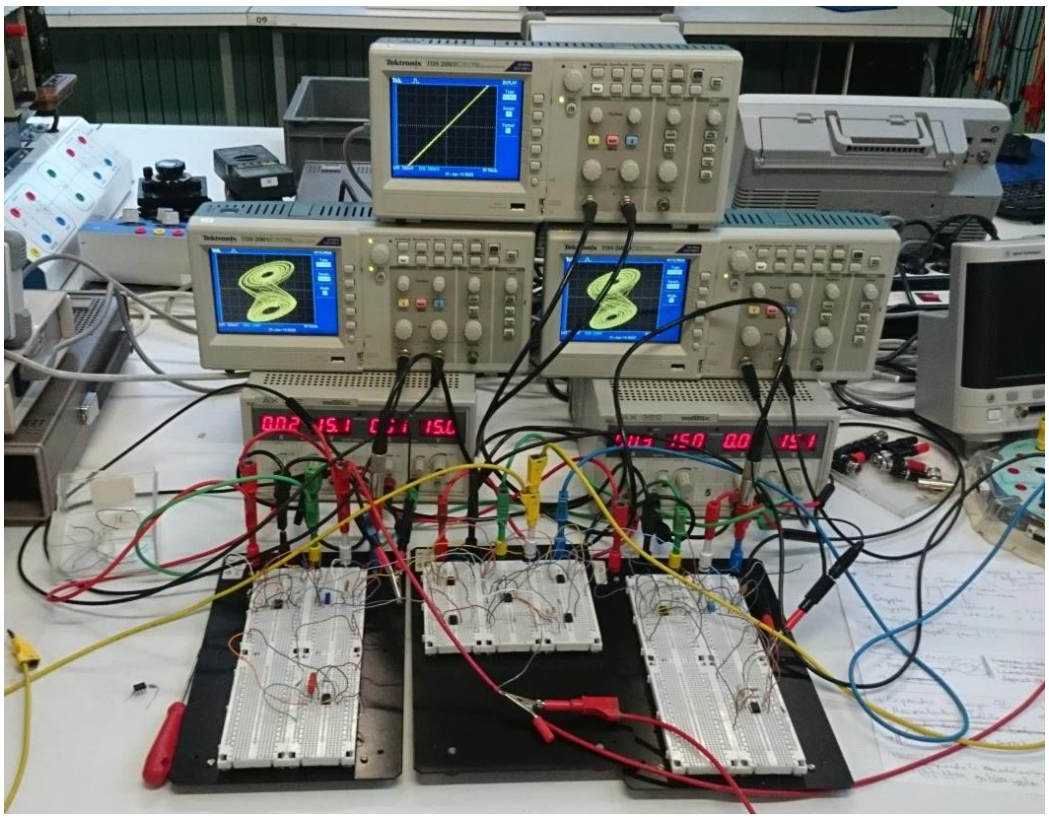
TRANSFERT ET CHAOS

-Cryptographie d'un message par synchronisation de deux oscillateurs chaotiques de Chua-



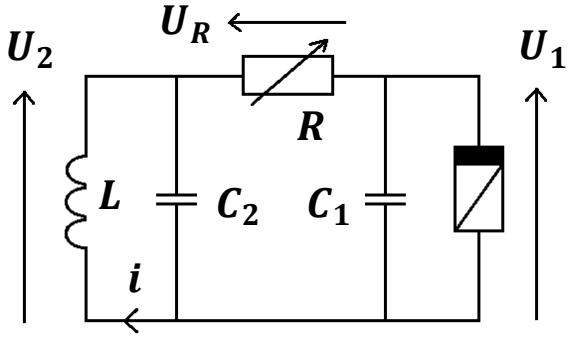
I- L'oscillateur chaotique et la synchronisation

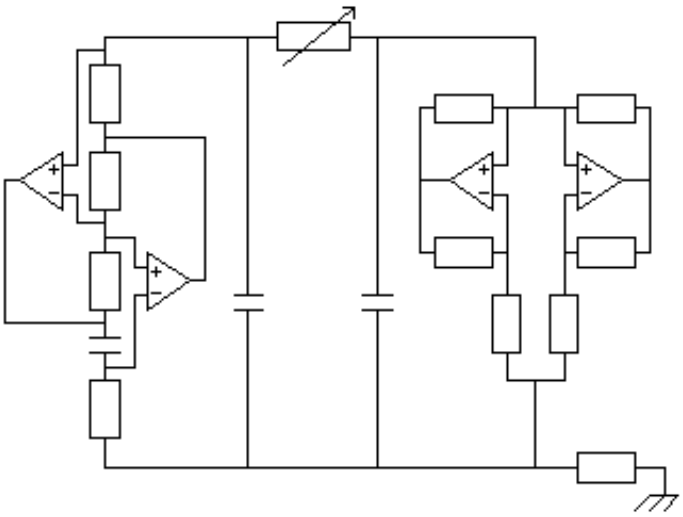
II- Le transfert d'informations

III- La sécurité du cryptage

I- L'oscillateur chaotique et la synchronisation

A. *Etude de l'oscillateur de Chua*

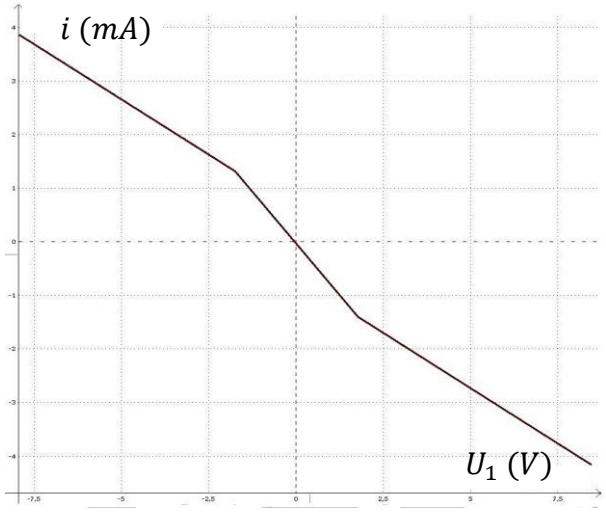




$L = 10mH$; $C_1 = 4{,}7nF$; $C_2 = 47nF$
$R \rightarrow$ *potentiomètre variable*

Caractéristique expérimentale de la diode de Chua

La caractéristique de la diode de Chua est *affine par morceaux*.



$$f(x_1) = -m_0 \cdot x_1 + \frac{1}{2}(m_0 - m_1)[|x_1 + 1| - |x_1 - 1|]$$

$m_0 = 0{,}411 \cdot 10^{-3}\ mA.V^{-1}$
$m_1 = 0{,}797 \cdot 10^{-3}\ mA.V^{-1}$

L'étude du circuit donne :

$$\begin{cases} \frac{dU_1}{dt} = -\frac{1}{C_1} f(U_1) + \frac{1}{RC_1} U_2 - \frac{1}{RC_1} U_1 & (E1) \\ \frac{dU_2}{dt} = -\frac{1}{RC_2} U_2 + \frac{1}{RC_2} U_1 + \frac{1}{C_2} i_L & (E2) \\ \frac{di_L}{dt} = -\frac{1}{L} U_2 & (E3) \end{cases}$$

