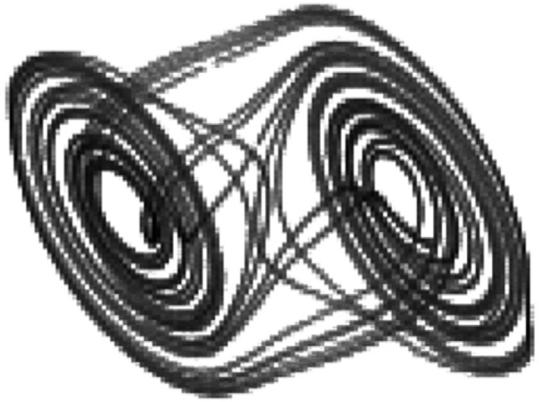
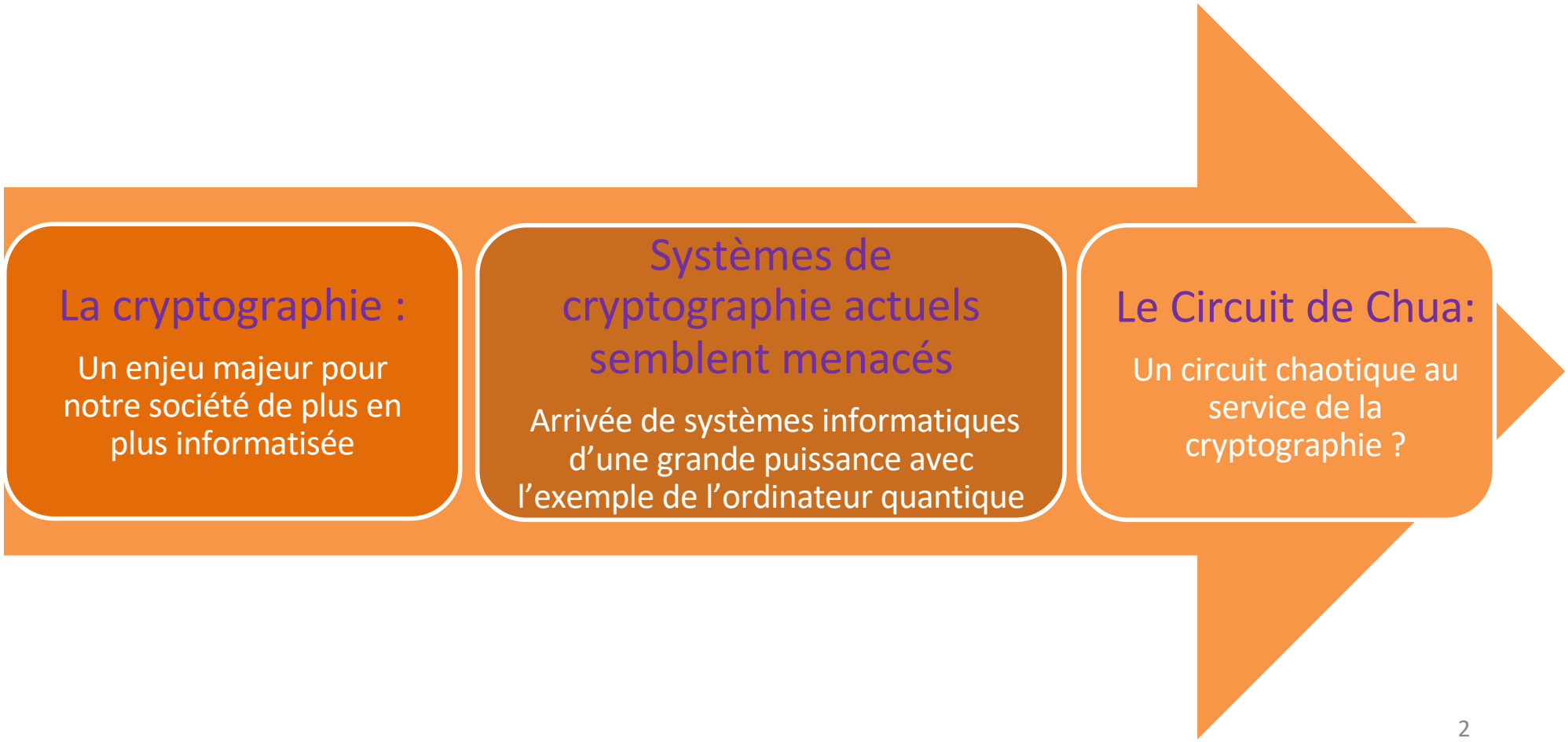
LE CIRCUIT DE CHUA



Une application de l'utilisation du chaos au service de la cryptographie

Par Daniel Sbeiti

INTRODUCTION



PLAN

I-Présentation du circuit de Chua

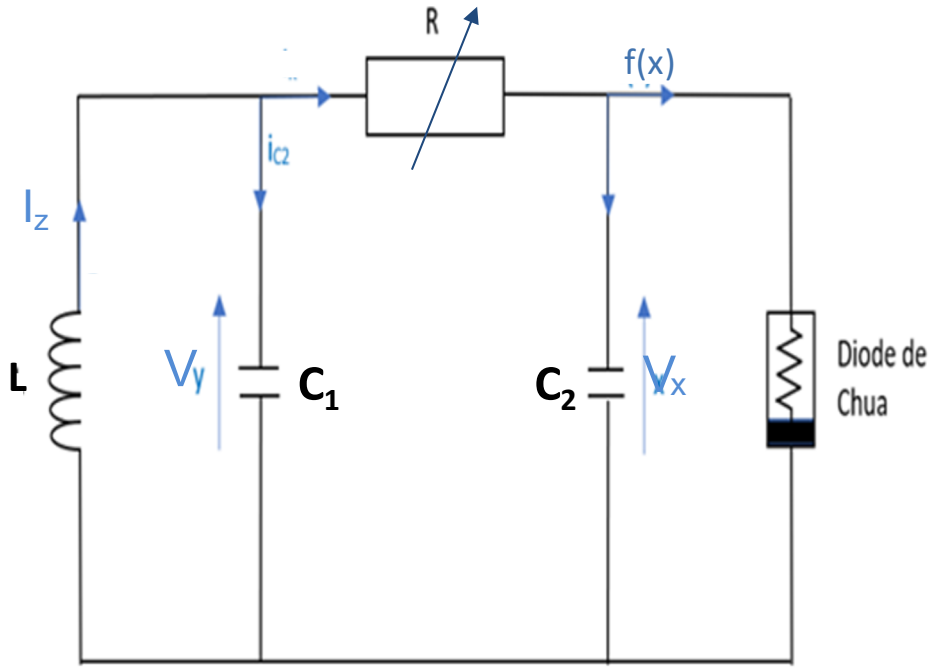
II-Analyse du signal généré par le circuit

