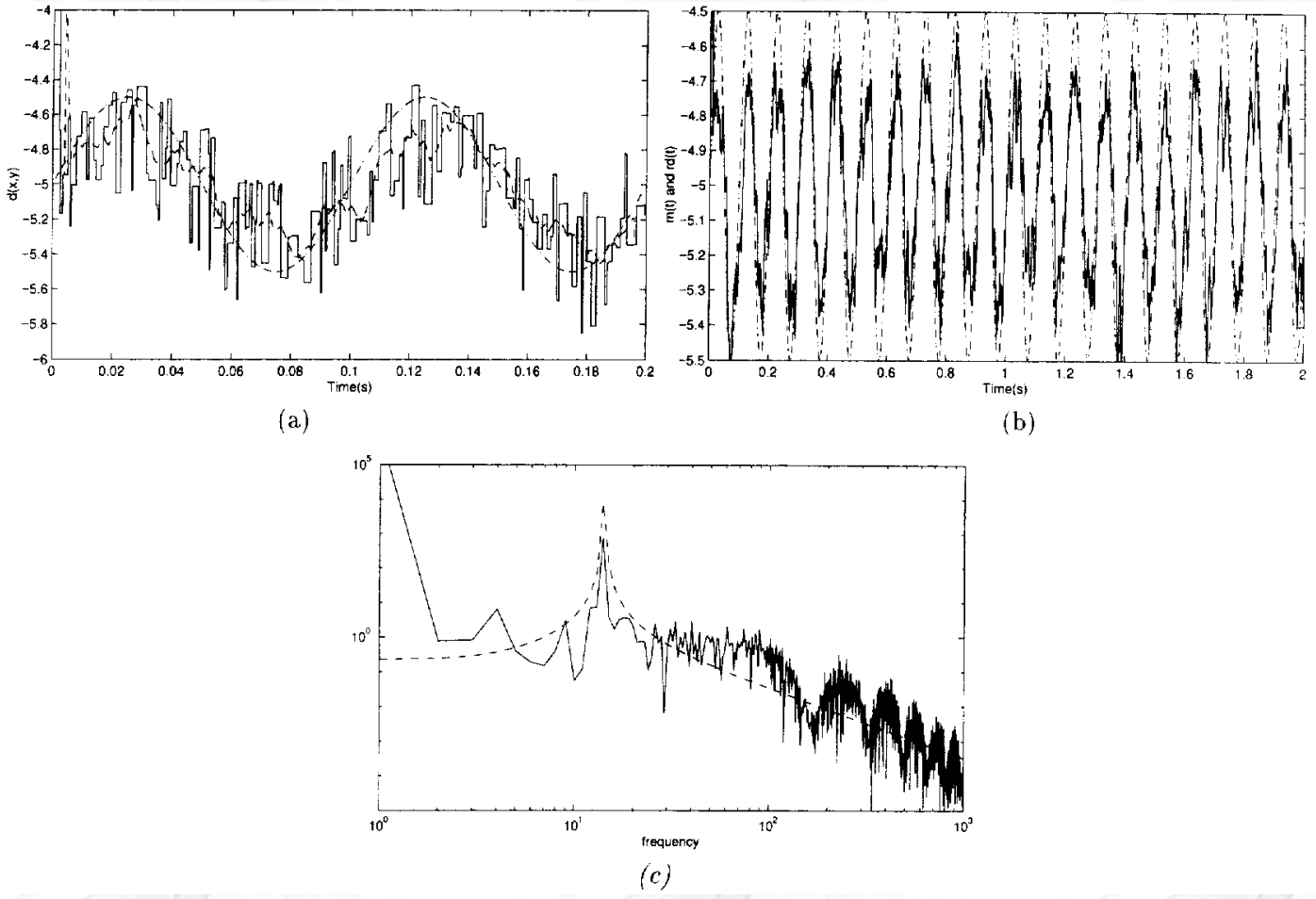


Security

- A tradeoff exits between the robustness and the sensitivity to parameter mismatch (i.e., the security against the brute-force attack).
- Many chaotic modulation schemes have been found insecure [K.M. Short, IJBC 1996; Tao Yang et al., PhysicaD/PLA, 1998], via different attacks.



A typical attack was demonstrated in [Tao Yang et al., PLA 245(1998):495-510] by using fuzzy return maps.



CIE, SZU
Shenzhen

11 Nov., 2005

7 Inverse System Approach [U. Feldmann et al., IJCTA 1996]

- It is an incorporated approach of designing synchronization and encryption.
- It has a good correspondence to the basic principle of symmetry encryption in cryptology: $C = E(P, K)$ and $P = D(C, K)$, where $E(\cdot, \cdot)$ and $D(\cdot, \cdot)$ are realized with chaotic systems.
- However, it cannot be considered as a concrete encryption structure, like chaotic masking, CSK and chaotic modulation.
- Most chaotic cryptosystems designed via inverse system approach are not sufficiently secure against known/chosen-plaintext attacks, since the encryption structure is too simple.

CIE, SZU
Shenzhen

11 Nov., 2005

8 Chaos Control

Chaos control techniques can be used to target a chaotic trajectory to represent a symbolic sequence, i.e., to transmit a bit sequence for digital communications.

- Q: What about to generalize this idea for secure communications?
- A: It is insecure to direct use it for secure communication, especially under the known/chosen-plaintext attacks.
- Q: Is it possible to combine this method with other scheme to design securer chaotic cryptosystems?
- A: Yes, it is possible. A scheme has been proposed very recently in [Chien & Liao, CSF 24(2005):241-255]. The security is still under study.

CIE, SZU
Shenzhen

11 Nov., 2005

9 Attacks

A. Direct Extraction of the Plaintext

B. Estimation of the Carrier Signal

C. Parameter Identification

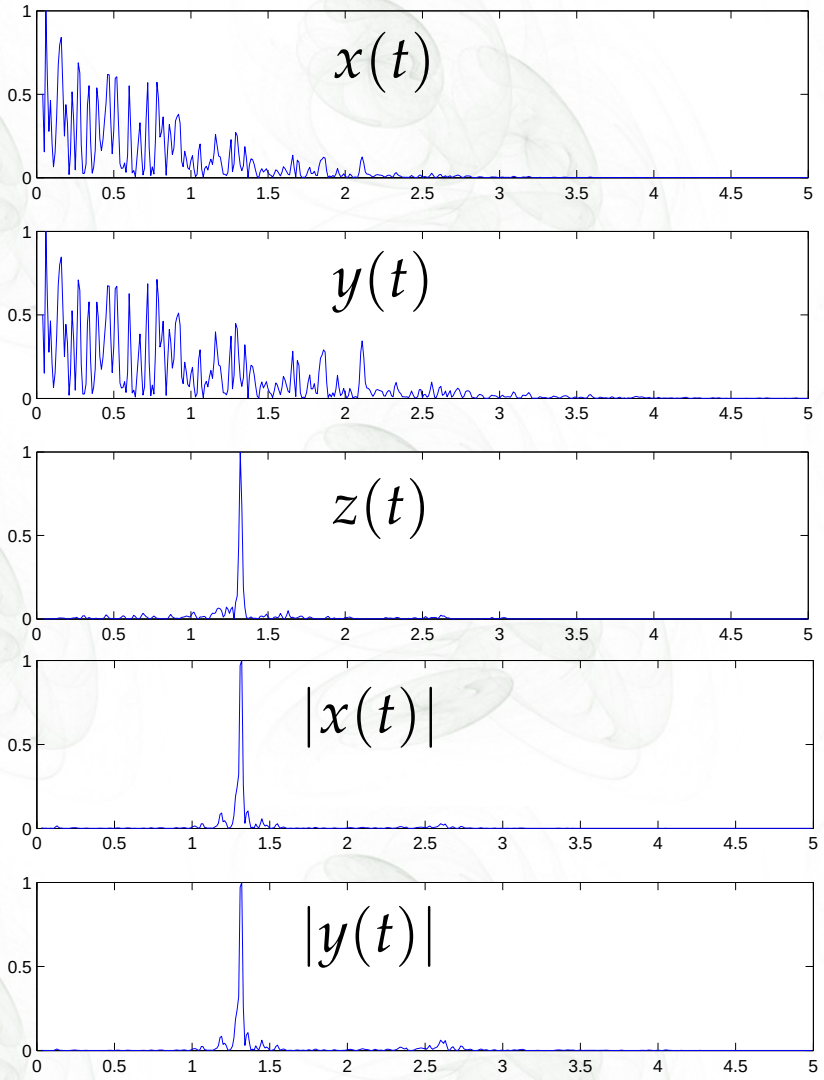
D. More Powerful Cryptographical Attacks...

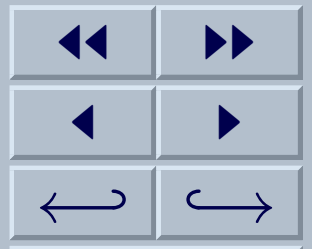
A. Direct Extraction of the Plaintext

A.1. Power Spectral (Filtering) Analysis

- Q: Does a chaotic system really have wide-band power spectra?
- A: Continuous chaos $\neq$ white noise $\Rightarrow$ the power spectra of many 3-D chaotic systems are much simpler (i.e., worse) than expected.
- Q: Does this mean that chaotic masking and (simple) CSK schemes always have limited applications?
- A: Yes (in my opinion).

A typical example: power spectra of the Lorenz system.