Après changement de variable :

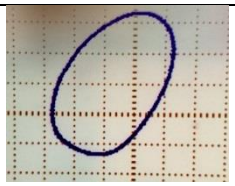
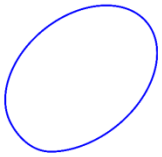
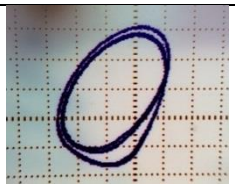
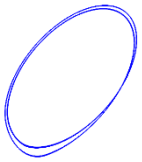
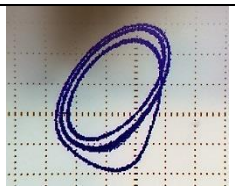
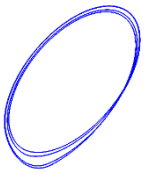
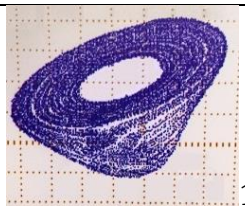
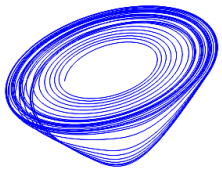
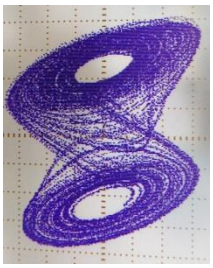
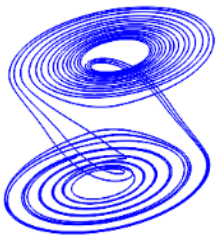
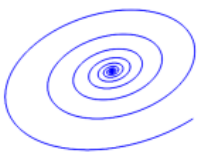
$$(S): \begin{cases} \dot{x}_1 = -x_1 + x_2 - Rf(x_1) \\ \dot{x}_2 = \varepsilon(x_1 - x_2 + x_3) \\ \dot{x}_3 = -Q^2 x_2 \end{cases}$$

$x_1 = u_1$; $x_2 = u_2$; $x_3 = Ri$
$\varepsilon = \frac{C_2}{C_1}$; $Q^2 = R^2 \frac{C_1}{L}$

Une *étude de la stabilité* permet de retrouverune bifurcation de Hopf qui correspond à l'apparition d'un cycle limite.

I- L'oscillateur chaotique et la synchronisation

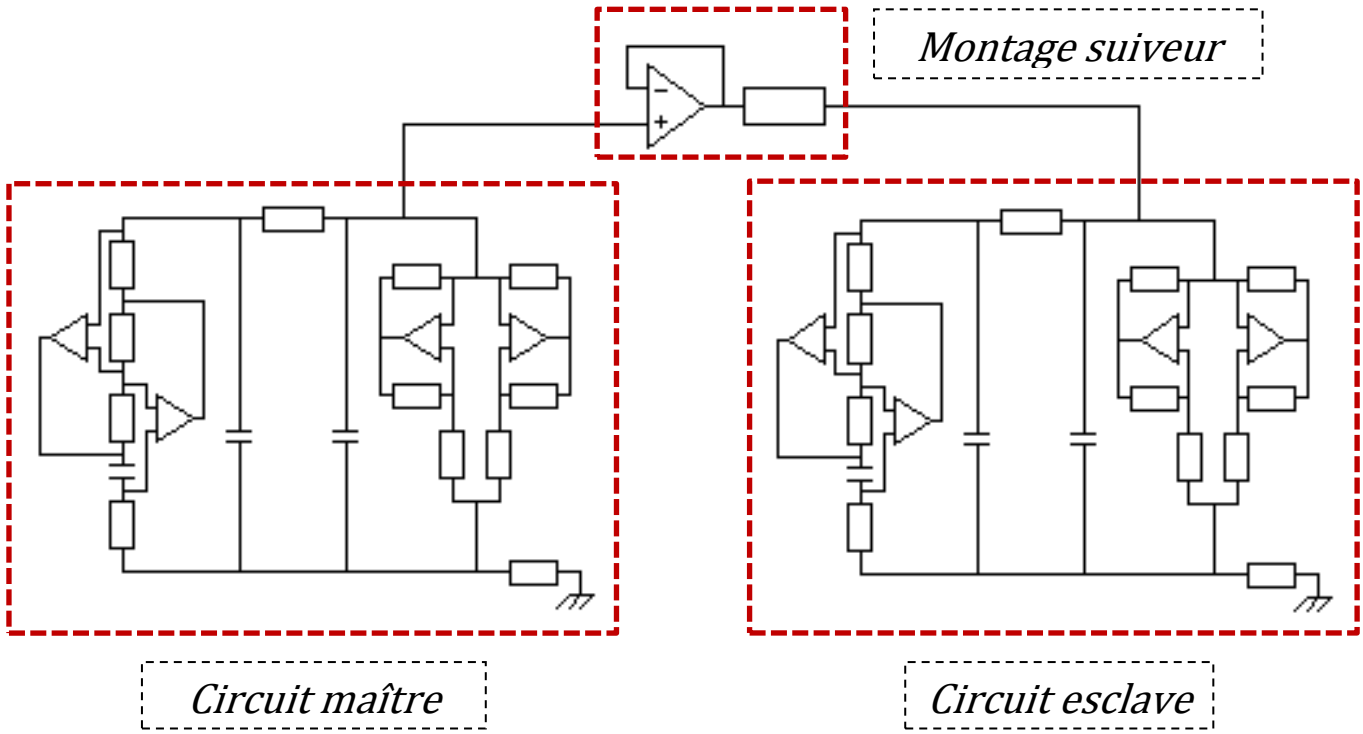
B- Les différents régimes chaotiques

Régime	Expérimental	Simulation (Maple)
Convergent		2500 Ω et plus ↓ 2026 Ω 
Période simple	 1900 Ω	2025 Ω ↓ 2015 Ω 
Double période	 1881 Ω	2014 Ω ↓ 2006 Ω 
Quadruple période	 1876 Ω	2005 Ω ↓ 2004 Ω 
Attracteur simple (type attracteur de Rössler)	 1847 Ω	2003 Ω ↓ 1984 Ω 
Attracteur double (type attracteur de Lorentz)	 1691 Ω	1983 Ω ↓ 1659 Ω 
Divergent		1658 Ω ↓ 0 Ω 