III-Application du circuit à la cryptographie

I-Présentation du circuit de Chua

1) Vue d'ensemble du circuit

Partie « oscillateur » du circuit



Circuit chaotique le plus simple en termes de composants :

L = 15 mH	C_1 = 10 nF	C_2 = 100 nF	R = (2,5±0,1) kΩ

Les équations du système : non linéaires :

$$\begin{cases} \frac{dVx}{dt} = \frac{1}{C1} \times \left(\frac{1}{R} (Vy - Vx) - f(x) \right) \\ \frac{dVy}{dt} = \frac{1}{C2} \times \left(Iz - \frac{1}{R} (Vy - Vx) \right) \\ \frac{dIz}{dt} = -\frac{Vy}{L} \end{cases}$$

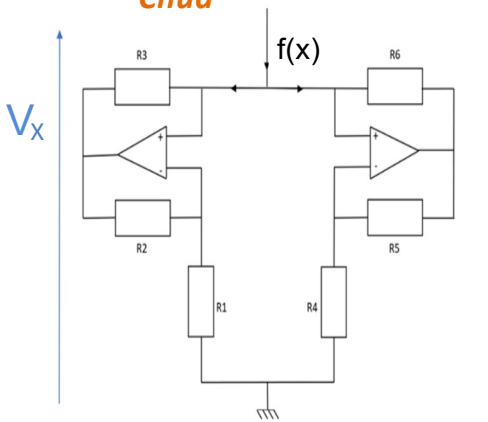
$$f(x) = m_0 x + 0{,}5 \times (m_1 - m_0)|x + V_{sat}| + 0{,}5 \times (m_0 - m_1)|x - V_{sat}|$$

$$Avec \quad m_1 = -\left(\frac{R2}{R1 \times R3} + \frac{R5}{R4 \times R6} \right) \quad et \quad m_0 = \frac{1}{R6} - \frac{R2}{R1 \times R3}$$

I-Présentation du circuit de Chua

2) La diode de Chua

Diode de Chua

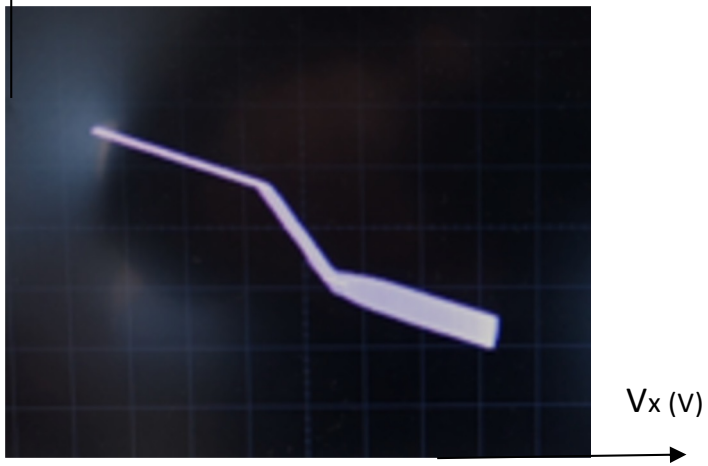


Caractéristique de la diode de Chua :

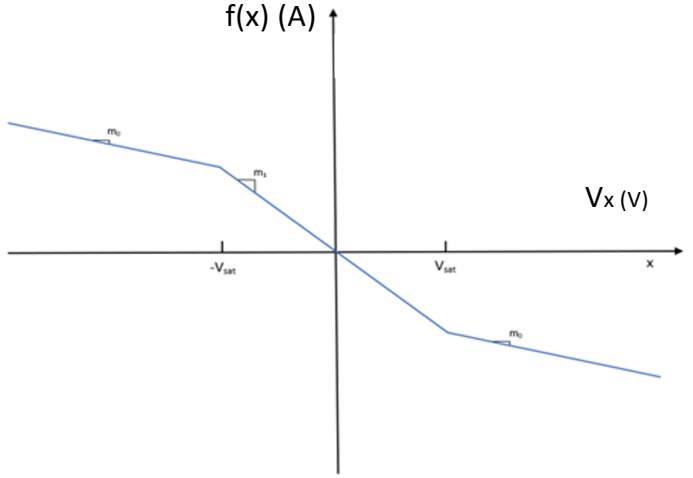
- Ligne brisée (équations non linéaires)
- Pente négative car apport d'énergie par résistance négatives

f(x) (A)

Courbe caractéristique expérimentale :



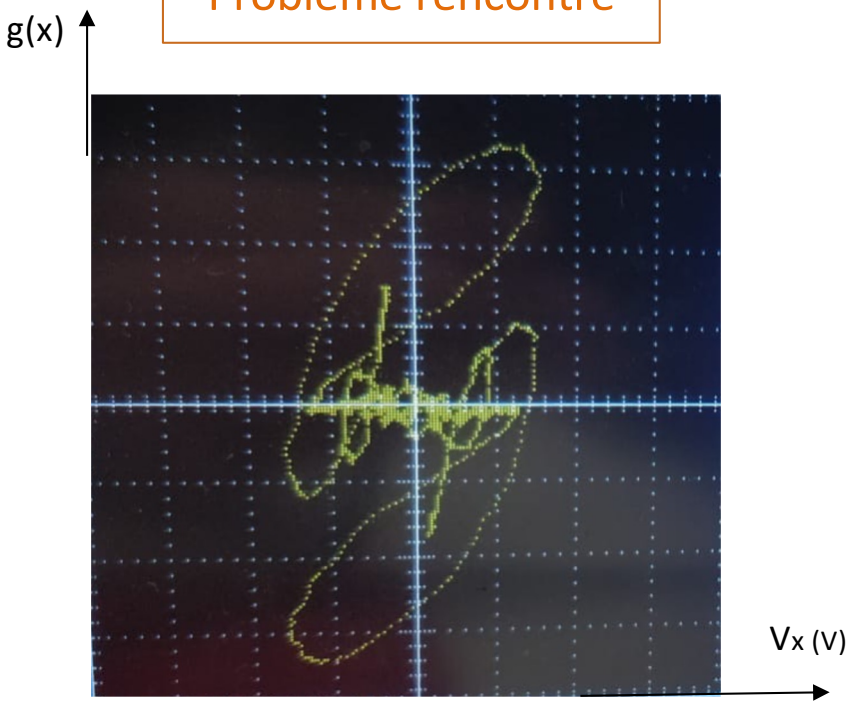
Attendu théorique :



