Ashraf A. Zaher
College of Engineering and Applied Sciences
American University of Kuwait
P. O. Box 3323 – Safat 13034 – Kuwait
azaher@auk.edu.kw

MODERN CYBERSECURITY
EDUCATIONAL AND TECHNICAL PERSPECTIVES

Chaos for Cybersecurity

25 November 2020

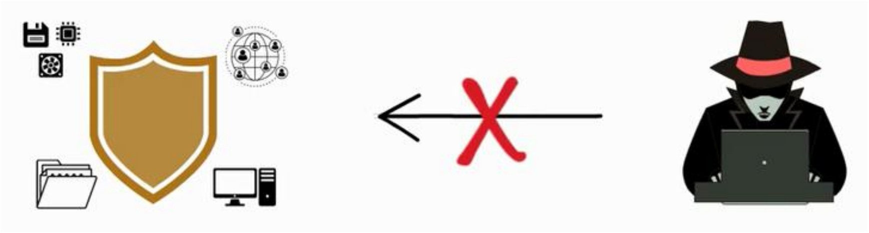
Exploring Cybersecurity

Introduction:

- Security problem: *a general overview*
- Old era: *before and during the 80s (closed/central systems)*
- New era: *sources of the problem and suggested remedies*

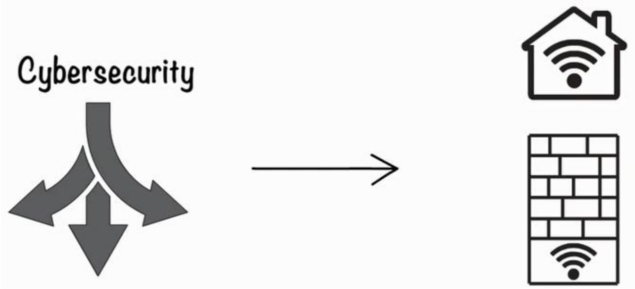
Main types of attacks:

- Malware/Phishing
- Man in the middle
- Password/Ransom
- Corporates related



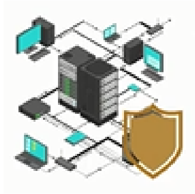
Related actions:

- Ethical hacking
- Designing security architectures and protocols
- Information security



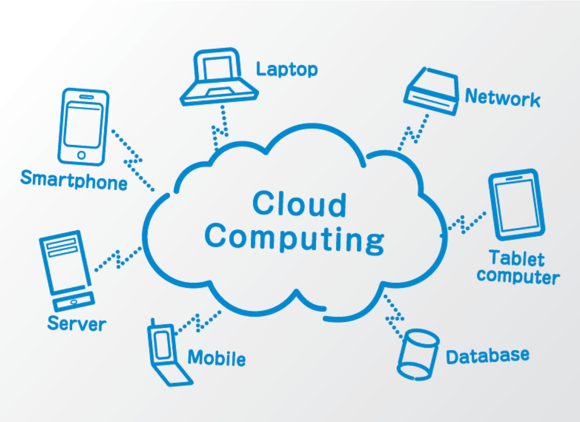
The problem in a nutshell:

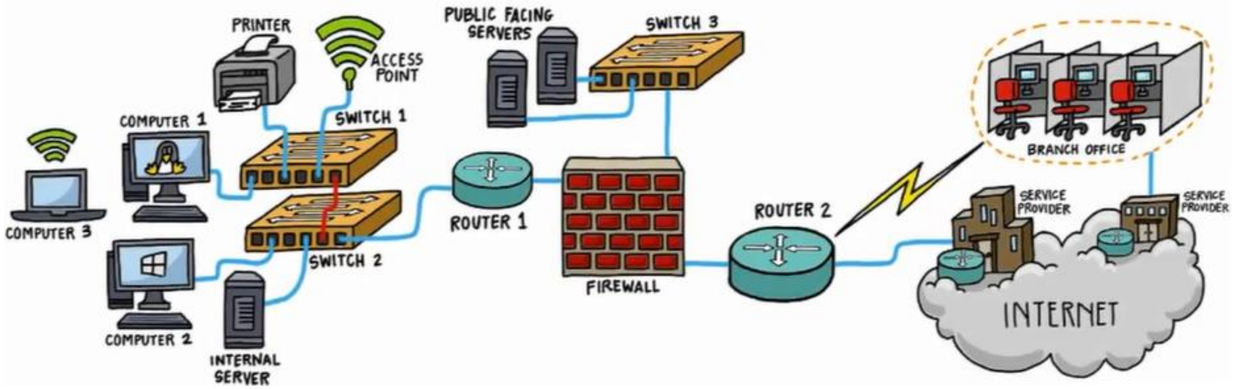
- Establishing secure communication
- Preserve the integrity of stored data



Exploring Cybersecurity

- **Introduction:**
  - Security problem: *a general overview*
  - Old era: *before and during the 80s (closed/central systems)*
  - New era: *sources of the problem and suggested remedies*

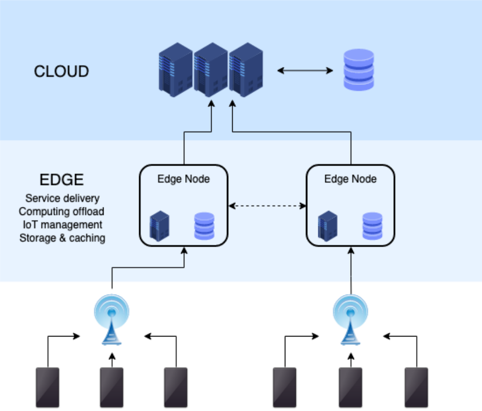


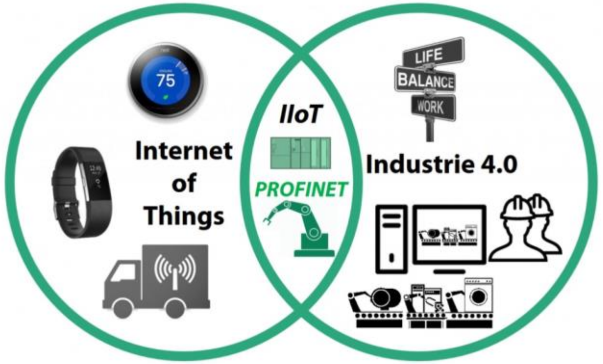


- Main ty
  - Malwa
  - Man in
  - Passw
  - Corpor

- Related
  - Ethical h
  - Designin nd prot
  - Informat

- The prob
  - Establish n
  - Preserve ta





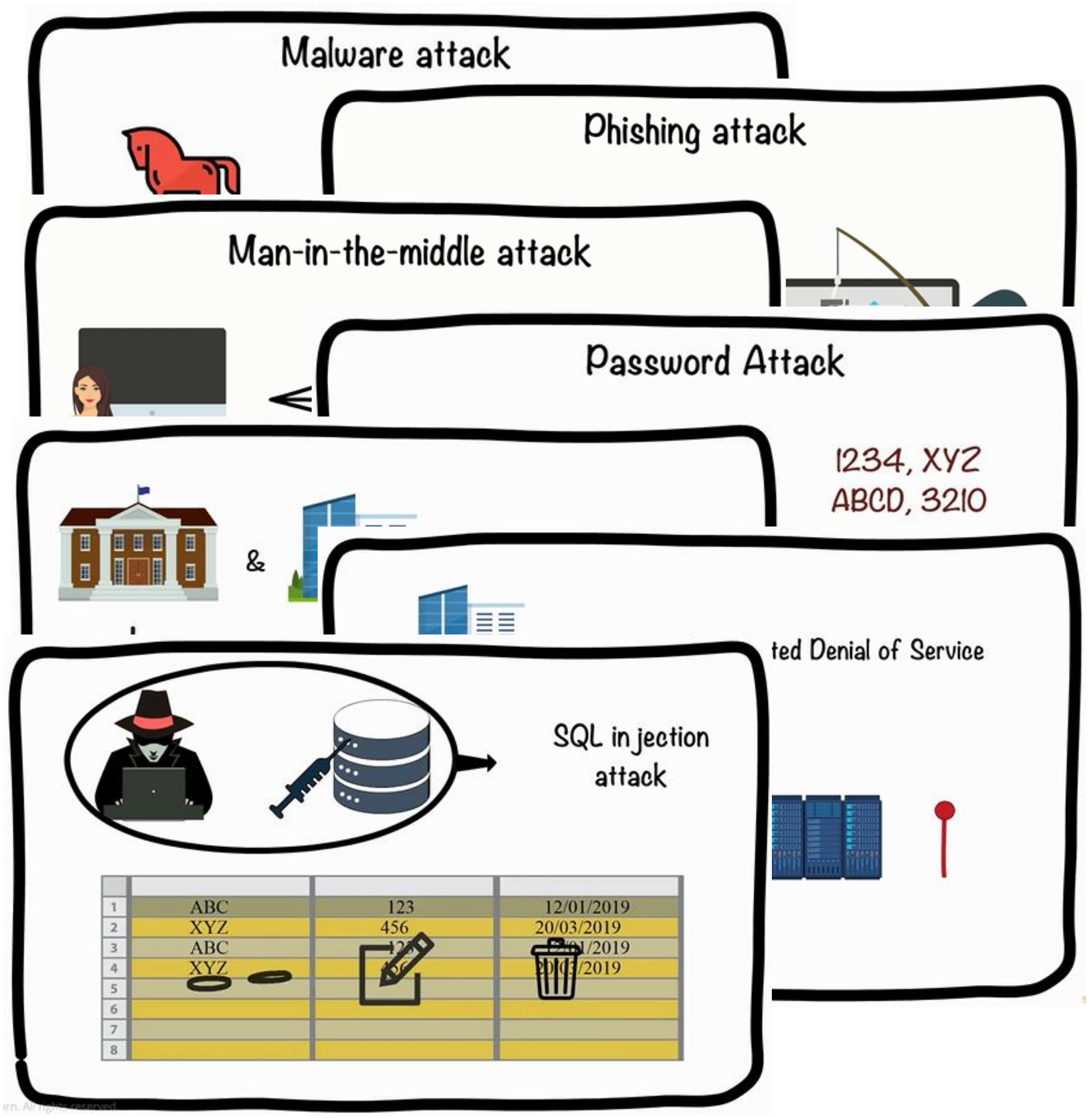
Exploring Cybersecurity

- ❑ **Introduction:**
  - ➢ Security problem: *a general overview*
  - ➢ Old era: *before and during the 80s (closed/central systems)*
  - ➢ New era: *sources of the problem and suggested remedies*