I- L'oscillateur chaotique et la synchronisation

C Synchronisation théorique et expérimentale

Principe de la synchronisation



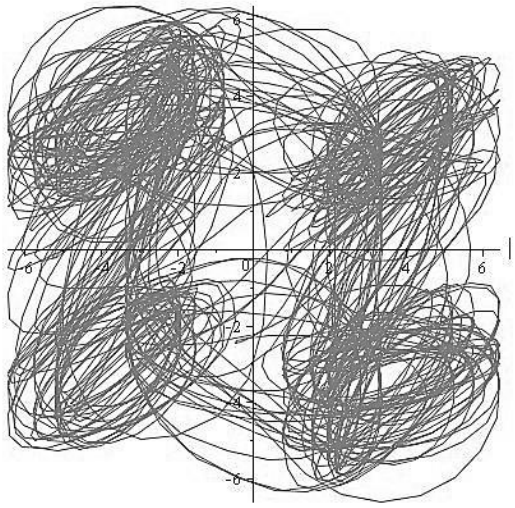
Synchronisation théorique

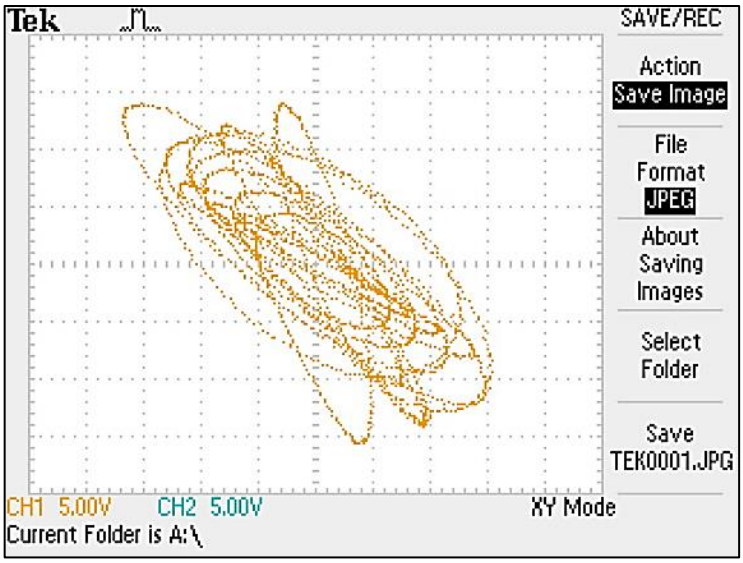
On suppose que le système d'équations qui caractérise le circuit esclave s'écrit ainsi :

$$(\hat{S}):\begin{pmatrix}\dot{\hat{x}}_1\\ \dot{\hat{x}}_2\\ \dot{\hat{x}}_3\end{pmatrix}=\begin{pmatrix}\alpha\left(x_2-x_1+f(x_1)\right)\\ x_1-x_2+x_3\\ -\beta x_2\end{pmatrix}+k(x_3-\hat{x}_3)$$

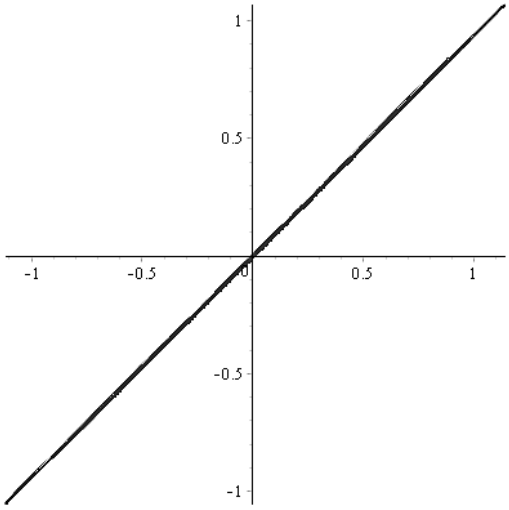
où k est le vecteur de rétroaction qui permet la synchronisation.
Alors le circuit Master et le circuit Slave seront globalement synchronisés de façon asymptotique.

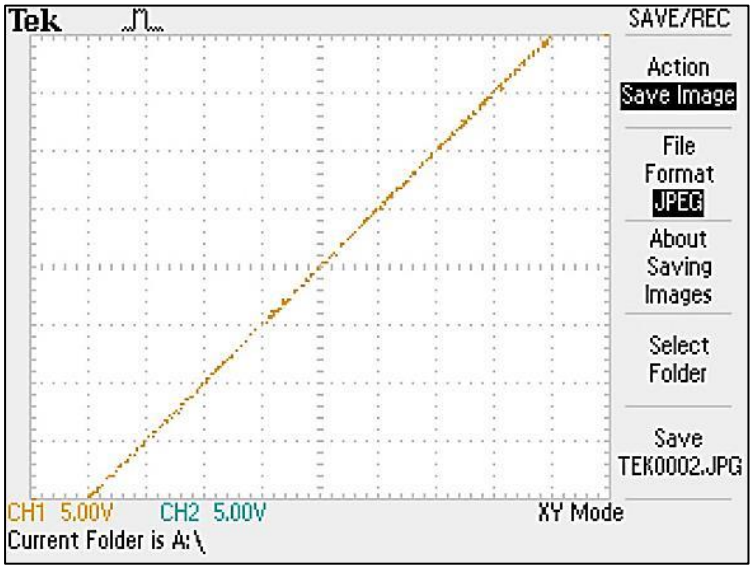
Synchronisation expérimentale et simulation





Circuits non synchronisés *: à gauche la simulation, à droite l'écran de l'oscilloscope.*