I-Présentation du circuit de Chua

3) Mise en oeuvre expérimentale

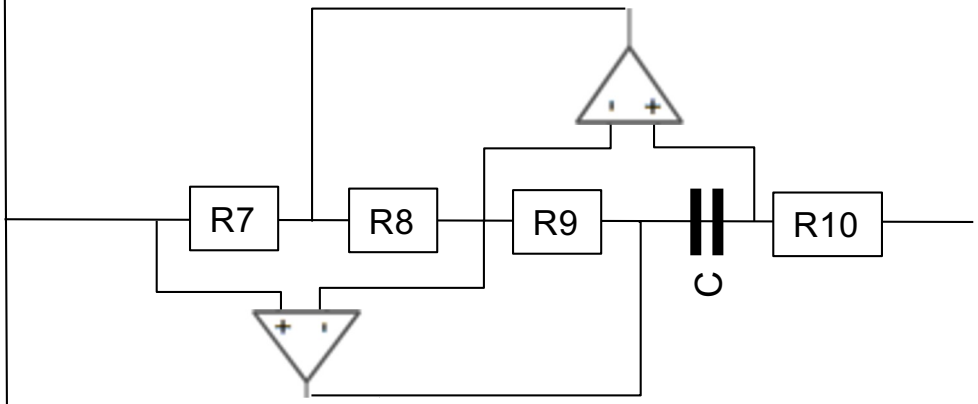
Problème rencontré



Représentation XY obtenue initialement à l'oscilloscope

- Échec car résistance interne 80Ω > 10Ω (max)
- Courbe qui converge vers la tension nulle

Solution :



Inductance simulé de résistance théoriquement nulle

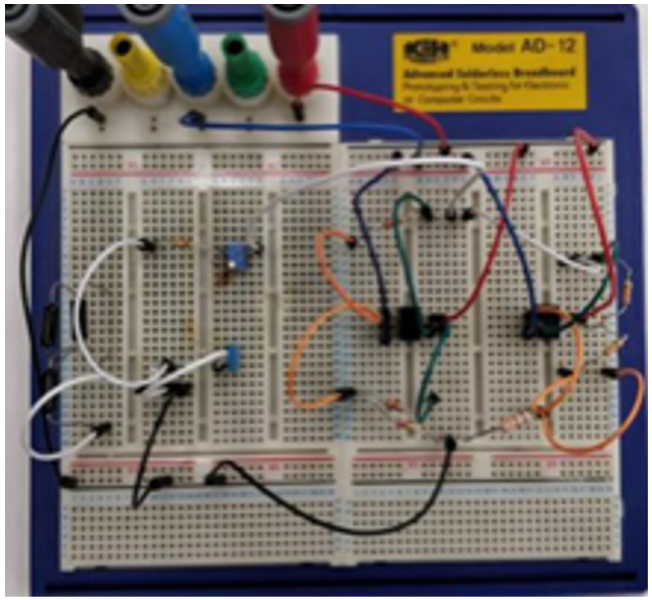
R_7, R_8, R_9, R_{10} = 100Ω, 1kΩ, 1kΩ, 2,5kΩ	R = 100 nF

I-Présentation du circuit de Chua

3) Mise en oeuvre expérimentale

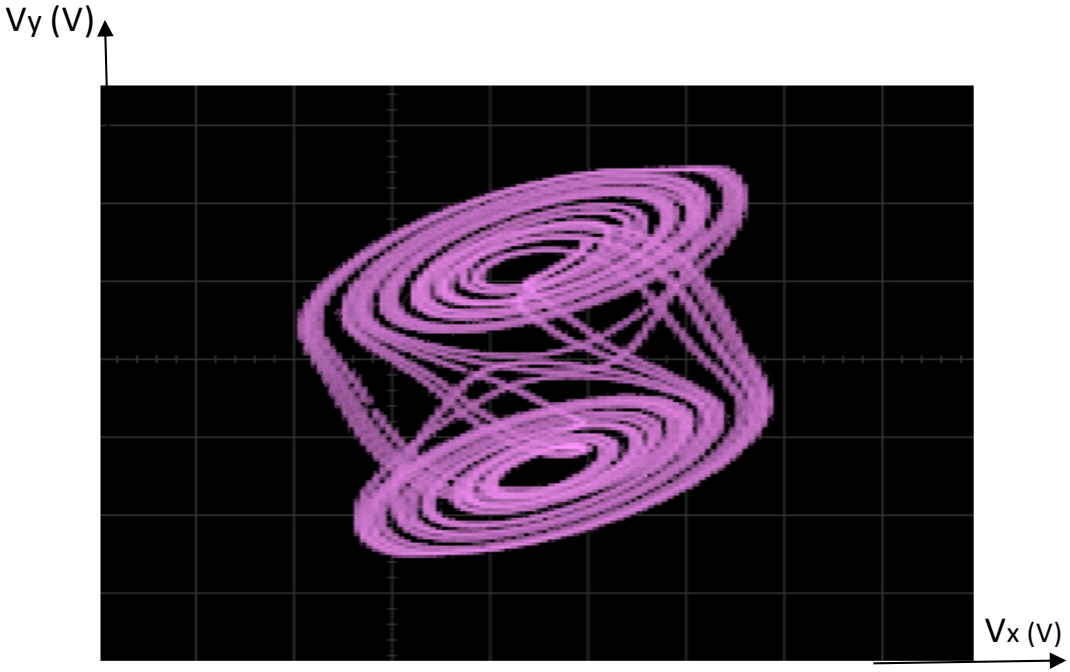
Circuit fonctionnel monté sur plaquette sans soudure :

- Diode de Chua à droite
- Oscillateur LC à gauche



Signal expérimental à l'oscilloscope en mode XY :

