Communication and secrecy with chaos

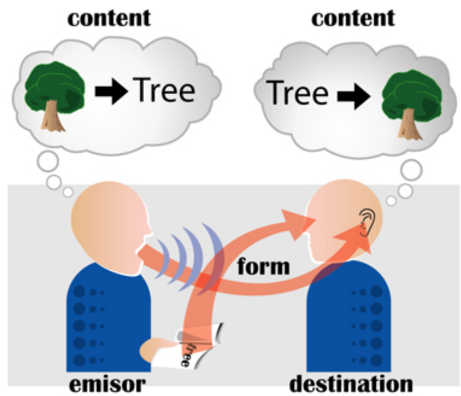
Murilo S. Baptista

University of Aberdeen

Institute for Complex Systems and Mathematical Biology

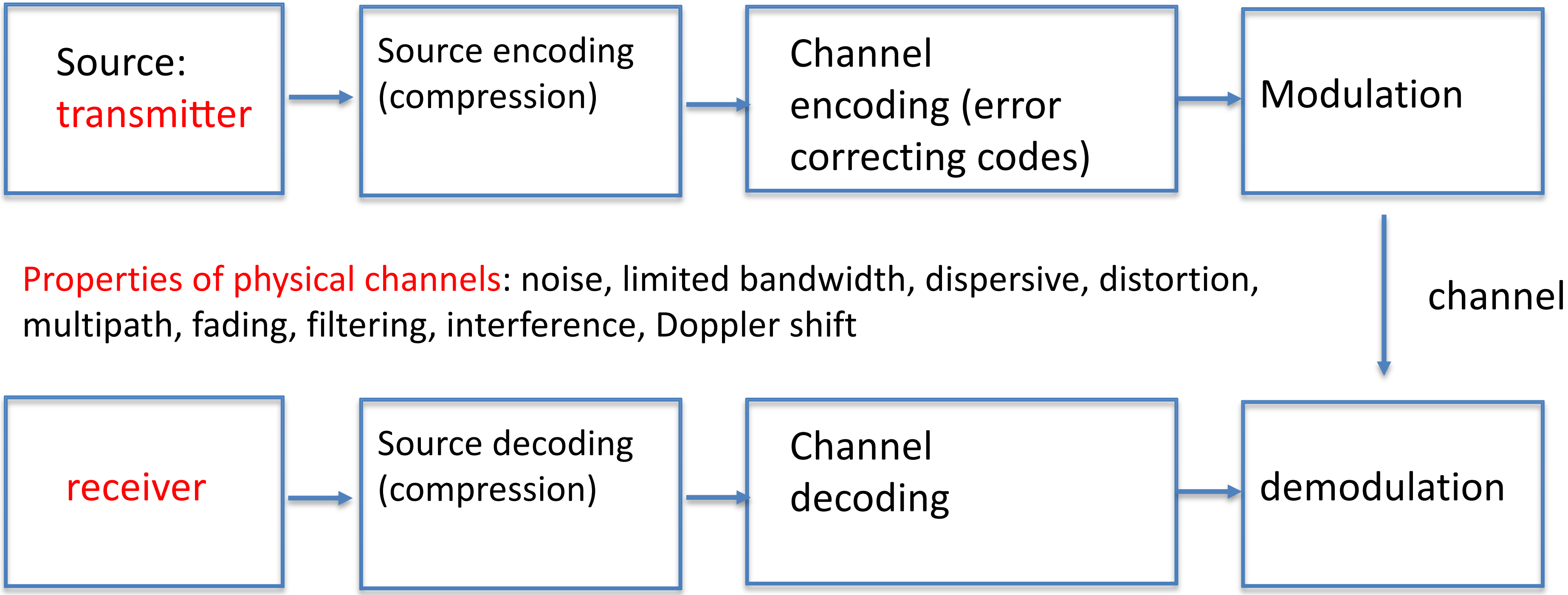
What is communication?

- **Communication** (from Latin *commūnicāre*, meaning "to share”) is the act of conveying intended meanings from one entity or group to another through the use of mutually understood signs and semiotic rules [Wikipedia].



- Technological communication systems use signals to transmit information throughout physical media (a channel).
  - The physical channel has finite bandwidth, thus limiting the rate of information hat can be transmitted → redundant information needs to be eliminated (source encoding);
  - The physical channel distorts the information, thus error corrector codes needs to be implemented → redundant information needs to be added (channel encoding) to allow full recovery of information
  - The physical channel might require specific waveforms → modulation might be necessary

Block diagram of a digital communication system



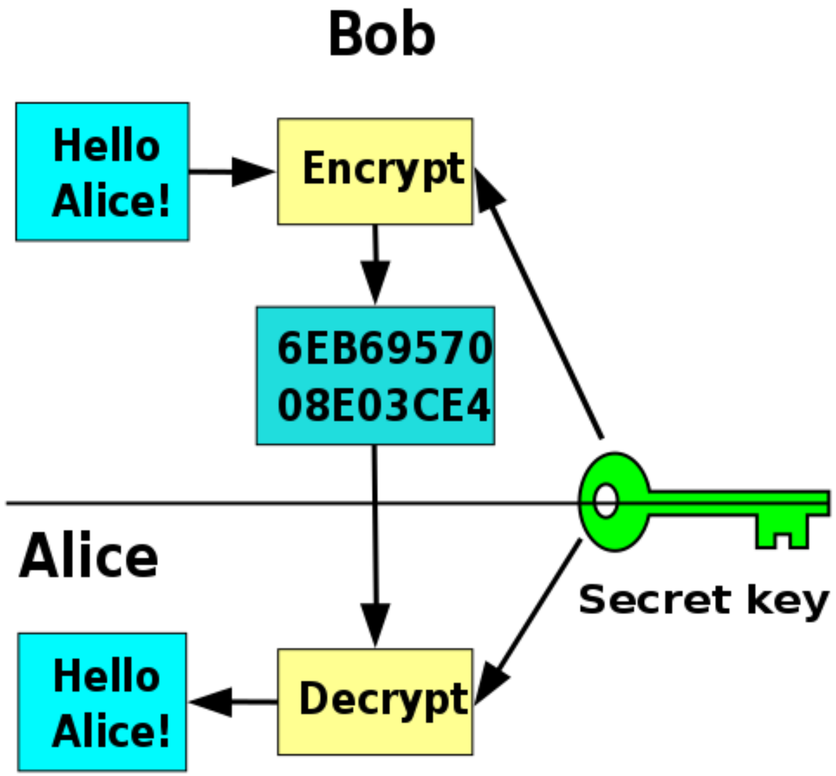
Properties of physical channels: noise, limited bandwidth, dispersive, distortion, multipath, fading, filtering, interference, Doppler shift

Standard digital communication requires several protocols to let communication to happen

What is cryptography

- Approaches to secure communication in the presence of an adversary

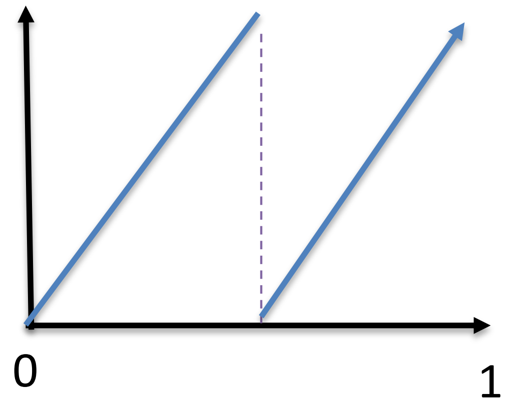
➢ Symmetric-key cryptography: refers to encryption methods in which both the sender and receiver share the same key



Wikipedia

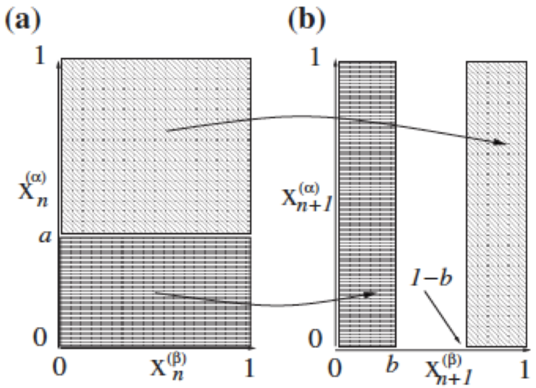
Chaotic systems - maps

Shift map: $x_{n+1} = 2x_n \,, mod\ 1$



Baker's map

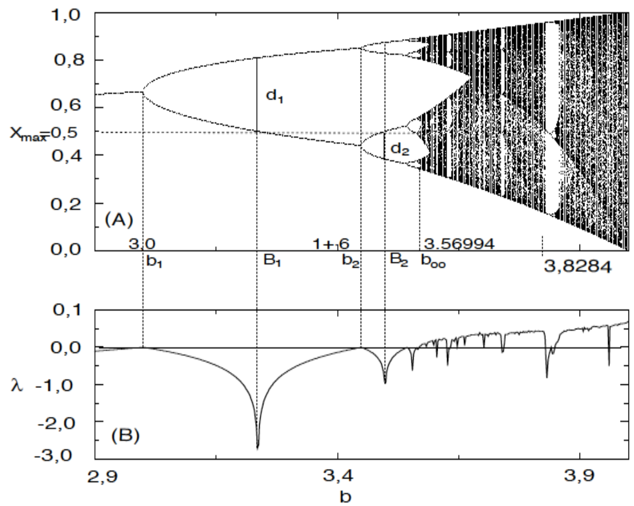
TRANSMISSION OF INFORMATION IN ACTIVE NETWORKS



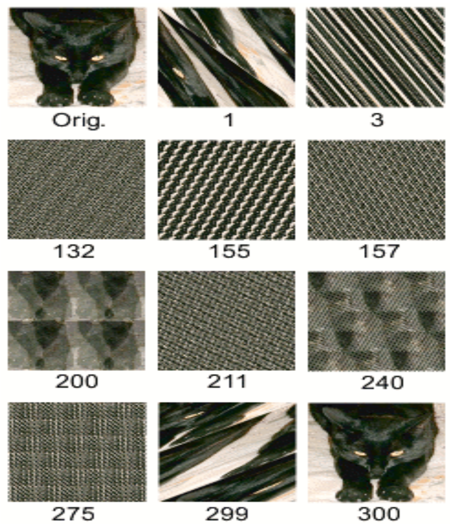
PHYSICAL REVIEW E 77, 026205 2008

Logistic map

$$x_{n+1} = \mathrm{b}\mathrm{x}_\mathrm{n}(1 - \mathrm{x}_\mathrm{n})$$

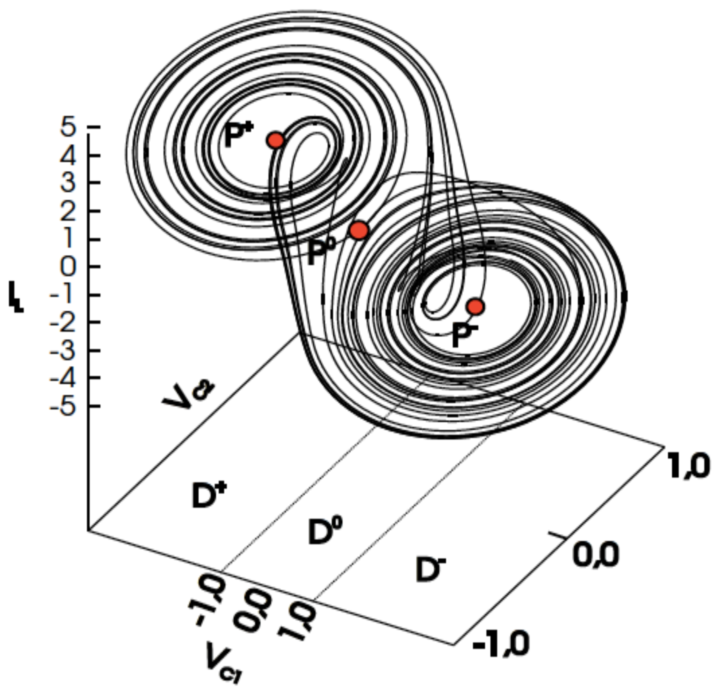


Arnold cat map (discrete version), N goes in the mod function. Also shown bellow. Image returns at N.

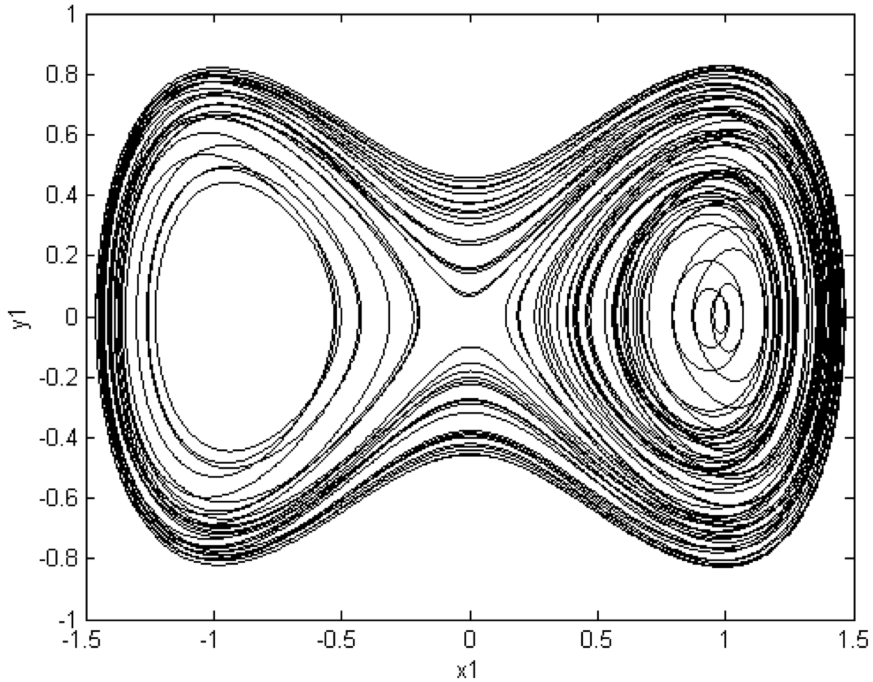


Chaotic systems – flows

Chua's circuit



A spatio-temporal convective cell



Vidal & Mancini, Int. J. Bif. and Chaos **30**, 749 (2010)