- ❑ **Main types of attacks:**
  - ➢ Malware/Phishing
  - ➢ Man in the middle
  - ➢ Password/Ransom
  - ➢ Corporates related

- ❑ **Related actions:**
  - ➢ Ethical hacking
  - ➢ Designing security architectures and protocols
  - ➢ Information security

- ❑ **The problem in a nutshell:**
  - ➢ Establishing secure communication
  - ➢ Preserve the integrity of stored data



Exploring Cybersecurity

- ❑ Introd
  - ➢ Secu
  - ➢ Old ed/centr
  - ➢ New ggested
- ❑ Main t
  - ➢ Malw
  - ➢ Man
  - ➢ Password / Ransom
  - ➢ Corporates related

Building and using VMs: platform agnostic (Host – Guest – Hypervisor)

Lowest level OS shell to access the OS kernel (e.g. Powershell)

(Configuration and maintenance)

- ❑ **Related actions:**
  - ➢ Ethical hacking
  - ➢ Designing security architectures and protocols
  - ➢ Information security
- ❑ The problem in a nuts
  - ➢ Establishing secure comm
  - ➢ Preserve the integrity of

Encryption/decryption

(4-layer TCP/IP and the 7-layer OSI)

Exploring Cybersecurity

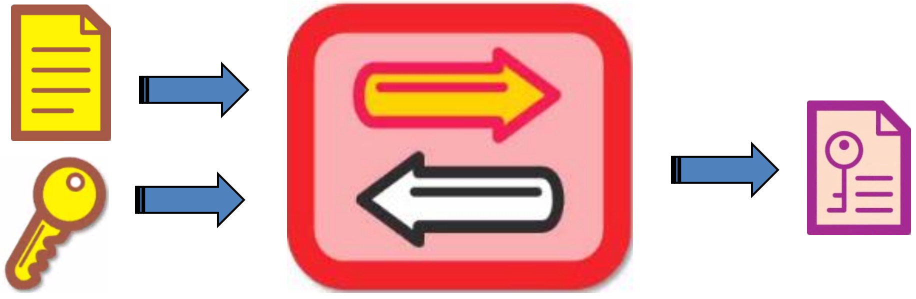
- ❑ **Introduction:**
  - Security problem: *a general overview*
  - Old era: *before and during the 80s (closed/central systems)*
  - New era: *sources of the problem and suggested remedies*
- ❑ **Main types of attacks:**
  - Malware/Phishing
  - Man in the middle
  - Password/Ransom
  - Corporates related
- ❑ **Related actions:**
  - Ethical hacking
  - Designing security architectures and protocols
  - Information security
- ❑ **The problem in a nutshell:**
  - Establishing secure communication
  - Preserve the integrity of stored data

cryptography

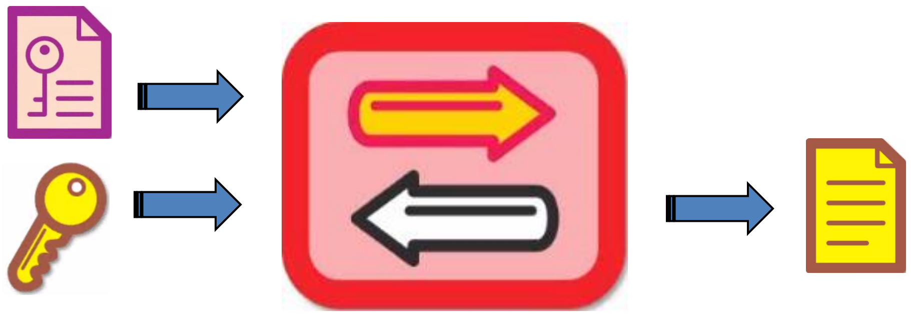
using Chaos

- **Cryptology combines the two Greek terms:**
  - *κρυπτός (Kryptos = Secret)*
  - *λόγος (Logos = Study)*
- **Describes the science or study of hiding, securely transmitting, and recovering information.**
- **It is divided into two main categories:**
  - **Cryptography – dealing with securing information.**
  - **Cryptanalysis – trying to break security (*legally* and *illegally*).**
- **Most important applications:**
  - **Banking,**
  - **Electronic Commerce,**
  - **Telecommunications,**
  - **Military, and**
  - **Protection of intellectual properties.**

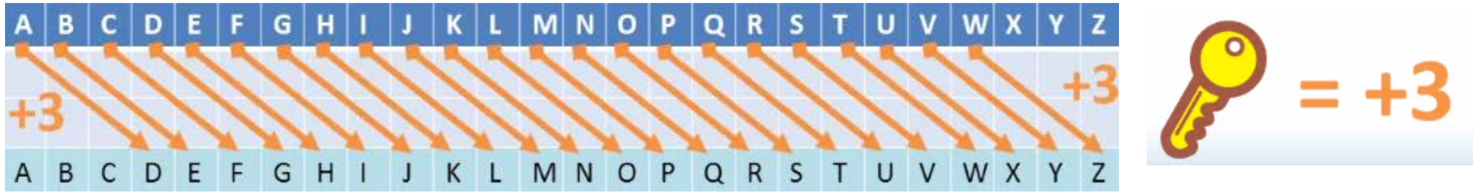
Exploring Cybersecurity

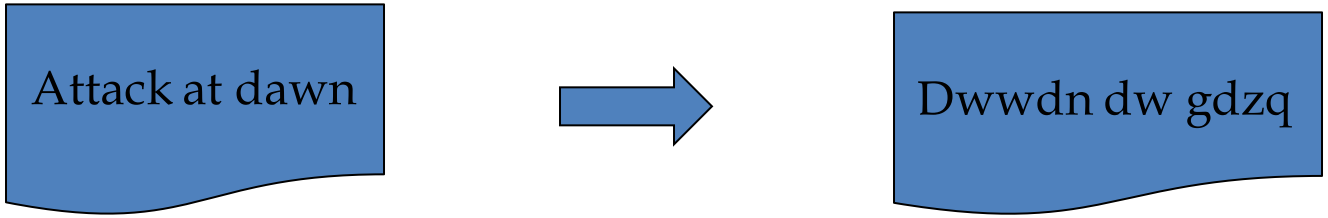


Encryption

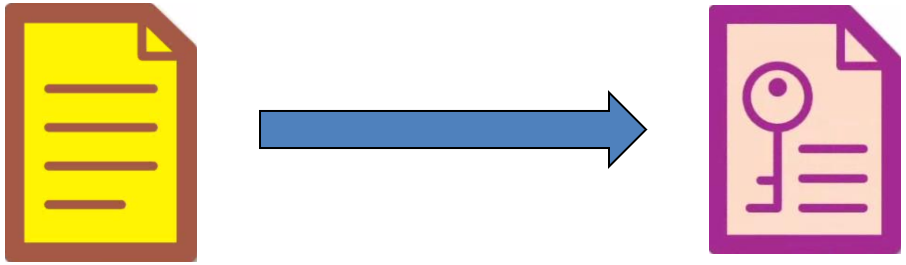


Decryption


A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
+3
+3
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
= +3



Plaintext

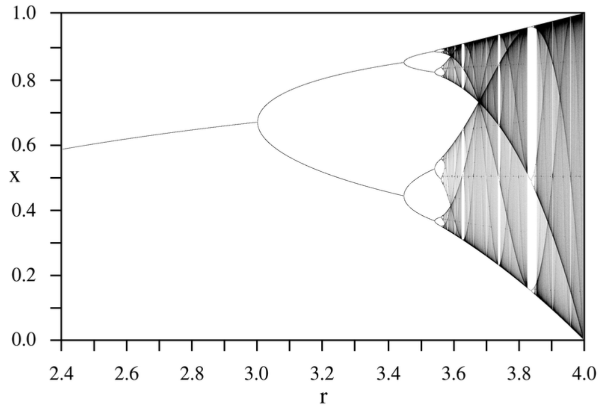


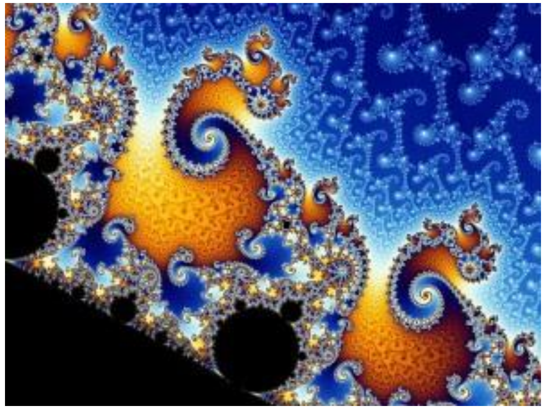
Ciphertext

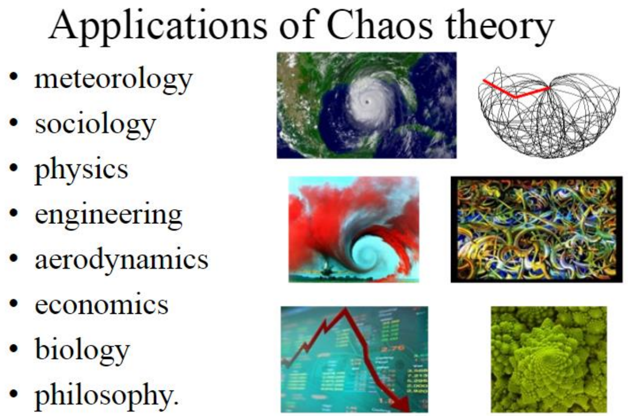
- **Steganography**
- **Watermarking**

What is Chaos

- ❑ **Definitions:**
  - ➢ *Traditional:* Merriam-Webster dictionary
  - ➢ *Scientific:* Physics and Engineering
- ❑ **History:**
  - ➢ *Brief chronological order*
  - ➢ *Lorenz story (demo)*
- ❑ **Examples and most famous contributors:**
  - ➢ Continuous-time (Analog)
    - ○ *Lorenz*
    - ○ *Others: Rossler, Chua, …*
  - ➢ Discrete-time (Digital)
    - ○ *The logistic map*
    - ○ *The Henon map*
- ❑ **Methods of Analysis:**
  - ➢ *Analytical (Math-based)*
  - ➢ *Simulation (coding)*
- ❑ **Most important applications:**
  - ➢ *Secure communication*
  - ➢ *True random numbers generation*







Applications of Chaos theory

- meteorology
- sociology
- physics
- engineering
- aerodynamics
- economics
- biology
- philosophy.