- Après quelques mois, ce signal est enfin obtenu !
  D'après la littérature : *double attracteur de Chua.*



I-Présentation du circuit de Chua

3) Mise en oeuvre expérimentale

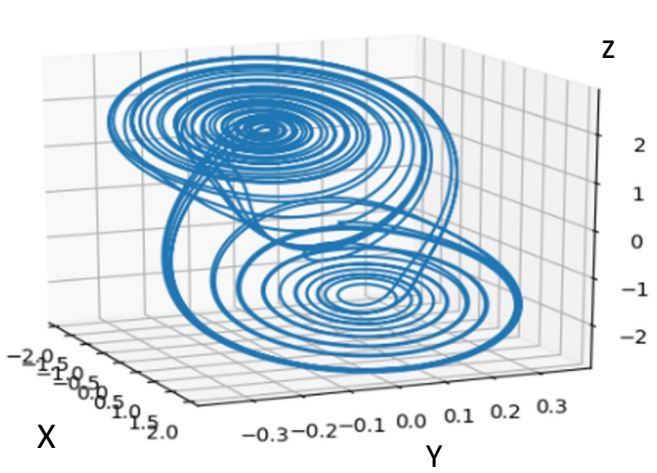
Résolution Python des équations du circuit, affichage de la solution X, Y, Z :

- Double attracteur caractéristique d'un régime chaotique
- Forte sensibilité aux conditions initiales

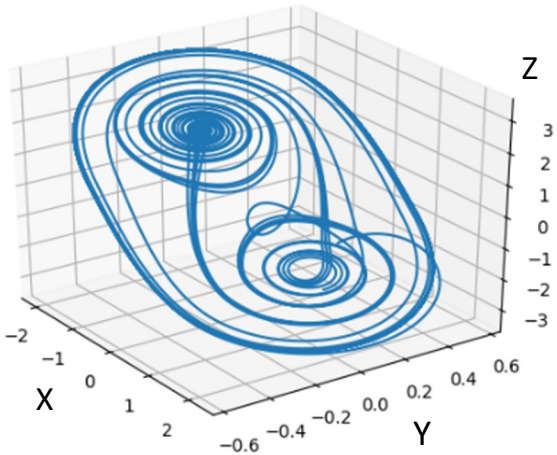
Adimensionnement des variables :

- $X = \frac{x}{x_c}$
- $Z = \frac{R \times z}{x_c}$
- $Y = \frac{y}{x_c}$
- $T = \frac{t}{R \times C_2}$

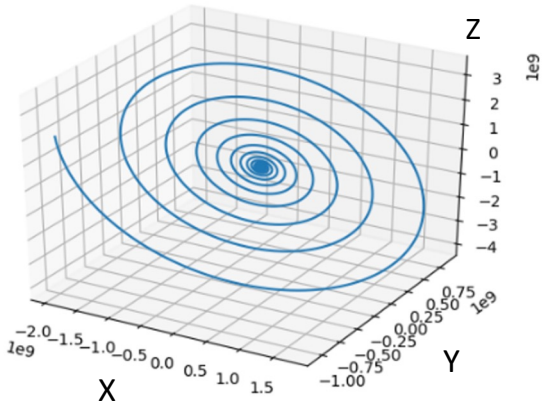
X_0 = 0,7mV ; Y_0 = 0 mV ;
Z_0 = 0 mV



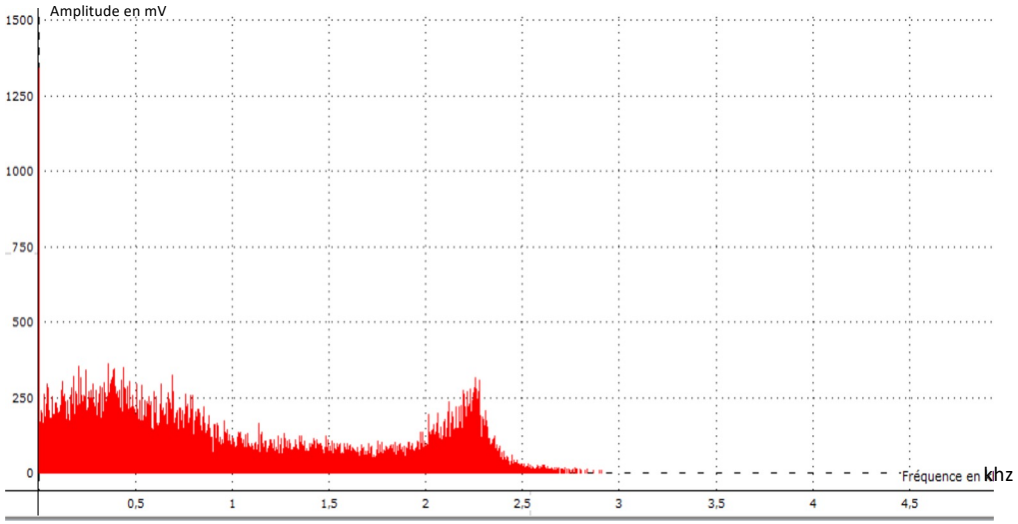
X_0 = 2,01mV ; Y_0 = 0 mV ;
Z_0 = 0 mV



X_0 = 2,07 mV ; Y_0 = 0 mV ;
Z_0 = 0 mV



II- Analyse du signal



FFT du signal échantillonné (Te = 10µs, 256 000 points)

