Technical University
of Iasi, Romania

Faculty of Electronics and
Telecommunications

Signals, Circuits and
Systems laboratory

Circuite neliniare pentru prelucrarea semnalelor

Aplicatii ale dinamicii haotice

Cuprins

- Evitarea comportarii dinamice de tip haotic:
  - Definirea catastrofei
  - Determinarea parametrilor sistemului pentru diverse comportari dinamice
  - Diagrama de bifurcatie
- Comunicatii bazate pe sincronizarea haotica:
  - Criptarea haotica
- Dinamica neliniara a convertoarelor analog – numerice
  - Convertoare algoritmice
  - Modulatoare sigma – delta
- Generatoare de zgomot haotice:
  - Generatoare analogice / discrete
  - Generatoare de numere aleatoare
  - Estimarea parametrilor statistici

Definirea catastrofei

- Discutia comportarii sistemelor la *variatia parametrilor* – **analiza parametrica**
- Un sistem dinamic analogic sau discret:

$$\begin{cases} \mathbf{x}'(t) = \mathbf{f}\left(\mathbf{x}(t), \mathbf{p}\right) \\ y(t) = g\left(\mathbf{x}(t), \mathbf{p}\right) \end{cases} \qquad \begin{cases} \mathbf{x}[k+1] = \mathbf{f}\left(\mathbf{x}[k], \mathbf{p}\right) \\ y[k] = g\left(\mathbf{x}[k], \mathbf{p}\right) \end{cases}$$

se numeste **structural stabil**, daca *tipul* sau de comportare dinamica ramane ne-modificat la *micile variatii* ale parametrilor in jurul valorilor nominale:

$$\forall \varepsilon > 0: \quad \mathbf{p} = \mathbf{p}_0 + \varepsilon$$

- **Catastrofa** este *schimbarea tipului* de comportare dinamica a unui sistem la o variatie oricat de mica a parametrilor in jurul valorilor nominale.
  - *Exemplu*: situatia de **limita de stabilitate,** in cazul sistemelor liniare, poate devni stabilitate sau instabilitate la cea mai mica variatie a parametrilor oscilatorului liniar

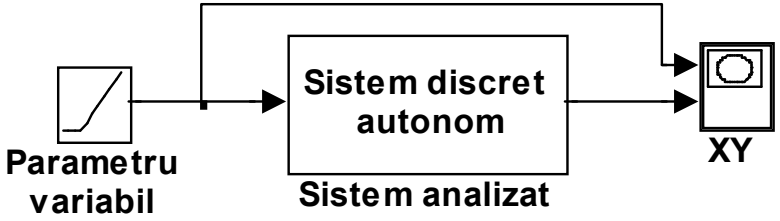
Diagrama de bifurcatie

- **Diagrama de bifurcatie** este reprezentarea grafica a multimilor *atractoare* ale unui sistem in functie de *variatia unui parametru* al acelui sistem.
- In cazul **sistemelor discrete**, pentru *fiecare valoare* a parametrului:
  - Se generaza traiectoria sistemului;
  - Se elimina regimul tranzitoriu de la inceputul acesteia;
  - Se pozeaza punctele ramase in dreptul valorii curente a parametrului;
  - Se incrementeaza parametrul.
- In cazul sistemelor analogice, etapele de la cazul discret, sunt precedate de:
  - Discretizarea sistemului analogic prin sectionare Poincare;

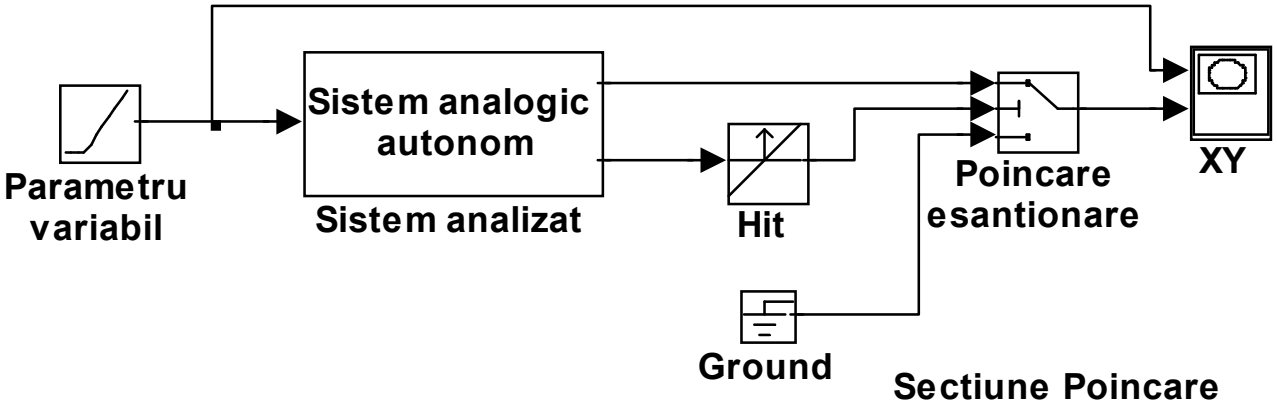
pentru a atasa un sistem discret prototipului analogic, in mod minimal din punctul de vedere al frecventei de esantionare.