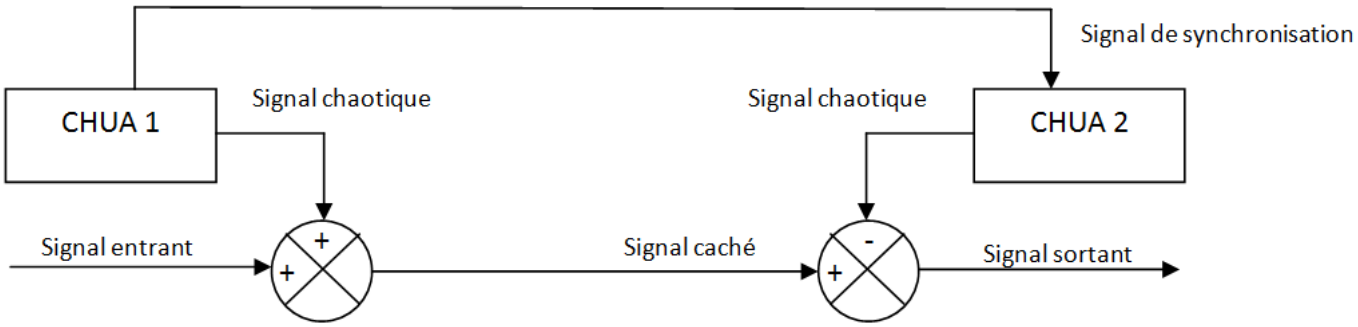




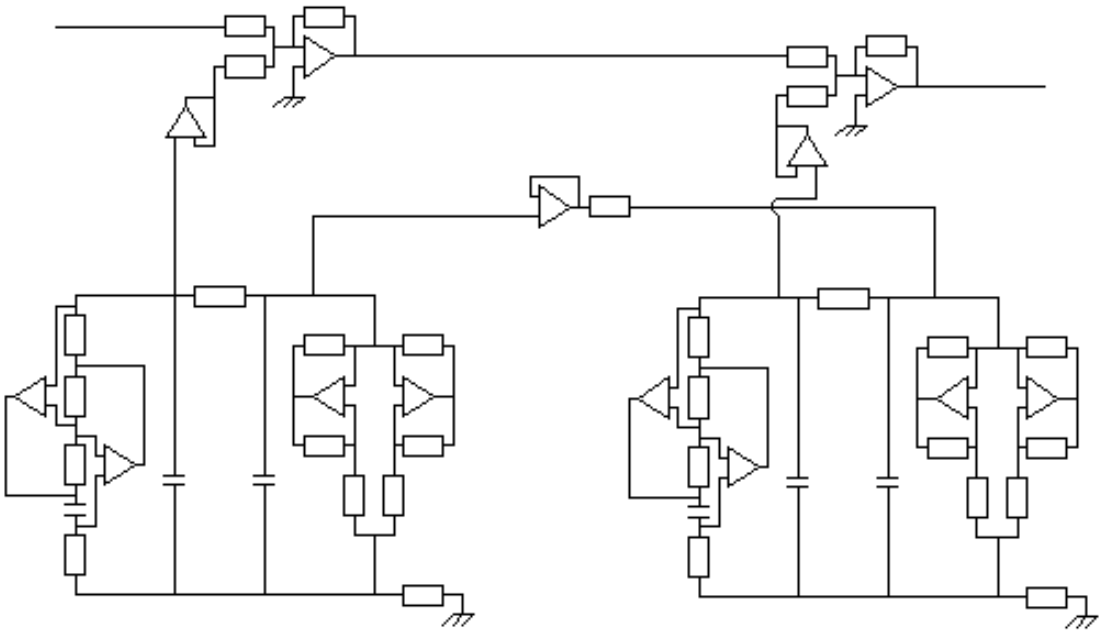
Circuits synchronisés *: à gauche la simulation, à droite l'écran de l'oscilloscope.*

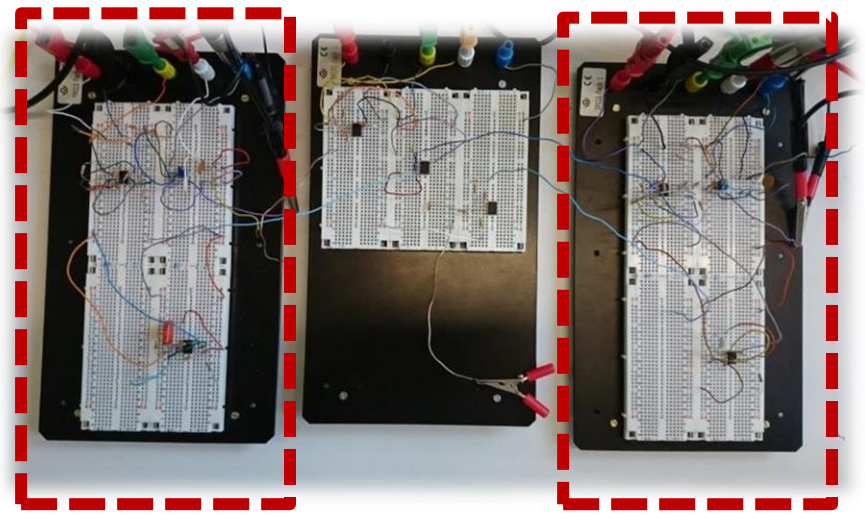
II- Le transfert d'informations

A. Principe du montage



Montage expérimental





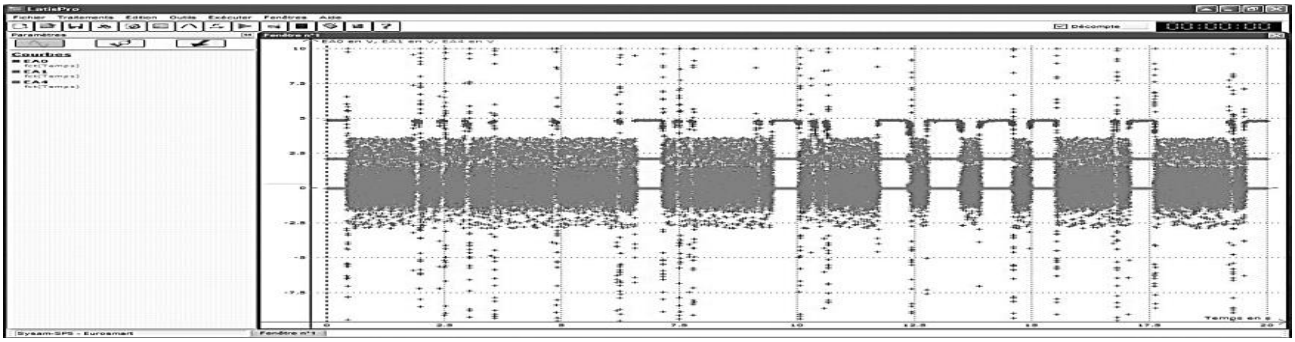
Circuit maître

Circuit esclave

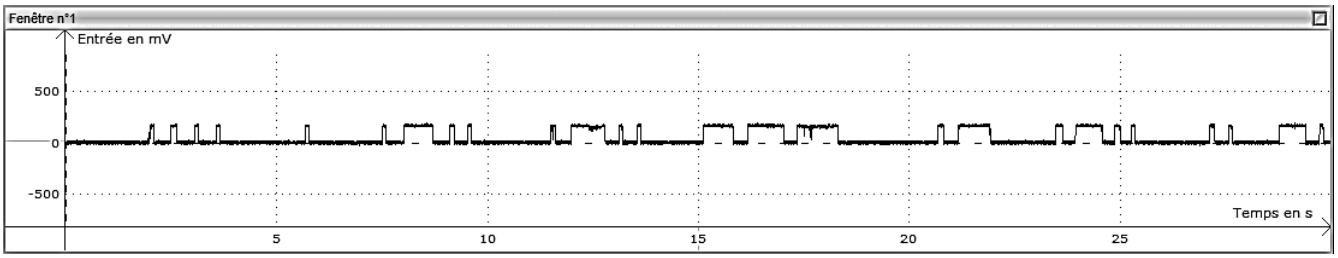
II- Le transfert d'informations

B. Résultats expérimentaux : transmission d'un message

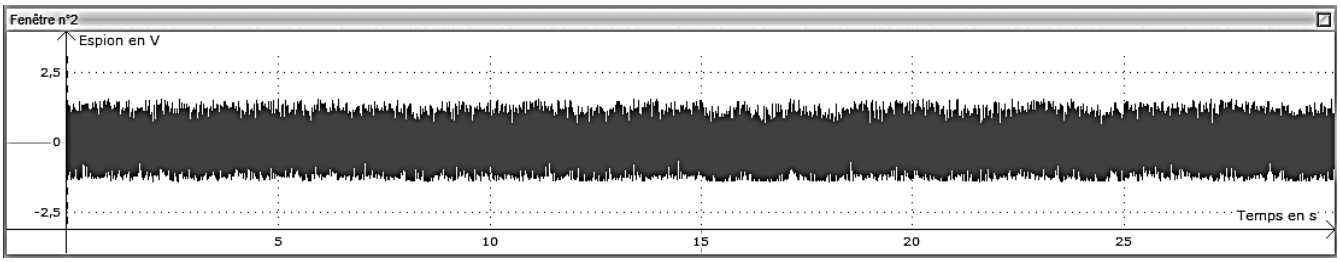
On observe à l'aide du logiciel Latis-pro :