Analyse des résultats

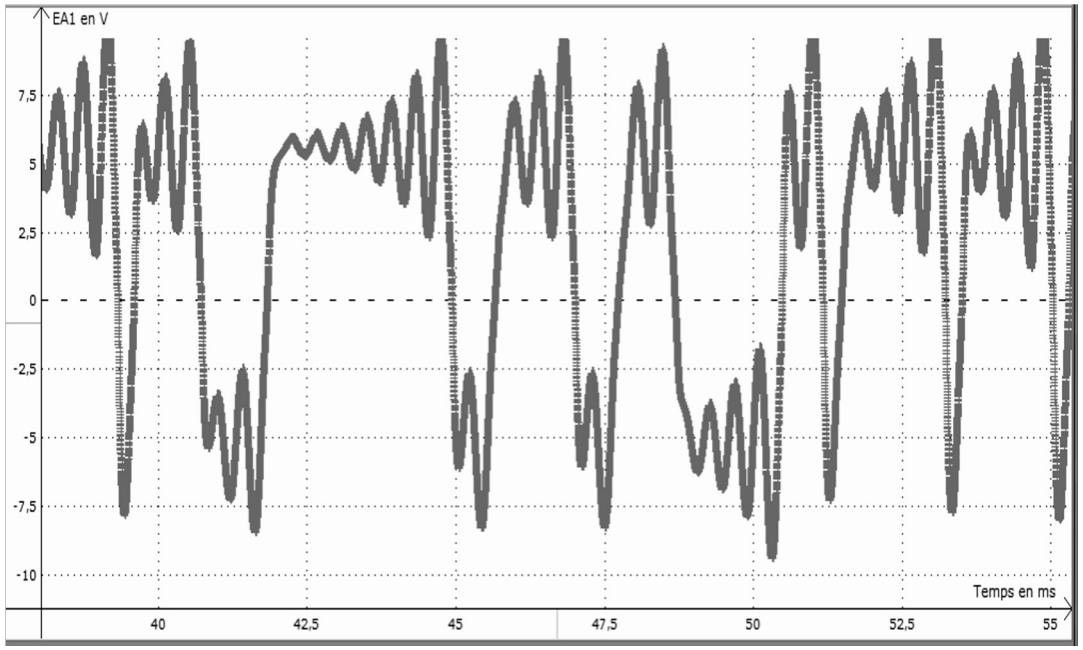
- Pas de fréquences prédominantes
- Fréquence à 2,3 kHz attendue (passage par le circuit LC), n'est pas une limite à l'utilisation
- Composante continue ?

Limites rencontrées

- Nécessité d'un analyseur de spectre analogique
- Ici analyseur de spectre numérique, fréquences caractéristiques "fantômes" car fenêtre limitée

III- Les applications

1) La RNG : *Random number generator* : principe



Signal échantillonné sur Latis Pro, Te = 10µs, 256 000 points

Principe :

- Générer des séquences de bits à partir d'une propriété du signal.

Propriété exploitée :

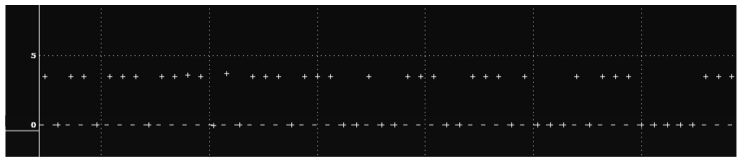
- Signe du signal : oscille aléatoirement entre signe positif et négatif.

- Signal relevé positif → 1
  Signal relevé négatif → 0

III- Les applications

1) La RNG : résultats

Échantillonnage du signal sortant du comparateur :



COURBE BITS

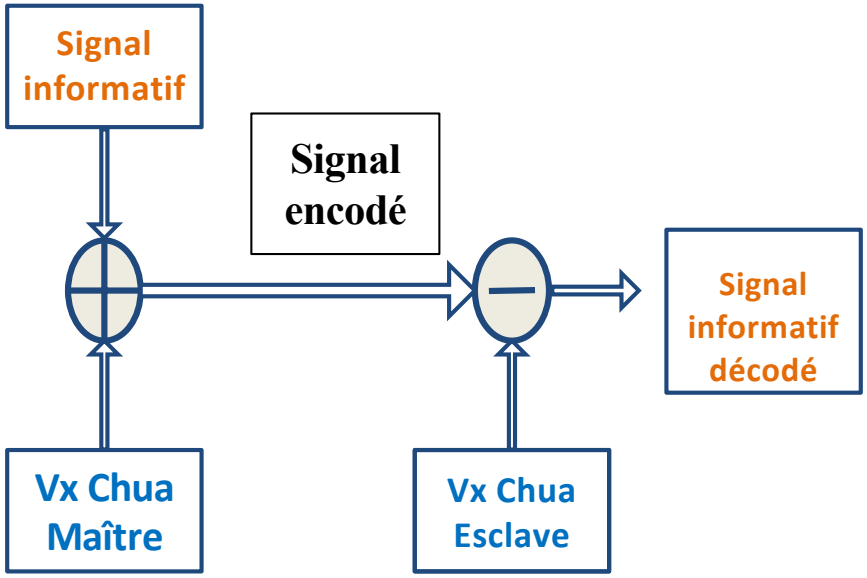
0 0 1 0 1 0 0 0 1 0 1 0

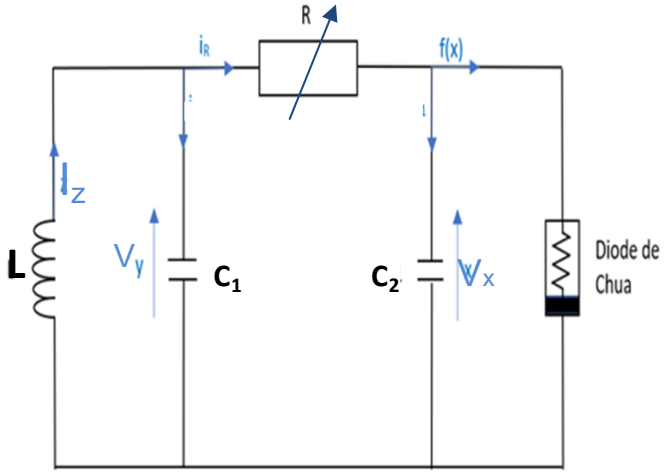
Résultats :

- Séquences exploitables (génération de mots de passes)
- Valeur moyenne sur 1000 points (1 ou 0) : 0,56
  Origine probable : leger offset

III- Les applications

2) Encodage - Décodage : principe





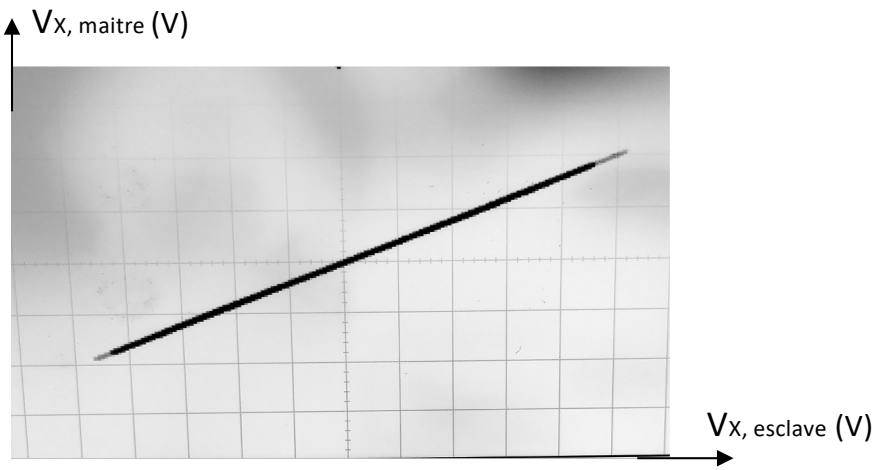
Synchronisation :