Schema de principiu

- Cazul sistemelor discrete:



- Cazul sistemelor analogice:

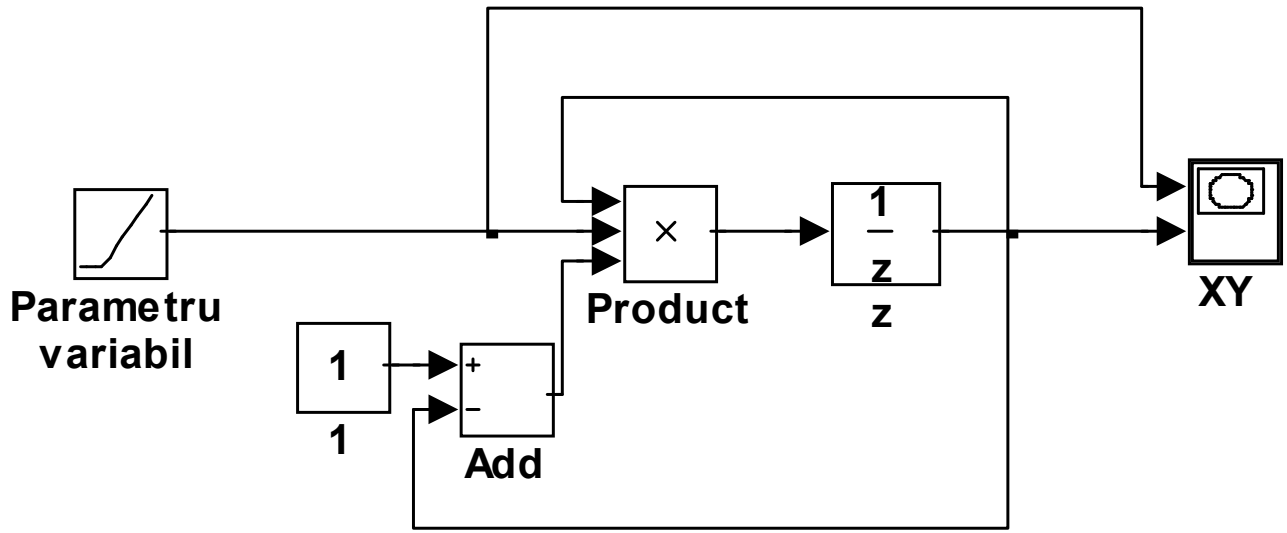


Simulari: sistem discret logistic

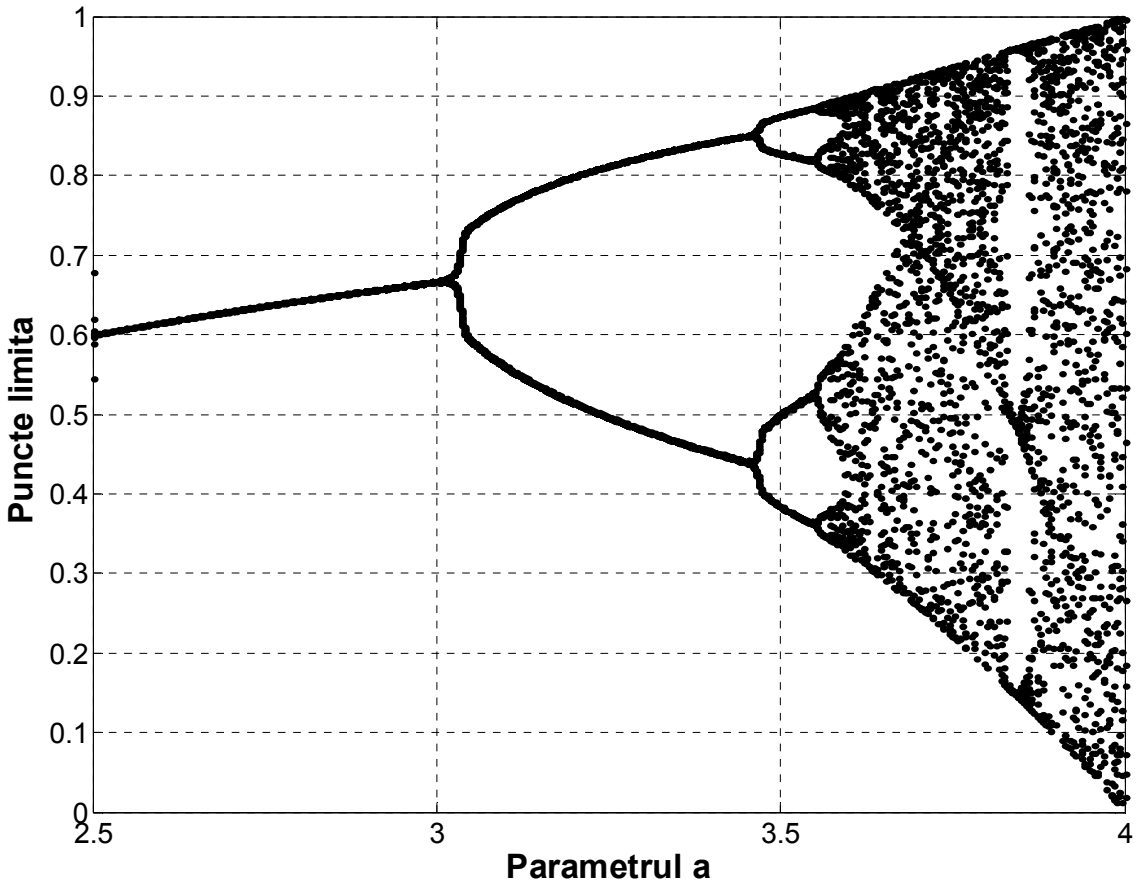
- Sistemul discret logistic este dat de ecuatia de stare:

$$x[k+1] = a \cdot x[k] \cdot \left(1 - x[k]\right)$$

- Iar diagrama de bifurcatie poate fi schitata cu schema de simulare:



Rezultat de simulare

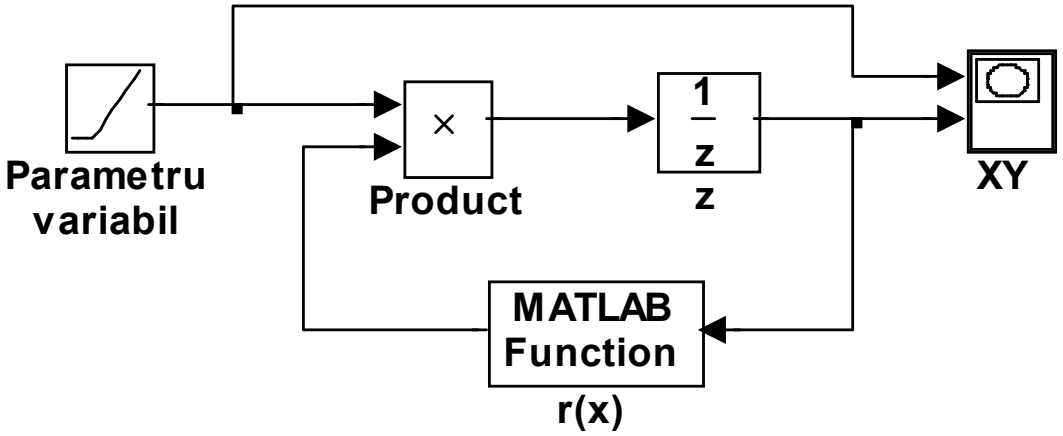


Sistem discret aditiv de ordinul 1

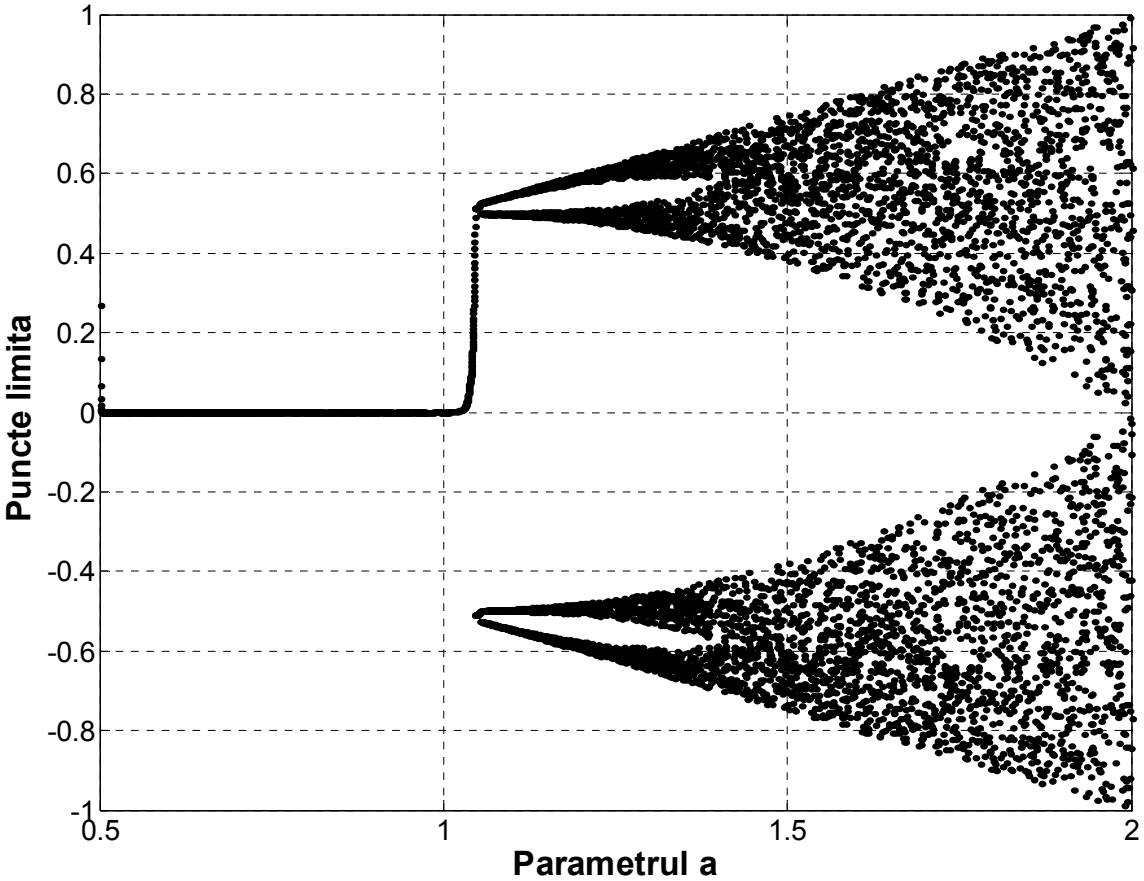
- Sistemul discret aditiv este dat de ecuatia de stare:

$$x[k+1] = a \cdot \left(x[k] - round\left(x[k] \right) \right)$$

- Iar diagrama de bifurcatie poate fi schitata cu schema de simulare:



Rezultat de simulare

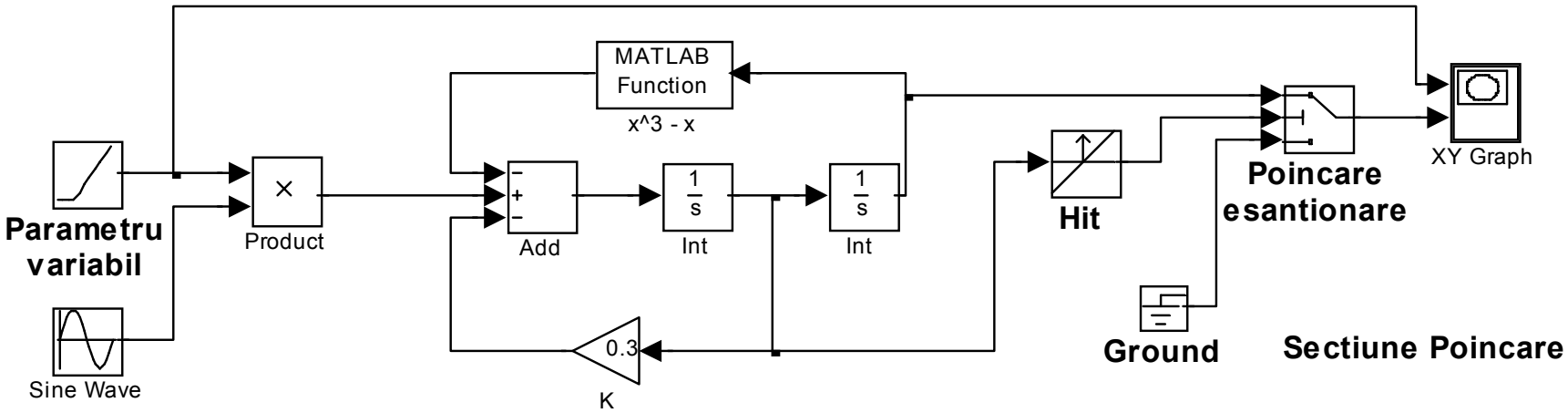


Sistem analogic tip Duffing

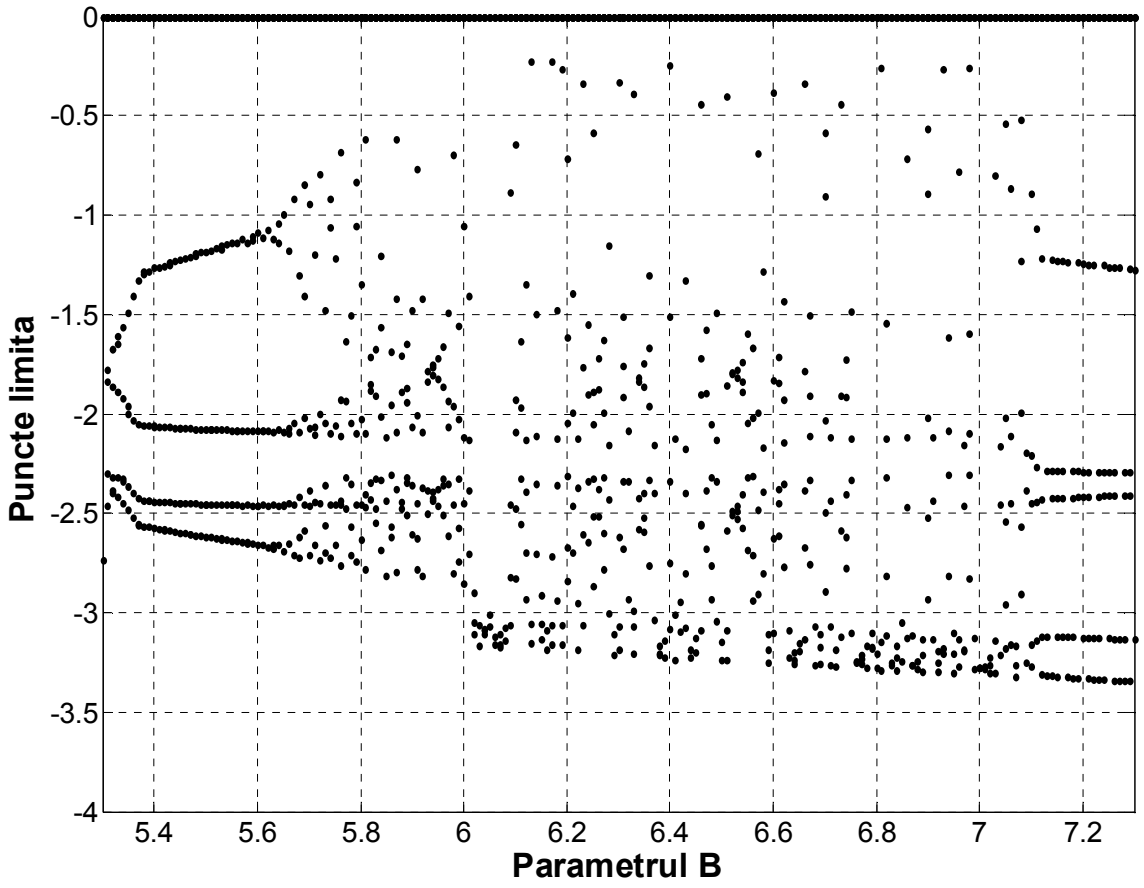
- Sistemul Duffing este unul analogic, ne-autonom, de ordinul 2, cu neliniaritate cubica:

$$\begin{cases} x_1' = -k \cdot x_1 - x_2^3 + x_2 - B \sin \omega_0 t \\ x_2' = x_1 \end{cases}$$

- Parametrul de interes, pentru care se va trasa diagrama de bifurcatie, este amplitudinea semnalului armonic de intrare, B:



Rezultat de simulare



Aplicabilitate

- Prin analiza diagramei de bifurcatie se pot observa:
  - Tipurile de comportari dinamice ale sistemului neliniar studiat
  - Gama de valori ale parametrului supus modificarii pentru care se manifesta comportamentele puse in evidenta
  - Punctele de bifurcatie
- Identificarea tipurilor de comportari se face dupa numarul de puncte ale diagramei pentru o valoare fixata a parametrului:
  - 1 punct = punct fix (ciclu limita simplu)