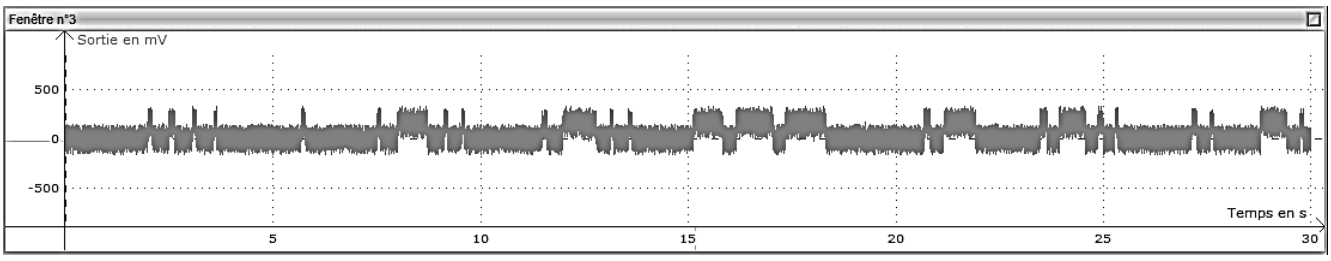
Mauvais montage : court-circuit



Signal d'entrée



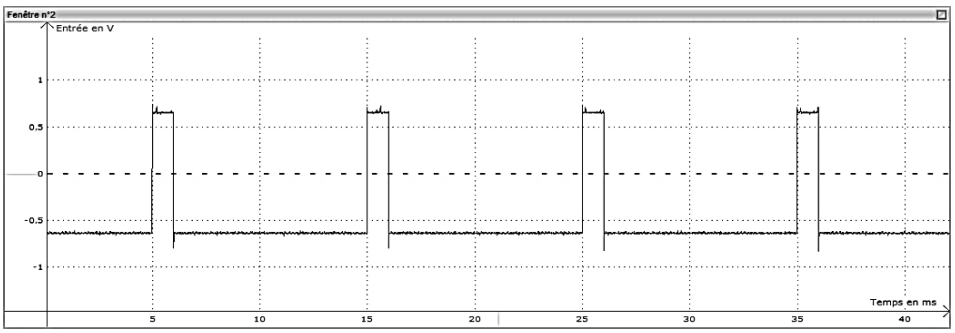
Signal capté par l'espion



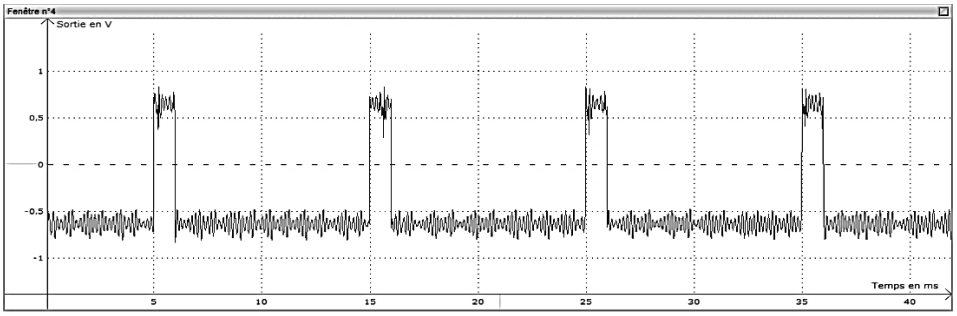
Signal de sortie

II- Le transfert d'informations

c. Simulation numérique et confrontation à l'expérience

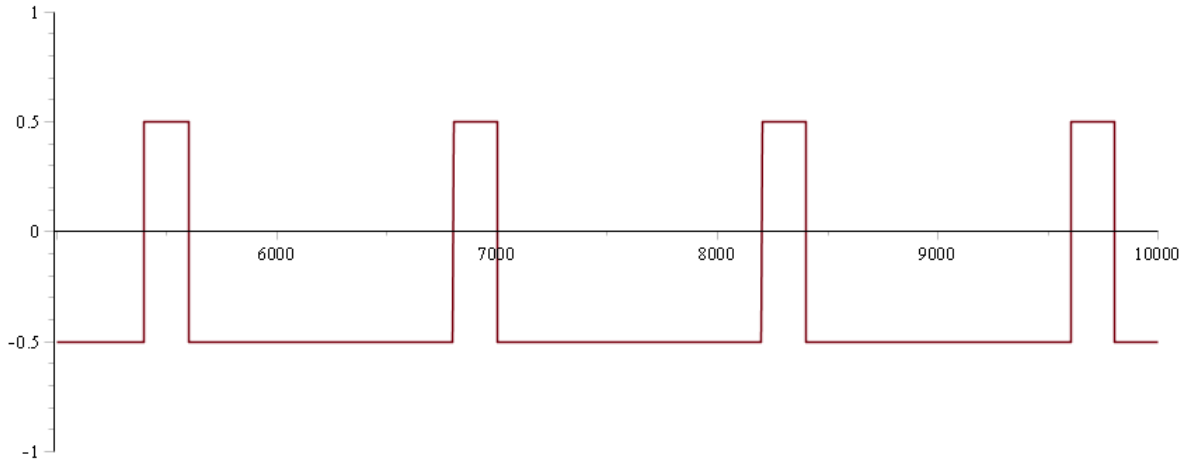


Signal entrant

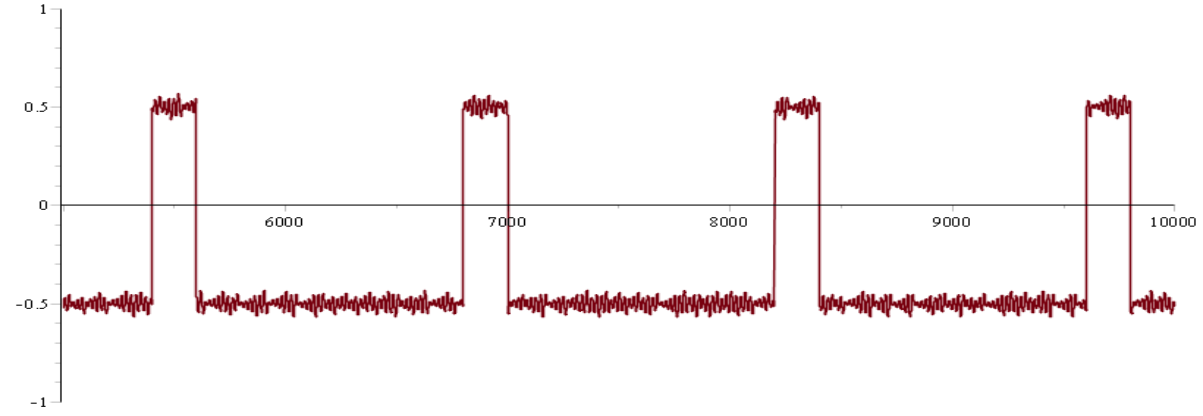


Signal sortant

```
> plot(message(k), k=5000..10000, (-1)..(1));