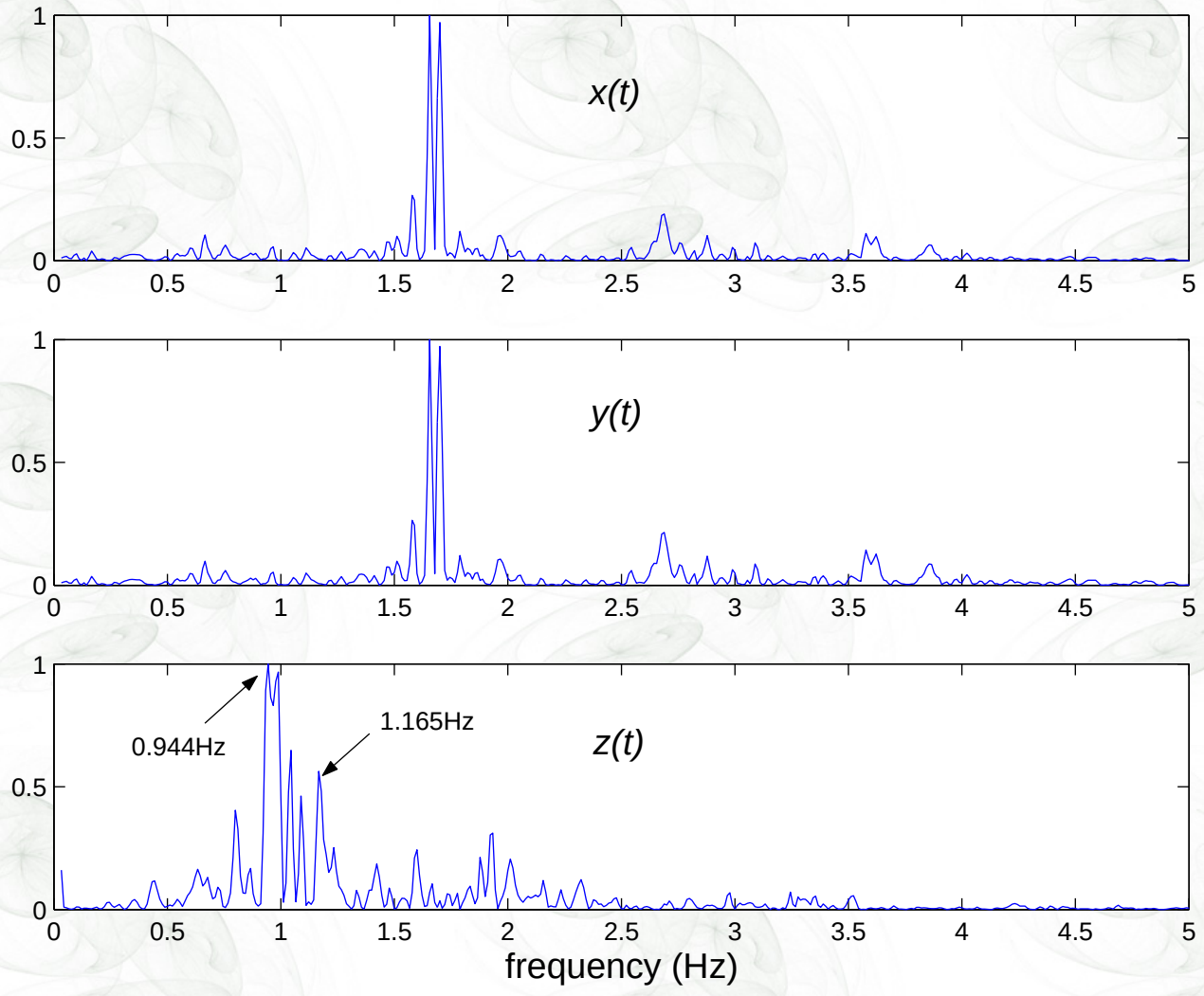




CIE, SZU
Shenzhen

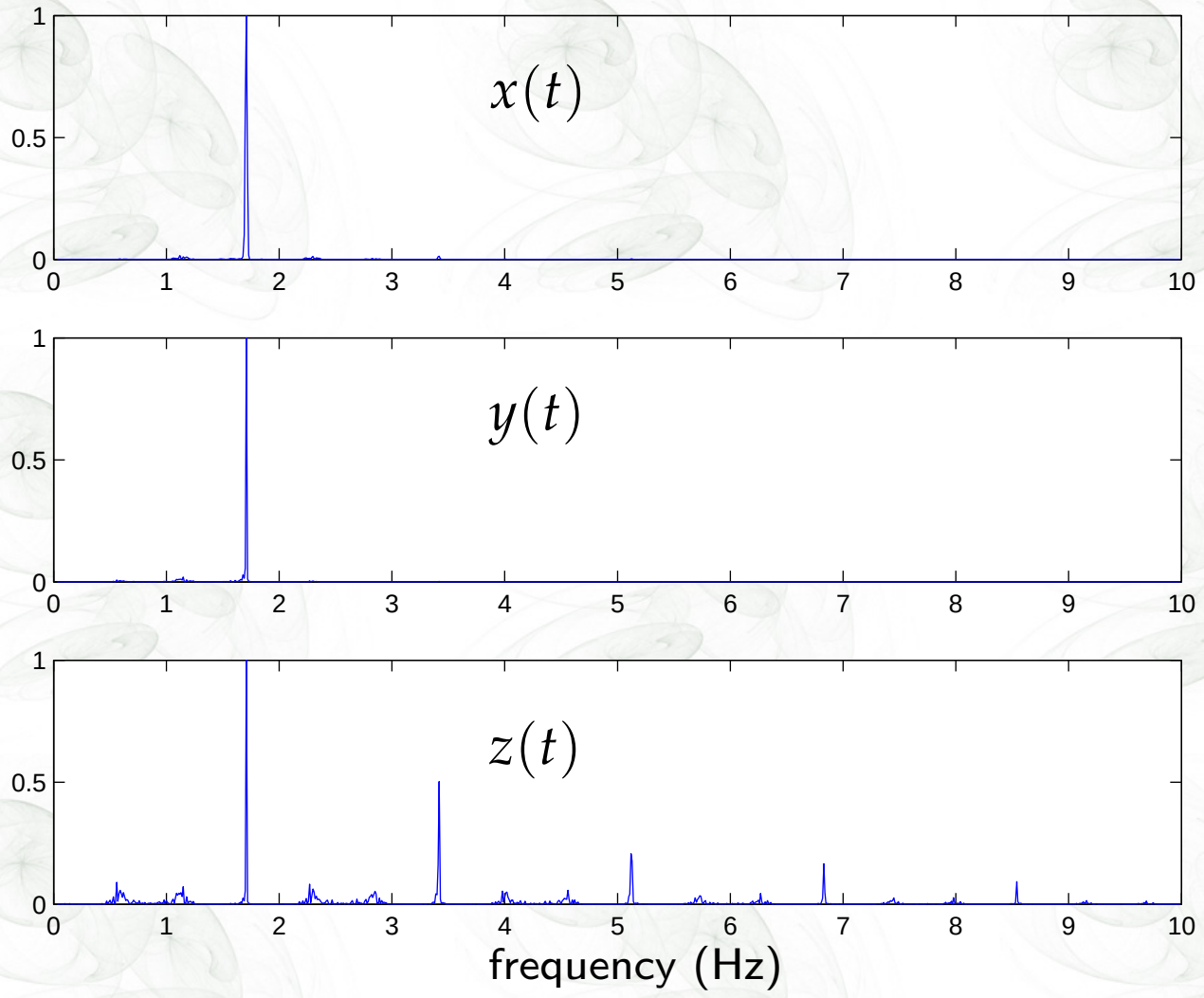
11 Nov., 2005

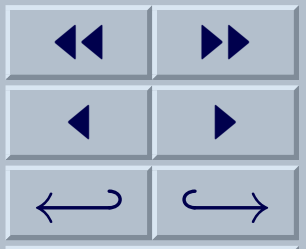
Yet another example: power spectra of the Chen system.



CIE, SZU
Shenzhen
11 Nov., 2005

The third example: power spectra of the Rössler system.





CIE, SZU
Shenzhen

11 Nov., 2005

A real attack to a chaotic masking system based on the Lorenz system.

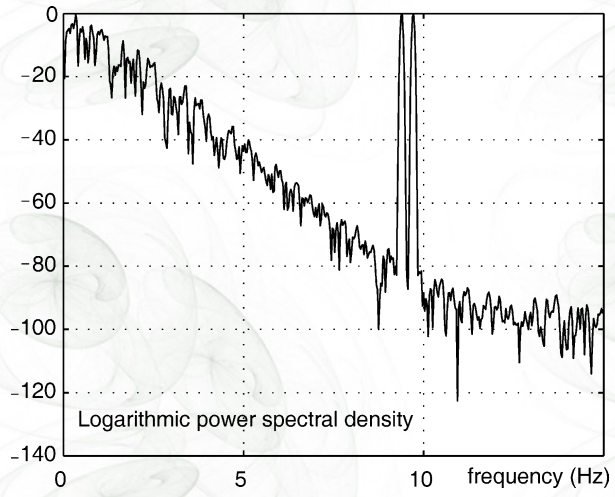


Fig. 1. Power spectral density analysis of the ciphertext signal. The peaks at $59/2\pi$ Hz and at $61/2\pi$ Hz correspond to the plaintext frequency. The spectrum was calculated using a 4096-point Discrete Fourier Transform with a 4-term Blackman–Harris window.

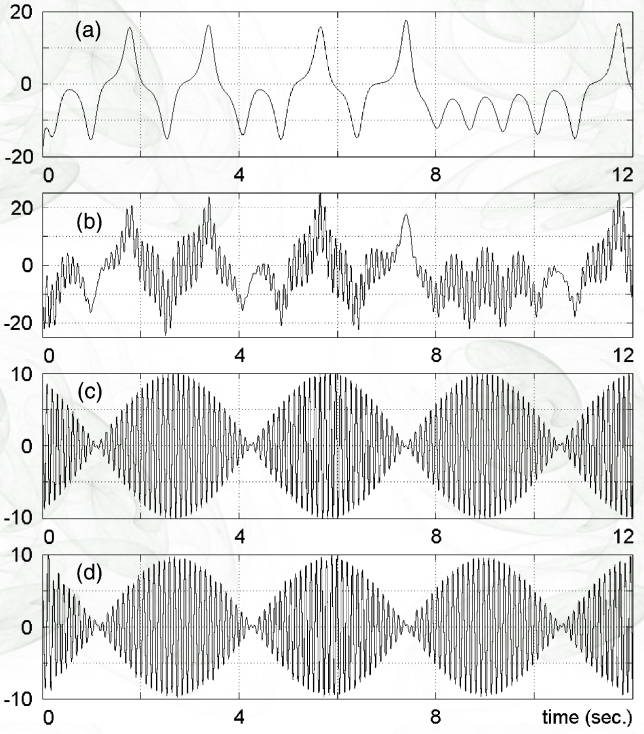
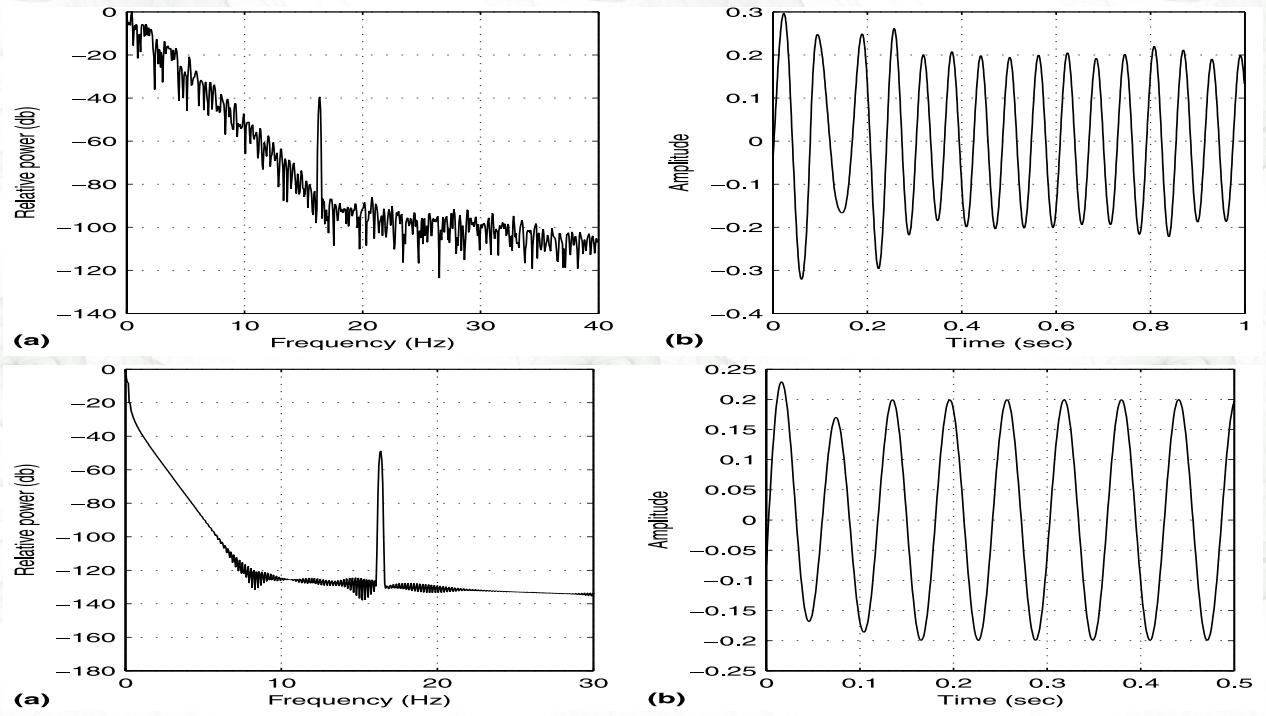