Candidates for cryptography in cybersecurity

Definitions of Chaos

- ❑ **Definitions:**
  - ➢ *Traditional:* Merriam-Webster dictionary
  - ➢ *Scientific:* Physics and Engineering

Chaos is a state of utter confusion or disorder; a total lack of organization or order.

Chaos is an aperiodic long-time behavior arising in a deterministic dynamical system that exhibits a sensitive dependence on initial conditions.

- ❑ **History:**
  - ➢ *Brief chronological order*
  - ➢ *Lorenz story (demo)*
- ❑ **Examples and most famous contributors:**
  - ➢ Continuous-time (Analog)
    - o *Lorenz*
    - o *Others: Rossler, Chua, …*
  - ➢ Discrete-time (Digital)
    - o *The logistic map*
    - o *The Henon map*
- ❑ **Methods of Analysis:**
  - ➢ *Analytical (Math-based)*
  - ➢ *Simulation (coding)*
- ❑ **Most important applications:**
  - ➢ *Secure communication*
  - ➢ *True random numbers generation*

History of Chaos

- ❑ **Definition:**
  - ➢ *Traditional:* Merriam-Webster dictionary
  - ➢ *Scientific:* Physics and Engineering
- ❑ **History:**
  - ➢ *Brief chronological order*
  - ➢ *Lorenz story (demo)*

Lorenz, a meteorologist, was running computerized equations to theoretically model and predict weather conditions. Having run a particular sequence, he decided to replicate it. What he found was, contrary to his expectations, these results were radically different from his first outcomes. **Lorenz** had, in fact, entered not precisely the same number, .506127, but the rounded figure of .506.

- ❑ **Examples and most famous contributors:**
  - ➢ Continuous-time (Analog)
    - ○ *Lorenz*
    - ○ *Others: Rossler, Chua, …*
  - ➢ Discrete-time (Digital)
    - ○ *The logistic map*
    - ○ *The Henon map*
- ❑ **Methods of Analysis:**
  - ➢ *Analytical (Math-based)*
  - ➢ *Simulation (coding)*
- ❑ **Most important applications:**
  - ➢ *Secure communication*
  - ➢ *True random numbers generation*

❑ Exact model:

$$\frac{\partial}{\partial t}\left(\nabla^2\psi\right) = -\frac{\partial\left(\psi,\nabla^2\psi\right)}{\partial(x,z)} + \nu\nabla^4\psi + g\alpha\frac{dT}{dx}$$

$$\frac{\partial}{\partial t}T = -\frac{\partial(\psi,T)}{\partial(x,z)} + \frac{\Delta T}{H}\frac{\partial\psi}{\partial x} + \kappa\nabla^2 T$$

H: uniform depth
ΔT: imposed temperature difference
g: gravity
a: buoyancy
κ: thermal diffusivity
ν: kinematic viscosity
ψ: stream function
T: departure of temperature
Ra: Rayleigh number
Ra_c: critical Rayleigh number

❑ Simplified model:

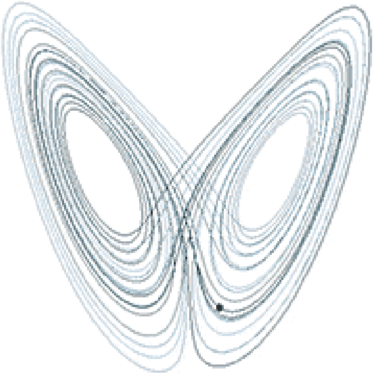
$$\dot{x} = \sigma(y - x)$$
$$\dot{y} = -xz + \rho x - y$$
$$\dot{z} = xy - \beta z$$

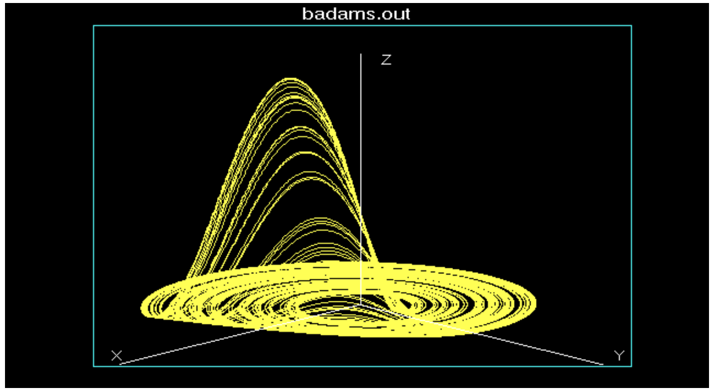
x: convective intensity
y: temperature difference between descending and ascending currents
z: difference in vertical temperature profile

❑ Ref.: Atmos. Sci. **20,** 130 (1963)

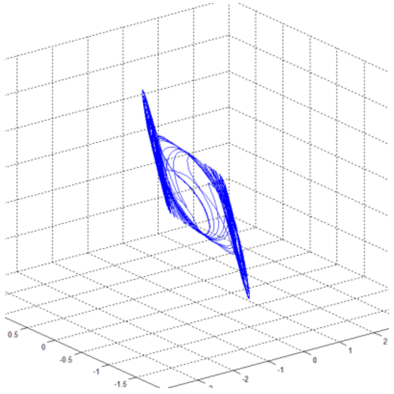
Examples & most famous contributors in Chaos

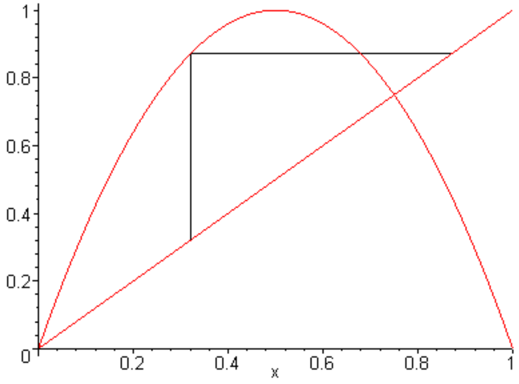
- ❑ **Definition:**
  - ➢ *Traditional:* Merriam-Webster dictionary
  - ➢ *Scientific:* Physics and Engineering
- ❑ **History:**
  - ➢ *Brief chronological order*
  - ➢ *Lorenz story (demo)*

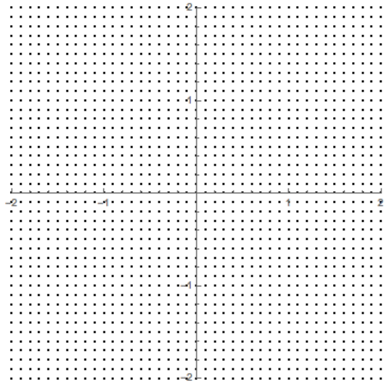




- ❑ **Examples and most famous contributors:**
  - ➢ Continuous-time (Analog)
    - ○ *Lorenz*
    - ○ *Others: Rossler, Chua, …*
  - ➢ Discrete-time (Digital)
    - ○ *The logistic map*
    - ○ *The Henon map*







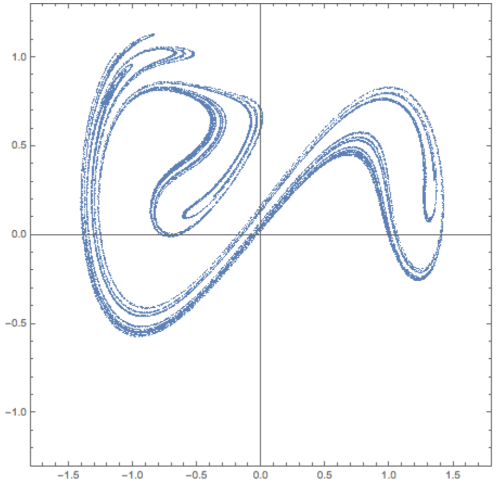
- ❑ **Methods of Analysis:**
  - ➢ *Analytical (Math-based)*
  - ➢ *Simulation (coding)*
- ❑ **Most important applications:**
  - ➢ *Secure communication*
  - ➢ *True random numbers generation*

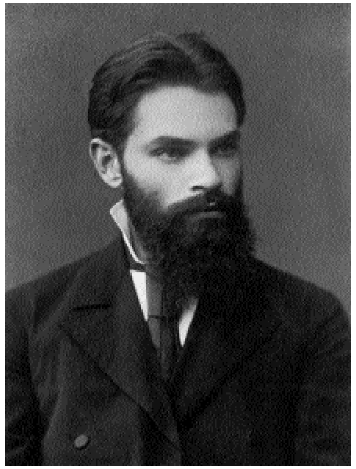
Current technology removed the clear boundaries between analog and digital chaotic systems; e.g. using FPGAs many analog systems could be almost identical to their digital approximations.