```

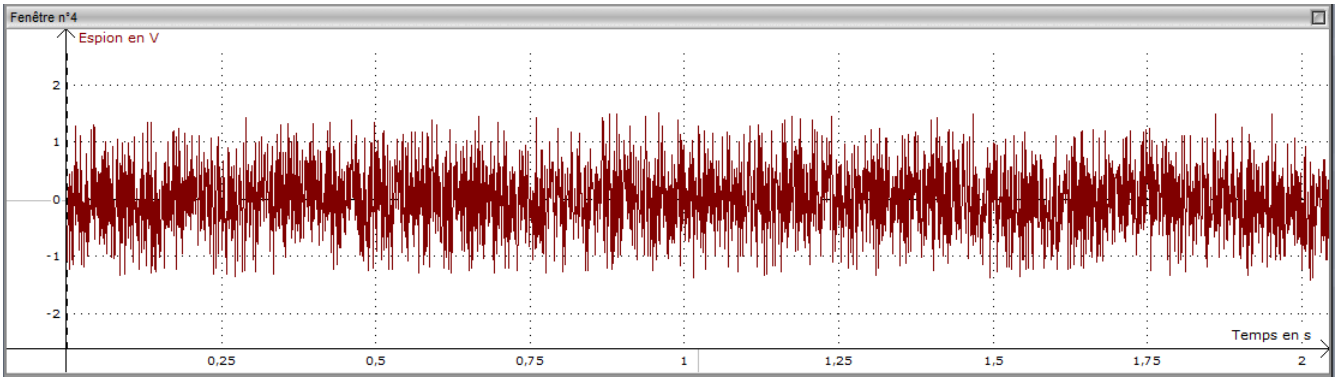



```
> plot([seq([k, subs(Solsynchr(k/10), y(t)) + message(k) - subs(Solsynchr(k/10), yss(t))], k=5000..10000)], 5000..10000, (-1)..(1));
```

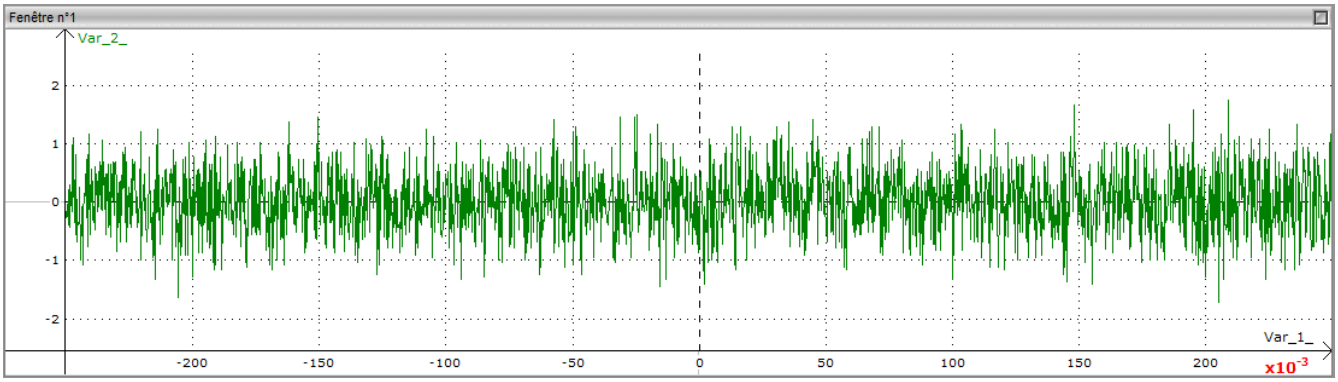


III- La sécurité du cryptage

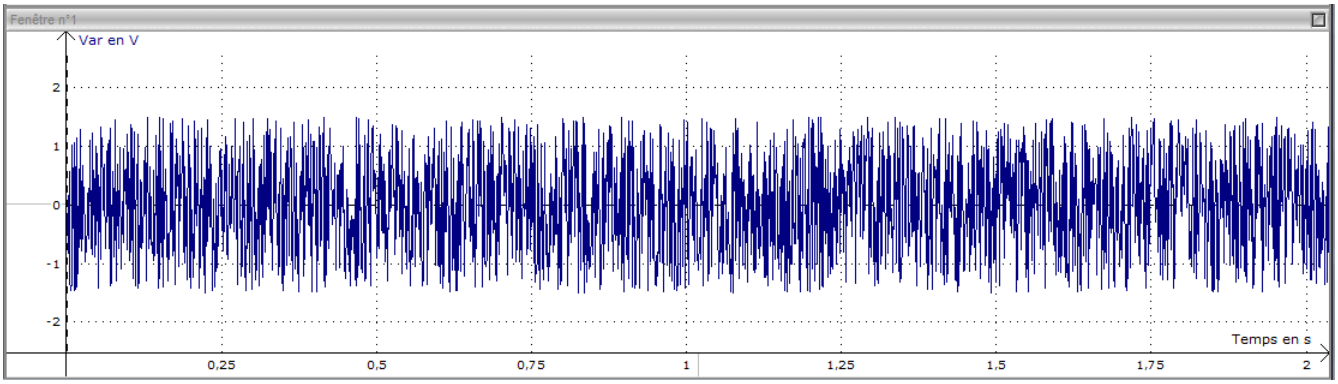
A. La stéganographie



Signal capté par l'espion



Bruit émis par un GBF



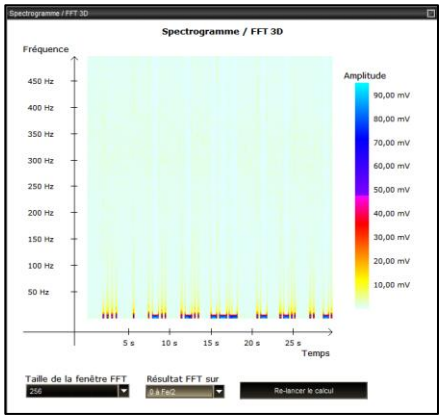
Bruit modélisé (variable aléatoire)