Fig. 2. Plaintext recovery with ciphertext filtering attack. The high-pass filter employed was a four-pole Butterworth with a frequency cutoff of 33 rad/s. Time histories of: (a) x component of the Lorenz chaotic attractor; (b) the ciphertext, $s(t)$; (c) the plaintext, $i(t) = 10\cos(60t)\cos(t)$; (d) the recovered plaintext with a high-pass filter.

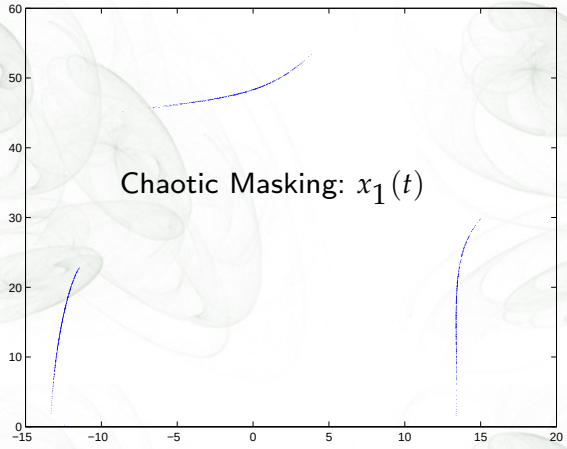
Gonzalo Álvarez and Shujun Li, "Breaking network security based on synchronized chaos," *Computer Communications*, 27(16):1679-1681, 2004

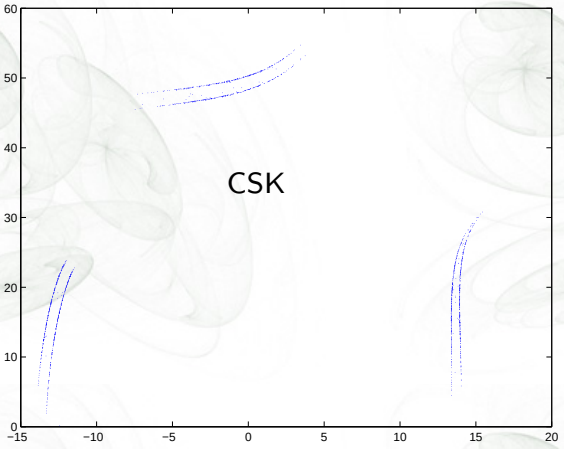
Yet another real attack to two chaotic masking systems based on the Lorenz system and the hyperchaotic Rössler systems.

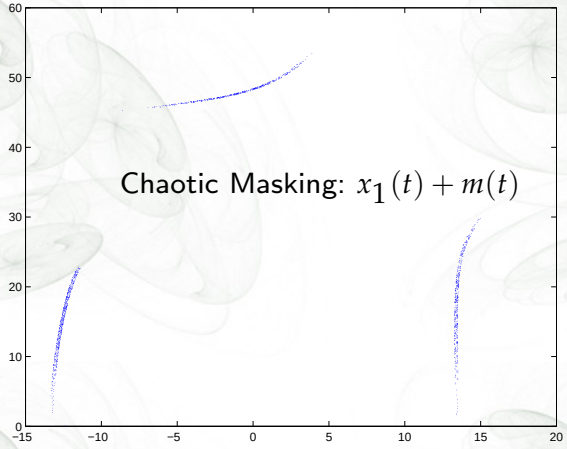


Gonzalo Álvarez, Shujun Li, et al., "Breaking projective chaos synchronization secure communication using filtering and generalized synchronization," *Chaos, Solitons & Fractals*, vol. 24, no. 3, pp. 775-783, 2005

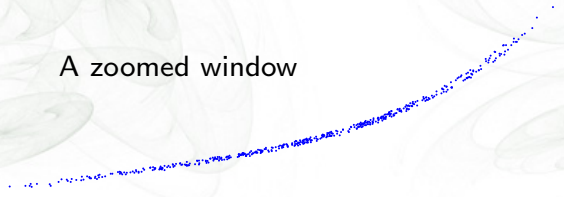
A.2. Return-Map Analysis





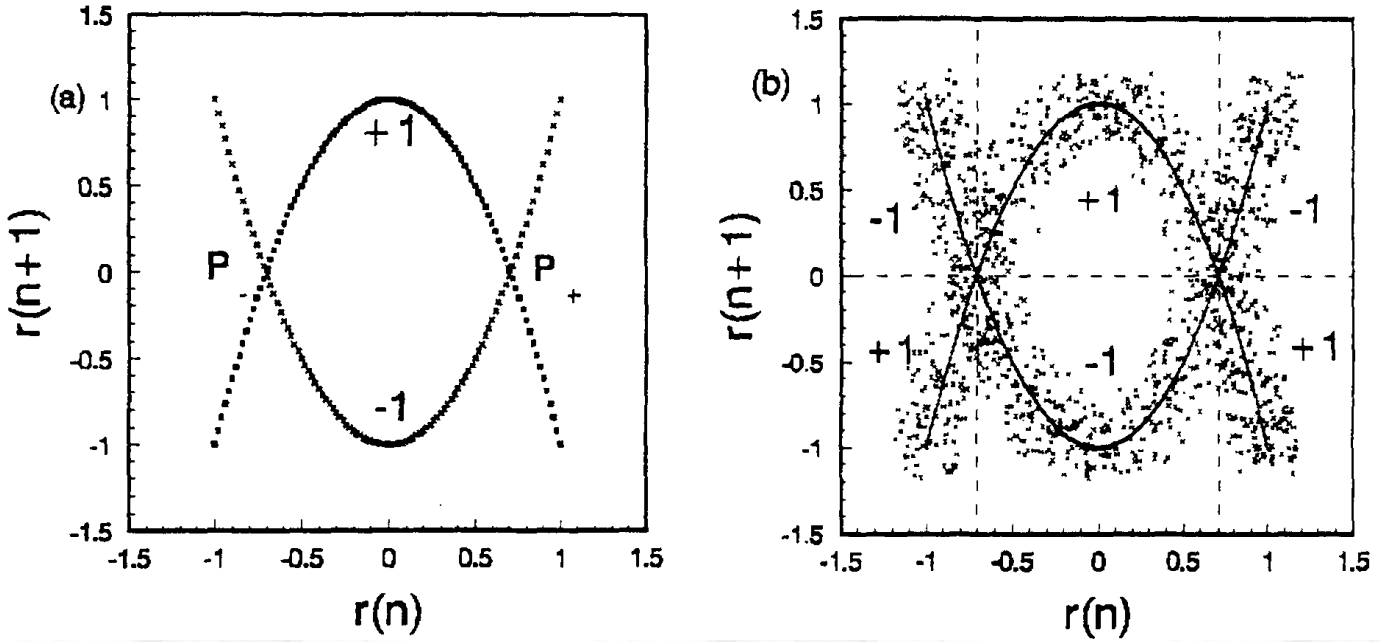


A zoomed window



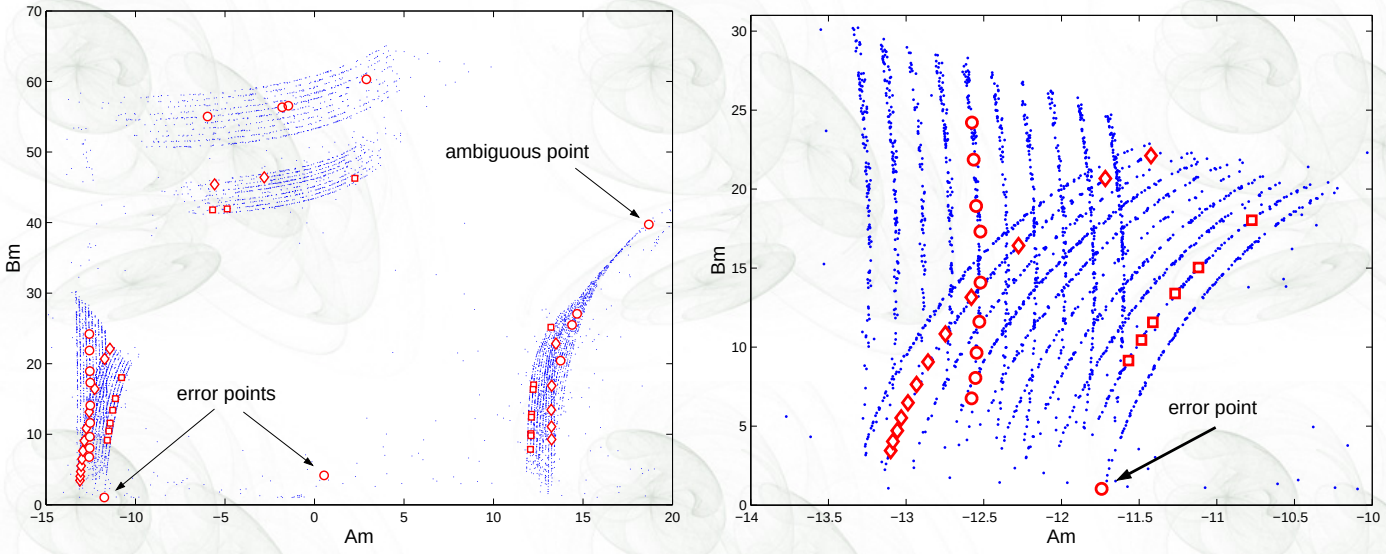
Shujun Li et al., "Breaking a chaos-based secure communication scheme designed by an improved modulation method," *Chaos, Solitons & Fractals*, vol. 25, no. 1, pp. 109-120, 2005