Methods of analyzing Chaos

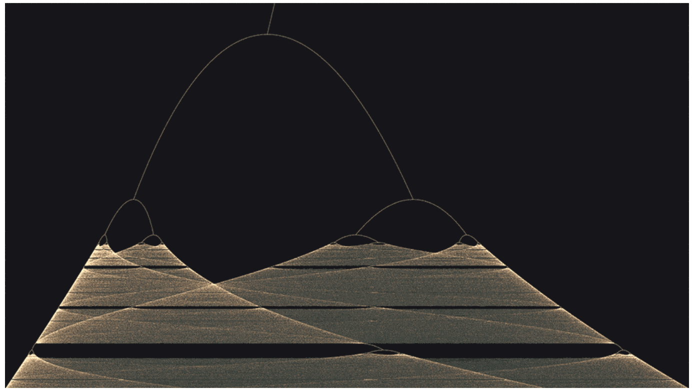
- ❑ **Definition:**
  - ➢ *Traditional:* Merriam-Webster dictionary
  - ➢ *Scientific:* Physics and Engineering
- ❑ **History:**
  - ➢ *Brief chronological order*
  - ➢ *Lorenz story (demo)*
- ❑ **Examples and most famous contributors:**
  - ➢ Continuous-time (Analog)
    - o *Lorenz*
    - o *Others: Rossler, Chua, …*
  - ➢ Discrete-time (Digital)
    - o *The logistic map*
    - o *The Henon map*
- ❑ **Methods of Analysis:**
  - ➢ *Analytical (Math-based)*
  - ➢ *Simulation (coding)*
- ❑ **Most important applications:**
  - ➢ *Secure communication*
  - ➢ *True random numbers generation*

Henri Poincaré





Alexander Lyapunov

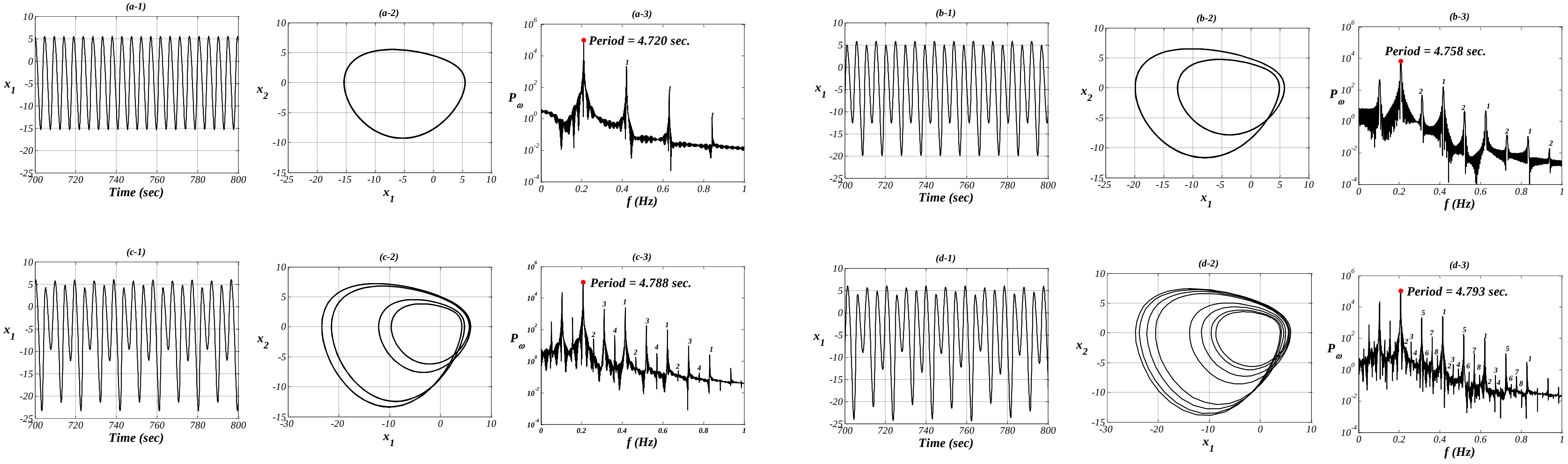


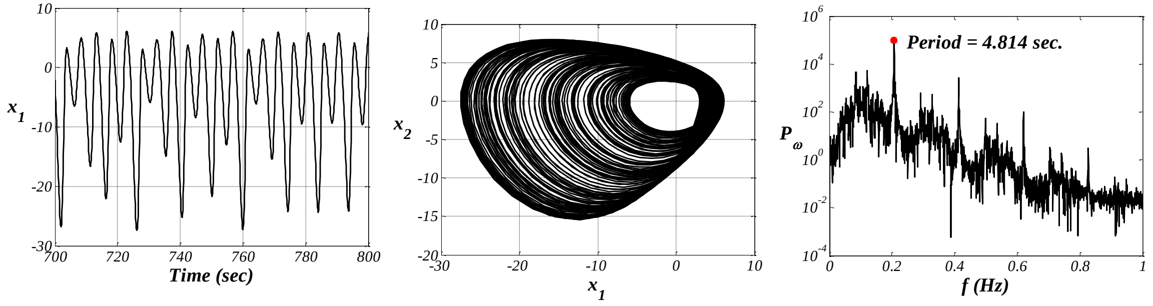
$$\boxed{\lambda_i = \lim_{t\to\infty} \frac{1}{t} \log_2 \frac{p_i(t)}{p_i(0)}}$$

What is Chaos

- ❑ **Definition:**
  - ➢ *Traditional:* Merriam-Webster dictionary
  - ➢ *Scientific:* Physics and Engineering
- ❑ **History:**
  - ➢ *Brief chronological order*
  - ➢ *Lorenz story (demo)*
- ❑ **Examples and most famous contributors:**
  - ➢ Continuous-time (Analog)
    - o *Lorenz*
    - o *Others: Rossler, Chua, …*
  - ➢ Discrete-time (Digital)
    - o *The logistic map*
    - o *The Henon map*
- ❑ **Methods of Analysis:**
  - ➢ *Analytical*
  - ➢ *Simulation (coding)*
- ❑ **Most important applications:**
  - ➢ *Secure communication*
  - ➢ *True random numbers generation*

Route to Chaos: Period Doubling





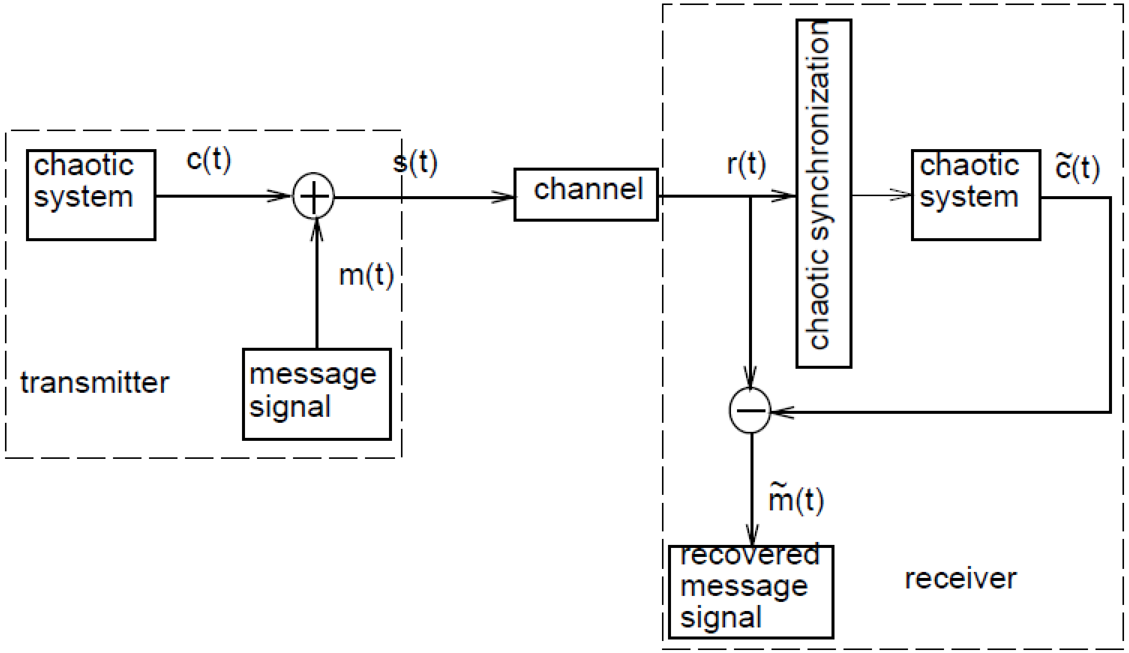
- Power spectrums of chaotic systems resemble white noise; thus making them an ideal choice for carrying and hiding signals over communication channels.
- They can be easily generated using both analog or digital hardware.
- Two different and/or equivalent chaotic systems can be easily synchronized using different control methods.

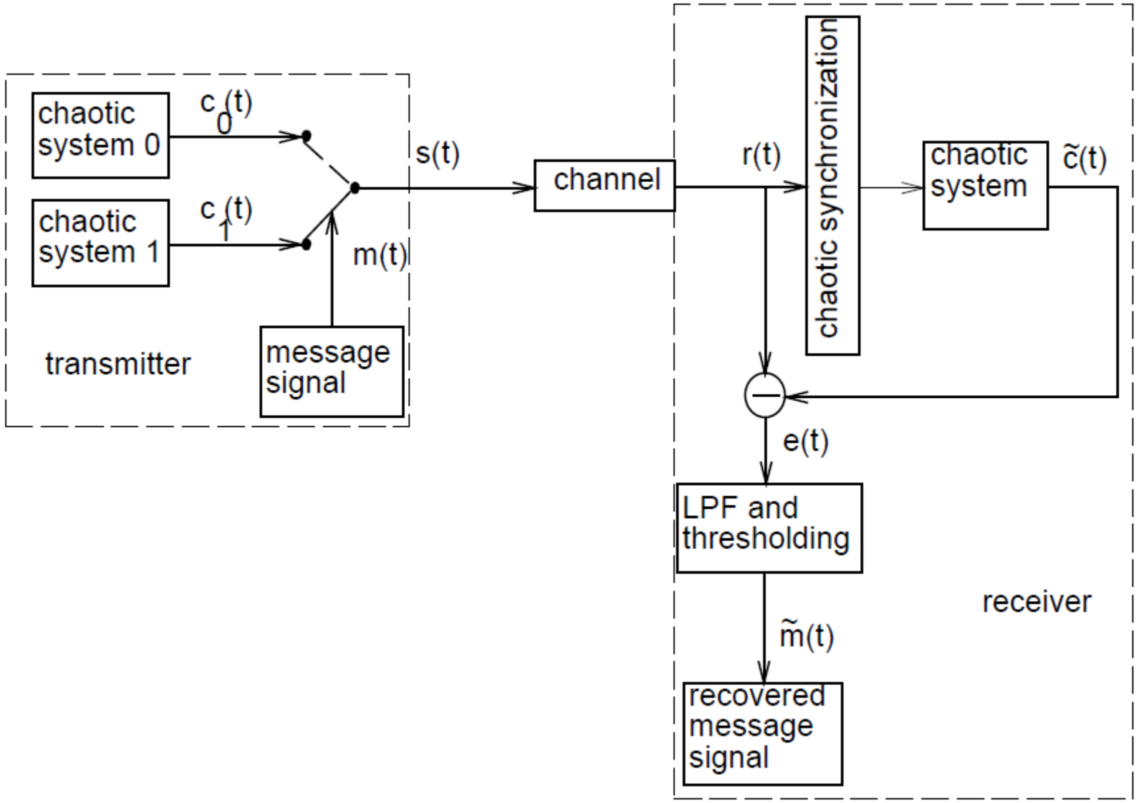
Types of Chaos-based Secure Communication