Defining chaos – sensibility to the initial conditions

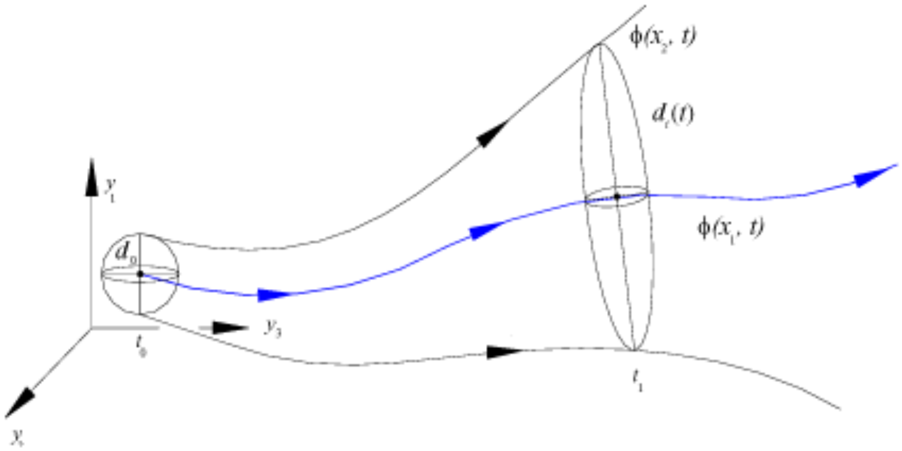
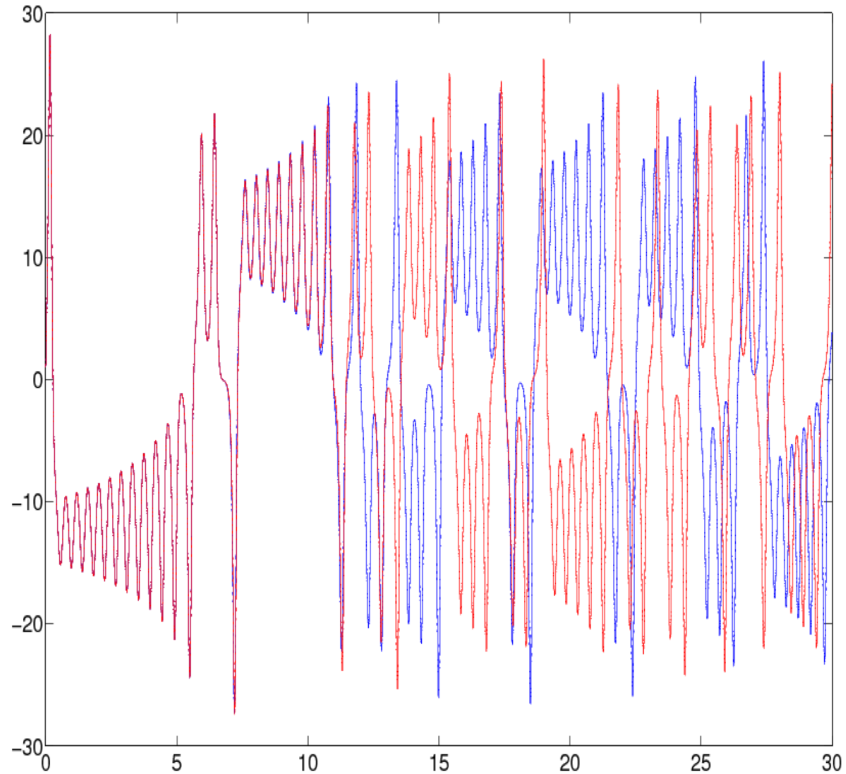


Figure 10. Estimation of Lyapunov exponents.

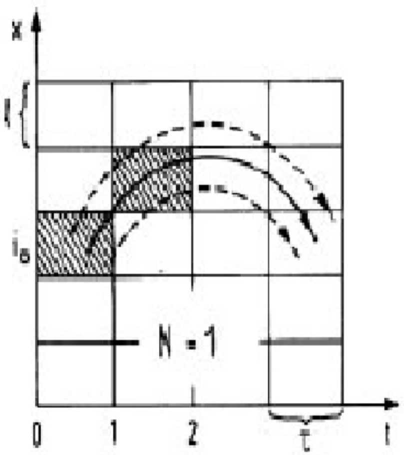
M. Savi, J. Braz. Soc. Mech. Sci. & Eng. vol.27 (2005).



Lyapunov exponent: $\lambda = \frac{1}{t}\log\left\{\frac{d_i(t)}{d_0}\right\}$

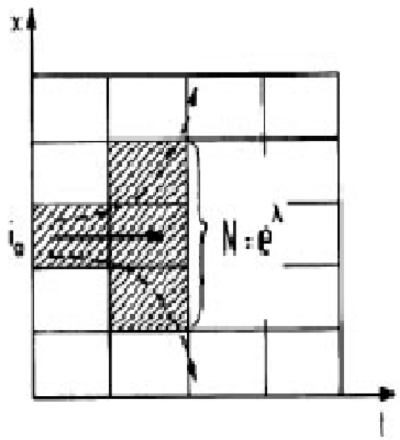
Chaos, KS-entropy and Mutual Information Rate

Regular motion



Initially adjacent points stay adjacent
$P_{i_0} = l,\ P_{i_0 i_1} = l \cdot 1$
$K = 0$

Chaotic motion

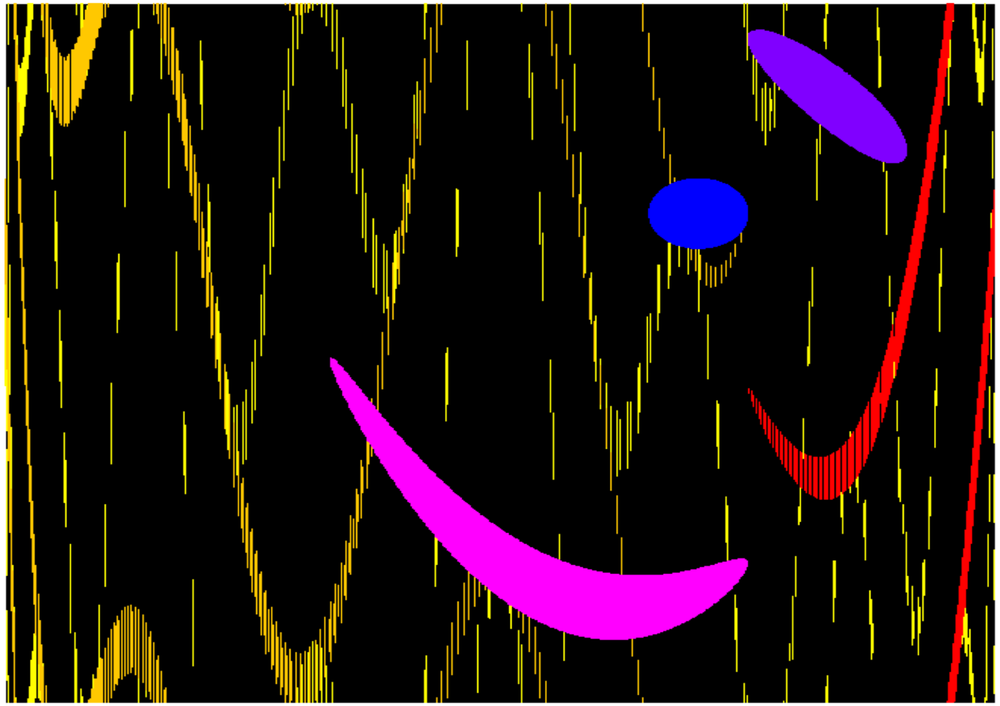


Initially adjacent points become exponentially separated
$P_{i_0} = l,\ P_{i_0 i_1} = l\,\mathrm{e}^{-\lambda}$
$K = \lambda > 0$

- Pesin's equality: $K = \sum^{+} \lambda_i$
- Ruelle's inequality: $K \leq \sum^{+} \lambda_i$
- Baptista's upper bound for MI:

  $I_c \leq \lambda_1 - \lambda_2$

Defining chaos : Transitive

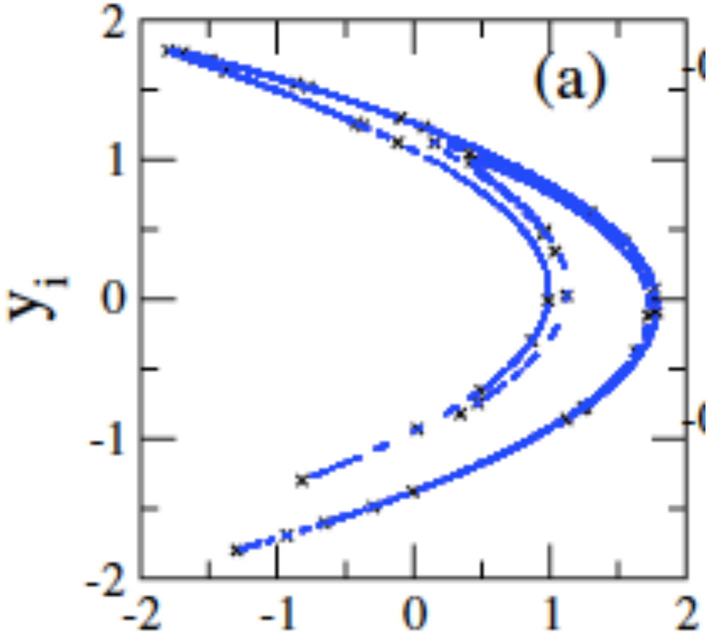


wikipedia

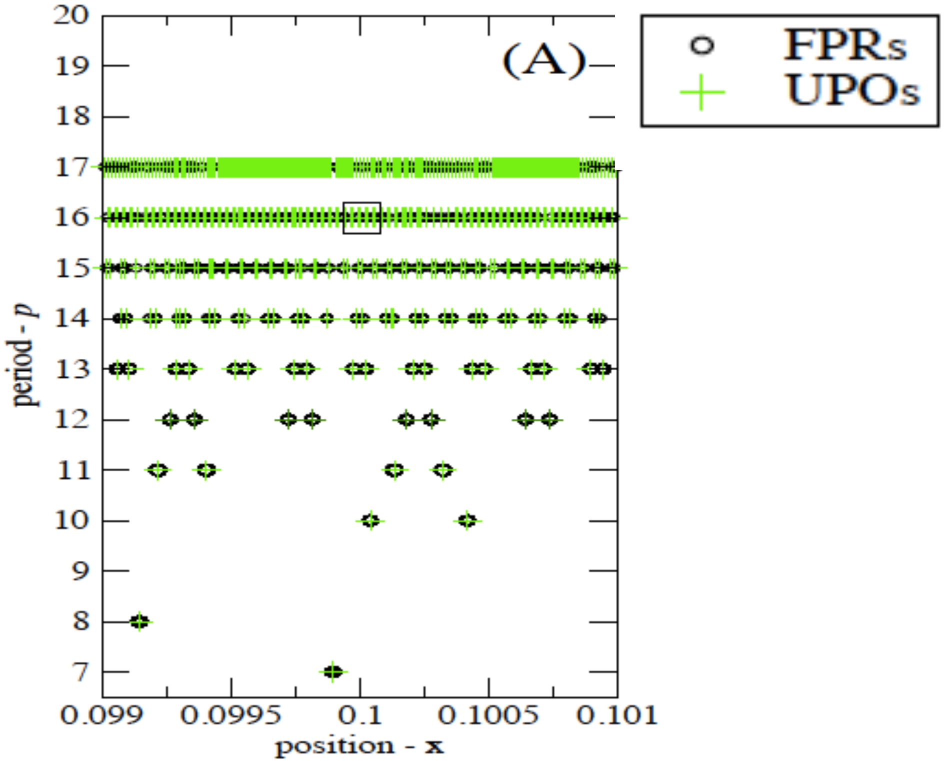
Chaos is transitive, and therefore recurrence is to be expected

Poincare Recurrence Theorem: states that certain systems will, after a sufficiently long but finite time, return to a state very close to the initial state.

Defining chaos: dense periodic orbits



Baptista, Phys. Rev. Lett., 95, 094101 (2005)

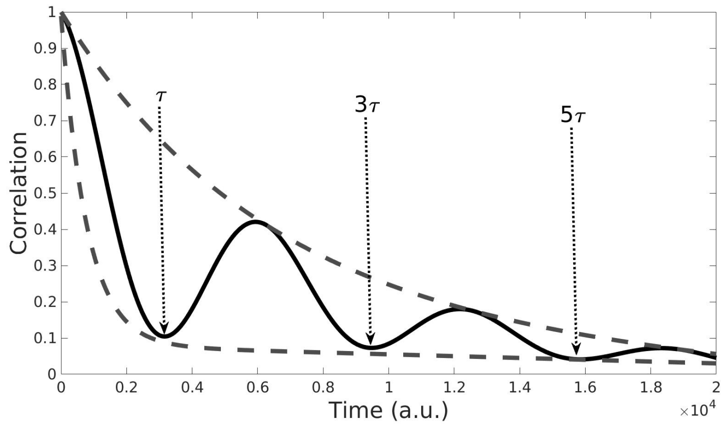


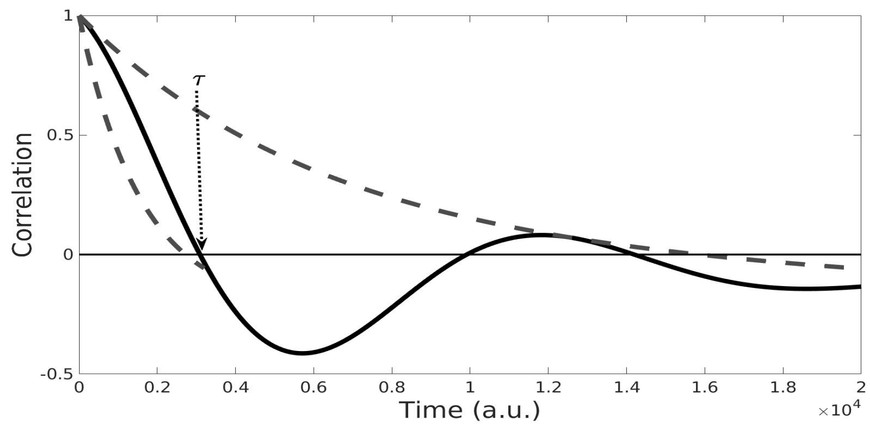
Pinto, Baptista, Laborial, Commun Nonlinear Sci Numer Simulat **16,** 863 (2011).

Decay of correlation

$$C_{\Psi,\phi}(n) = \int_I \phi\big(f^n(x)\big)\Psi(x)d\mu - \int_I \phi(x)\,d\mu \int_I \Psi(x)d\mu\,,$$

$$C_{A,B}(n) = \mu\big(A \cap f^{-n}(B)\big) - \mu(A)\mu(B),$$

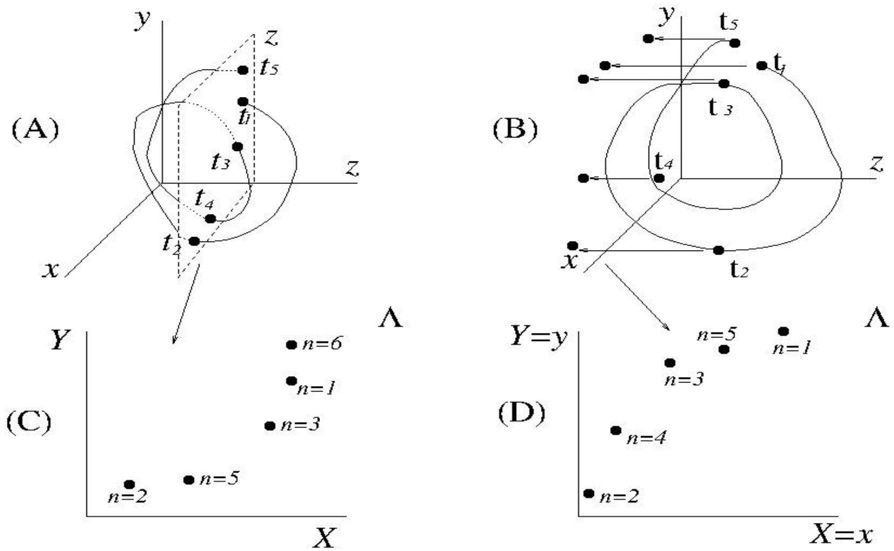


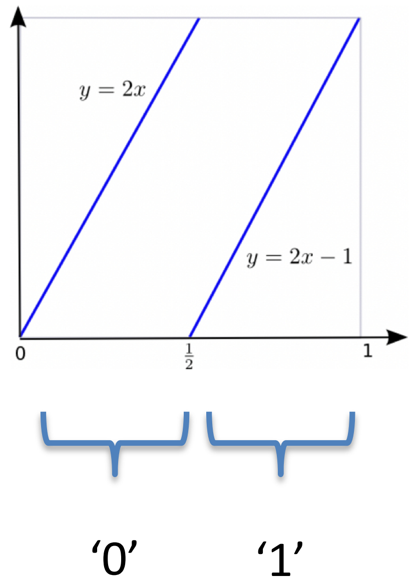


As the correlation decays, the mutual information decays as well as.