III- La sécurité du cryptage

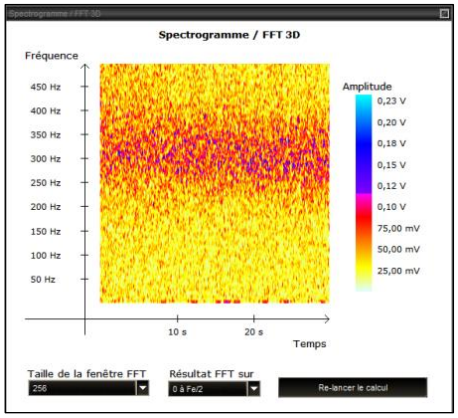
B. Mise en défaut de la sécurité

ANALYSE SPECTRALE

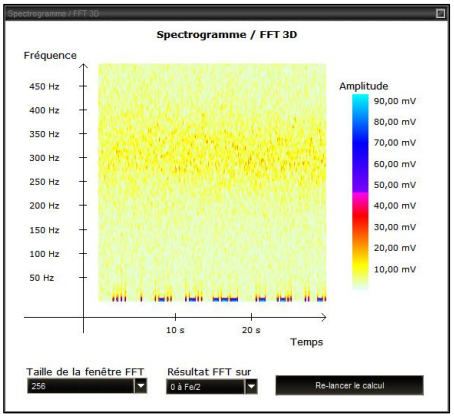
Spectrogrammes : fréquence en fonction du temps
(transformée de Fourier glissante à l'aide du logiciel Latis-pro)



Signal entrant

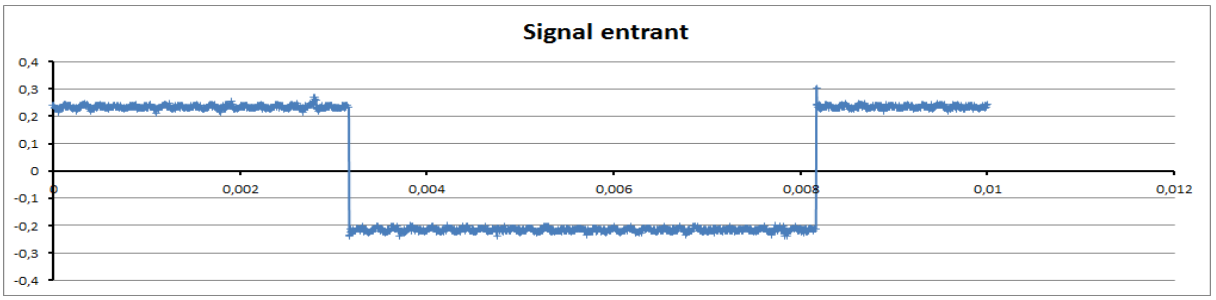


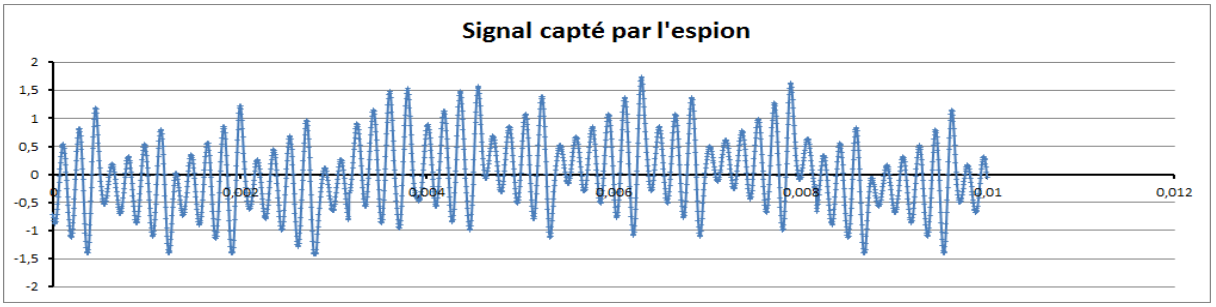
Signal capté par l'espion

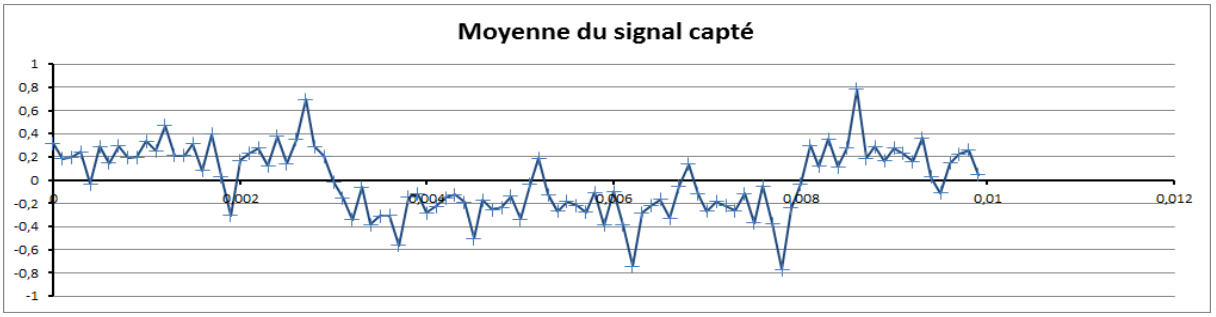


Signal sortant

MOYENNE sur le signal capté à l'aide d'un tableur.