  - 2 puncte = ciclu limita de lungime 2 (ciclu limita cu dublarea perioadei)
  - nr. mic de puncte discret repartizate = ciclu limita de lungime egala cu nr. puncte (ciclu limita cu multiplicarea perioadei)
  - nr. mare de puncte continuu repartizate pe un domeniu=comportare cuasiperiodica sau haotica

Securitatea comunicatiilor

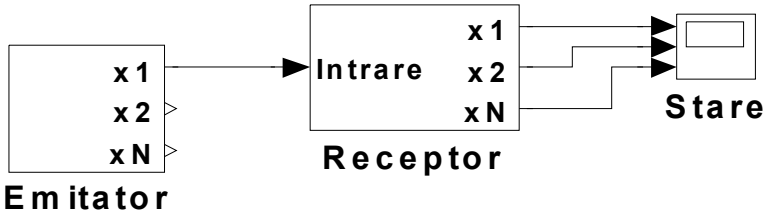
- **Securitatea comunicatiilor** cuprinde aspecte cum ar fi:
  - Autentificarea emitatorului
  - Confidentialitatea mesajului
  - Integritatea datelor
  - Confirmarea receptiei (receipt)
  - Marcarea timpului (timestamping)
- **Criptarea** intervine in special la asigurarea *confidentialitatii mesajului*
- Criptarea clasica se bazeaza pe teoria a informatiei si metodele de *codare cu alfabet finit*
- Implicit, metodele clasice de criptare se bazeaza pe *metode algebrice*
- Pentru criptare si decriptare, este necesara o **cheie de criptare**:
  - Algoritmi de criptare *simetrici* (cu *cheie privata*)
  - Algoritmi de criptare *asimetrici* (cu *cheie publica*)

Securitatea comunicatiilor (cont.)