Chaotic source (digital) encoding: find a Markov generating partition [E.Bollt, "Markov Partitions"]

- One needs to discretize the trajectory by making a map





Often, one needs to work with an approximate Markov partition:

- Rubido, Grebogi, Baptista, CHAOS 28, 033611 (2018).

Chaos introduces a constraint to the communication system

- Similarly to the physical channel that has an information capacity, the capacity to transmit information using an unperturbed chaotic system is given by the sum of the positive Lyapunov exponents (Shannon's entropy of unstable periodic orbits per time unit).
- Digital encoding limited to the symbolic sequence of the UPOs

The raise of Communication with Chaos

VOLUME 64, NUMBER 8 PHYSICAL REVIEW LETTERS 19 FEBRUARY 1990

[12014 citations]

Synchronization in Chaotic Systems

Louis M. Pecora and Thomas L. Carroll

- [2124 citations] Cuomo, K. M. and Oppenheim, A. V. "Circuit implementation of synchronized chaos with applications to communications" *Phys. Rev. Lett.* **71**, 65 (1993).
- [697 citations] Hayes, S., Grebogi, C. & Ott, E. 'Communicating with chaos'. *Phys. Rev. Lett.*, **70**, 3031 (1993).

[8134 citations] OTT, E., GREBOGI, C. & YORKE, JA. (1990). 'Controlling chaos'. *Physical Review Letters*, vol 64, no. 11, pp. 1196-1199.

The raise of Communication with Chaos

VOLUME 64, NUMBER 8 PHYSICAL REVIEW LETTERS 19 FEBRUARY 1990

Synchronization in Chaotic Systems

Louis M. Pecora and Thomas L. Carroll

Given two coupled systems represented by the state variables $\overrightarrow{x_t}$ and $\overrightarrow{y_r}$ (transmitter and receiver), complete synchronization is defined by:

$$\overrightarrow{x_t} = \overrightarrow{y_r}$$

The ability to design synchronizing systems in nonlinear and, especially, chaotic systems may open interesting opportunities for applications of chaos to communications, exploiting the unique features of chaotic signals.

Recent interesting results[13,14] suggest the possibility of extending the synchronization concept to that of a metaphor for some neural processes. Freeman has suggested

Cuomo and Oppenheim method

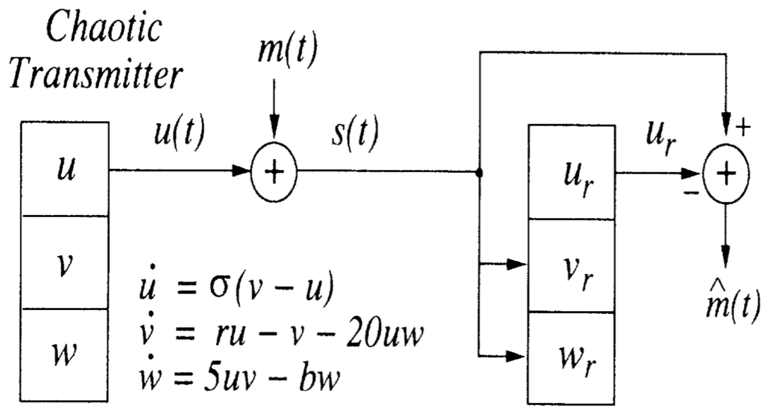


FIG. 5. Chaotic signal masking system.

$$\dot{u}_r = 16(v_r - u_r)\,,$$

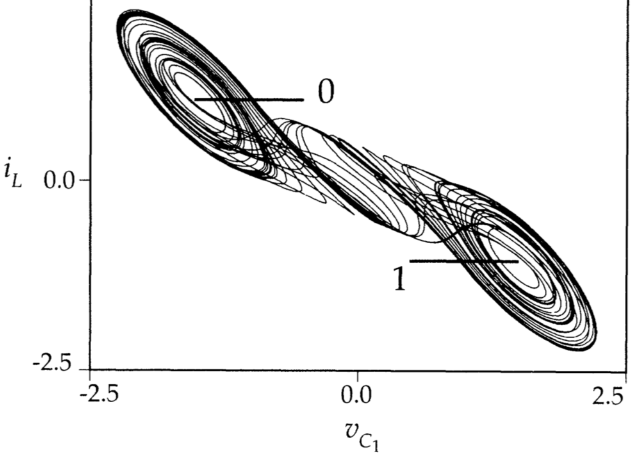
$$\dot{v}_r = 45.6s(t) - v_r - 20s(t)w_r\,,$$

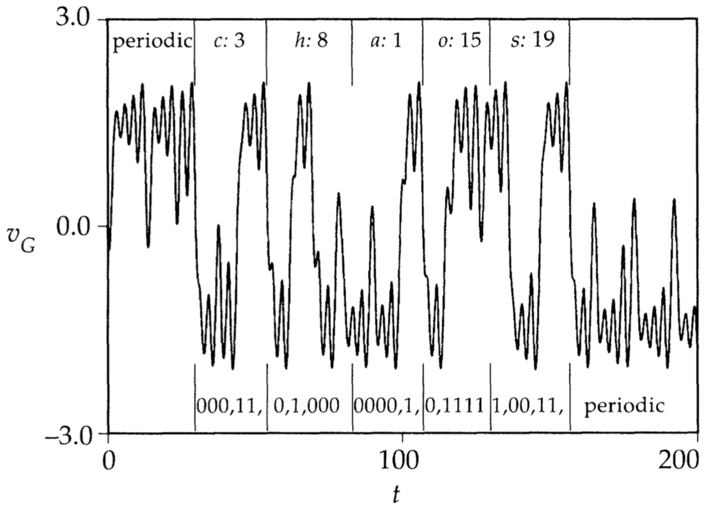
$$\dot{w}_r = 5s(t)v_r - 4w_r\,.$$

- Power of message m(t) significantly smaller than u(t)
- “Decoding” can be realized by making $s(t)-u_r$.

- This work has raised the possibility of having a communication system that would naturally provide security, given the entropic unpredictable nature of chaos.
- It would also be robust to noise due to the aperiodic broadband nature of chaos
- However, method was shown to be insecure, since dynamics of transmitter can be fully reconstructed. Noise could also destroy synchronization.
- Extracting message can be done even without reconstruction of attractor as shown by Pérez and Cerdeira, Phys. Rev. Lett. 74 1970 (1995).

Hayes, Grebogi, Ott, Communicating with chaos, PRL (1993)





- Small perturbations can be used to control the future state of a chaotic trajectory. Chaos has flexibility to do the source encode!

- Capacity to encode using chaos (in the ideal channel) is not any longer provided by the Shannon's entropy (given by the probability with which UPOs appear, or their symbolic sequences), but by the topological entropy, i.e., calculated by the number of different UPOs

Parlitz and co-authors (1994)

- General Approach for Chaotic Synchronization with Applications to Communication", Phys. Rev. Lett. **74**, 5028 (1995) -> method worked on the basis of splitting the dynamics and into passive and active subsystems.
- Robust communication based on chaotic spreading sequences, Phys. Lett. A, **188** 146 (1994) :
  - does chaos create efficient masking and encoding system that transmit reliably information (i.e., small errors) in the presence of external influences (e.g., noise in the channel)?
  - chaotic signal: x_n
  - Binary message: $b_k \in [-1,1]$
  - Transmitted signal: $\mathrm{s_n} = x_n b_k + e_n$
    - e_n is noise
  - "Decoding" done by correlating $\mathrm{s_n}$ with x_n(needs to be known!)

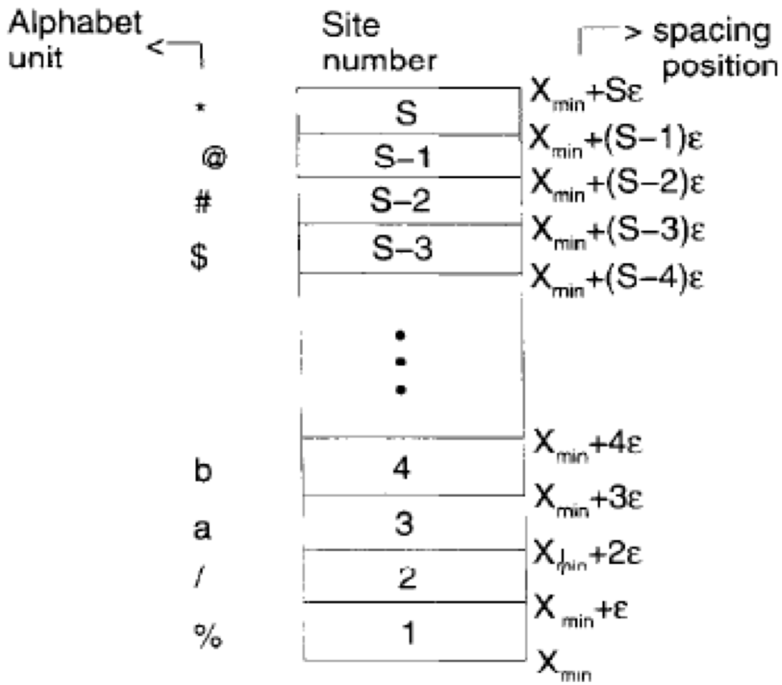
Security in chaos, by 1996 and in Maryland

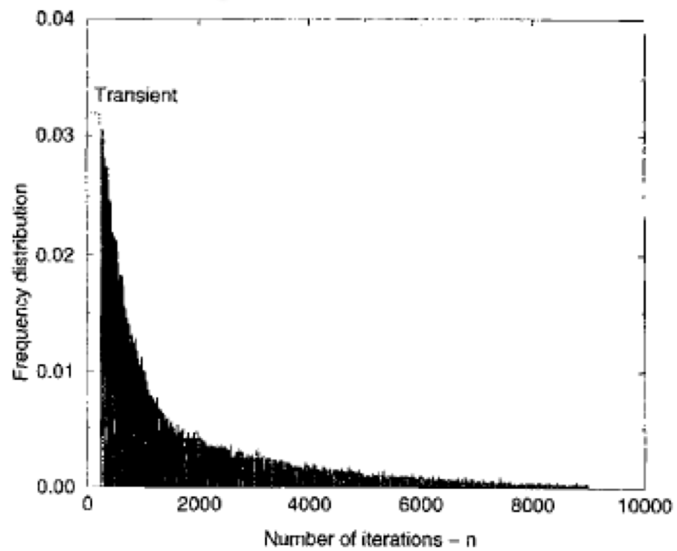
- Chaotic signals are deterministic, and therefore may contain full information about dynamical system generating it, allowing also determination of the initial conditions (a typical secret key).
- Communication by chaotic wavesignals providing simultaneously security seemed not to be possible.

I had just arrived for my post-doc at the University of Maryland….

Cryptography with chaos

- Over a pint in a pub close to my hotel, had the idea that one use as should just send a function of the trajectory that is naturally de-correlated: Return Times (not the first)





The state of the art of cryptography with chaos by M. Jeaneth Machicao, PhD Thesis

Tabela 2 – Estado da arte do caos, criptografia e a pseudo-aleatoriedade ao longo dos anos.

1986	Wolfram usou o autômato celular elementar com regra 30 como sistema criptográfico. (105) Atualmente a linguagem de programação Wolfram Mathematica usa esta mesma estratégia. (180)
1989	Matthews (106), propus o primeiro PRNG baseado no mapa logístico com propósitos de criptografia.
1989	Wheeler (107), quebrou o algoritmo de Matthews (106) ao encontrar certa degradação nele.
1991	Wheeler & Matthews (108), juntaram esforços para propor um novo algoritmo de encriptação caótico.
1991	Habutsu et al. (109), propuseram um cifrador de bloco baseado no mapa da tenda.
1991	Biham (110), quebrou o algoritmo do Habutsu et al. (109), por meio do um ataque de texto cifrado.
1998	Baptista (111), propus um algoritmo de encriptação usando o mapa logístico aproveitando da propriedade de transitividade.
1999	Álvarez et al. (112), propuseram um algoritmo de encriptação usando o mapa da tenda.
2000	Álvarez et al. (113), quebraram o próprio algoritmo proposto em 1999. (112)
2001	Shujun Li et al. (114), melhoraram o algoritmo de Álvarez et al. (112) contra a criptoanálise.
2001	W. Wong et al. (115), propuseram uma otimização do algoritmo do Baptista. (111)
2002	K. Wong (116), propus uma outra variante no algoritmo do Baptista (111) usando tabela dinâmica.
2003	Álvarez et al. (117) quebraram o algoritmo do Baptista. (111)
2004	Álvarez et al. (118) quebrou o algoritmo do W. Wong et al. (115) No mesmo ano, o mesmo time Álvarez et al. (119) também quebraram o algoritmo de K. Wong. (116)
2006	Addabbo et al. (120), propus um PRNG baseado no mapa da tenda.
2009	Patidar et al. (121) propuseram um PRNG baseado no mapa logístico.
2009	Ali & Nejib (122) estudaram o mapa logístico como um PRNG.
2009	Cecen et al. (123) também estudaram ao mapa logístico, e aprofundaram na análise da região $\mu = [3.5599, 4)$.
2010	Pareek et al. (124) usaram a combinação de dois mapas da tenda com diferentes parâmetros acoplados.
2010	Marco et al. (125) propuseram um algoritmo de encriptação baseado no atrator de Lorenz.
2011	Dabal & Pelka (127) propuseram um sistema criptográfico baseado no mapa logístico usando $\mu = 4$ implementado em FPGA.
2011	Machicao et al. (51), propuseram um algoritmo criptografia baseada nas propriedades caóticas do autômato celular da família *Life-Like*.
2011	Behnia et al. (128) propuseram um PRNG baseado numa generalização do mapa logístico. Nesse mesmo trabalho criticaram as falhas do mapa logístico original.
2011	Addabbo et al. (129) fizeram uma revisão dos principais CB-PRNGs e propuseram um gerador baseado na congruência não linear.
2011	Luca et al. (130) analisaram o mapa da tenda como PRNG.
2012	Li et al. (131) propuseram uma melhora no gerador usando o mapa logístico por meio de reinserção de sementes (condição inicial).
2012	Persohn & Povinelli (132) estudaram a periodicidade do mapa logístico como PRNG como consequência da precisão finita.
2013	Lequan et al. (133) fizeram uma análise comparativa dos principais PRNGs da literatura.
2014	François et al. (134) propuseram um PRNG baseado na combinação de três mapas caóticos.
2015	Machicao et al. (7) encontraram padrões nos modos de operação usados pelos sistemas criptográficos.
2017	Machicao & Bruno (135), melhoraram a pseudo-aleatoriedade do mapa logístico (proposta desta tese).

Fonte: Elaborada pela autora.