- Generations of Chaos-Based Secure Communication Systems:
  1. Additive masking & Shift-keying
  2. Parameter modulation & non-autonomous modulation
  3. Cryptosystems
  4. Impulsive synchronization

Types of Chaos-based Secure Communication

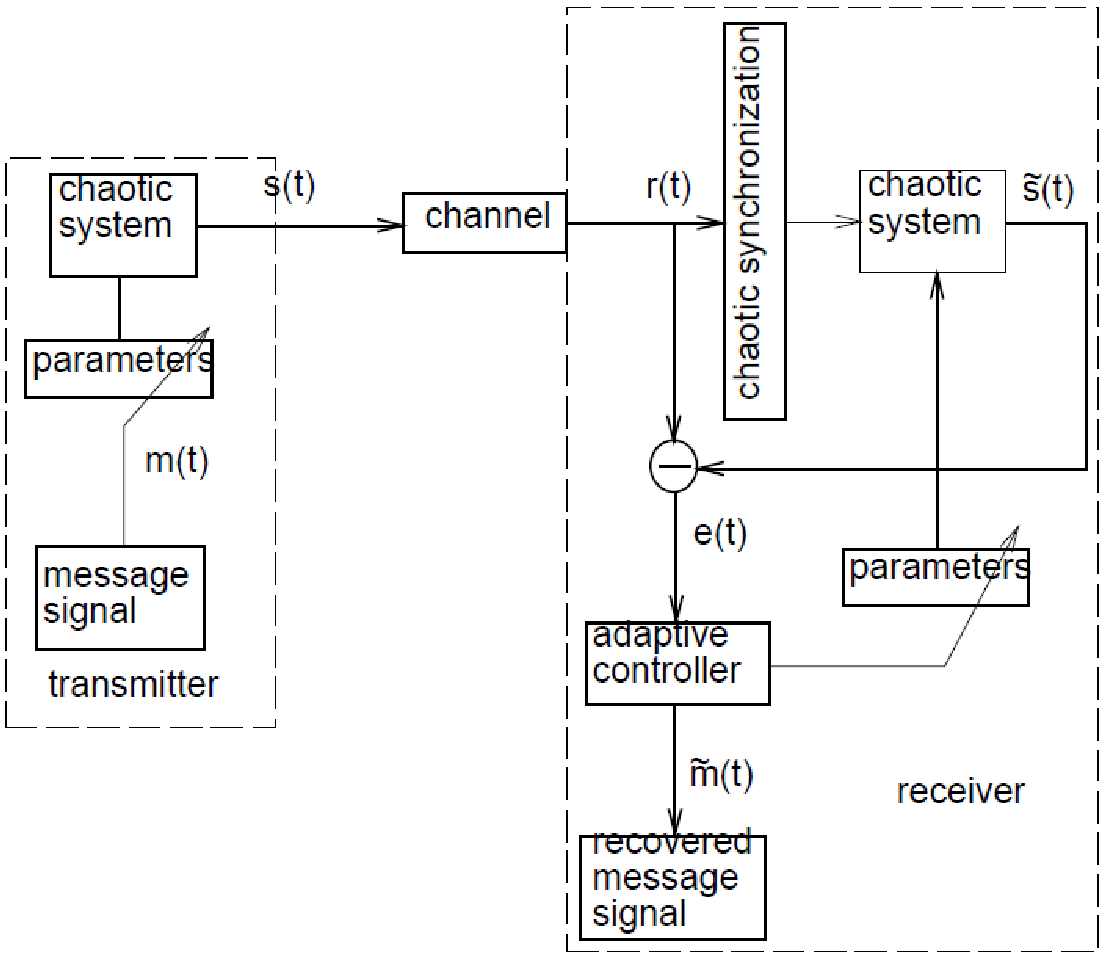
- Generations of Chaos-Based Secure Communication Systems:
  1. **Additive masking & Shift-keying**
  2. Parameter modulation
  3. Cryptosystems
  4. Impulsive synchronization





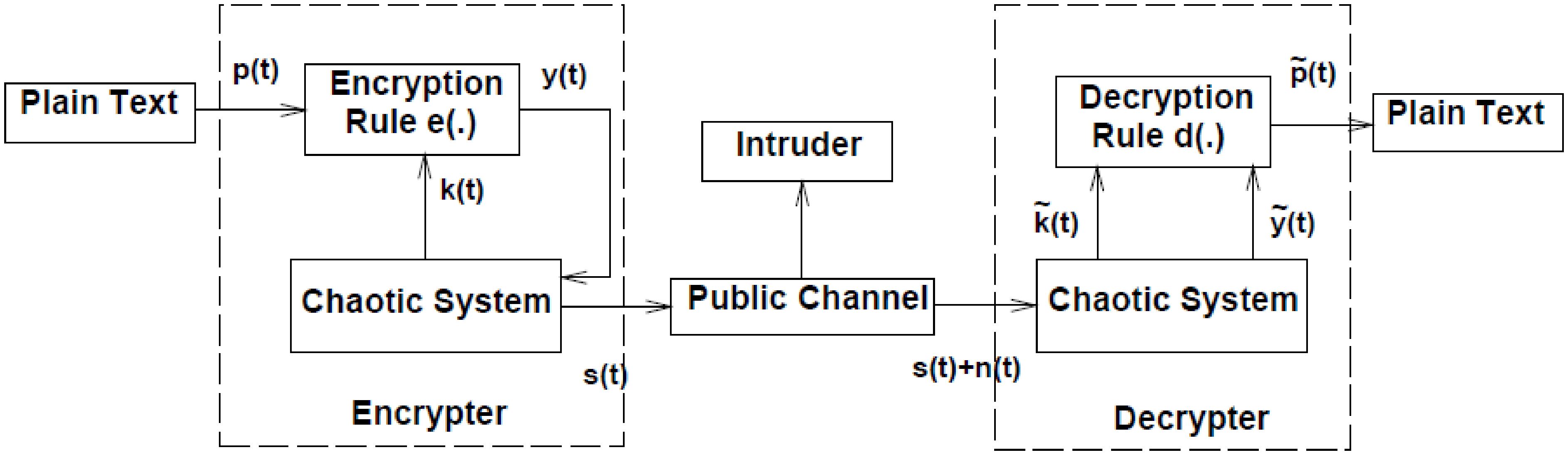
Types of Chaos-based Secure Communication

- Generations of Chaos-Based Secure Communication Systems:
  1. Additive masking & Shift-keying,
  2. **Parameter modulation**
  3. Cryptosystems
  4. Impulsive synchronization



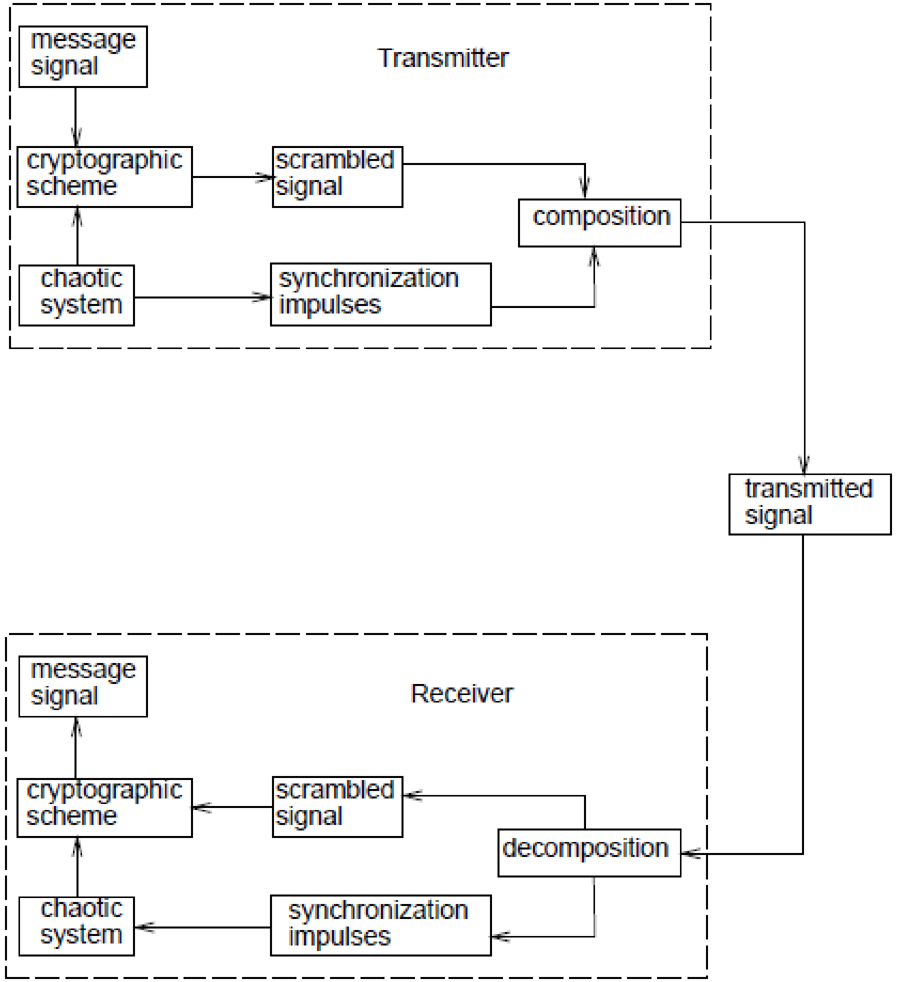
Types of Chaos-based Secure Communication