A.2. Return-Map Analysis: DCSK



Chang-song Zhou & Tian-lun Chen, "Extracting information masked by chaos and contaminated with noise - Some considerations on the security of communication approaches using chaos," *Physics Letters A*, 234(6):429-435, 1997

A.2. Return-Map Analysis: MS-CSK



Shujun Li et al., "Return-Map Cryptanalysis Revisited," submitted to *IJBC*, 2004

A.3. Power Energy Analysis

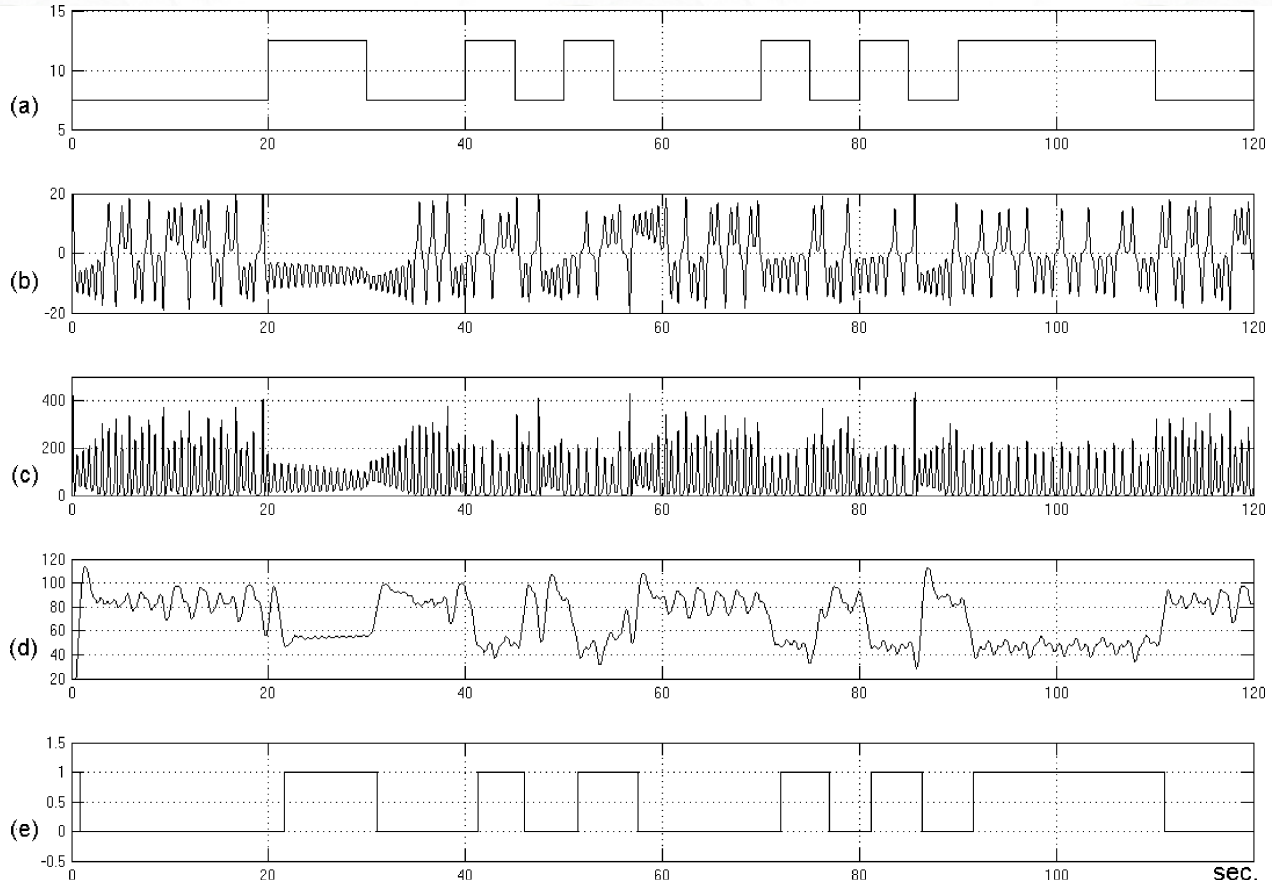
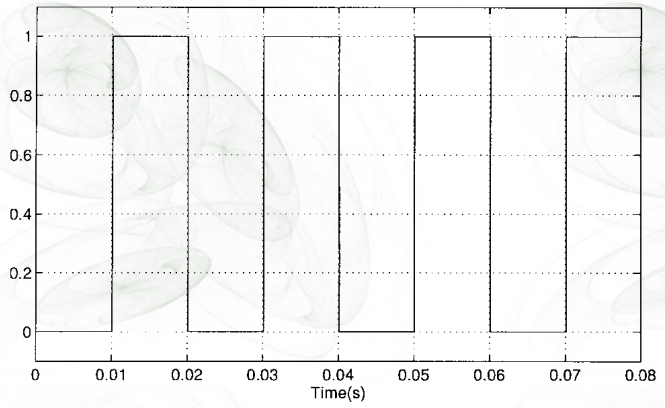


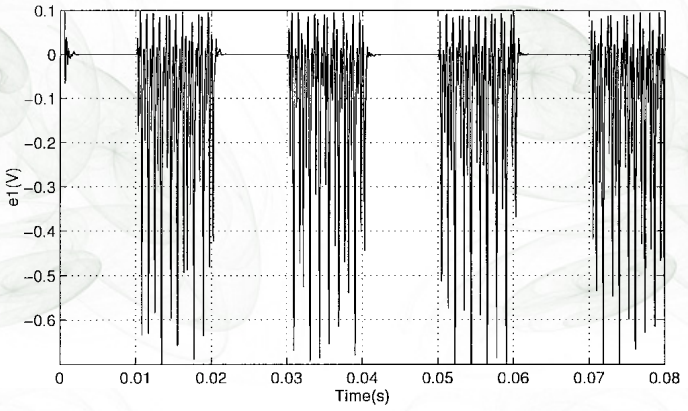
Fig. 2. Power signal attack: (a) plaintext; (b) ciphertext, x_1; (c) squared ciphertext signal, x_1^2; (d) low-pass filtered squared ciphertext signal; (e) recovered plaintext.

Gonzalo Álvarez et al., "Breaking parameter modulated chaotic secure communication system," *Chaos, Solitons & Fractals*, 21(4):783-787, 2004

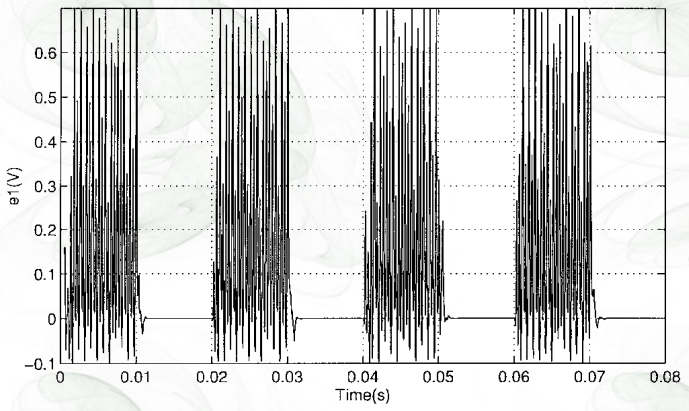
A.4. GS (Generalized Synchronization)



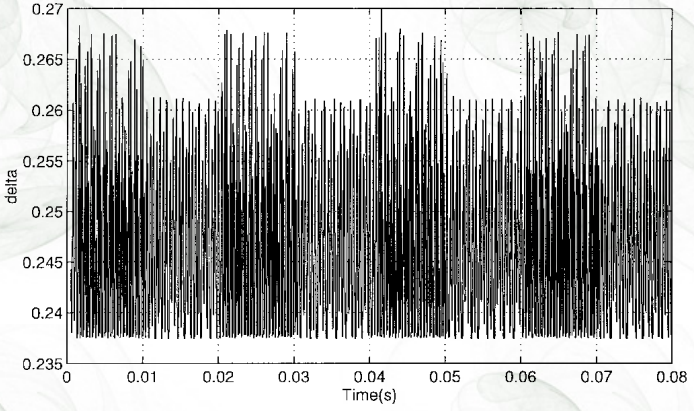
(a)



(b)

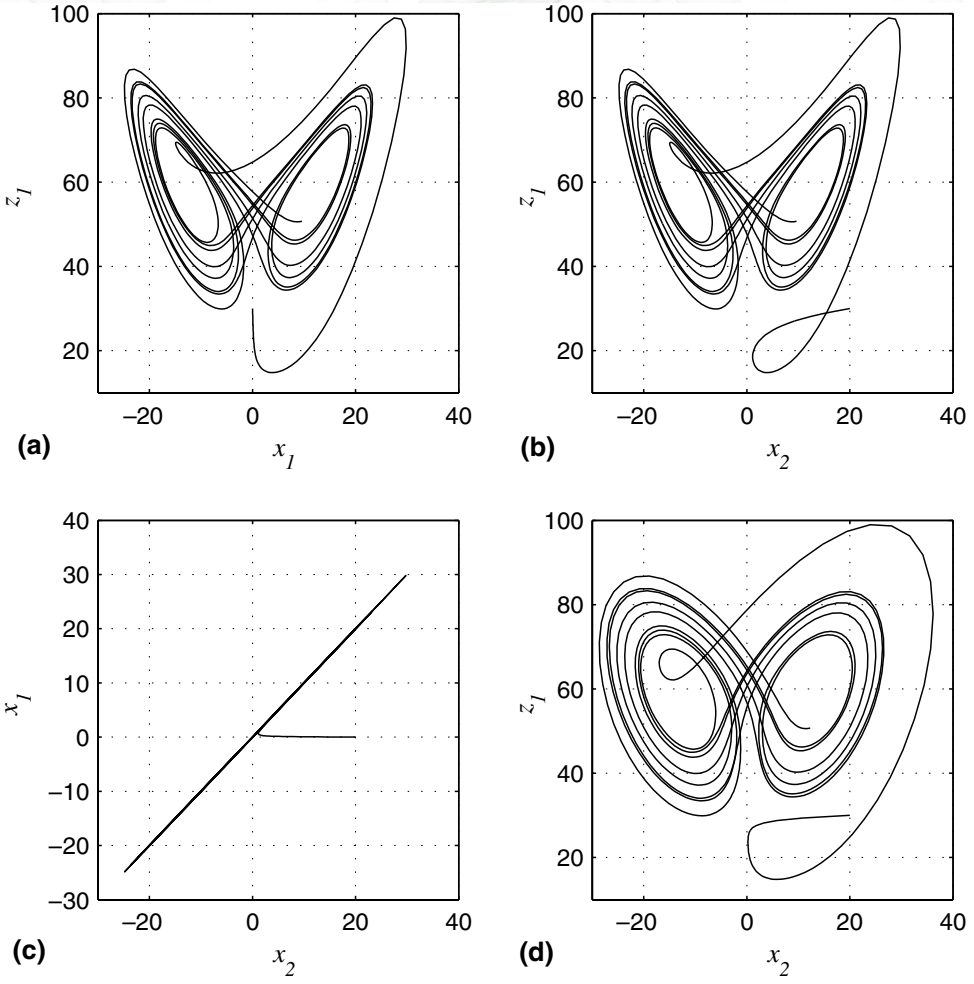


(c)