Not the first, but the first to explore an ergodic property of chaos that is suitable for encryption.

Chaos Naturally offers the advantages of digital communication, but with integrated protocols

- (year 2000) Chaos can offer an integrated communication system that does compaction, cryptography, is robust to noise, provides dropout robustness (due to chaos redundancy and determinism), and also offers multiplexing: Baptista et al., Phys. Rev. E, Phys. Rev. E **62**, 4835 (2000).

- (year 2002) Moreover, in low-noise physical non-ideal channels, the channel capacity of a chaos-based communication systems does not depend on the noise level, but rather on the system's Kolmogorov-Sinai entropy: Baptista and Lopez, Phys. Rev. E, Phys. Rev. E **65**, 055201(Rapid Communication) (2002).

Non-ideal channels: limited bandwidth

- There was great recognition that chaos-based communication needs to tackle non-ideal channels of communication

  - Works have shown that filtering chaotic signals to fit the available bandwidth of the channel does not disturb synchronization:
    - Rulkov and Tsimring, Int. J. of Circuit Theory and Applications **27**, 555 (1999).
    - Eisencraft and Gerken, in: Anais do XVIII Simpósio Brasileiro de Telecomunicações, Gramado, Brasil, 2001

- Recent extensions to maps and to digital communication systems based on sync from filtered signals recently done by Eisencraft and collaborators in

  - Commun Nonlinear Sci Numer Simulat, **17** 4707 (2012).
  - Commun Nonlinear Sci Numer Simulat, **37** 374 (2016).

- Symbolic sequence of filtered signals can be recovered: Int. J. Bif. and Chaos, **22**, 1250199 (2012).

From 2000 on there is a surge of works in cryptography with chaos.

- Can chaos be as good as Quantum Cryptography?
- In Vidal, Baptista, Mancini, Int. J. Bif. and Chaos, 22, 1250243 (2012), we have shown that classical chaos-based cryptography inherits naturally properties of quantum cryptosystems

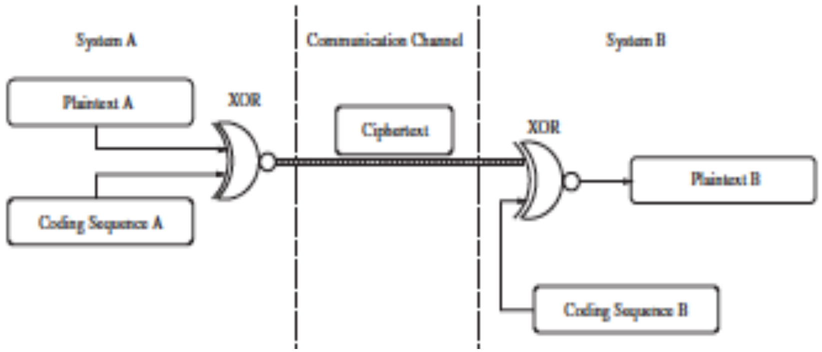
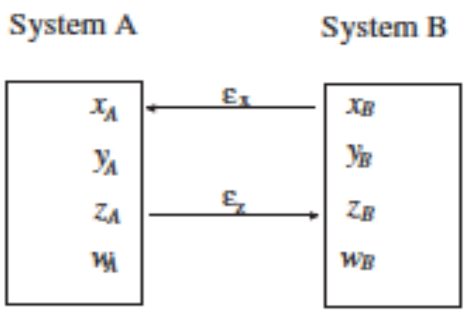
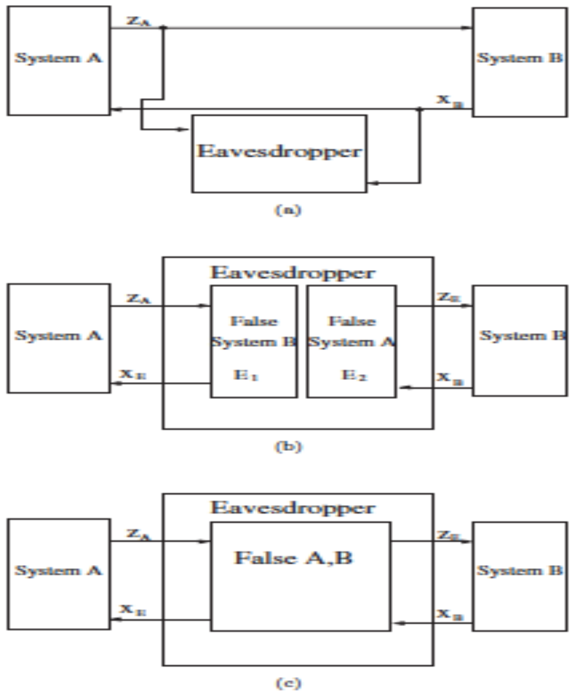


Table 1. XOR operation.

Input A	Input B	Output A XOR B
0	0	0
0	1	1
1	0	1
1	1	0



Synchronization as in Cuomo style, but bidirectional, to generate symmetric secret key



a) Listener: do not synchronize in time

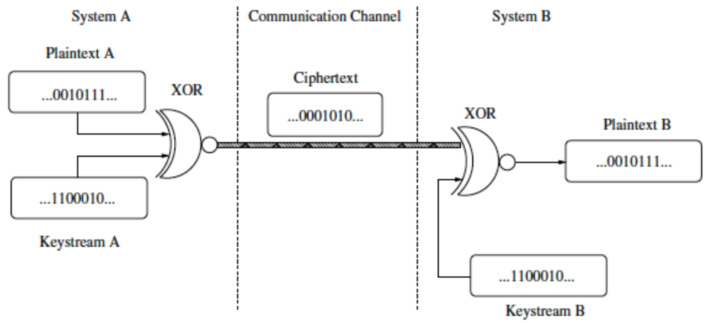
b) And c) Men in the middle, disturb synchronization, and can therefore be detected

Cryptography in the new era

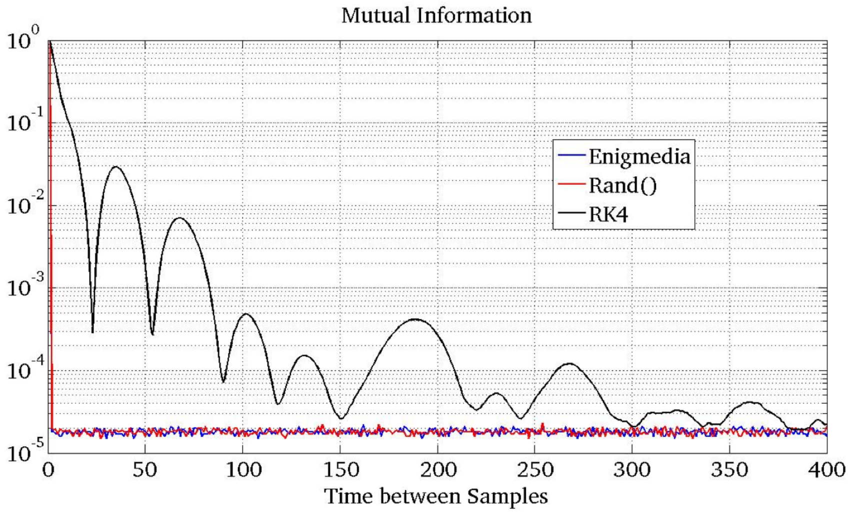
- By 2010, there is great recognition that cryptographic methods need to be light (low computational power), fast (high bit rates), light (constraint resources environment, such as IoT), easily implemented (descentralised), but still secure
  - NETFLIX: Security measures if implemented in the master server would require several weeks to be implemented to attend their 80 million users. The cryptosystem that allowed you to watch movies today is light (and can be implemented in the local servers), fast (HD videos) and easily implemented (low complexity), not to alter performance of streaming.

- In the review security Pisarchik and Zanin“Chaotic map cryptography and Int. J. of Computer Research **19** , 49 (2012), a drawback of chaos-based communication systems is made in terms of their sped to encrypt: too slow!

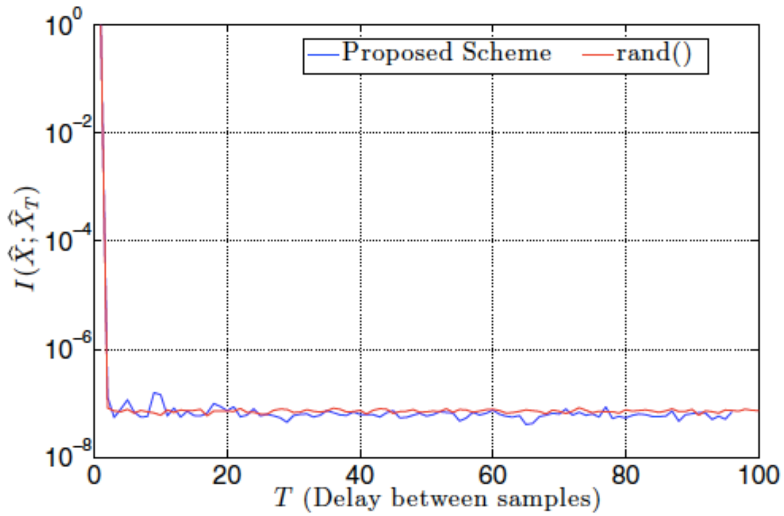
A fast and light stream cipher for smartphones [Eur. Phys. J. Special Topics **223**, 1601 (2014)]



Choosing time for Poincare-timing map:



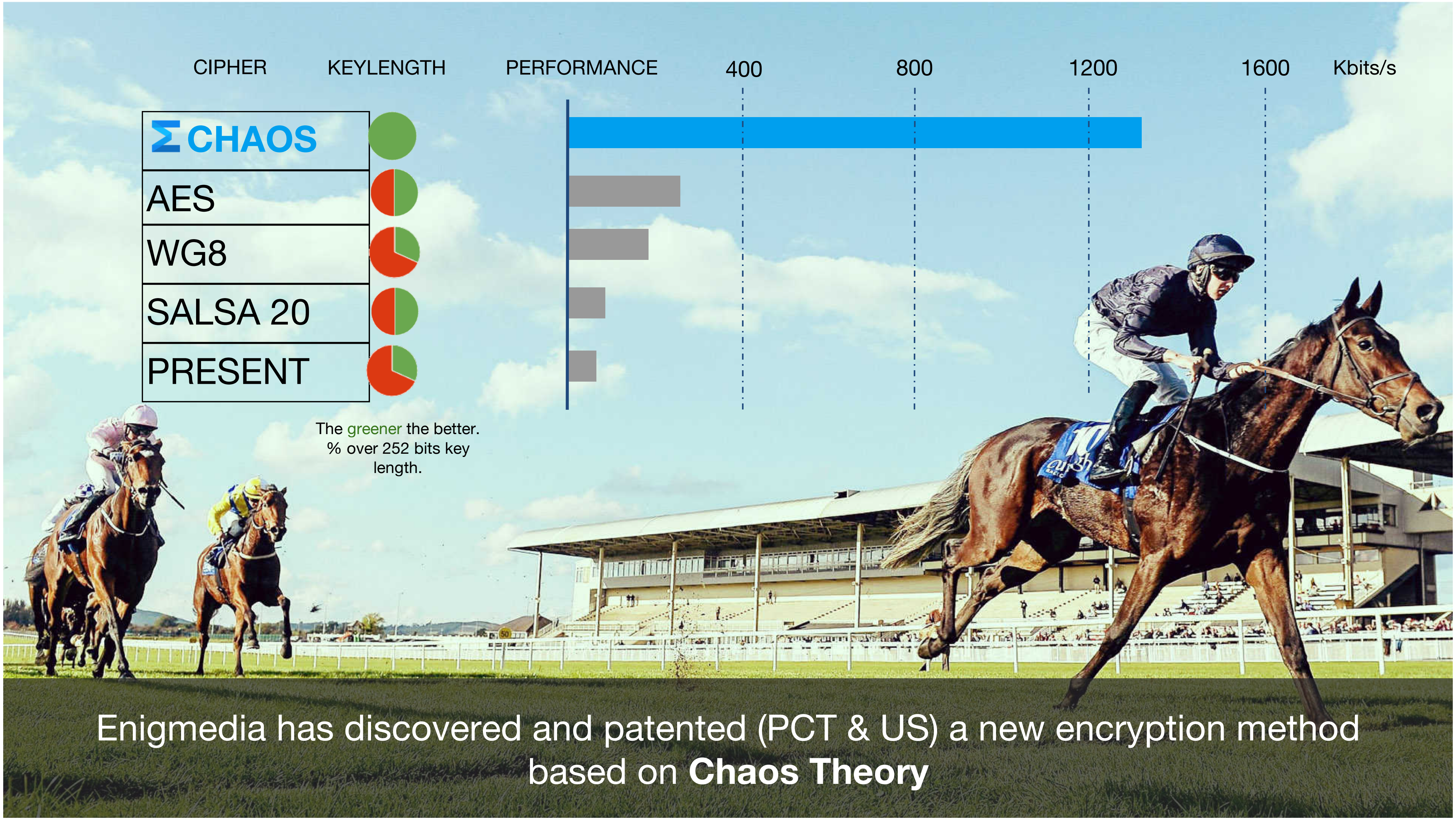
After discretization:



Paper led to a patent and formed the core for ENIGMEDIA cypher ΣCHAOS

See also: “Fast and Secure Chaos-Based Cryptosystem for Images”, Int. J. of Bif. and Chaos, **26**, 1650021 (2016).


Data is the new oil.
Cybersecurity is the way to protect the data...
and encryption is the key.
Encryption is a **CHALLENGE** for:
- low powered devices
- high throughput comms
- Real-time comms


CIPHER
KEYLENGTH
PERFORMANCE
400
800
1200
1600
Kbits/s
CHAOS
AES
WG8
SALSA 20
PRESENT
The greener the better.
% over 252 bits key
length.
Enigmedia has discovered and patented (PCT & US) a new encryption method
based on **Chaos Theory**

Tech Core: Validation

The fundamentals of Enigmedia's **technology** have been published by several **International Scientific Journals** and **Conferences** under peer-review process. Additionally, Enigmedia has a **scientific Advisory Board** composed by world-class recognized scientists, cryptographers and engineers who support its technology.

Whitfield Diffie
Discoverer of the Public Key Cryptography

tecnun

Pedro Crespo
Inventor of the ADSL

Murilo Baptista
Pioneer in Chaos Encryption

Hector Mancini
World Reference in Experimental Chaos

Enigmedia's **technology is currently being used** by public traded companies, law-enforcements and governments. Additionally, Enigmedia's developments have been **certified** with the **Common Criteria** by the **Spanish Intelligence Agency** and **Gartner** has highlighted Enigmedia's technology in its Market Guide.

Enigmedia is one of the founders of the **European Cyber Security Organisation.** This European Commission organisation is in charge of setting the EU's strategy regarding cybersecurity.

Enigmedia has presence at the **ISO,** the organisation in charge of creating the global standards. Enigmedia participates at the 27th subcommittee (IT security) workgroup 2 (encryption) together with other industrial and governmental key players.