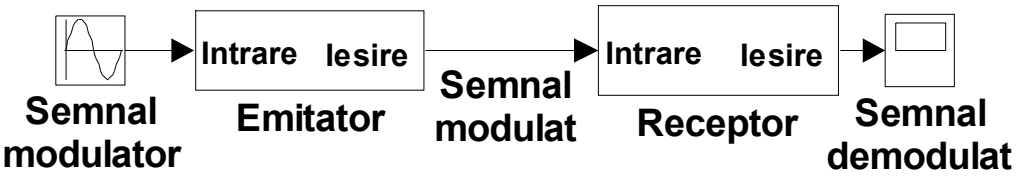
- **Criptarea haotica** se bazeaza pe *metode dinamice*
- Pentru compatibilitate cu *codarea clasica* si cu metodele actuale de *comunicatii digitale*, este necesara utilizarea de *surse si canale* cu alfabet finit
- Ca si in cazul clasic este necesara o **cheie de criptare**:
  - Parametrii sistemului emitator
  - Nr. biti in reprezentarea textului in clar si a textului criptat
  - *Eventual* conditia initiala a emitatorului
- Receptorul avand nevoie de aceiasi parametri cu ai emitatorului, criptarea haotica se clasifica in categoria sistemelor **simetrice**, cu **cheie privata**

Principiul criptarii haotice

- ***Sincronizare haotică:*** dezvoltarea unui canal de comunicații bazat sincronizarea pe o purtătoare generata de un sistem haotic;



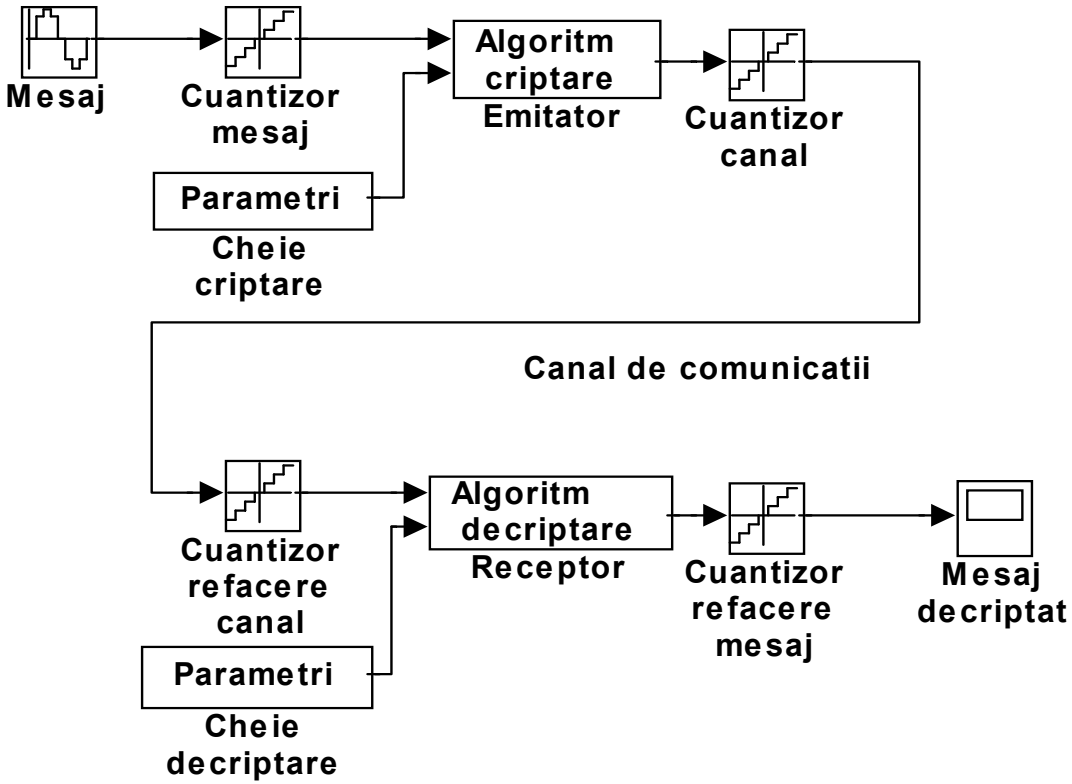
- ***Modulație haotică:*** metoda de grefare a semnalului util (modulator) pe purtătoarea de bandă largă;