- But : avoir le même signal dans les circuits maîtres et esclaves pour réussir décodage
- Montage suiveur utilisé pour que $V_{X,\,maitre} = V_{X,\,esclave}$

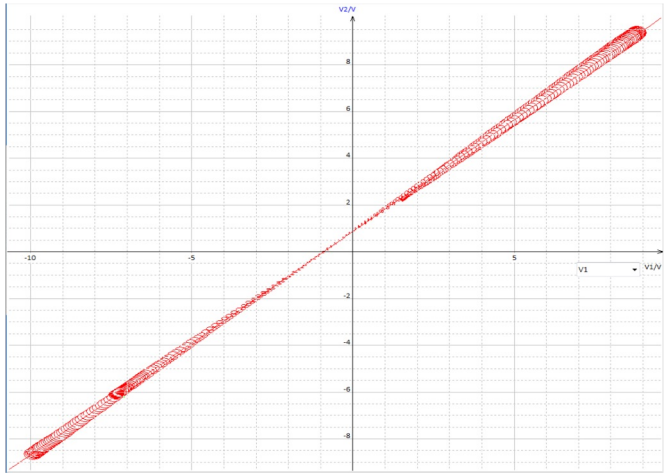
III- Les applications

2) Encodage - Décodage : synchronisation

- $V_{X,\,esclave} = A * V_{X,\,maitre} + B$
- $A = (994{,}8 \pm 0{,}7)$
  $B = (869 \pm 1)\,mV$
- $\chi^2 = 1{,}34$



Observation en XY à l'oscilloscope de $V_{X,\,maitre}$ et $V_{X,\,esclave}$

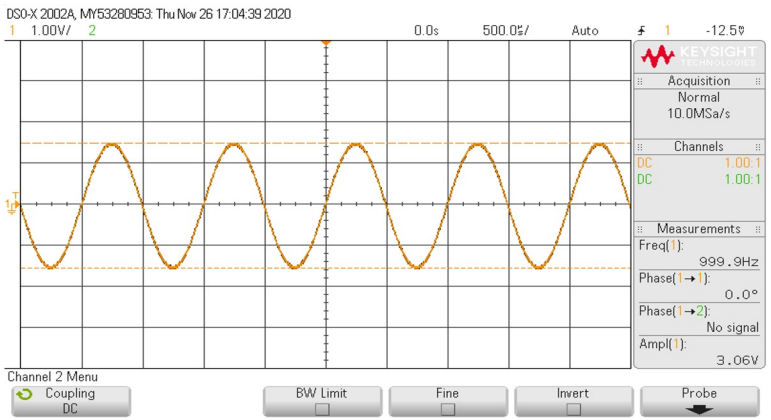


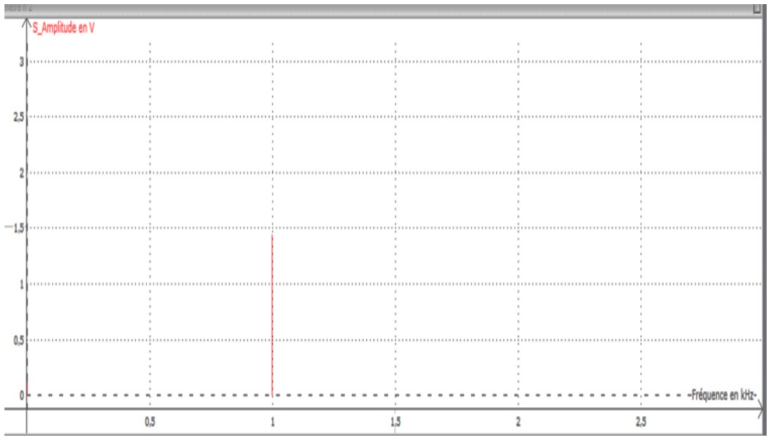
$V_{X,\,maitre}$ *en fonction de* $V_{X,\,esclave}$ avec incertitude sur LatisPro