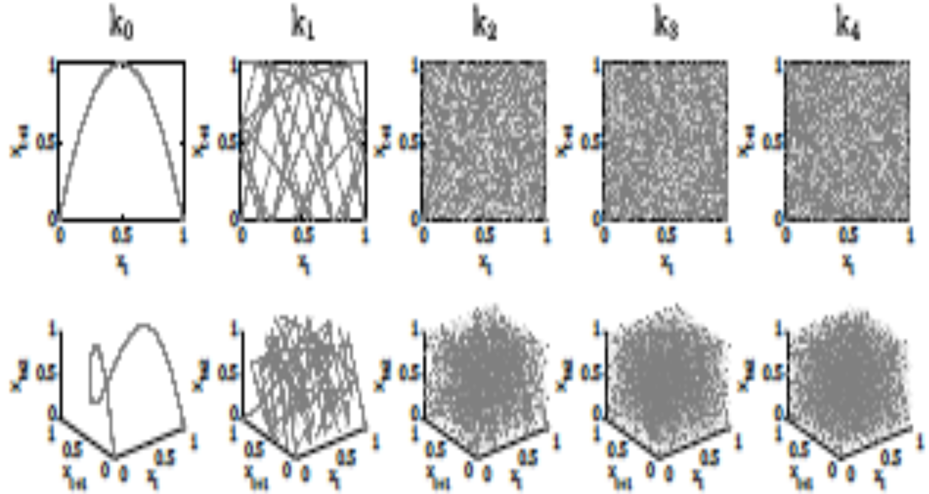
The k-map: encryption by the less significant digits

- Less significant digits of a chaotic trajectory carry little information about the initial condition (the past) and are uncorrelated to the future (thus highly entropic).
- Machicao and Bruno [Chaos, **27**, 053116, (2017)] have explored the “deepness” of chaos to create a very efficient and secure chaotic cypher

$$x_{t+1} = \mu x_t(1 - x_t) \,. \tag{4.1}$$

$$
\begin{aligned}
x_0 &= 0.36,\\
x_1 &= 0.92160,\\
x_2 &= 0.289013760,\\
x_3 &= 0.82193922612264960,\\
x_4 &= 0.585420538734197957594151502479360,\\
x_5 &= 0.97081332624943754555426458029594392767188359506591627109109596160.
\end{aligned}
$$

$$x_t^k = \phi_k(x_t) = x_t 10^k - \lfloor x_t 10^k \rfloor \,,$$



Cypher passes all Die Hard tests for $k \geq 9$

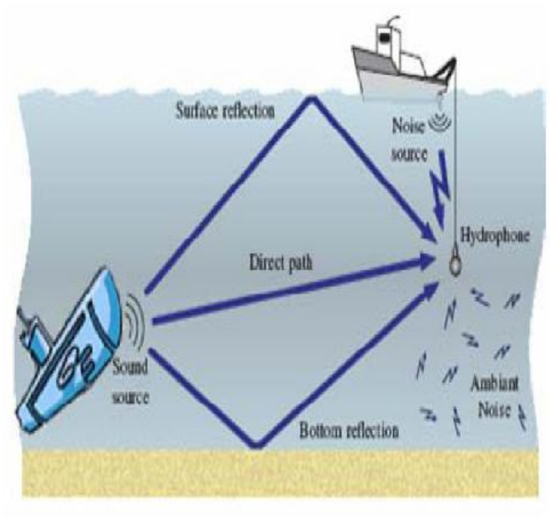
Wireless communication with chaos

Several reasons to go wireless

- Autonomy
- Remote sensing
- No wires and their costs involved
- GNSS (GPS, Galileo, etc)
- Better responsiveness (connect when you need where you are)
- Better access to information (connect in remote areas)
- Easier network expansion
- There are even more reasons…

However, channel is highly non-ideal

- Signal Attenuation
- Multipath
- Filtering
- Doppler effect
- Noise
- Time-varying fluctuations, dispersion, and propagation delays
- Multi-transmitter and multi-receiver
- In underwater: severe bandwidth limitations, battery power, sensors prone to failure…

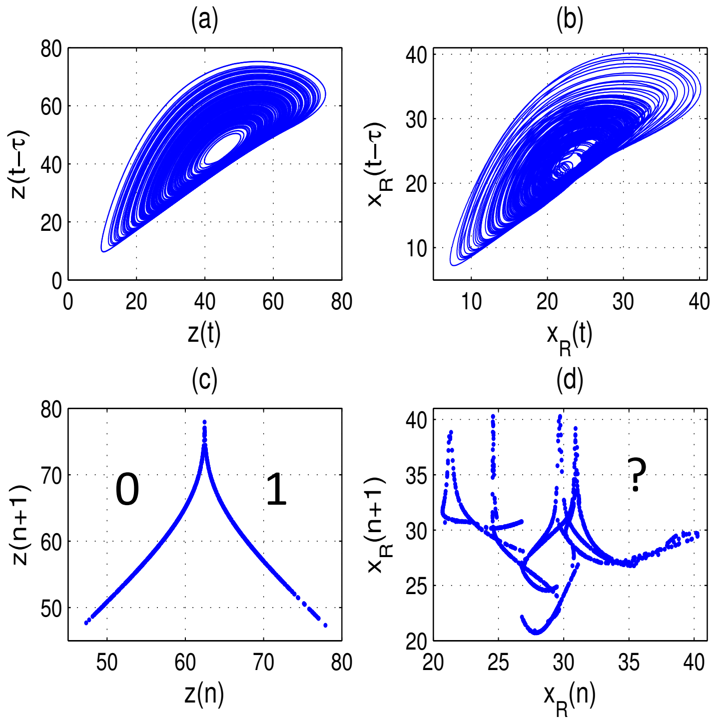


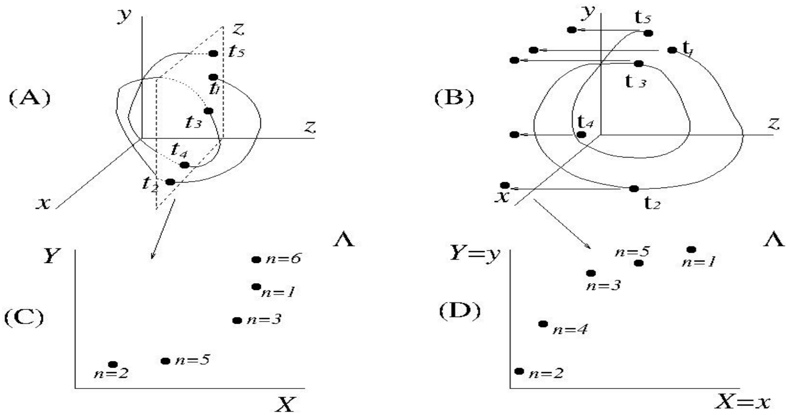
Our main theoretical result for wireless

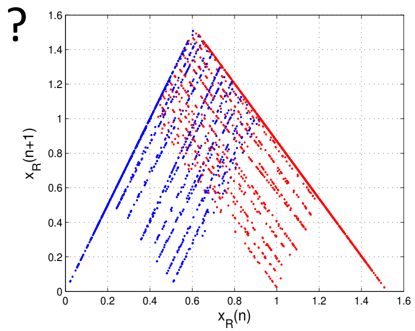
- The wireless channel (with filtering, multipath, and strong attenuation) does not alter the Lyapunov exponents: for some chaotic systems, this implies that the information transmitted is fully preserved.
- If chaotic generator is appropriately chosen, signal received, after being transmitted over a moderated non-ideal channel, has the same topological features of transmitted signal: decoding is trivial and without error.

Encoding and decoding chaos

- information contained in the signal is not destroyed by the action of the CBWC (Remind Pesin’s equality).
- Decoding might be however difficult







Notice preservation of form of map of the received signal!

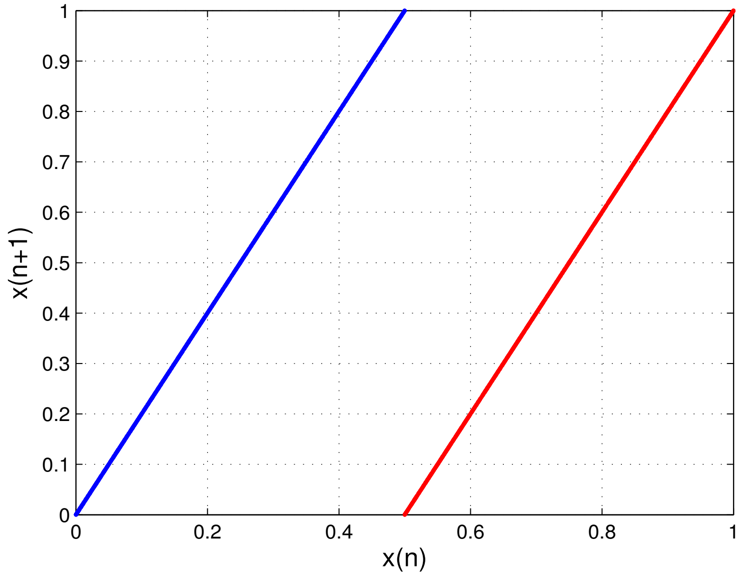
Maps with constant Jacobian

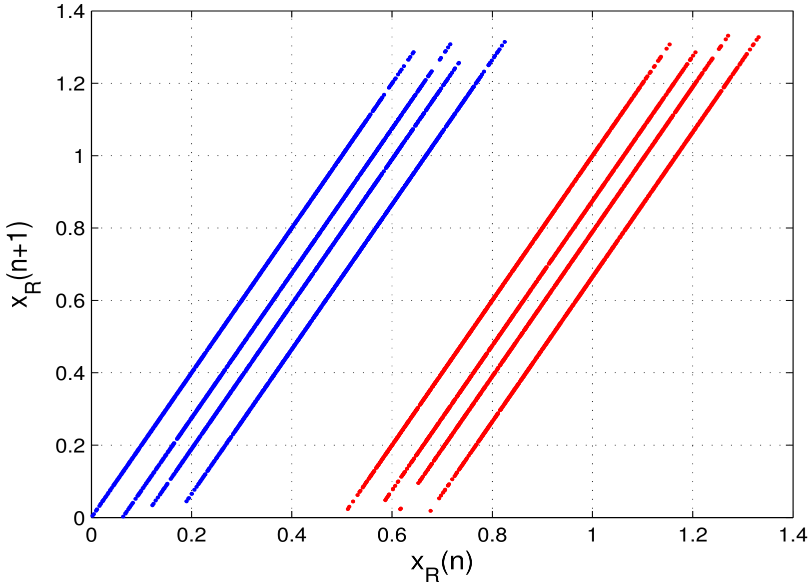
Since Lyapunov exponents are preserved, it is to expect that if x_T is generated by a map with a constant Jacobian such as

$$x_{n+1} = 2x_n, \bmod 1$$

then, x_R will possess the same functional form

Example (shift map)





So, the received signal preserves all the properties of the transmitted signal, and moreover can be trivially decoded

Is there a flow with these special properties? YES!

$$\ddot{x} - 2\zeta\dot{x} + (w^2 + \zeta^2)(x - s) = 0$$

or

$$\dot{x} = y$$

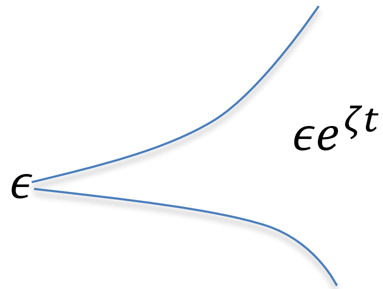
$$\dot{y} = 2\zeta y - (w^2 + \zeta^2)(x - s)$$

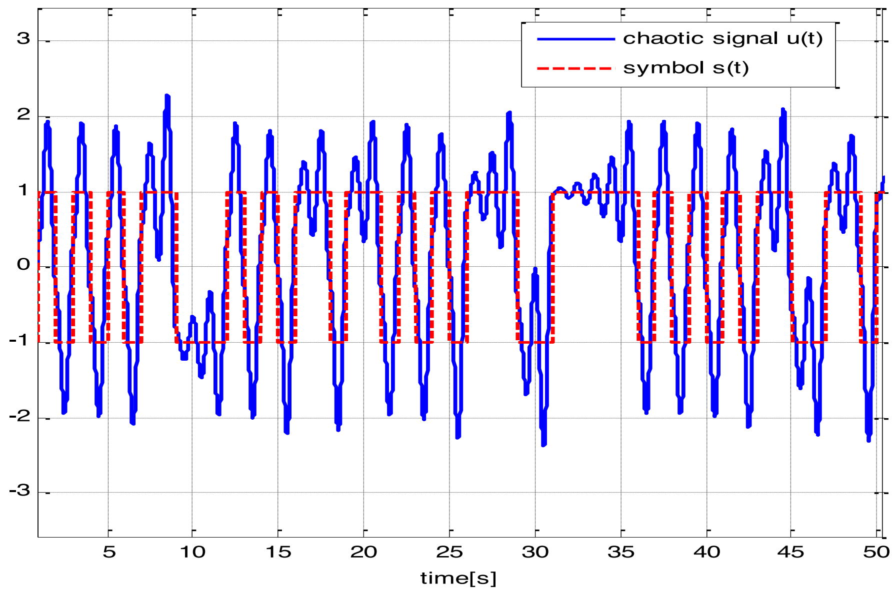
$$0 < \zeta \le \ln(2), w = 2\pi, \text{ and}$$

$$s = \mathrm{sgn}(x) = \begin{cases} 1, & x \ge 0 \\ -1, & x < 0 \end{cases}$$

s switches value only at $\dot{x} = 0$

Period set to 1s here





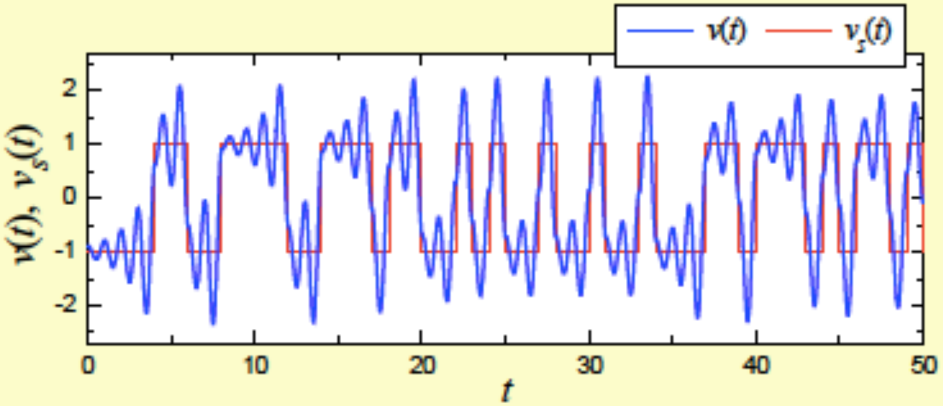
[N. J. Corron et al. Chaos, **20**, 023123 (2010)]