- Generations of Chaos-Based Secure Communication Systems:
  1. Additive masking & Shift-keying
  2. Parameter modulation
  3. Cryptosystems
  4. Impulsive synchronization



Types of Chaos-based Secure Communication

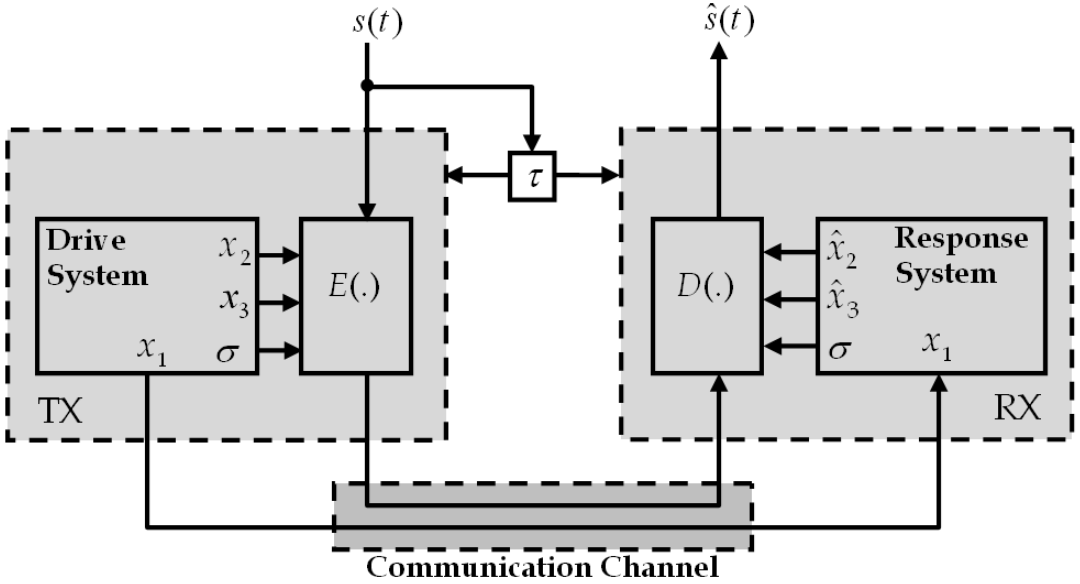
- Generations of Chaos-Based Secure Communication Systems:
  1. Additive masking & Shift-keying
  2. Parameter modulation
  3. Cryptosystems
  4. **Impulsive synchronization**



An example of chaos-based secure communication

1. Synchronization
2. Parameter update law
3. Encryption & Decryption

$$\tau\dot{x}_1 = -\sigma x_1 + \sigma x_2$$
$$\tau\dot{x}_2 = \rho x_1 - x_2 - x_1 x_3$$
$$\tau\dot{x}_3 = -\beta x_3 + x_1 x_2$$



$$E(X,\alpha,s,t) = x_1^2 + (\alpha^2 + x_1^2)s(t)$$
$$\hat{s}(t) = D(\hat{X},\hat{\alpha},s,t) = (E(X,\alpha,s,t) - \hat{x}_1^2)/(\hat{\alpha}^2 + \hat{x}_1^2)$$

(1) Achieving Synchronization

- **Observed States:** $$\dot{\hat{x}}_2 = \rho x_1 - \hat{x}_2 + x_1 \hat{x}_3$$ $$\dot{\hat{x}}_3 = -\beta \hat{x}_3 - x_1 \hat{x}_2$$

- **Error Dynamics:** $e_i = \hat{x}_i - x_i , i = 2,3$

- **Lyapunov Function:** $L_{23} = 0.5(e_2^2 + e_3^2)$

- **Verifying Stability:** $\dot{L}_{23} = (e_1 \dot{e}_1 + e_3 \dot{e}_3) = -(e_2^2 + \beta e_3^2) < 0$

(2) Identifying the secret key

- **Goals:**
  - ➢ **Decoupled from the synchronization process**
  - ➢ **Should have adjustable convergence rate**

$$\begin{aligned}\dot{\hat{x}}_1 &= -\hat{\sigma}\hat{x}_1 + \hat{\sigma}\hat{x}_2\\ \dot{\hat{x}}_2 &= \rho x_1 - \hat{x}_2 - x_1\hat{x}_3\\ \dot{\hat{x}}_3 &= -\beta\hat{x}_3 + x_1\hat{x}_2\end{aligned} \quad\Longrightarrow\quad \begin{aligned}e_i &= \hat{x}_i - x_i \text{ },i = 1,2,3\\ e_\sigma &= \hat{\sigma} - \sigma\end{aligned}$$

- **Error dynamics:**

$$\begin{aligned}\dot{e}_1 = \dot{\hat{x}}_1 - \dot{x}_1 &= (-\hat{\sigma}\hat{x}_1 + \hat{\sigma}\hat{x}_2) + (\sigma x_1 - \sigma x_2)\\ &= (-\hat{\sigma}\hat{x}_1 + \hat{\sigma}\hat{x}_2 + \hat{\sigma}x_1 - \hat{\sigma}x_2) + (\sigma x_1 - \sigma x_2 - \hat{\sigma}x_1 + \hat{\sigma}x_2)\\ &= \hat{\sigma}[(\hat{x}_2 - x_2) - (\hat{x}_1 - x_1)] + (\hat{\sigma} - \sigma)(x_2 - x_1)\\ &= \hat{\sigma}(e_2 - e_1) + e_\sigma(x_2 - x_1)\end{aligned}$$

$$\begin{aligned}\dot{e}_2 = \dot{\hat{x}}_2 - \dot{x}_2 &= (\rho x_1 - \hat{x}_2 - x_1\hat{x}_3) - (\rho x_1 - x_2 - x_1x_3)\\ &= -(\hat{x}_2 - x_2) - x_1(\hat{x}_3 - x_3)\\ &= -e_2 - x_1e_3\end{aligned}$$

$$\begin{aligned}\dot{e}_3 = \dot{\hat{x}}_3 - \dot{x}_3 &= (-\beta\hat{x}_3 + x_1\hat{x}_2) - (-\beta x_3 + x_1x_2)\\ &= -\beta(\hat{x}_3 - x_3) + x_1(\hat{x}_2 - x_2)\\ &= -\beta e_3 + x_1e_2\end{aligned}$$

(2) Identifying the secret key

- **Changes:**
  - **Modified Lyapunov function**
  - **Designing the parameter update law**

$$L = 0.5[e_1^2 + \mu_{23}(e_2^2 + e_3^2) + \mu_\sigma e_\sigma^2]$$

$$\begin{aligned}\dot{L} &= e_1\dot{e}_1 + \mu_{23}e_2\dot{e}_2 + \mu_{23}e_3\dot{e}_3 + \mu_\sigma e_\sigma \dot{e}_\sigma \\ &= (\hat{\sigma}e_1e_2 - \hat{\sigma}e_1^2 + x_2e_1e_\sigma - x_1e_1e_\sigma) - (\mu_{23}e_2^2 + \mu_{23}x_1e_2e_3) + (\mu_{23}x_1e_2e_3 - \mu_{23}\beta e_3^2) + \mu_\sigma e_\sigma \dot{\hat{\sigma}} \\ &= -(\hat{\sigma}e_1^2 - \hat{\sigma}e_1e_2 + \mu_{23}e_2^2) - \mu_{23}\beta e_3^2 + e_\sigma[e_1(x_2 - x_1) + \mu_\sigma \dot{\hat{\sigma}}]\end{aligned}$$

$$\mu_{23} = \frac{\hat{\sigma}}{4}, 0 \le \hat{\sigma} \le \sigma_{\max}$$

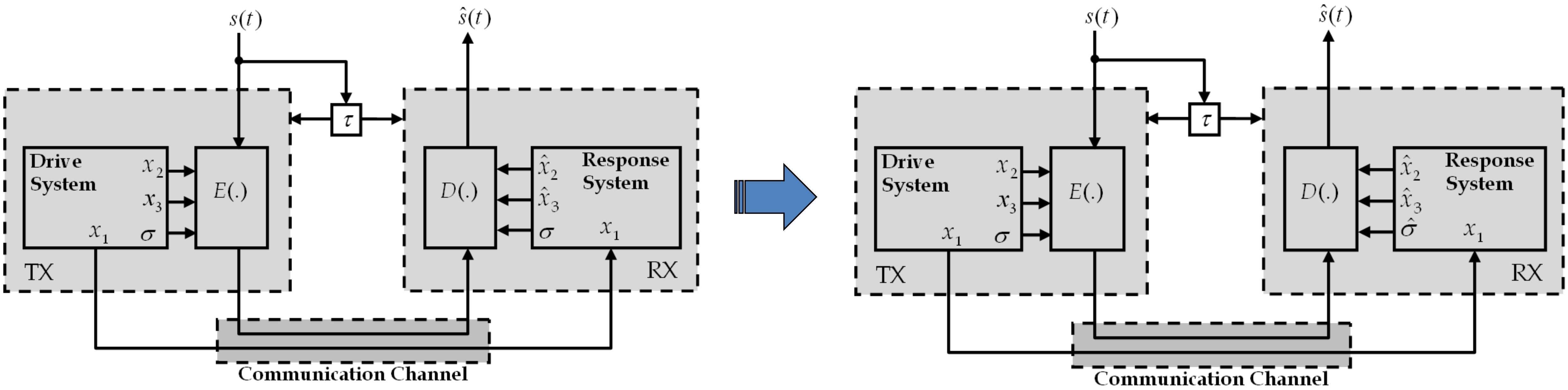
$$\dot{\hat{\sigma}} = -\frac{1}{\mu_{23}}(x_2 - x_1)e_1 = -\frac{1}{\sigma\mu_{23}}e_1\dot{x}_1 = k\dot{x}_1(x_1 - \hat{x}_1)$$

$$\dot{L} = -[(\sqrt{\hat{\sigma}}e_1)^2 - 2\sqrt{\hat{\sigma}}\frac{\sqrt{\hat{\sigma}}}{2}e_1e_2 + (\frac{\sqrt{\hat{\sigma}}}{2}e_2)^2] - \frac{\hat{\sigma}}{4}\beta e_3^2 = -(\sqrt{\hat{\sigma}}e_1 - \frac{\sqrt{\hat{\sigma}}}{2}e_2)^2 - \frac{\hat{\sigma}}{4}\beta e_3^2 \le 0$$