III- Les applications

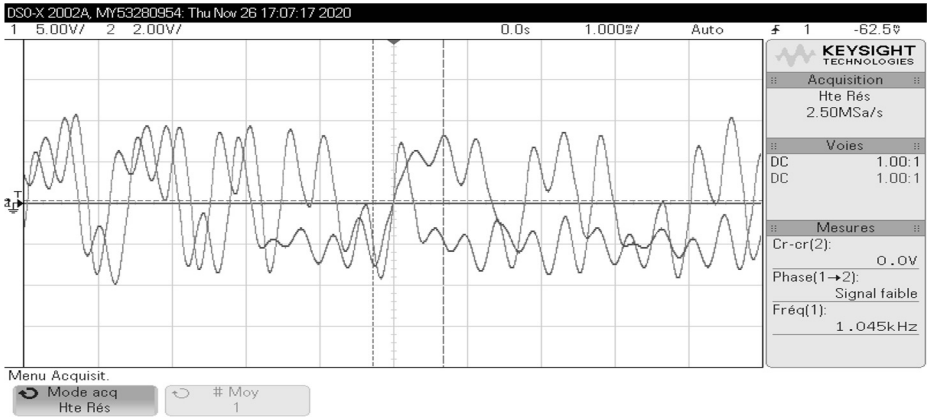
3) Encryptage d'un signal

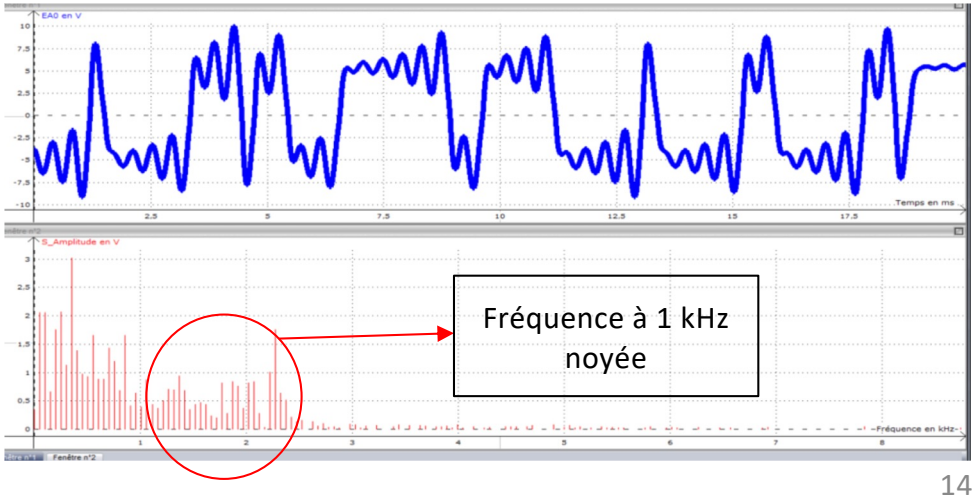
Signal à coder :





Signal codé :

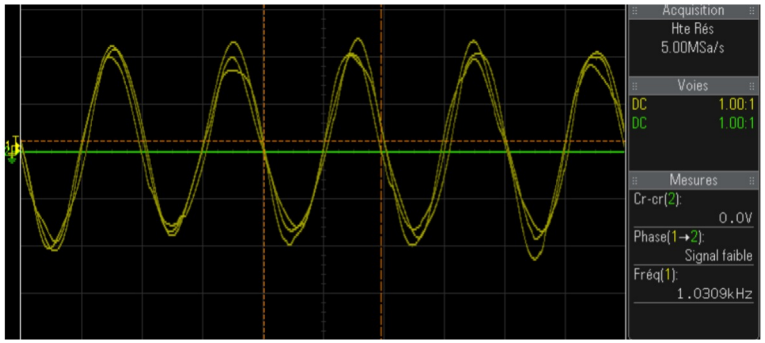




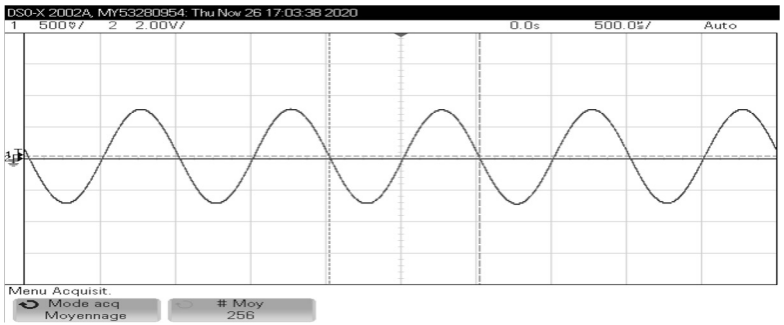
III- Les applications

3) Encryptage d'un signal

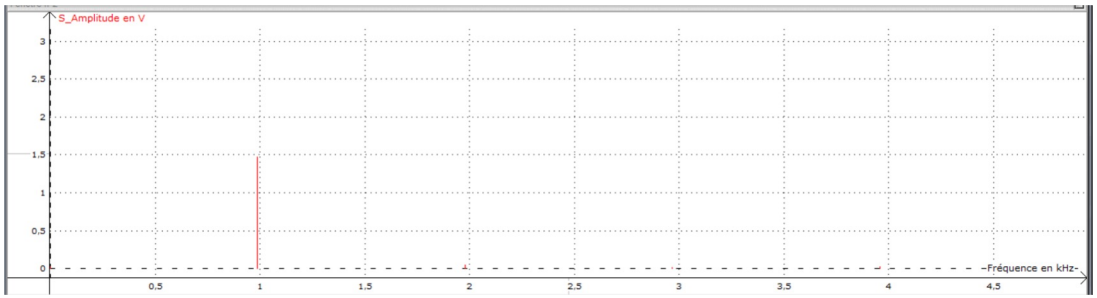
Signal décodé brut :



Signal décodé moyenné :



Analyse de Fourier de signal décodé :



Evaluation quantitative de la qualité d'encodage:

- TDH : *Taux de Distorsion Harmonique*
- Mesure écart relatif entre deux signaux (en tension efficace)
- Ecart experimental ici de 4%, très bas.

LIMITES

LIMITES RENCONTRÉES

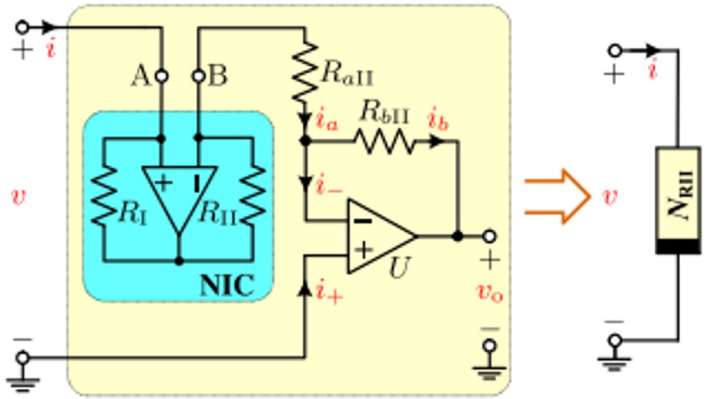
- L'ARQS imposent de courtes distances
- Communications filaires seulement
- Qualité de l'encodage dépendante de la précision des appareils de synchronisation
- Il existe des circuits chaotiques plus complexes mais plus efficaces

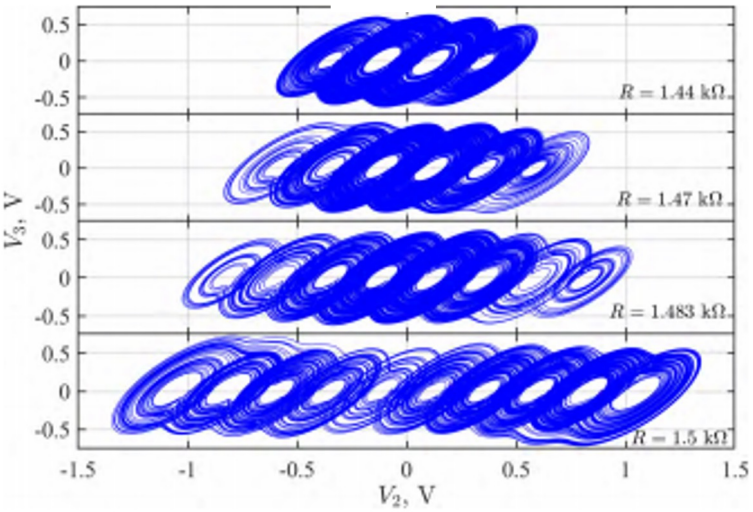
FLEXIBILITÉ ET FIDÉLITÉ

- Toute nature de signal
- Toutes les fréquences conventionnellement utilisées
- Signal décodé fidèle à celui encodé
- Apparition d'un leger bruit