Matched Filter for Chaos

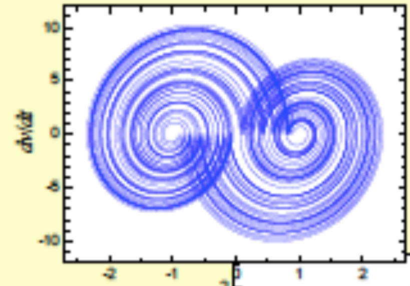
Hybrid Dynamical System

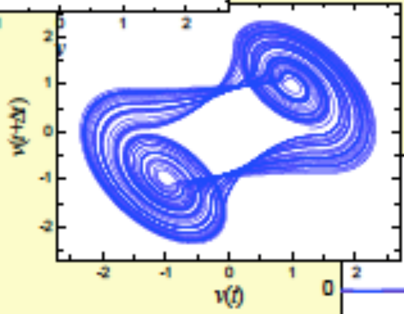
$$\frac{d^2v}{dt^2}-2\beta\frac{dv}{dt}+\left(\omega^2+\beta^2\right)\cdot\left(v-v_s\right)=0$$

$$\frac{dv}{dt}=0 \quad\Rightarrow\quad v_s=\mathrm{sgn}\left(v\right)$$



Exact Analytic Solution

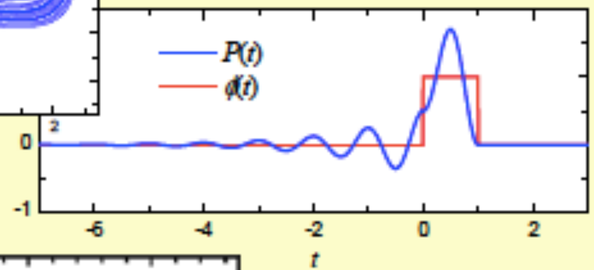




$$v\left(t\right)=\sum_{m=-\infty}^{\infty}s_m\cdot P\left(t-m\right)$$

$$v_s\left(t\right)=\sum_{m=-\infty}^{\infty}s_m\cdot\phi\left(t-m\right)$$

$$s_m=\pm1$$

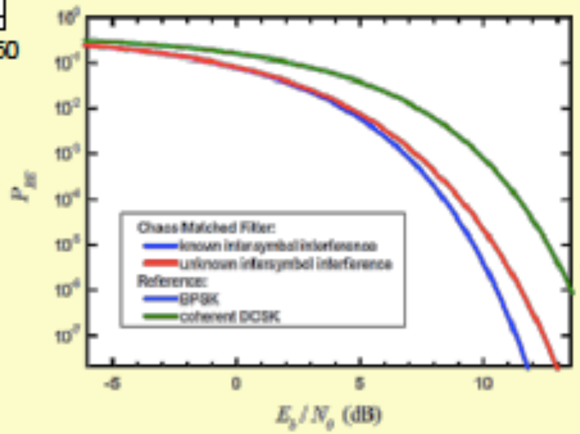


Matched Filter Receiver

Optimal Receiver in AWGN

$$\frac{d^2x}{dt^2}+2\beta\frac{dx}{dt}+\left(\omega^2+\beta^2\right)\left(x-v\right)=0$$

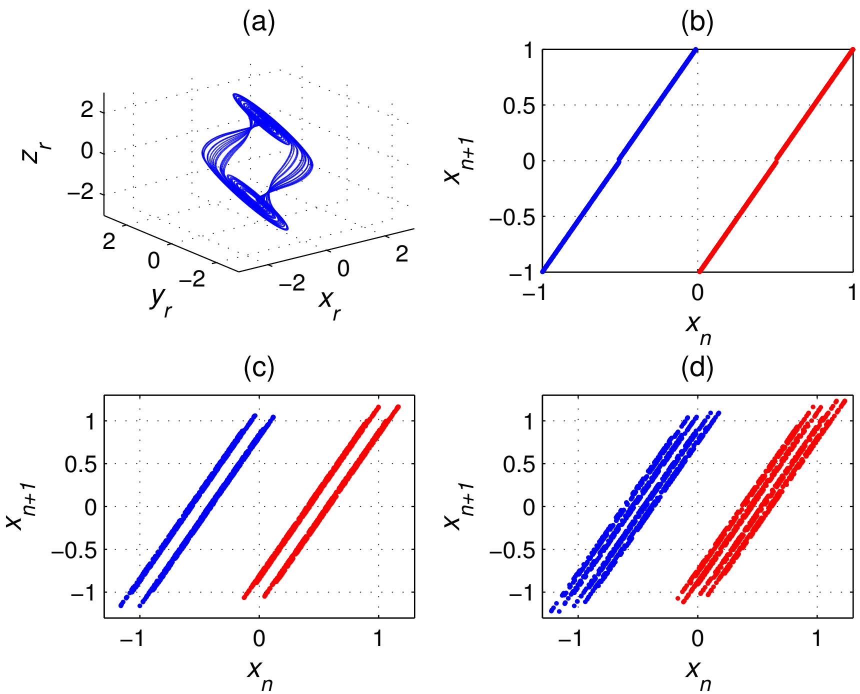
$$\frac{dy}{dt}=x\left(t+1\right)-x\left(t\right)$$



BPSK Performance using Hayes Symbolic Dynamics Encoding

– NJ Corron, JN Blakely, MT Stahl, "A matched filter for chaos," *Chaos* 20, 023123 (2010)

Illustration of Communication System



$$T_s = 1$$

transmitted

Received

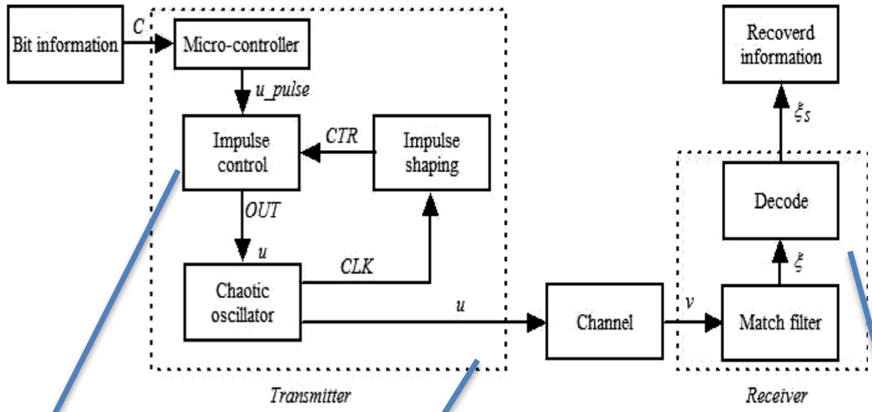
2 paths

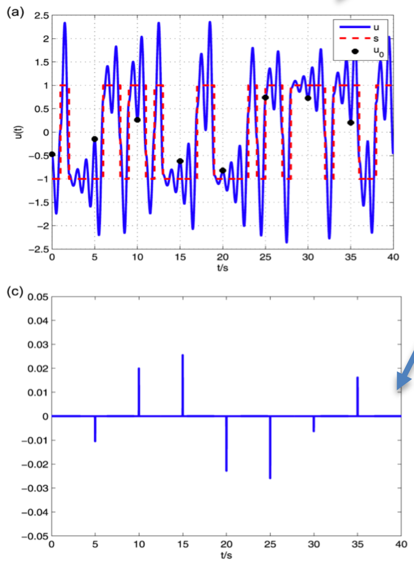
3 paths

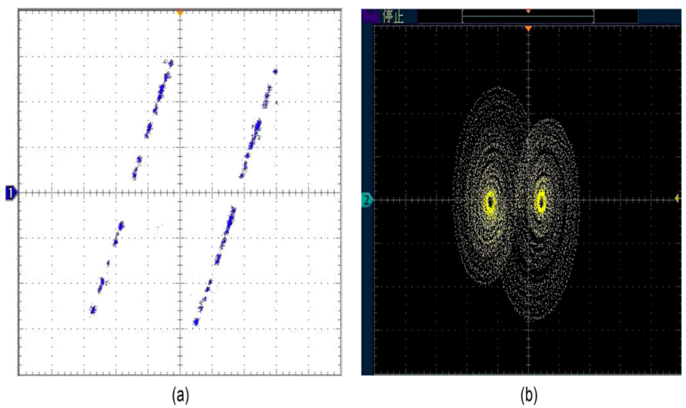
H.-P. Ren, M. S. Baptista, C. Grebogi, "Wireless Communication and Transmission Encoding Method", UK Patent Cooperation Treaty (PCT), Application Number PCT/2015/051411,

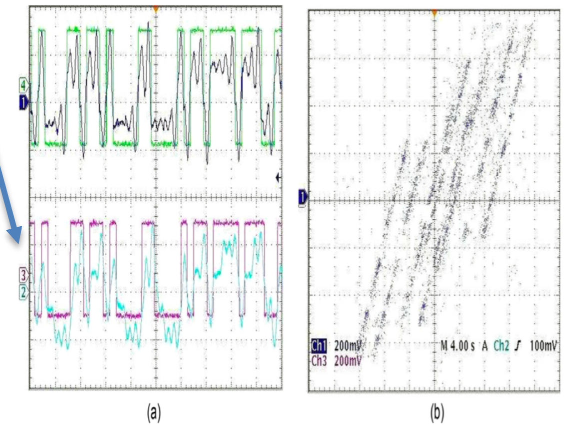
- Binary encoding: provided by s parameter: s=1 means '1' (redbranch), s=-1 means '0' (blue branch). Parameter s is specified by controlling initial conditions with small perturbations.
- Binary decoding: '0' if in blue branch or'1' otherwise
- Each path adds a new branch
- Equivalence principle: N transmitters system are equivalent to a system with 1 transmitter and N paths. So, MIMO communication systems would simply add new branches for each input

Emulating a wireless channel with an electronic channel





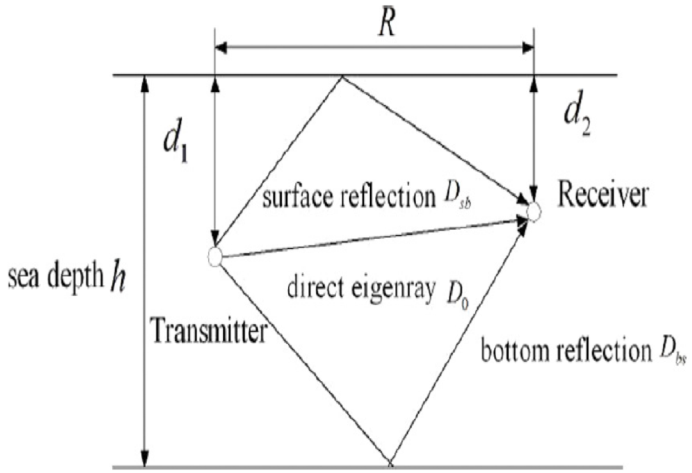


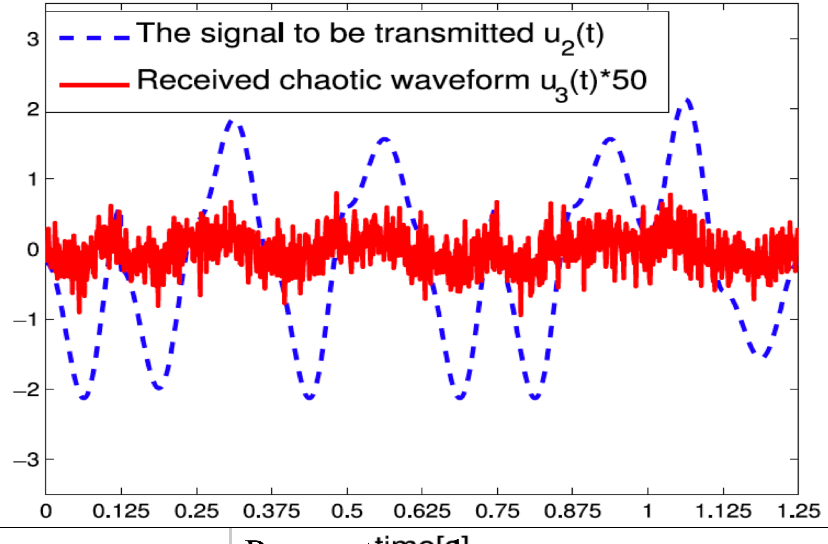


[Ren, et al. Chaos **26**, 083117 (2016)]

Decoding for strongly non-ideal wireless channels

What if channel strongly disrupts signal, such as in the underwater channel?





Parameter name	Parameter value	Parameter name	Parameter value
Sea depth *h*	100 m	Seabed sound speed *c*1	1650 m/s
Temperature of seawater *T*	20 ◦C	Seawater density *ρ*	1023 kg/m3
Transmitter depth *d*1	30 m	Seabed density *ρ*1	1500 kg/m3
Receiver depth *d*2	50 m	Seawater salinity *S*	35 ppt
Propagation distance *R*	1200 m	Transducer RMS movement *σd*	0.25 m
Seawater sound speed *c*	1539 m/s	Number of multiple paths	6
1 surface/bottom reflections s b	2 1	4 surface/bottom reflections s b	4 5
2 surface/bottom reflections s b	3 2	5 surface/bottom reflections s b	2 3
3 surface/bottom reflections s b	4 3		

Decoding for strongly non-ideal wireless channels

- **The hybrid system admits a matched filter** [N. J. Corron, Chaos, **20**, 023123, (2010)] that maximises signal-to-noise performance can be used:

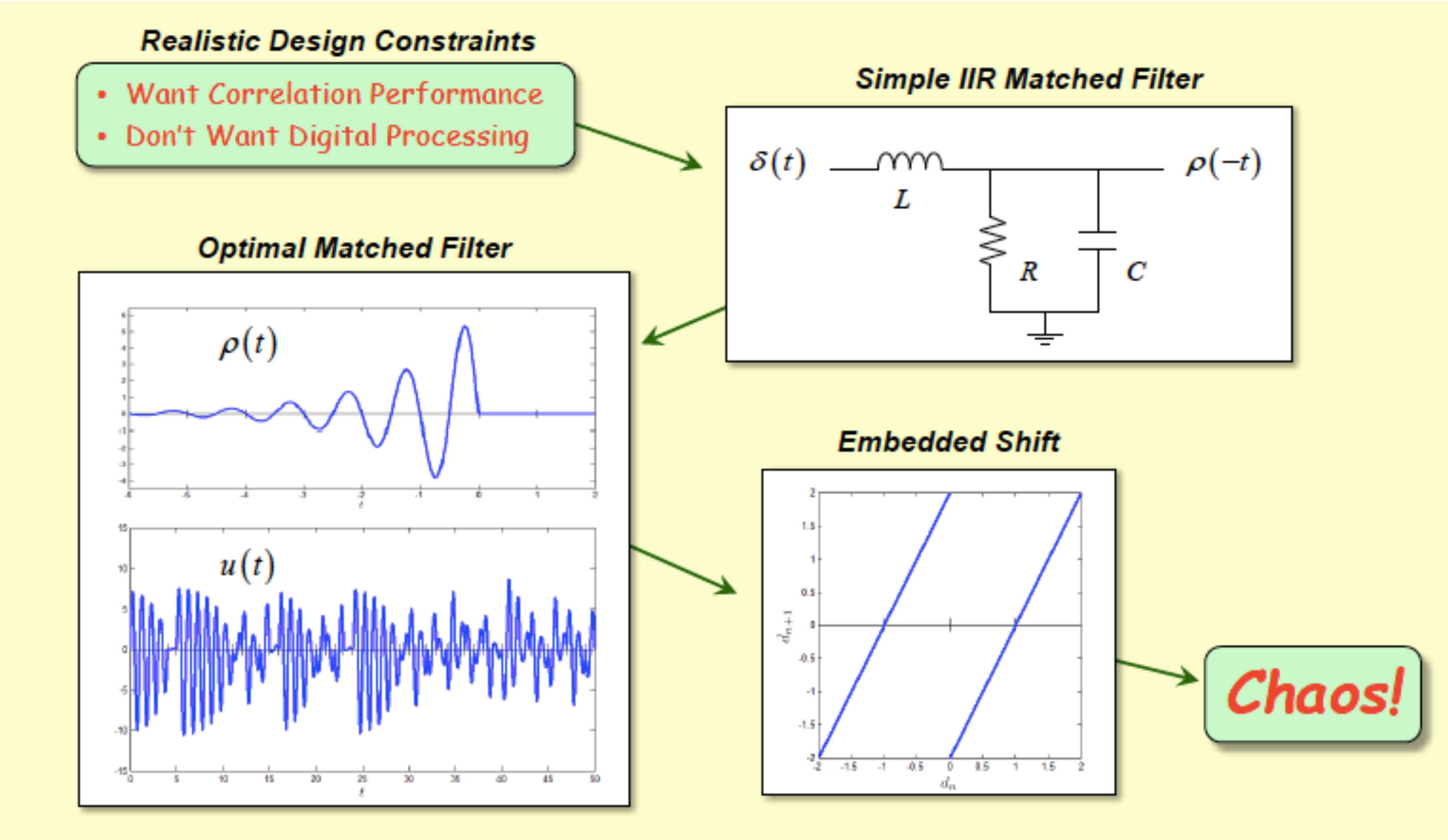
$$\dot{\eta} = v\left(t + \frac{1}{f}\right) - v(t)$$

$$\ddot{\xi} + 2\beta\dot{\xi} + (\omega^2 + \beta^2)\xi = (\omega^2 + \beta^2)\eta(t),$$

where v is received signal, f is base frequency ($\omega = 2\pi f$), $\beta = f\zeta$, where $\zeta$is the Lyapunov Exp.