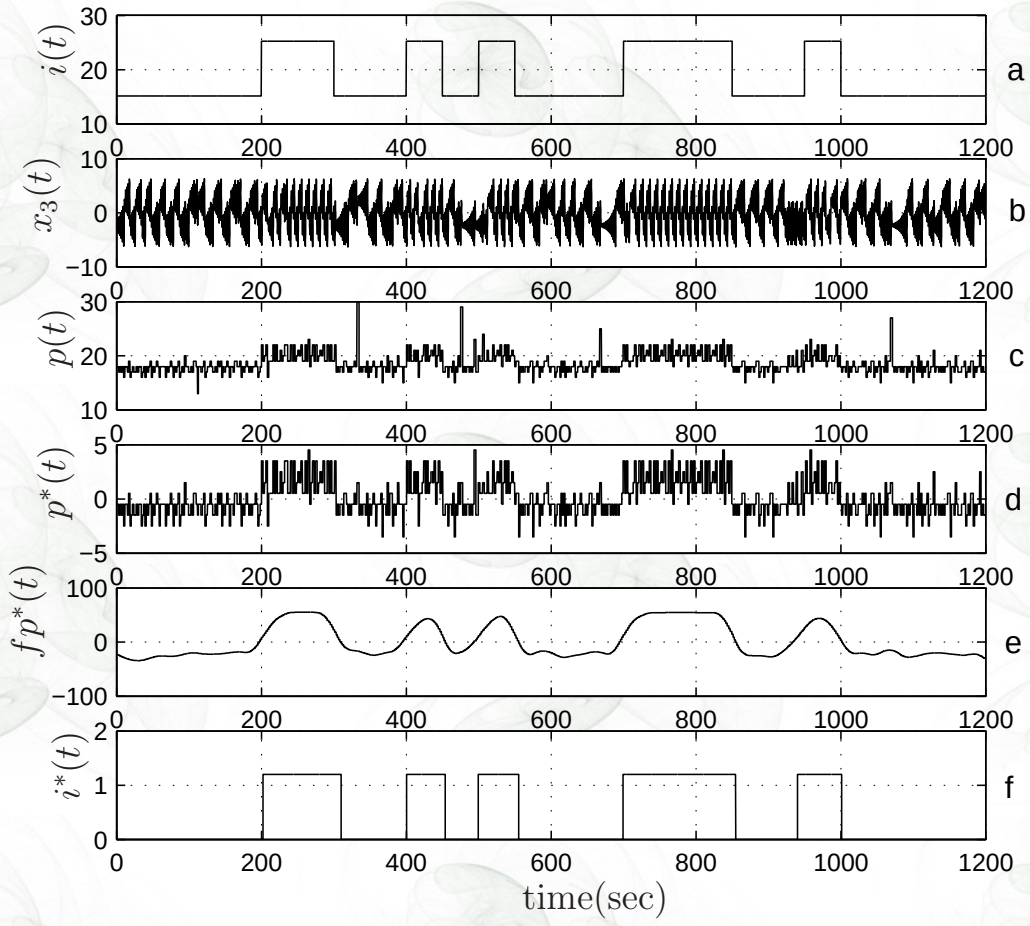
(d)

Tao Yang et al., "Breaking Chaotic Switching Using Generalized Synchronization: Examples," *IEEE Trans. CAS-I*, 45(10):1062-1067, 1998



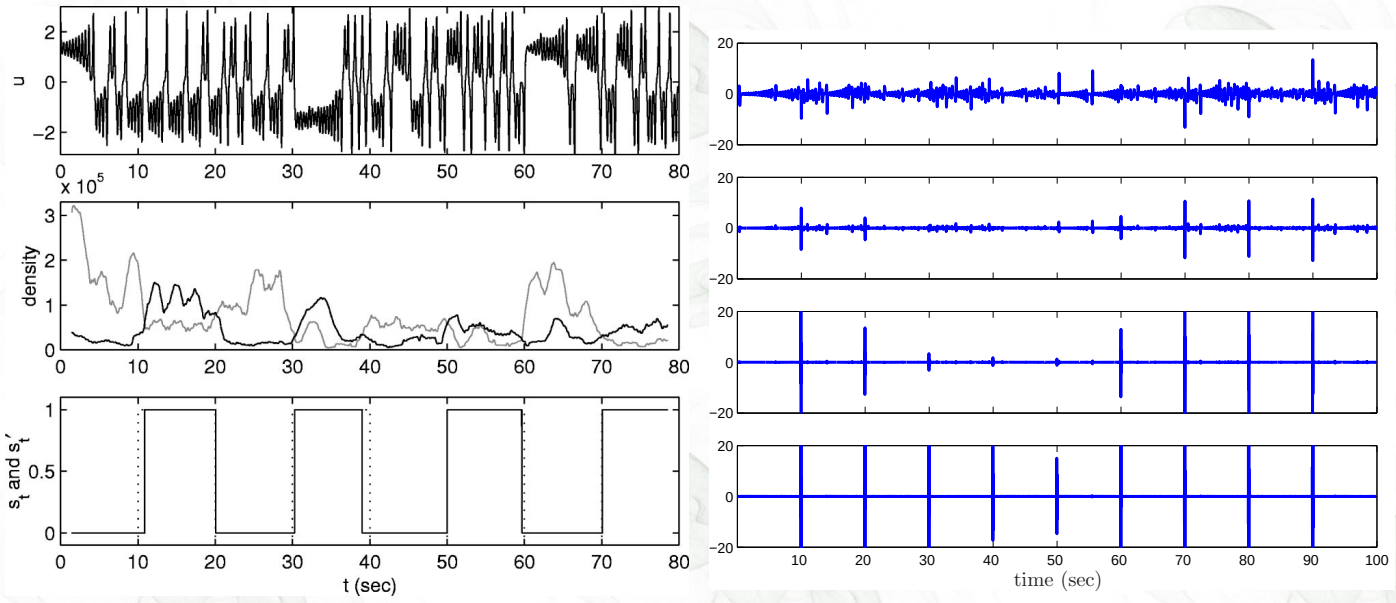
Gonzalo Álvarez, Shujun Li, et al., "Breaking projective chaos synchronization secure communication using filtering and generalized synchronization," *Chaos, Solitons & Fractals*, vol. 24, no. 3, pp. 775-783, 2005

A.5. Short-Time Period (STZCR [T. Yang, 1995])



Gonzalo Álvarez & Shujun Li, "Estimating short-time period to break different types of chaotic modulation based secure communications," arXiv:nlin.CD/0406039, 2004

A.6. Switching Detection

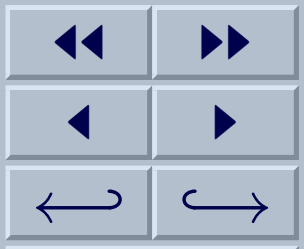


[1] Christian Storm & Walter J. Freeman, "Detection and classification of nonlinear dynamic switching events," *Physical Review E*, 66(5):057202, 2002

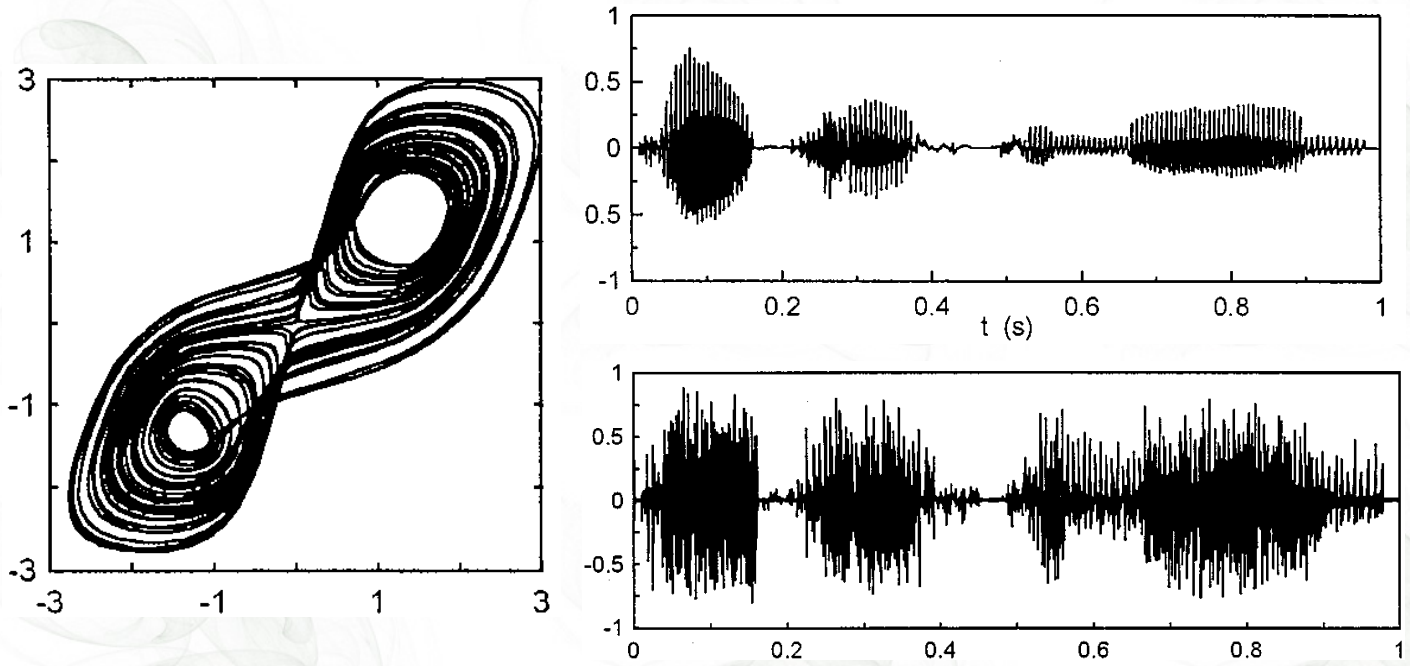
[2] Shujun Li et al., "Return-Map Cryptanalysis Revisited," submitted to *IJBC*, 2004

B. Estimation of the Carrier Signal

- The only known method is Short's nonlinear dynamic (NLD) forecasting technique [IJBC 1994,1996,1997; PRE 1998; IEEETCASI 2000].
- NLD forecasting technique is valid for many chaotic masking and some chaotic modulation schemes (including some hyperchaotic and time-delay systems).
- The basic idea is to reconstruct the embedded dynamics of the underlying chaotic systems from the transmitted signal $s(t)$, and then remove the estimated carrier signal $\hat{x}_1(t)$ from $s(t)$ to get $m(t)$.
- This technique cannot work well for most chaotic modulation schemes, and cannot exactly recover the plaintext signal.