LIMITES

D’après les travaux de Ning Wang et Chengqing Li

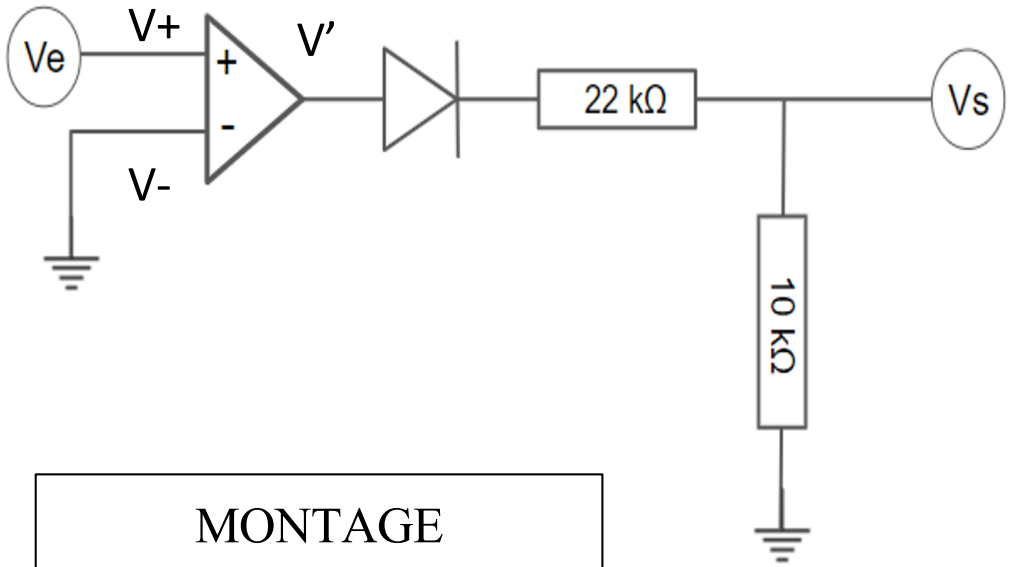




Autre version de la diode de Chua

Attracteurs de Chua multiple obtenu

IV - Annexe : La RNG comparateur



MONTAGE COMPARATEUR UTILISE

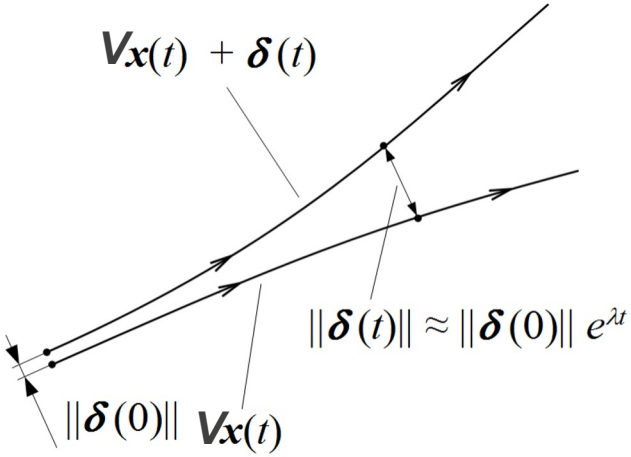
Principe :

- **Si Ve > 0V** (*ie* V+ > V-) :
  V' = +Vsat > 0V
  Diode passante
  Vs = + Vsat *(ici Vsat/3,2)*

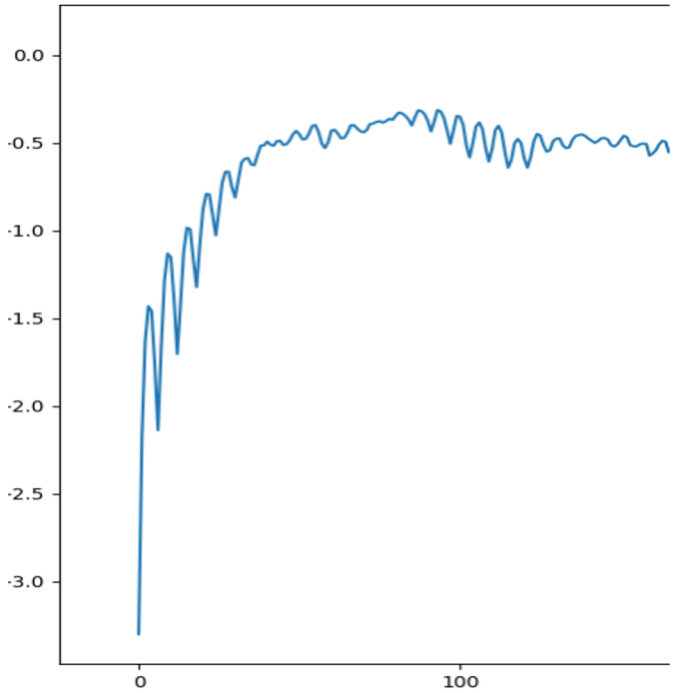
- **Si Ve < 0V** (*ie* V+ < V-) :
  Diode bloquée
  V' = 0V

- On relève périodiquement Vs

IV - Annexe : L'exposant de Lyapunov



Pente à l'origine de ln(δ(t)) ⇒ λ



Tracé adimensionné de ln(δ) en fonction de t (Python)

Mise en œuvre grâce à un algorithme adapté du net:

- Valeur obtenue : 0,5 ± 0,2 ; Valeur en littérature : 0,23± 0,02
- λ > 0
- Limites de l'algorithme : 1 seule dimension considérée sur 3

IV - Annexe : Additionneur - Soustracteur

Circuit additionneur

Circuit soustracteur