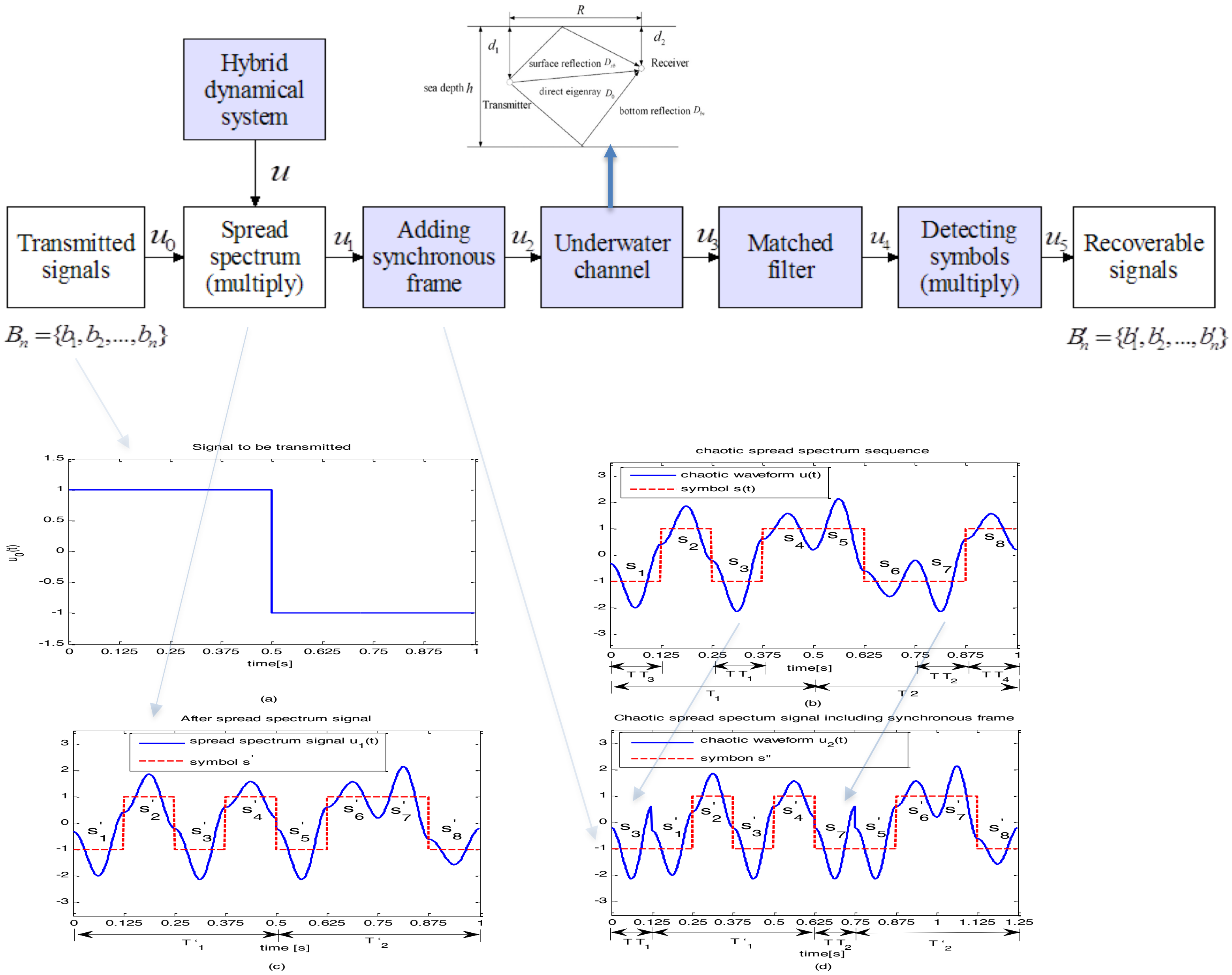
- **Hybrid system as well is being written above with a time-transformation to allow that parameter *f* defines the base frequency.**
- **System allows very simple hardware implementation.**
- A conjecture is made that the optimal communication waveform for any stable infinite impulse response filter must be chaotic [Corron et al., Proc. R. Soc. A **471**, 20150222 (2015)].

Ideal Communication Waveforms are Chaotic



– NJ Corron, JN Blakely, "Chaos in optimal communication waveforms," *Proc. R. Soc. A* 471, 20150222 (2015)

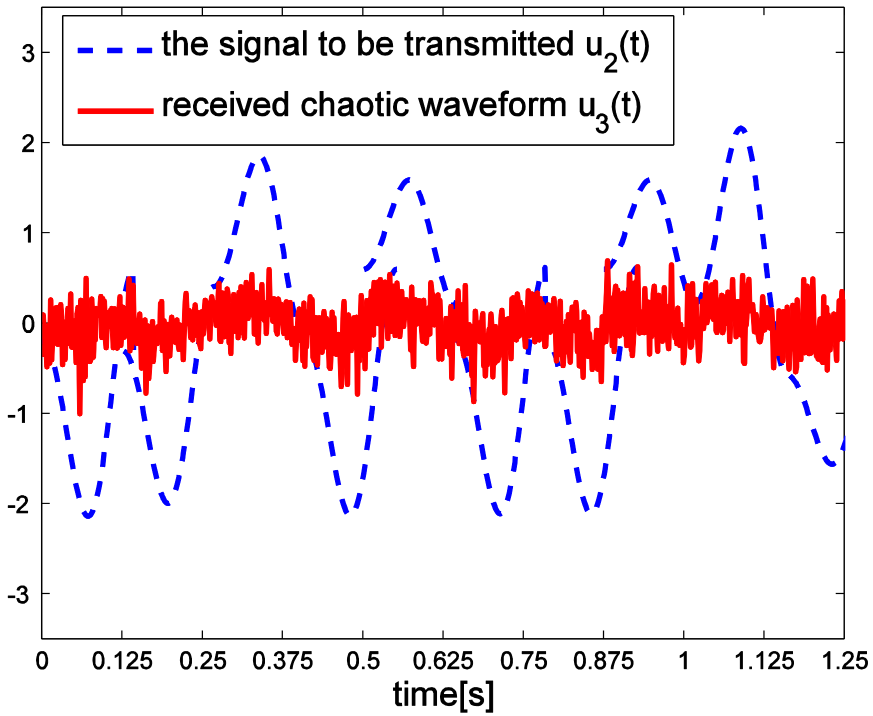
Our chaos-based (direct sequence) spread spectrum - Method:1

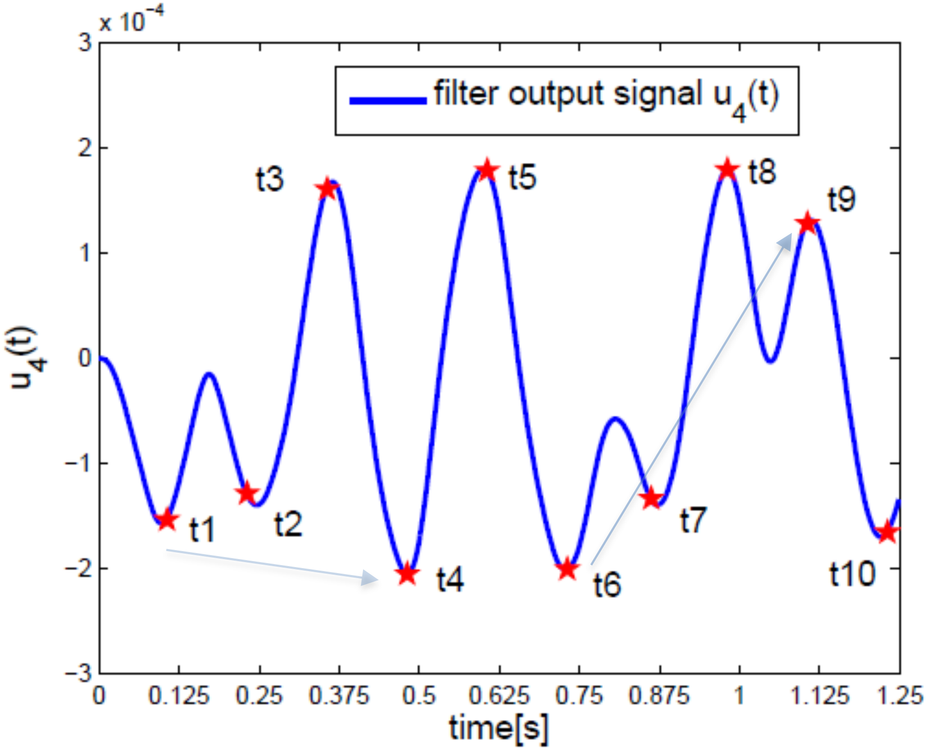


[Ren, et al. A chaotic spread spectrum system for underwater acoustic communication, Physica A, 478, 77-92, (2017)].

Method 1

- Filtering and decoding





$$t_1 = T_c - \Delta t = 0.1063s,\ \ \sigma_1 = sign(u_4(t_1)) = -1,\ \ t_4 = 4T_c - \Delta t = 0.4813s,\ \ \sigma_4 = sign(u_4(t_4)) = -1,$$

$$t_6 = 6T_c - \Delta t = 0.7313s,\ \sigma_6 = sign(u_4(t_6)) = -1,\ \ t_9 = 9T_c - \Delta t = 1.1063s,\ \ \sigma_9 = sign(u_4(t_9)) = 1,$$

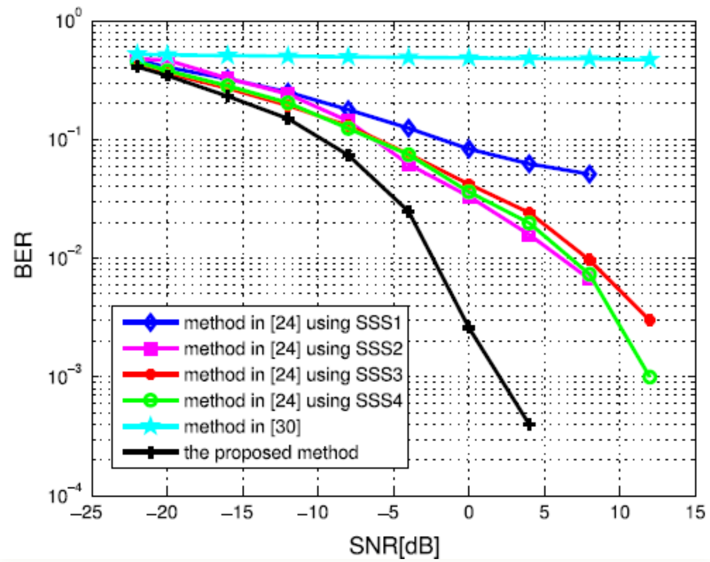
Decode as $b_1 = \sigma_1 \times \sigma_4 = 1,\ \ b_2 = \sigma_6 \times \sigma_9 = -1$

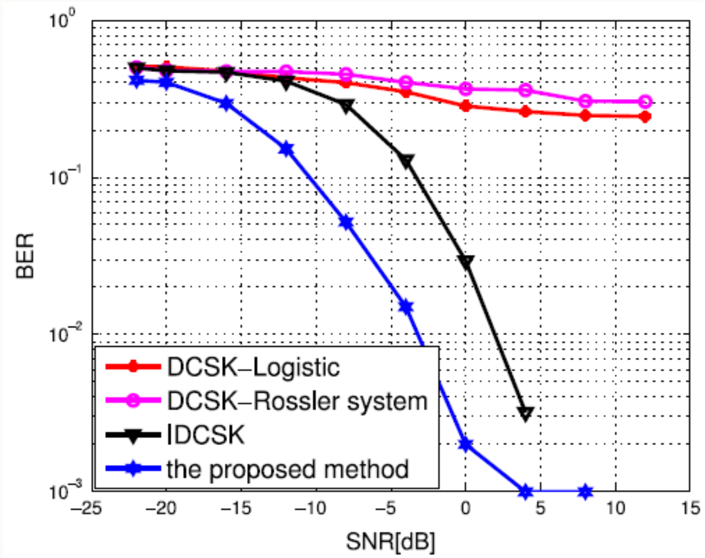
Method 1 – Performance analysis

- Comparison of different chaotic spread spectrum communication methods

Comparison of different chaotic spread spectrum systems.