An example of NLD forecasting



Zhenya He et al., "A Robust Digital Secure Communication Scheme Based on Sporadic Coupling Chaos Synchronization," *IEEE Trans. CAS-I*, 47(3):397-403, 2000

C. Parameter Identification

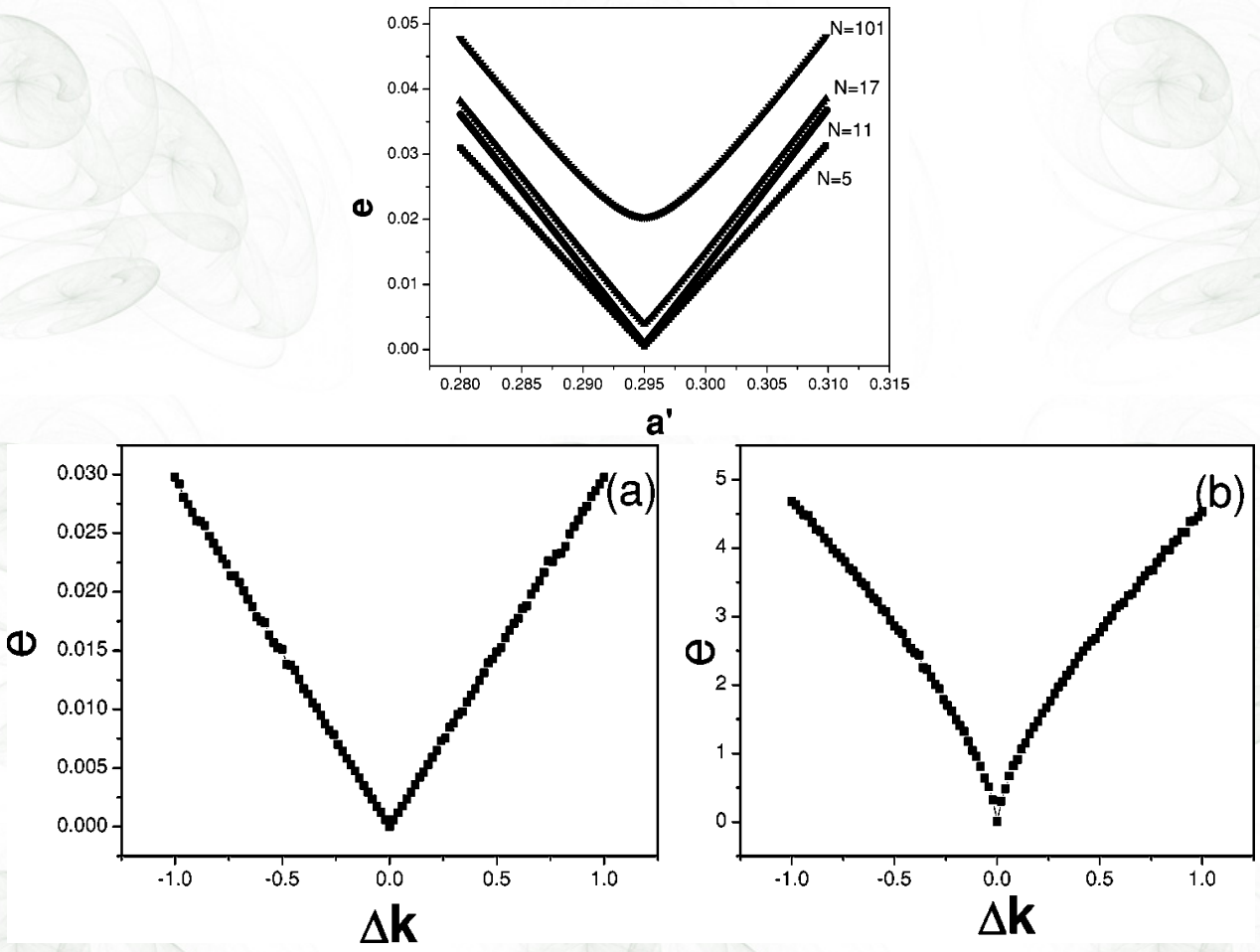
C.1. Security vs. Robustness

- There exists an essential trade-off between the security and the robustness of the chaotic cryptosystems based on analog devices, since it is difficult (costly) to maintain a very high accordance between the parameter values at the sender and the receiver ends.
- To ensure a key space of size not less than $O(2^{100})$, the chaotic systems must have a large number of secret parameters.
- It makes brute-force attacks feasible in practice, via an optimal searching algorithm.

CIE, SZU
Shenzhen

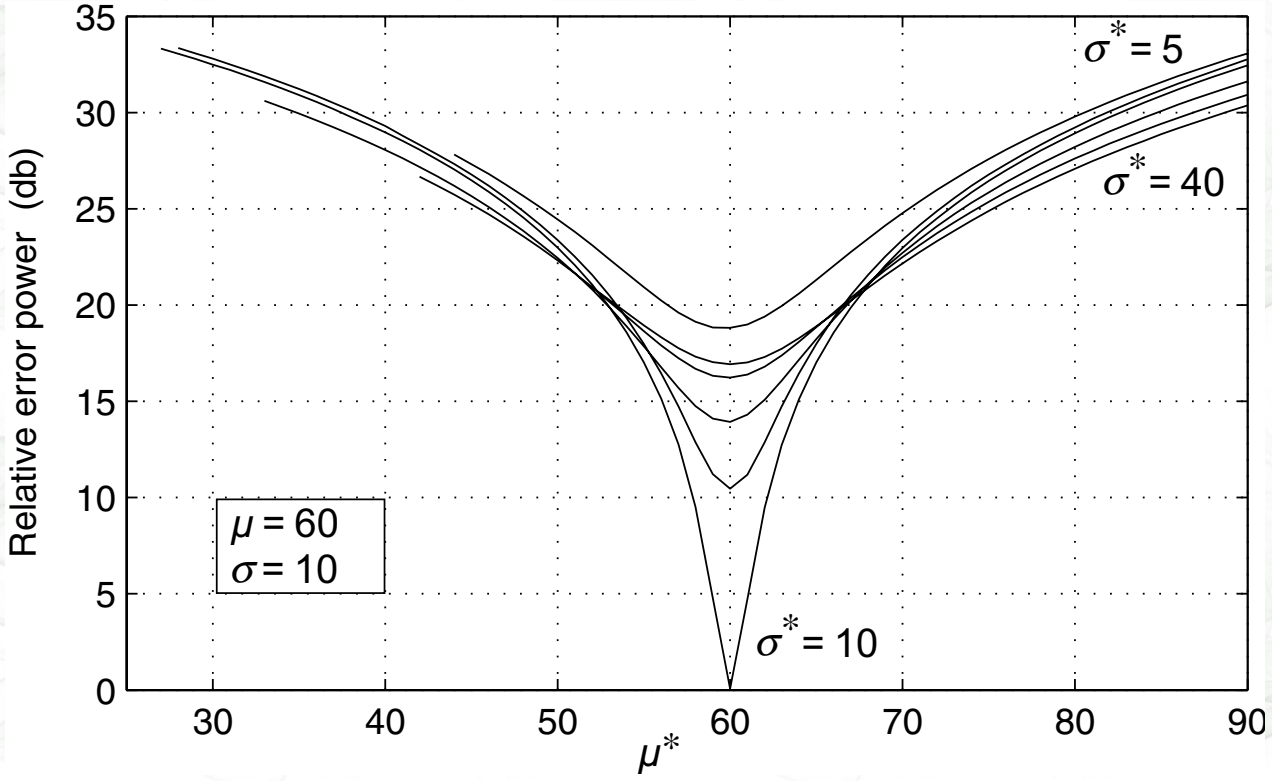
11 Nov., 2005

Two general cases



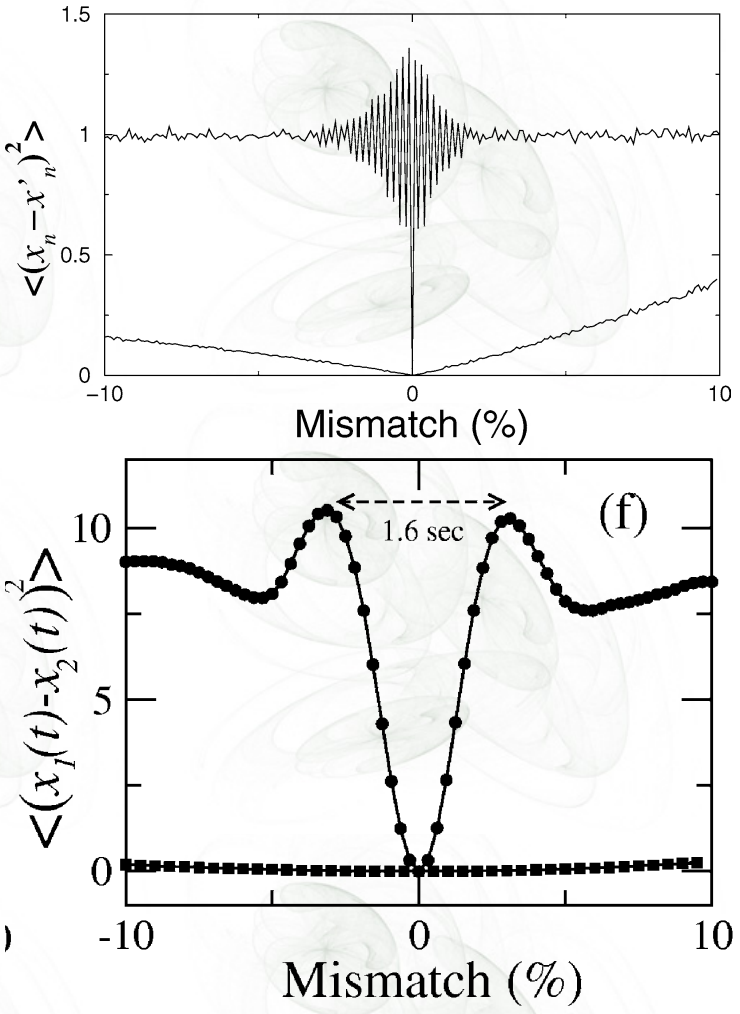
Xingang Wang et al., "Error function attack of chaos synchronization based encryption schemes," *Chaos*, 14(1):128-137, 2004