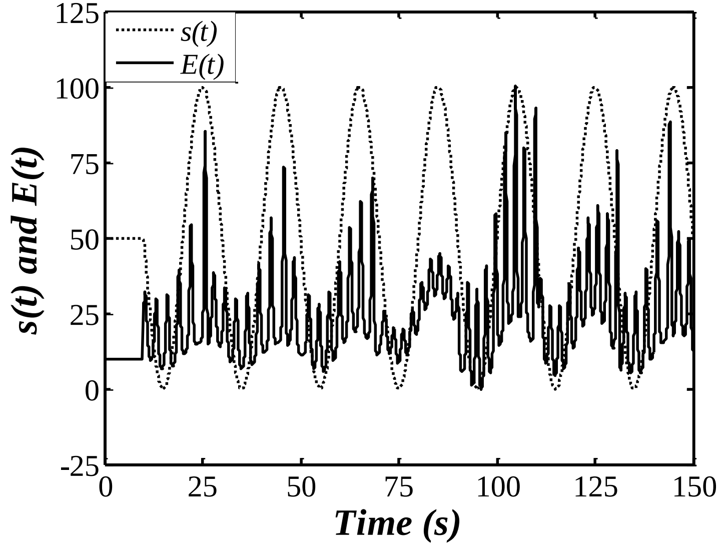
(3) Encryption & Decryption

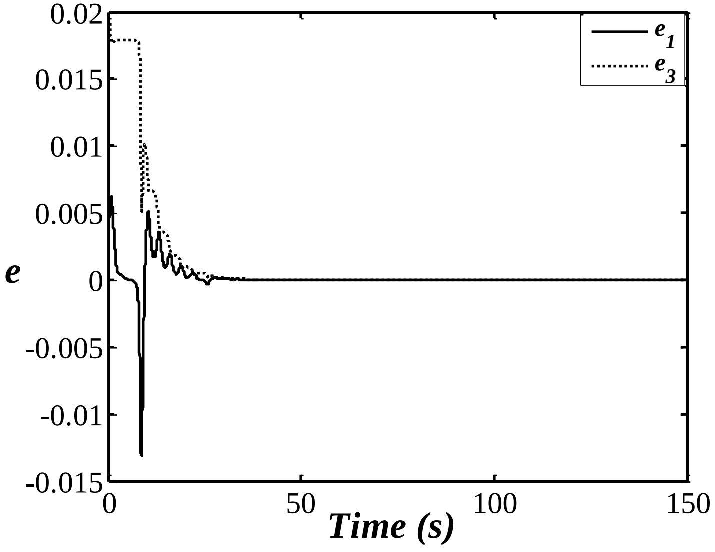
$$E(X,\alpha,s,t) = x_1^2 + (\alpha^2 + x_1^2)s(t)$$

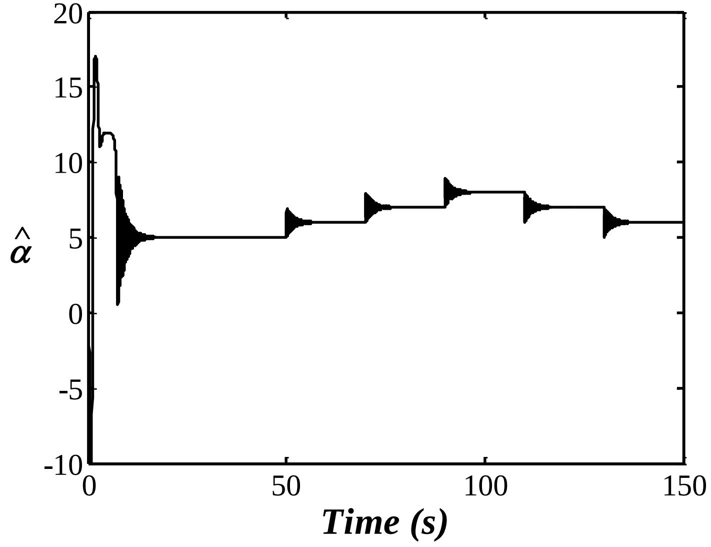
$$\hat{s}(t) = D(\hat{X},\hat{\alpha},s,t) = (E(X,\alpha,s,t) - \hat{x}_1^2)/(\hat{\alpha}^2 + \hat{x}_1^2)$$