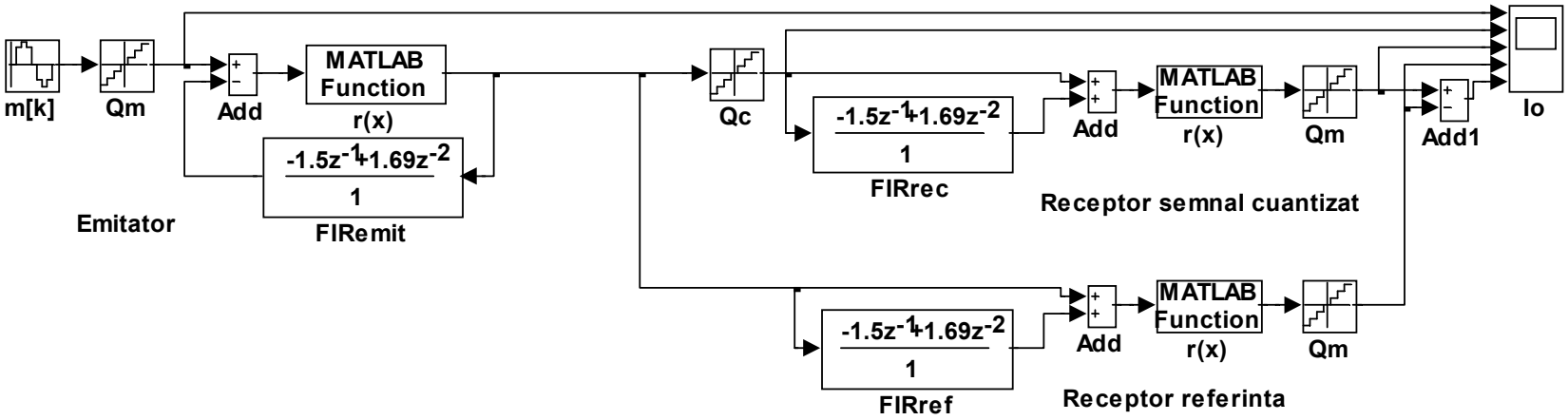
- **Criptarea haotica**: transmiterea unui *semnal modulator cuantizat* pe un *canal digital*

Notatii si scheme

- Sistem criptare / decriptare



Schema bloc de simulare cu sisteme aditive



Relatii de proiectare

- Eroarea de sincronizare datorata cuantizarii pe canalul de comunicatii este raspunsul receptorului la eroarea de cuantizare pe canal.
- **Dem.:** Semnalul receptionat poate fi exprimat aditiv:

$$\tilde{y}[k] = y[k] + p[k]$$

- Semnalul demodulat este: $$\tilde{m}[k] = r\left(\tilde{y}[k] + \sum_{n=1}^{N} \tilde{h}[n] \cdot \tilde{y}[k-n]\right)$$
- Scazand acest raspuns din cel de referinta si tinand cont de aditivitatea receptorului, obtinem:

$$\varepsilon[k] = r\left(p[k] + \sum_{n=1}^{N} \tilde{h}[n] \cdot p[k-n]\right)$$

Relatii de proiectare (cont.)

- Consecinte asupra marimilor statistice de ordinul 2:

$$R_{\varepsilon\varepsilon}[k] = R_{hh}[k] * R_{pp}[k] \qquad S_{\varepsilon\varepsilon}(e^{j\omega}) = S_{hh}(e^{j\omega}) \cdot \left| H(e^{j\omega}) \right|^2$$

- Consecinte asupra marimilor statistice de ordinul 1:

$$E(\varepsilon) = E(p) \cdot H(1) \qquad \varepsilon_{Max} = p_{Max} \cdot \sum_{n=1}^{N} \left| h[n] \right|$$

- Consecinte aspra reprezentarii binare a esantioanelor:

$$\varepsilon_{Max} < 0.5 \cdot 2^{-B_M} \qquad p_{Max} \cdot \sum_{n=1}^{N} \left| h[n] \right| < 2^{-B_M - 1}$$

$$p_{Max} = 2^{-B_P}$$

Relatii de proiectare (cont.)

- Rezulta:

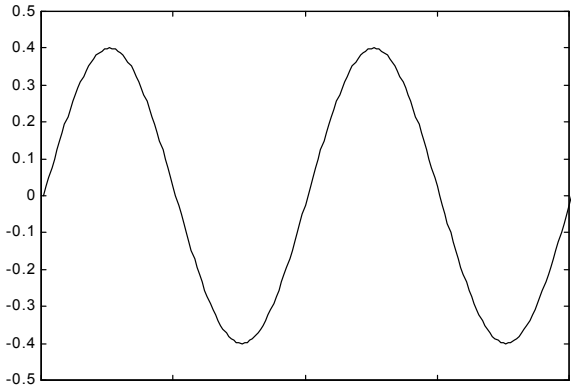
$$2^{-B_P} \cdot \sum_{n=1}^{N} \left| h[n] \right| < 2^{-B_M - 1}$$