The Lorenz case



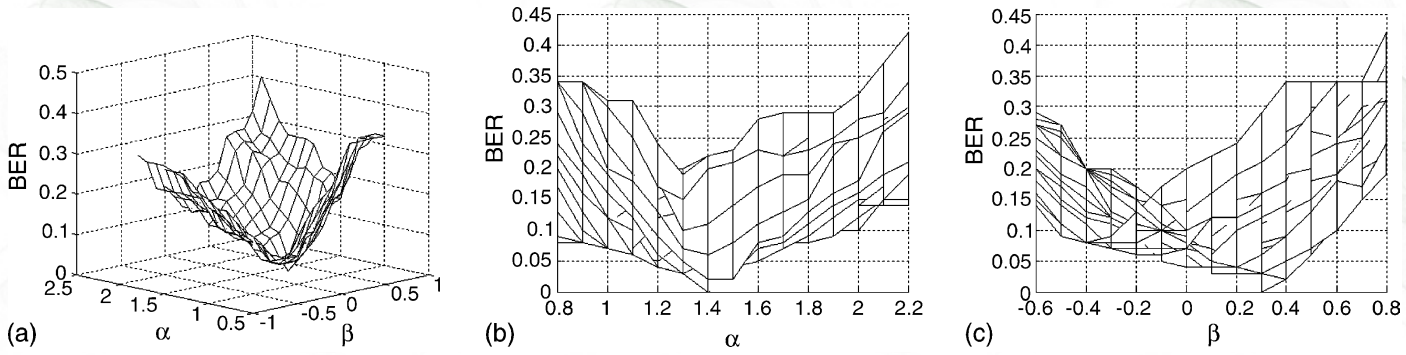
Gonzalo Álvarez et al., "Breaking projective chaos synchronization secure communication using filtering and generalized synchronization," *Chaos, Solitons & Fractals*, vol. 24, no. 3, pp. 775-783, 2005

Two time-delay cases



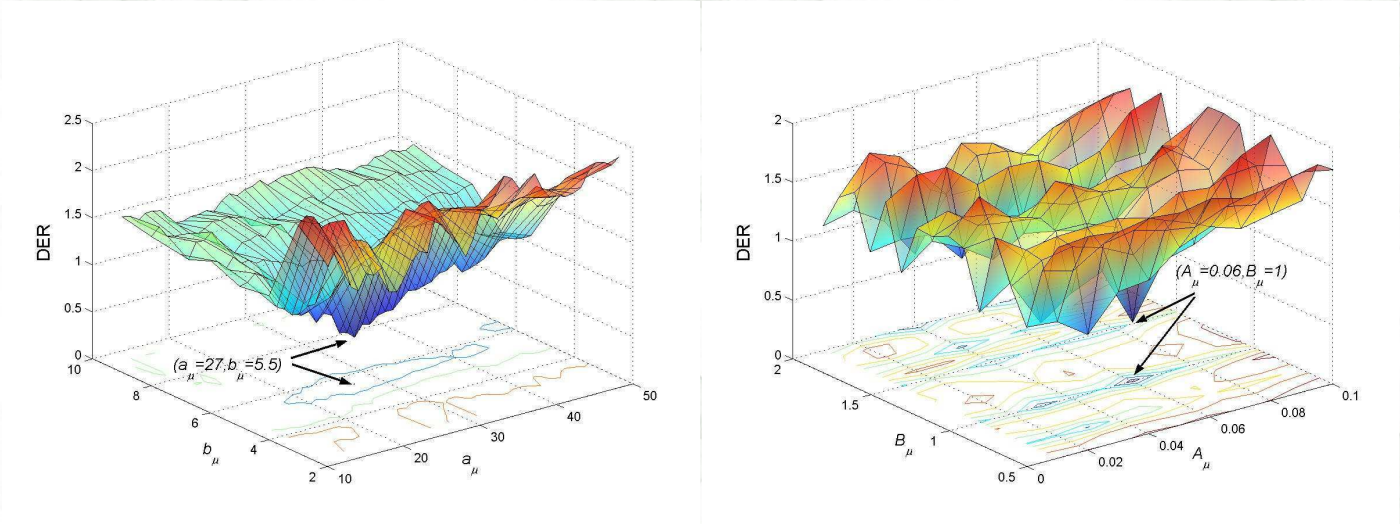
Chil-Min Kim et al., "Communication key using delay times in time-delayed chaos synchronization," *Physics Letters A*, 333(3-4):235-240, 2004

A discrete-time case: The Hénon map



Gonzalo Álvarez et al., "Cryptanalyzing a discrete-time chaos synchronization secure communication system," *Chaos, Solitons & Fractals*, 21(3):689-694, 2004

A discrete-time case: The tanh map [Minai & Pandian, Chaos 1998]

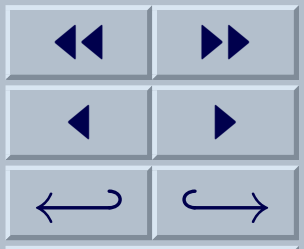


Shujun Li et al., "Breaking a chaos-noise-based secure communication scheme," *Chaos*, vol. 15, no. 1, article no. 013703, March 2005

C.2. Parameter Estimation

C.2a. Direct Parameter Estimation

- The first method was proposed by T. Beth et al. in EuroCrypt'94, which is based on Laplace transform of the transmitted signal (for the Chua system).
- A different method was proposed in [Vaidya & Angadi, CSF 17(2-3):379-386, 2003] for the Lorenz system and then was generalized to the Chua system in [Ling Liu et al., PLA 324(1):36-41, 2004].
- It can work in an offline manner and needs only a short-time segment of the transmitted signal.
- It can break both chaotic masking and CSK schemes, and can be generalized to even more chaotic systems.



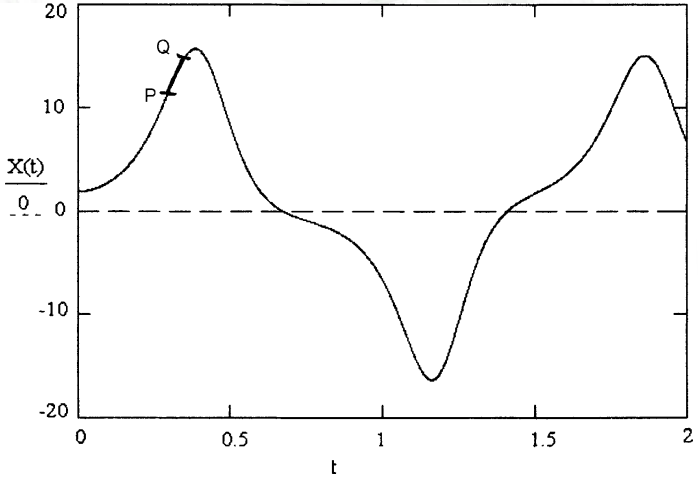
The Lorenz Case of Vaidya & Angadi's

Assume that $P = x$, $Q = \dot{x}$, $R = \ddot{x}$, $S = \dddot{x}$. When $P \neq 0$, we have

$$S = -P^3 a - P^2 Q + (abc - ab)P$$

$$+ ((-1-a)Qb + (-a-b-1)R) + \frac{QR + Q^2 + Q^2 a}{P}$$

The above equation is a trilinear system with three unknown parameters, which can be uniquely solved.

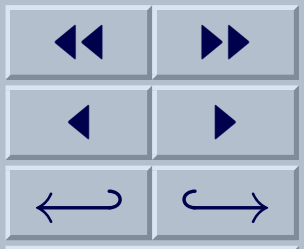


CIE, SZU
Shenzhen

11 Nov., 2005

C.2b. Adaptive Synchronization (Control)

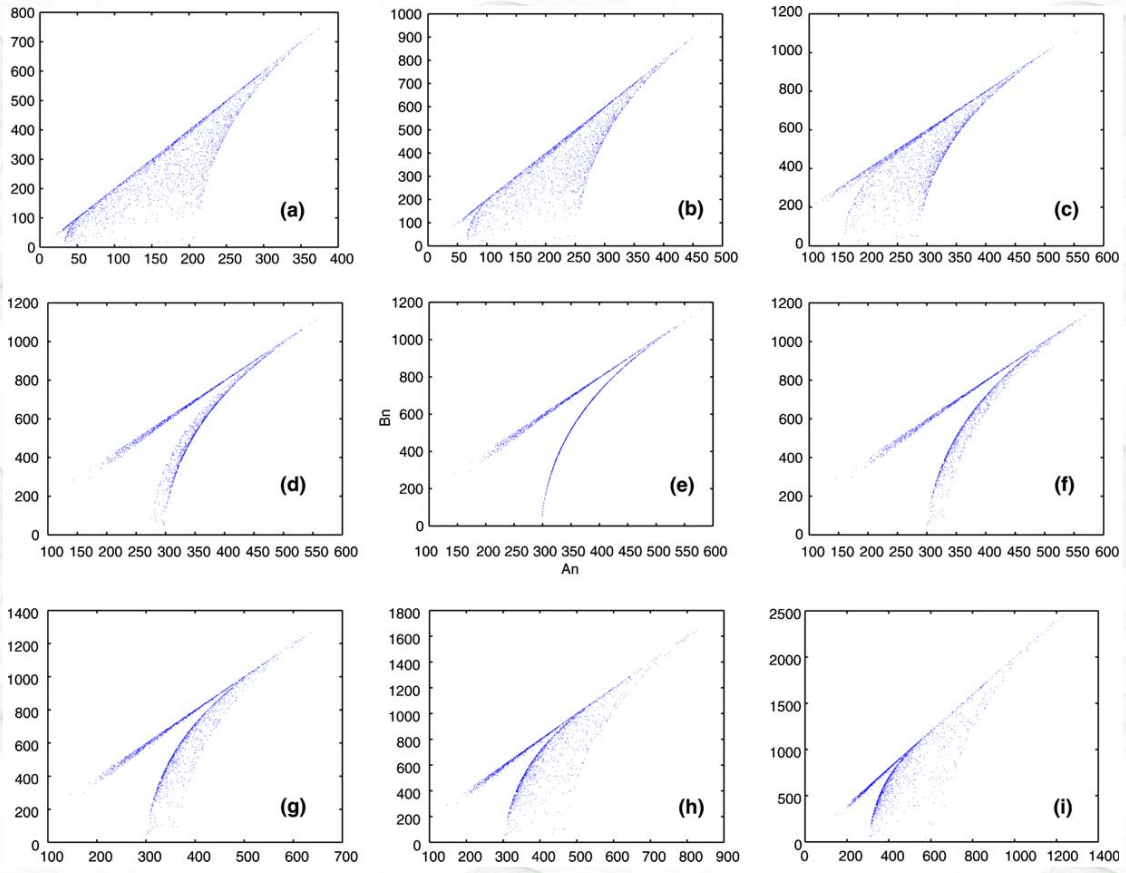
- Essentially speaking, it is an algorithm of searching the secret parameters by minimizing the synchronization error or optimizing other synchronization criteria.
- It should work in an online manner, since the synchronization performance has to be known to adjust the next value of the guessed parameters.
- A lot of different methods have been proposed, not limited in the area of chaotic cryptography. Some hyperchaotic and time-delay chaotic systems are also vulnerable to such an attacking method.
- It is another essential defect of analog chaos-based secure communication systems.