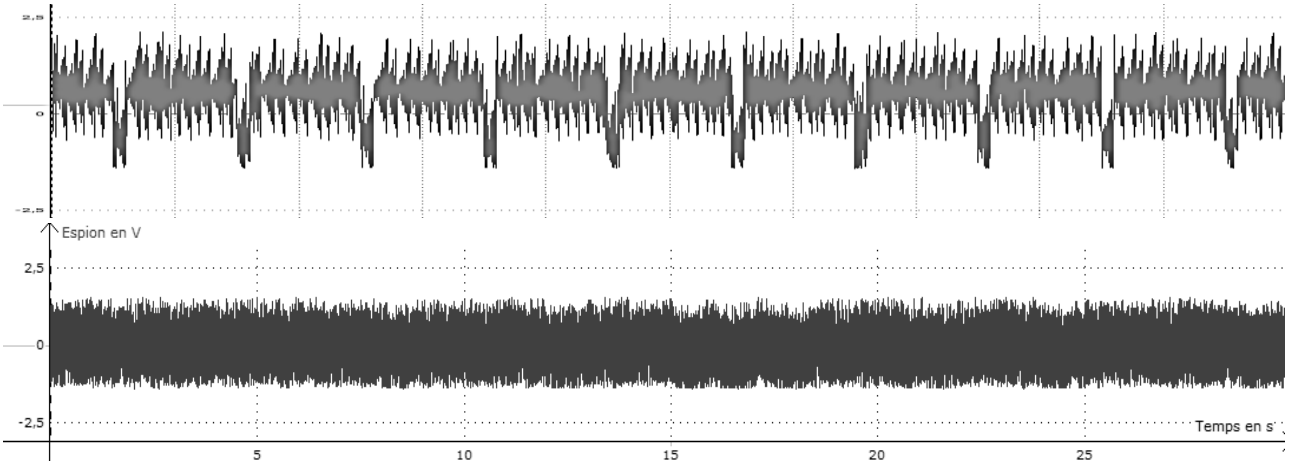


Fréquence d'échantillonnage : 200 *kHz*

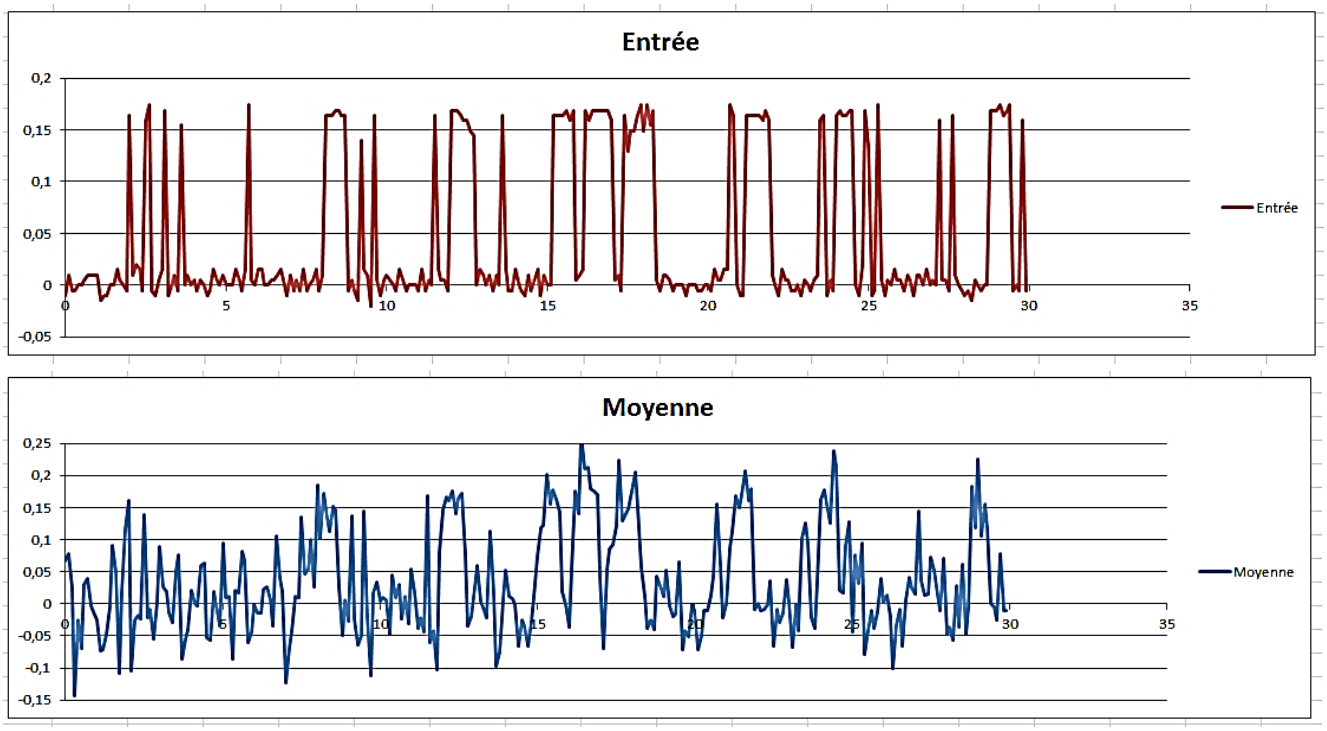
III- La sécurité du cryptage

C. Propositions de solutions

Diminuer l'amplitude du message



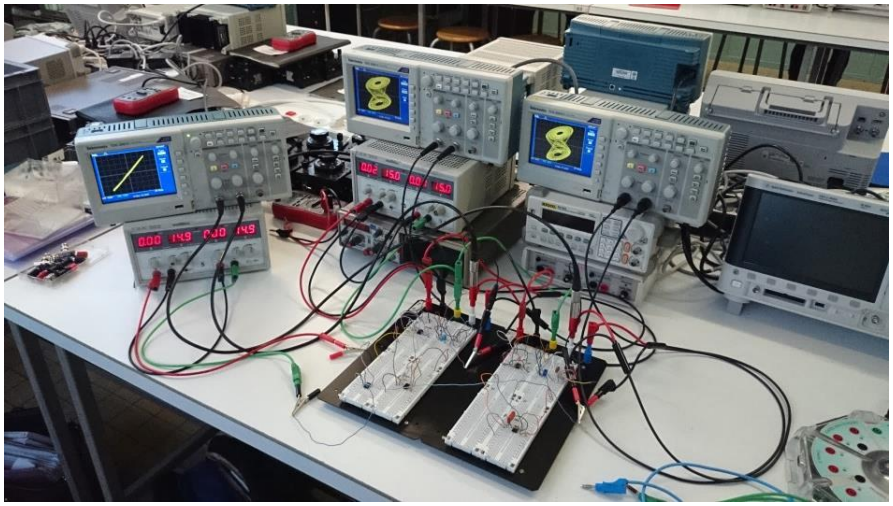
Augmenter la fréquence du message



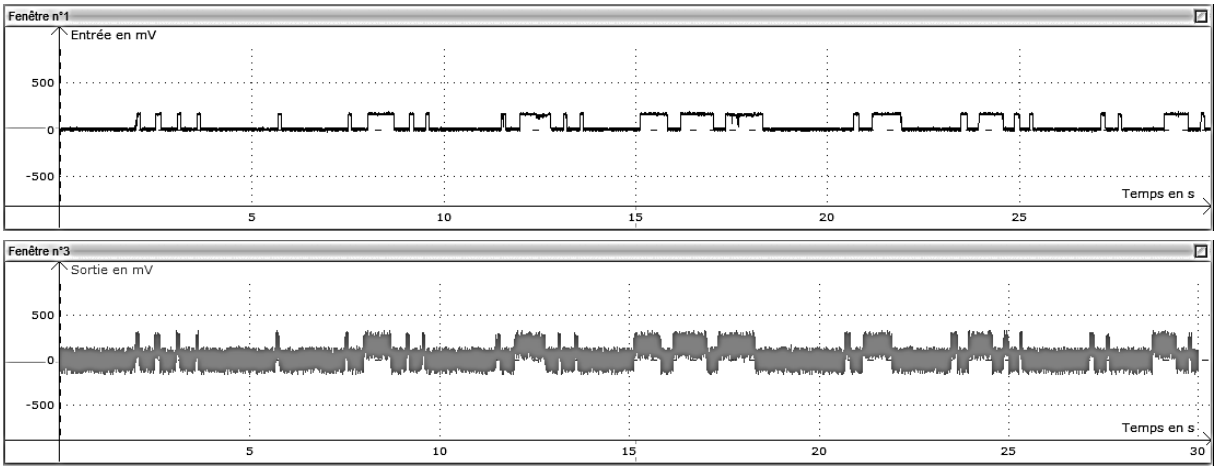
Fréquence d'échantillonnage : 1 *kHz*

CONCLUSION

- *Une méthode de cryptographie par chaos intéressante*



- *Une transmission efficace*



- *Des défauts de sécurité qu'on peut compenser*