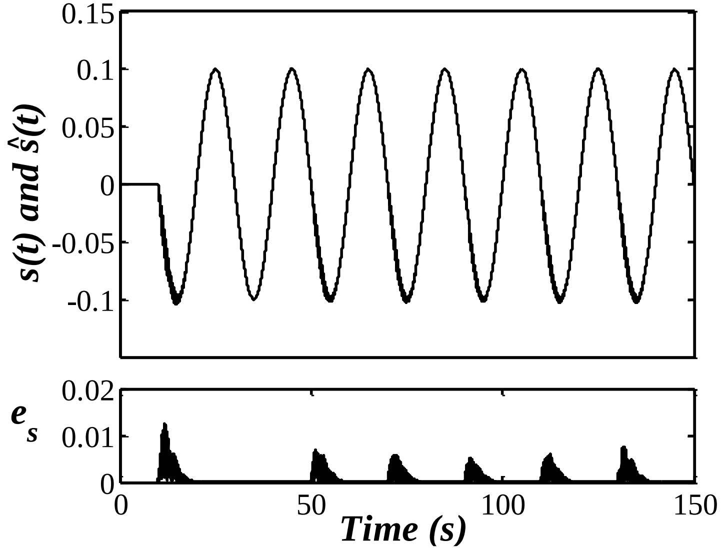


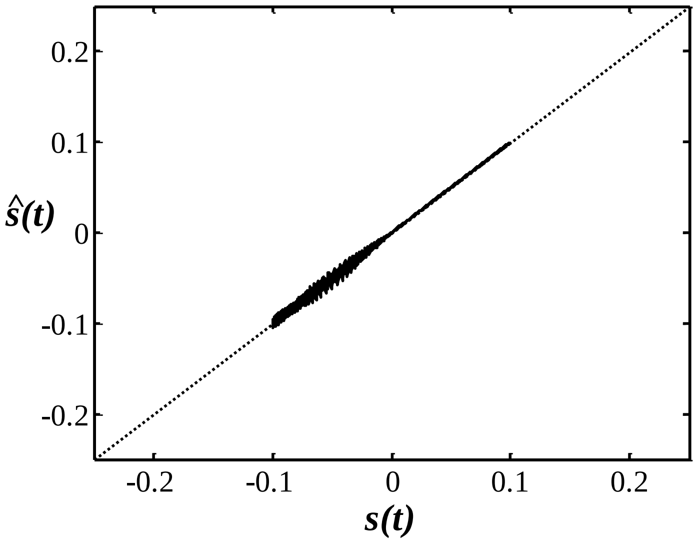
Simulation Results

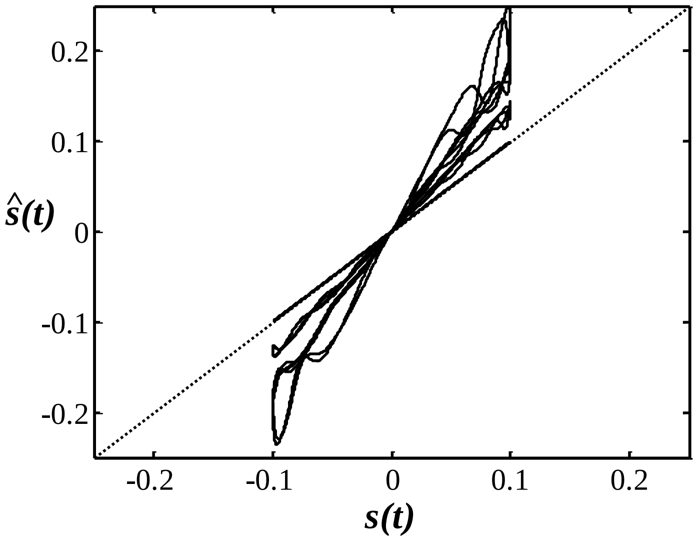




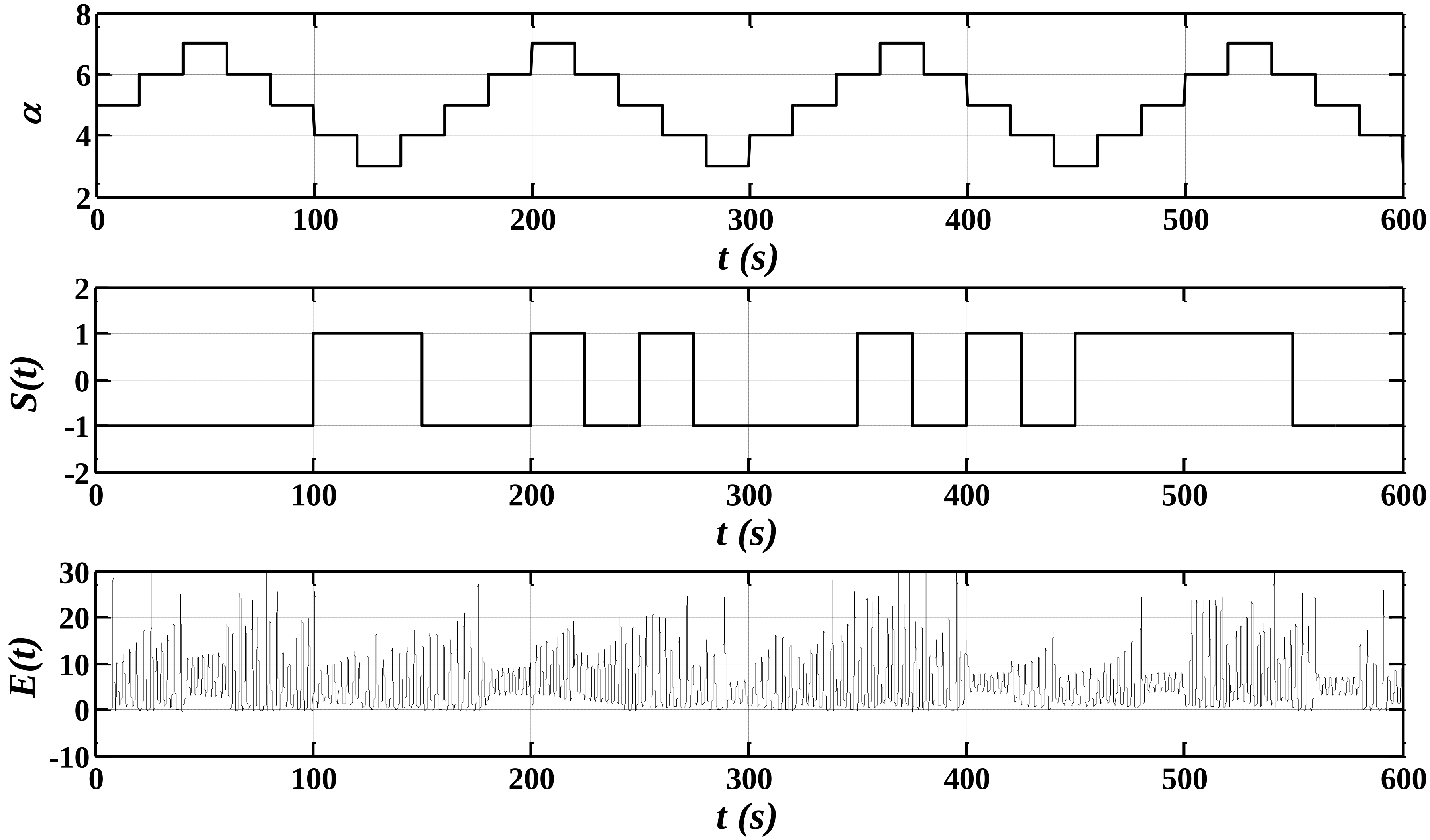




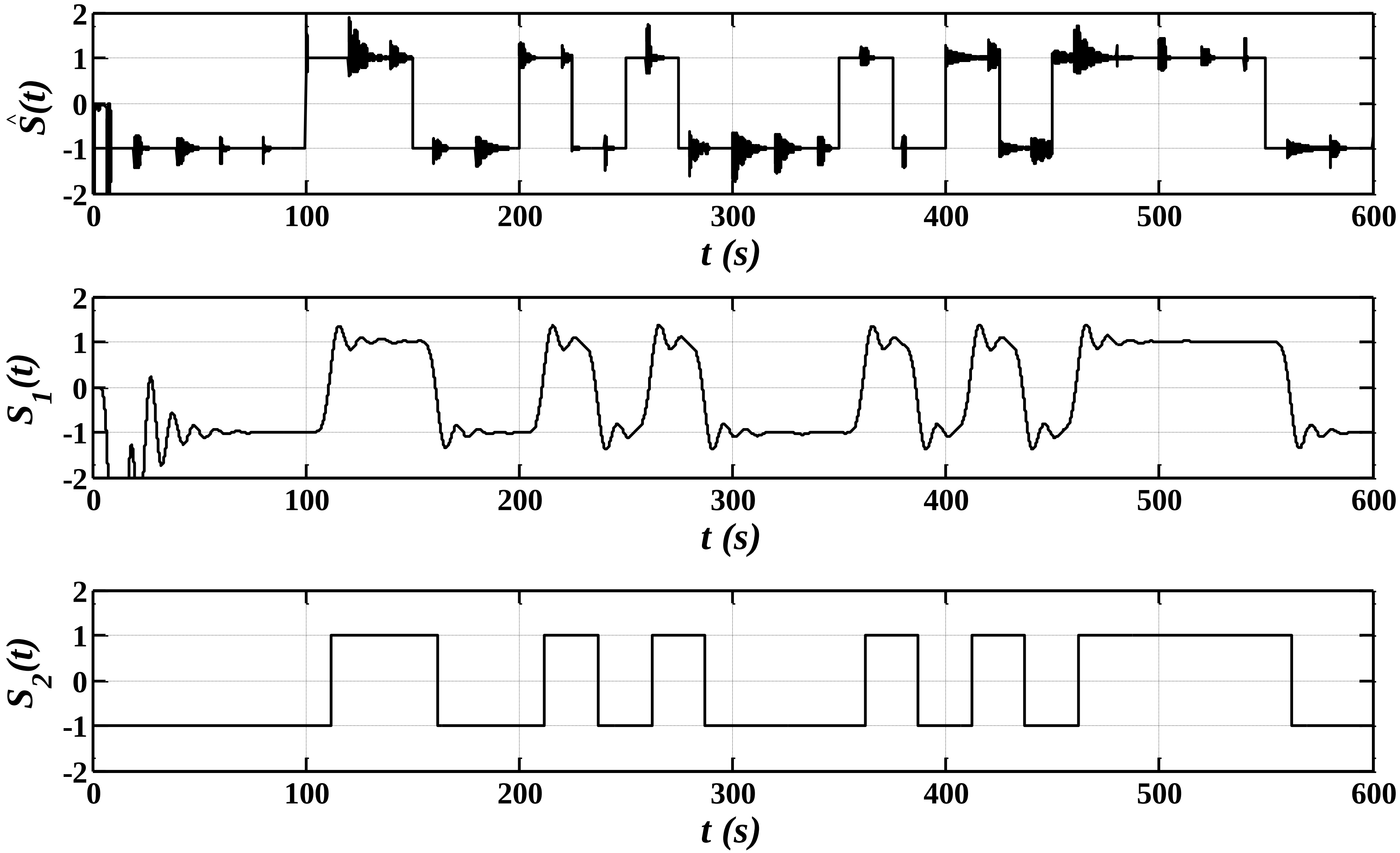




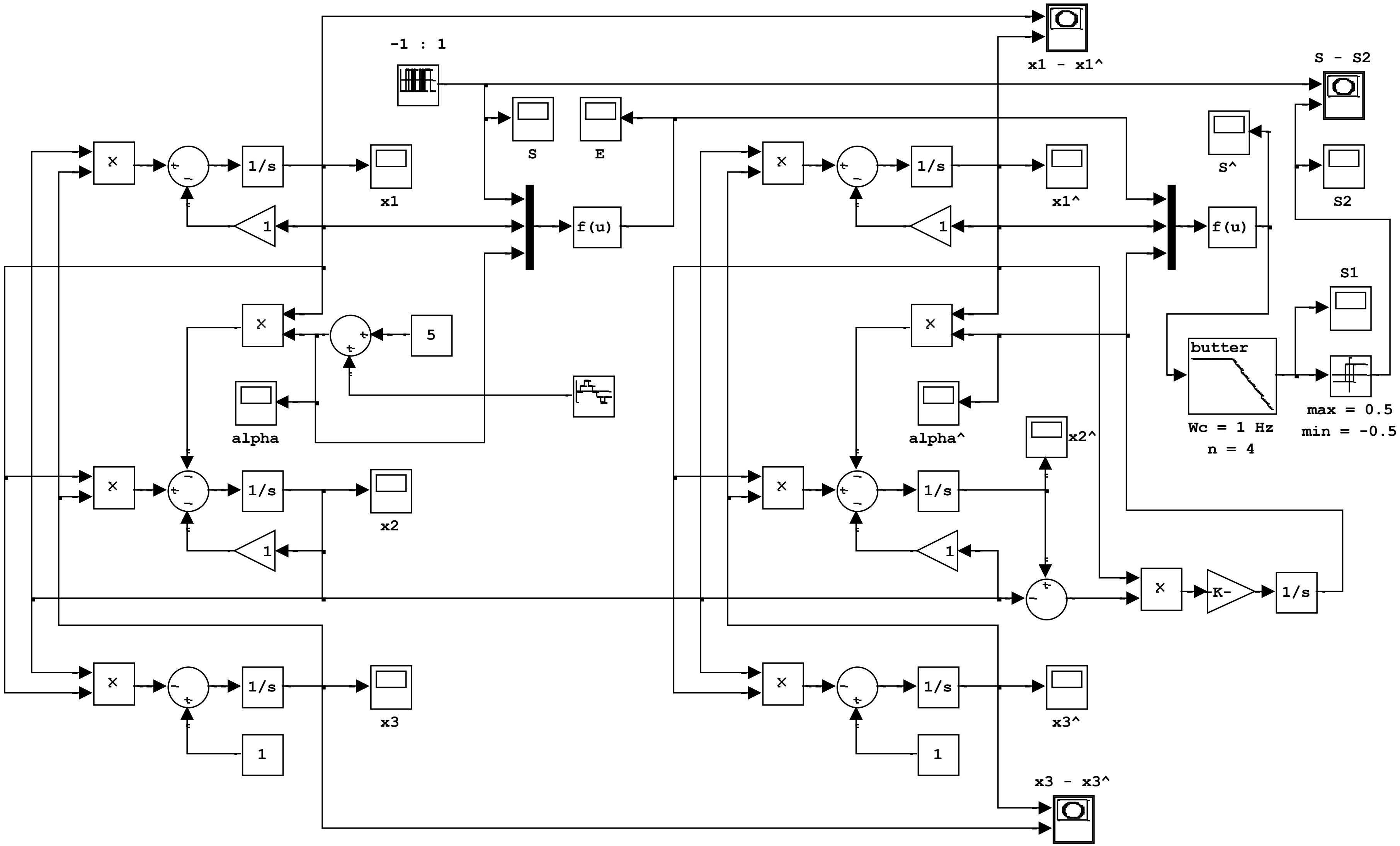
Simulation Results



Simulation Results



Simulation Results



Current Practices and Future Trends

❑ Theory and applications:

- ➢ Hyperchaotic systems
- ➢ Nature of the system
- ➢ Different Signals
- ➢ Real-time vs. offline operation
- ➢ Analog vs. digital implementation
- ➢ Adaptive techniques

❑ Impact on research:

- ➢ Multidisciplinary teams
- ➢ Revolutionary implementations
- ➢ Quantum chaos
- ➢ Compatibility with networks protocols
- ➢ Usage of bandwidth

Thank you very much

Q/A