Some Typical References

- Toni Stojanovski et al, "A Simple Method to Reveal the Parameters of the Lorenz System," *IJBC*, 6(12B):2645-2652, 1996
- Hervé Dedieu & Maciej J. Ogorzałek, "Identifiability and Identification of Chaotic Systems Based on Adaptive Synchronization," *IEEE Trans. CAS-I*, 44(10):948-962, 1997
- Changsong Zhou and C.-H. Lai, "Decoding information by following parameter modulation with parameter adaptive control," *Physical Review E*, 59(6):6629-6636, 1999
- J.B. Geddes et al., "Extraction of Signals from Chaotic Laster Data," *Physical Review Letters*, 83(25):5389-5392, 1999
- Chao Tao & Gonghuan Du, "Decoding Digital Information from the Cascaded Heterogeneous Chaotic Systems," *IJBC*, 13(6):1599-1608, 2003

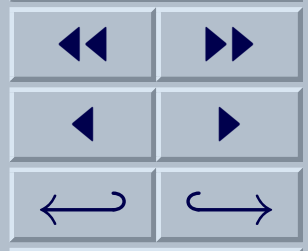
C.2c. Return-Map Method



Shujun Li et al., "Breaking a chaos-based secure communication scheme designed by an improved modulation method," *Chaos, Solitons & Fractals*, in press

D. More Powerful Cryptographical Attacks

- The parameter-estimation attacks become much easier in the chosen-ciphertext attacking scenario [Guojie Hu et al., "Chosen Ciphertext Attack on Chaos Communication Based on Chaotic Synchronization," *IEEE Trans. CAS-II*, 520(2):275-279, 2003].
- Divide-and-conquer attack (partially-known key attack) is possible for some chaotic cryptosystems, due to the fact that the key space is not a product of all sub-keys.



10 Countermeasures

Hyperchaos

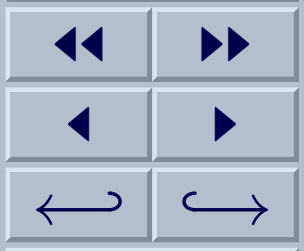
A popular idea, but many systems based on hyperchaos have been cryptanalyzed [Short & Parker, PRE 1998; Storm & Freeman, PRE 2002; Tao et al., IJBC 2004; Alvarez et al., CSF 2004].

Time-Delay Chaos

This idea is similar to hyperchaos, and some security defects have been found recently by many researchers [Zhou & Lai, PRE 1999; B.P. Bezruchko et al, PRE 2001; Ponomarenko & Prokhorov, PRE 2002; Vladimir S. Udaltsov et al, PLA 2003; Yan Zhang et al., CJP 2004].

Chaos + Encryption

- It was proposed by Tao Yang et al. in 1997 and called the 3rd-generation chaotic cryptosystem, and this idea was followed by many other researchers since then.
- I consider this idea as a basic remedy to enhance the security of all exiting chaos-based chaotic cryptosystems.
- Some security defects have been found in [Parker & Short, IEEETCASI 2001; Shujun Li et al., Chaos 2005]. It seems that the encryption function should not be too simple (like Yang's piecewise linear modular function).



Impulsive Synchronization

Impulsive complete synchronization of two Chua systems: $x_2 \to x_1$, $y_2 \to y_1$, $z_2 \to z_1$.

$$\begin{cases} \dot{x}_1 = p(-x_1 + y_1 - f(x_1)) \\ \dot{y}_1 = x_1 - y_1 + z_1 \\ \dot{z}_1 = -qy_1 - rz_1 \end{cases}$$

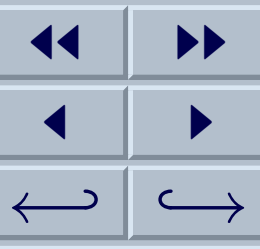
$$\downarrow \{x_1(t_i), y_1(t_i), z_1(t_i)\}$$

$$\begin{cases} \dot{x}_2 = p(-x_2 + y_2 - f(x_2)), & t \neq t_i \\ \dot{y}_2 = x_2 - y_2 + z_2, & t \neq t_i \\ \dot{z}_2 = -qy_2 - rz_2, & t \neq t_i \\ \begin{bmatrix} \Delta x_2 \\ \Delta y_2 \\ \Delta z_2 \end{bmatrix} = -\mathbf{B} \begin{bmatrix} x_1 - x_2 \\ y_1 - y_2 \\ z_1 - z_2 \end{bmatrix}, & t = t_i \end{cases}$$

Some Facts

- It was proposed by Tao Yang et al. in 1997 and called the 4th-generation chaotic cryptosystem, and then this idea was followed by some researchers.
- The basic idea is to change the continuous driving signal into impulsive (sporadic) driving signal(s), to resist various kinds of attacks.
- Generally, all variables of the master system have to be transmitted. A general form of the driving matrix is

$$\mathbf{B} = \begin{bmatrix} k_1 & 0 & 0 \\ 0 & k_2 & 0 \\ 0 & 0 & k_3 \end{bmatrix}.$$

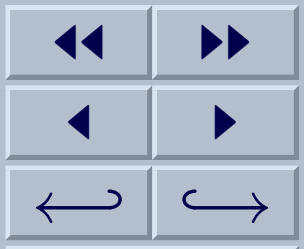


Security

- The fact that all variables of the master system have to be transmitted may bring potential security problems.
- It is doubtful that impulsive synchronization can provide an essential security against adaptive-synchronization based attacks, though Zhenya He's work [IEEETCAS-I/JCSC 2000] showed that one adaptive-synchronization based attack failed when the drive period ΔT is sufficiently large.
- It seems that a chaotic cryptosystem based on impulsive synchronization is insecure if the drive period ΔT is smaller than the bandwidth of the transmitted chaotic signal(s).

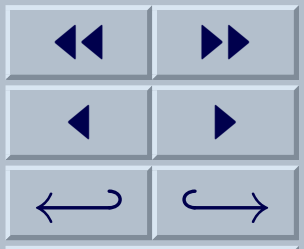
Re-Modulation

- Recently Bu & Wang [CSF 19(4):919 2004] proposed a new method of enhancing the security of chaotic masking and CSK schemes against return-map attack, by re-modulating the transmitted ciphertext signal $s(t) = x_1(t)$ with an external periodic signal $g(t) = A\cos(\omega t + \phi_0)x_3(t)$.
- Bu-Wang scheme was soon broken by three groups of researchers independently [Chin Yi Chee et al, CSF 21(5):1129 2004; Xiaogang Wu et al., CSF 22(2):367 2004; Gonzalo Álvarez et al., CSF 23(5):1749 2005], via similar (but different) attacks based on zero-crossing point detection.



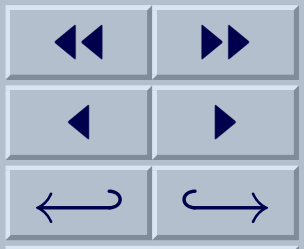
Re-Modulation (Continued)

- Xiaogang Wu et al. improved the Bu-Wang scheme by slightly changing the modulating signal to avoid zero-crossing points: $g(t) = A(\cos(\omega t + \phi_0) + M)x_3(t)$, where $M > 1$.
- Xiaogang Wu et al.'s modified scheme was soon broken again by Shujun Li et al. in 2004, by estimating parameters of the modulating signal, ω, ϕ_0 and M.
- From a cryptographical point of view, this method is not very efficient, since the key space is not a product of the two parts of the key.
- It is not clear whether or not this idea can be further generalized by using aperiodic modulating signals, without maintaining the synchronization performance.



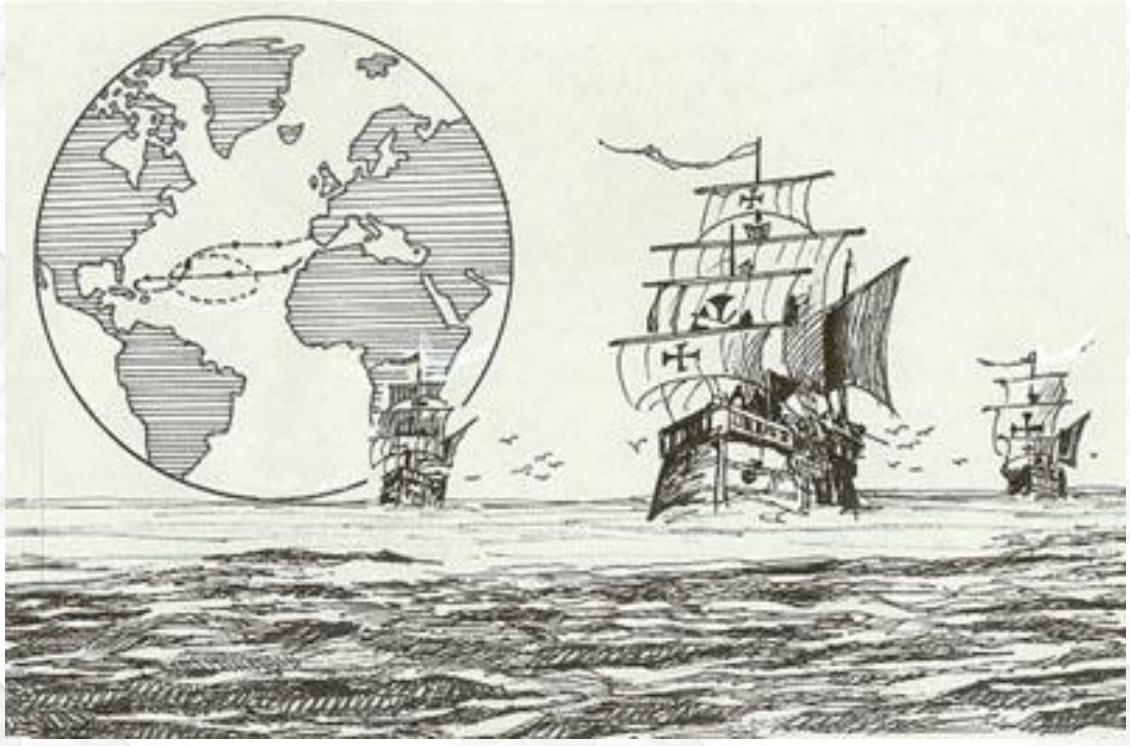
Projective Synchronization

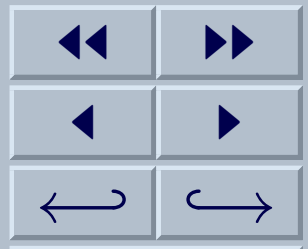
- The first published proposal was contributed by Zhigang Li & Daolin Xu [CSF 22(2):477 2004]. Two different schemes have been proposed by Bing-Hong Wang & Shouliang Bu in [IJMP-B 18(17-19):2415 2004] and by Chin Yi Chee & Daolin Xu [CSF 23(3):1063 2005].
- Li-Xu scheme has been broken by Gonzalo Álvarez and his co-workers (including me ☺) soon (including a hyperchaotic case), via a filtering attack and a GS-based attack (the latter is based the low sensitivity to parameter mismatch).
- It seems that only using projective synchronization cannot overcome the security problems of chaotic cryptosystems based on other synchronization modes.



Discrete-Time and Digital Chaos

It is a completely different world, like ...





CIE, SZU
Shenzhen

11 Nov., 2005

Thank you!

This presentation was made with Matthias Mühlich's pdfwin package, and compiled with PDFLaTeX and postprocessed with PPower4.

CIE, SZU
Shenzhen

11 Nov., 2005