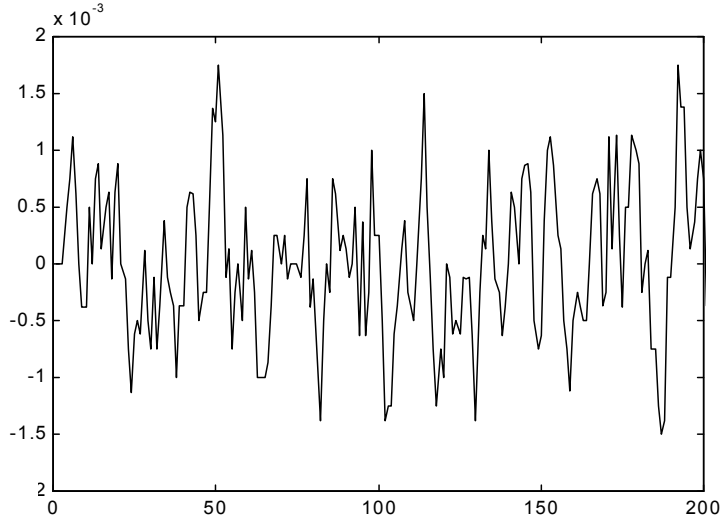
$$B_P - \lg_2 \left(\sum_{n=1}^{N} \left| h[n] \right| \right) > B_M + 1$$

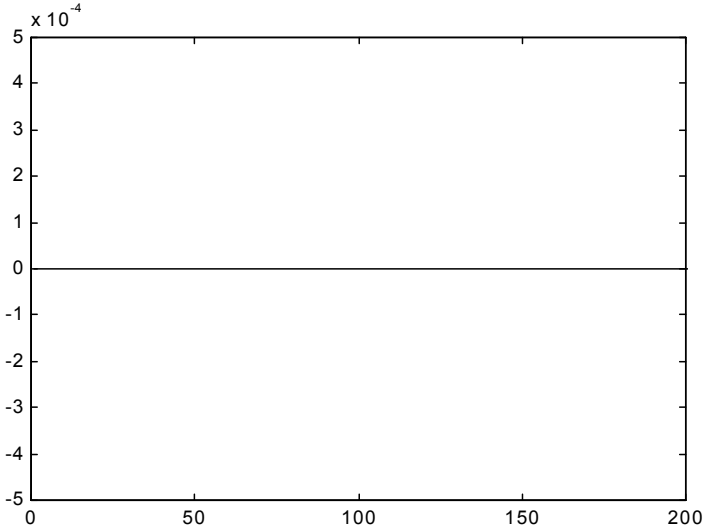
$$\Delta B = B_P - B_M > \lg_2 \left(2 \cdot \sum_{n=1}^{N} \left| h[n] \right| \right)$$

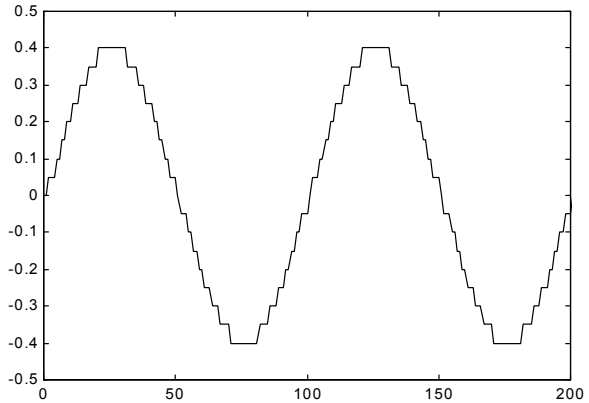
- Trebuie asigurat un compromis intre **valoarea exponentului Liapunov** maxim, dorit a fi mare, si **volumul suplimentar de date** transmis, dorit a fi minim.

Rezultate de simulare









Bibliografie

- Suport de curs: \Lab_Files\6TMPS_CNPS\Suport_Curs\
  - www.scs.etc.tuiasi.ro/
- Suport de laborator: \Lab_Files\6TMPS_CNPS\Suport_Laborator
  - www.scs.etc.tuiasi.ro/
- *I. Ciocoiu, V. Grigoras; "Tehnici moderne de procesare a semnalelor"*

Ed. Cermi 2005 (cap. 4 si 5):

- \Lab_Files\6TMPS_CNPS\Tehnici moderne de procesare a semnalelor
- *T. S. Parker, L. O. Chua; "Chaotic Dynamics Algorithms" 1989:*
  - \Lab_Files\6TMPS_CNPS\Chaotic Dynamics Algorithms - Parker & Chua
- *H. G. Schuster; "Deterministic Chaos" 1984*
- *J. Guckenheimer, P. Holmes; "Nonlinear Oscillations, Dynamical Systems and Bifurcations of Vector Fields" Springer-Verlag 1983*