Method	CBSS	CRSS	Proposed method
Modulation	BPSK	Complex modulation	None
Carrier frequency	50 kHz	50 kHz	50 kHz (base frequency)
Equalization	PTRM	None	None
Despreading method	Known spread sequence	UKF estimation	Synchronous frame
Symbol transmission rate	41.802 kbit/s		50 kbit/s
Information transmission rate	836.050 bit/s	1000 bit/s	980.39 bit/s

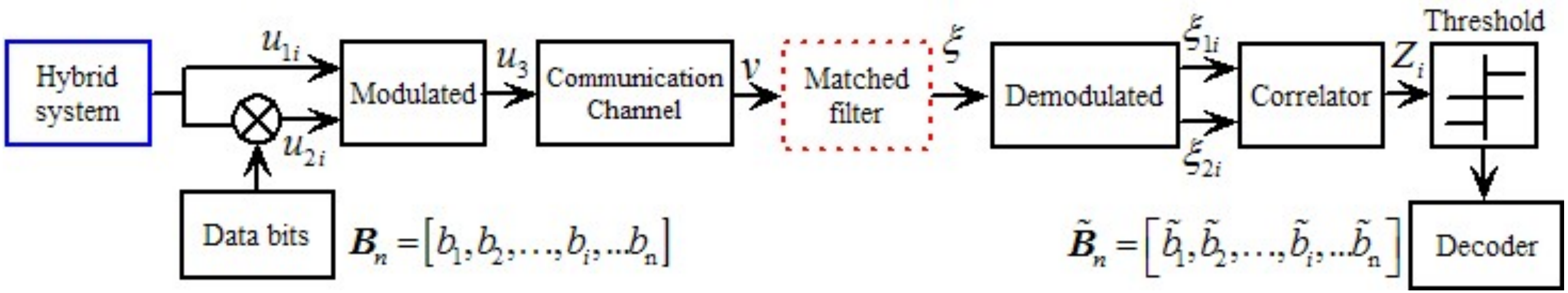




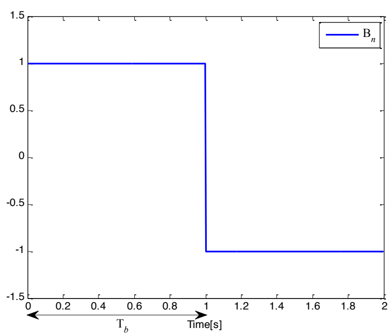
Comparison of DCSK and chaotic spread spectrum communication system

	DCSK	I-DCSK	Proposed method
Chaotic signal used	Logistic map, *Rössler* system	Logistic map	Hybrid dynamical system
Reference signal length	Full length	Mixed with data carrier	A little part of spread spectrum signal
Bit transmission rate	238.09 bit/s	476.19 bit/s	468.75 bit/s

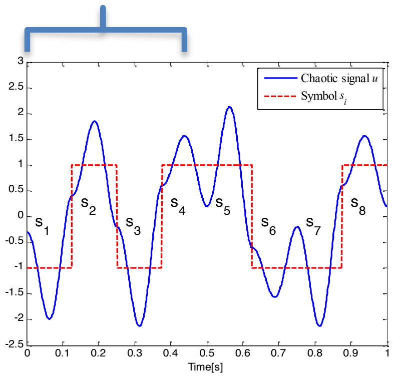
Differential Chaos Shift Key - Method 2



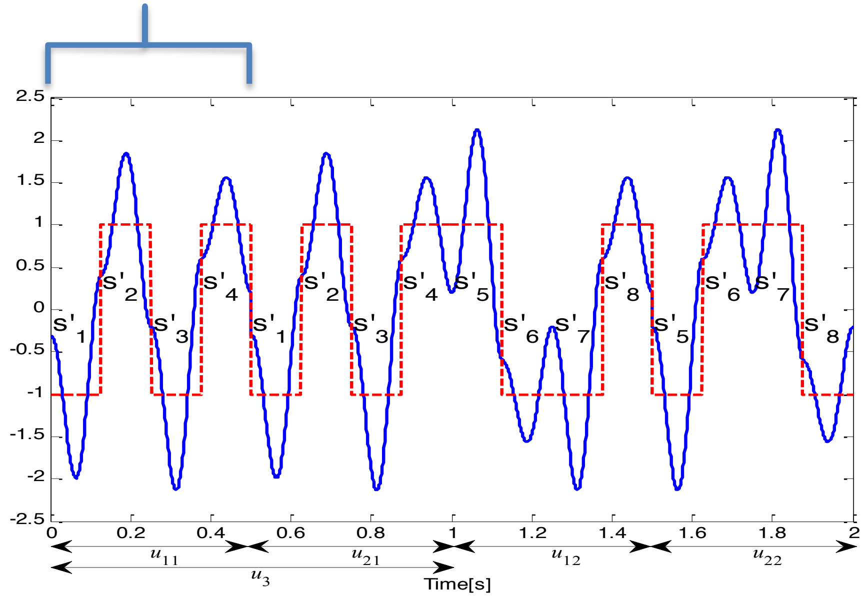
- Modulation



$\boldsymbol{B}$={+1,-1} to be transmitted



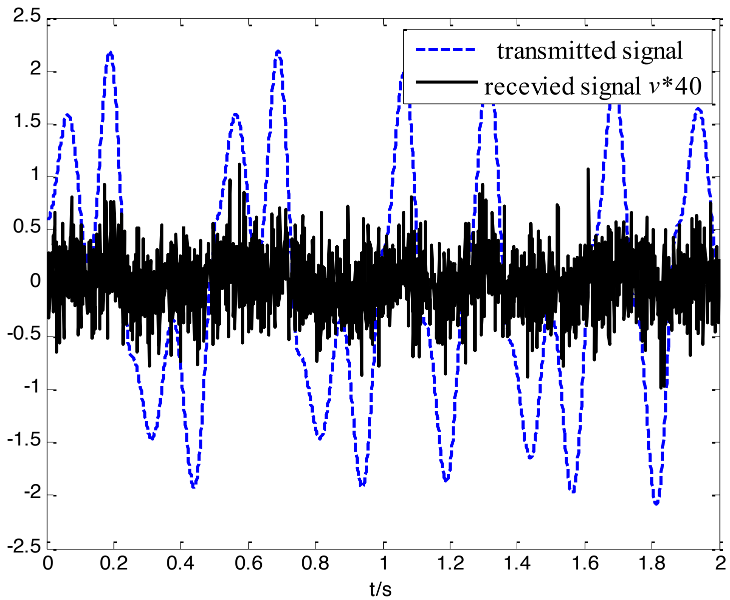
spreading gain L=8 (symbol generation rate [8bits/s] /Information transmission rate [1bits/s])



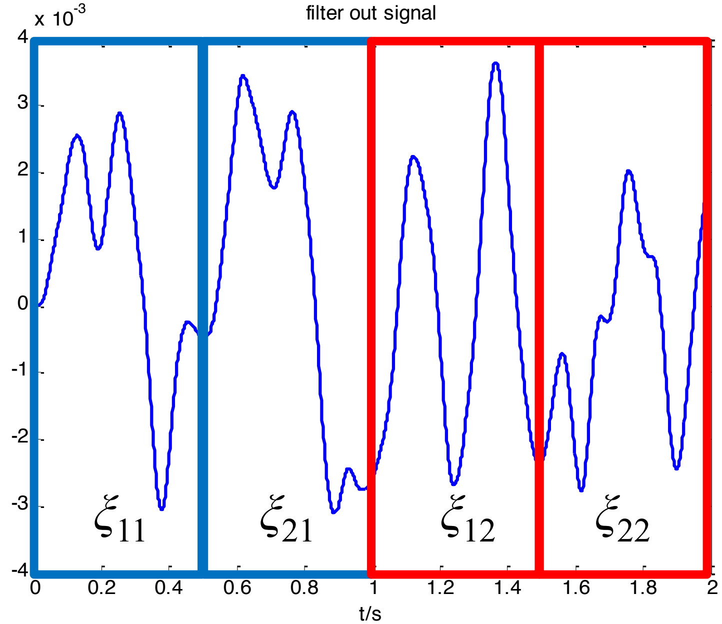
- u_{11} and u_{12} reference signals
- u_{21} and u_{22} modulated signal

[“Digital underwater communication with chaos”, submitted.]

Method 2



the transmitted signal and the received signal



First bit Second bit

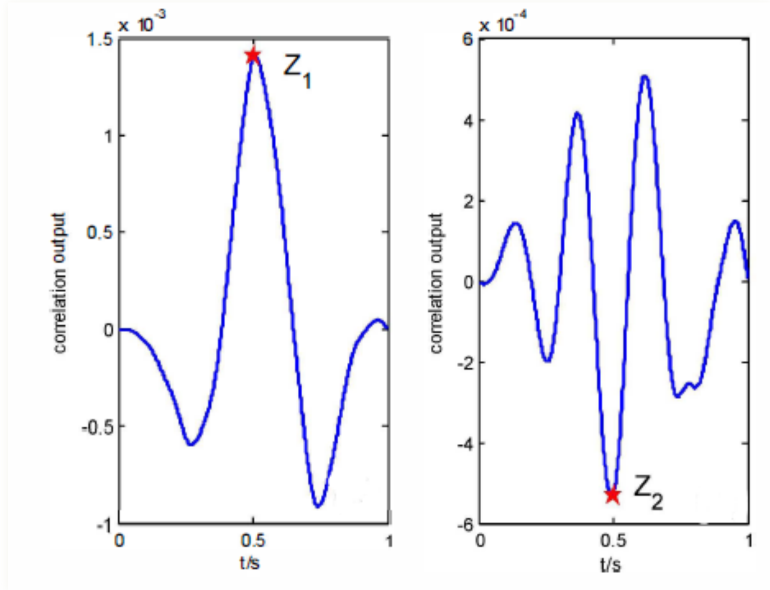
the output of the match filter

- **Demodulated**

$$\xi_{1i}=\xi(t),\quad (i\text{-}1)T_b\le t<(i\text{-}1)T_b+T_b/2,$$
$$\xi_{2i}=\xi(t),\quad (i\text{-}1)T_b+T_b/2\le t<iT_b,$$

$$Z_i(t)=\int_{(i-1)T_b}^{(i-1)T_b+T_b/2}\xi_{1i}(\tau)\,\xi_{2i}(t-\tau)\,d\tau$$

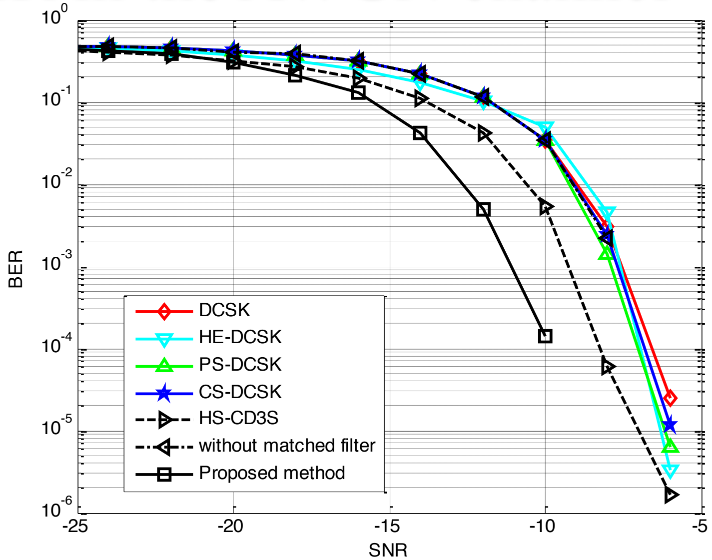
$$\tilde{b}_i=\begin{cases}+1 & Z_i\big((i-1)T_b+T_b/2\big)>0\\ -1 & Z_i\big((i-1)T_b+T_b/2\big)\le 0\end{cases}$$



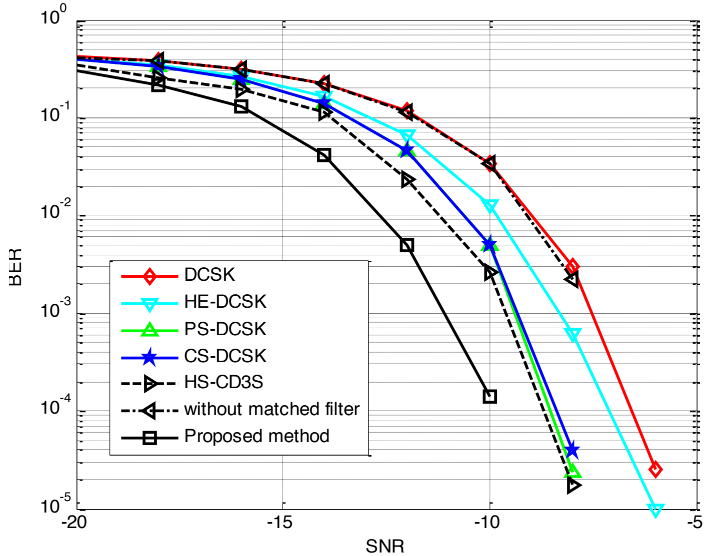
the correlation output of the filter out signal

Method 2 - Performance analysis

BER in the AWGN channel



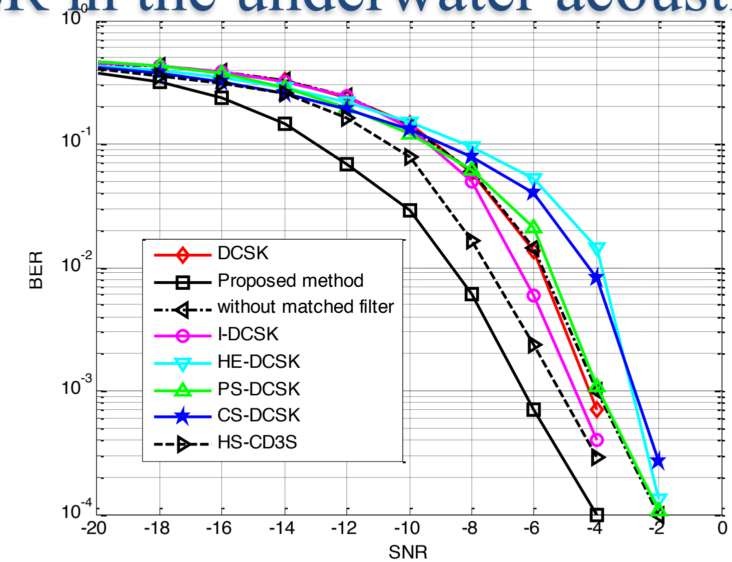
same spreading gain



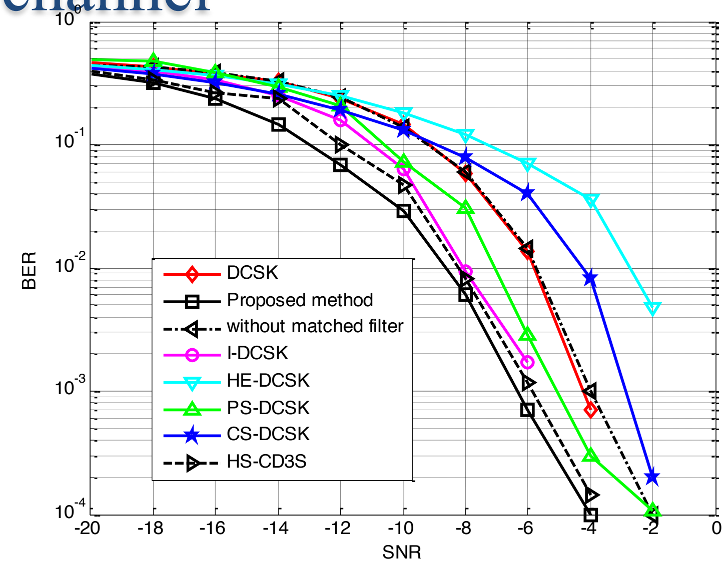
same data transmission rate

Base frequency
f=50kHz
Spreading gain
L=50

BER in the underwater acoustic channel



same spreading gain



same data transmission rate

Method 3

applied sciences

MDPI

Article

Chaos-Based Underwater Communication With Arbitrary Transducers and Bandwidth

Chao Bai [1], Hai-Peng Ren [1,*], Celso Grebogi [1,2] and Murilo S. Baptista [2]

1. Shaanxi Key Laboratory of Complex System Control and Intelligent Information Processing, Xi'an University of Technology, Xi'an 710048, China; bcxaut@foxmail.com (C.B.); grebogi@abdn.ac.uk (C.G.)
2. Institute for Complex System and Mathematical Biology, SUPA, University of Aberdeen, Aberdeen AB24 3UE, UK; murilo.baptista@abdn.ac.uk

* Correspondence: renhaipeng@xaut.edu.cn; Tel.: +86-029-8231-2401

Received: 30 October 2017; Accepted: 18 January 2018; Published: 24 January 2018

Concluding…

- Communication with chaos offers a research portfolio to do fundamental research as well as research with technological interest. You can be a scientist or an industrialist, or both !
- Search for "chaotic communication" in free patent online site has produced 21,189 patents
- I have not touched the applications of communication with chaos to understand biological, natural and social systems.
- I have also not touched block cyphers, suitable for images, and that explore the confusion and diffusion property of chaos.