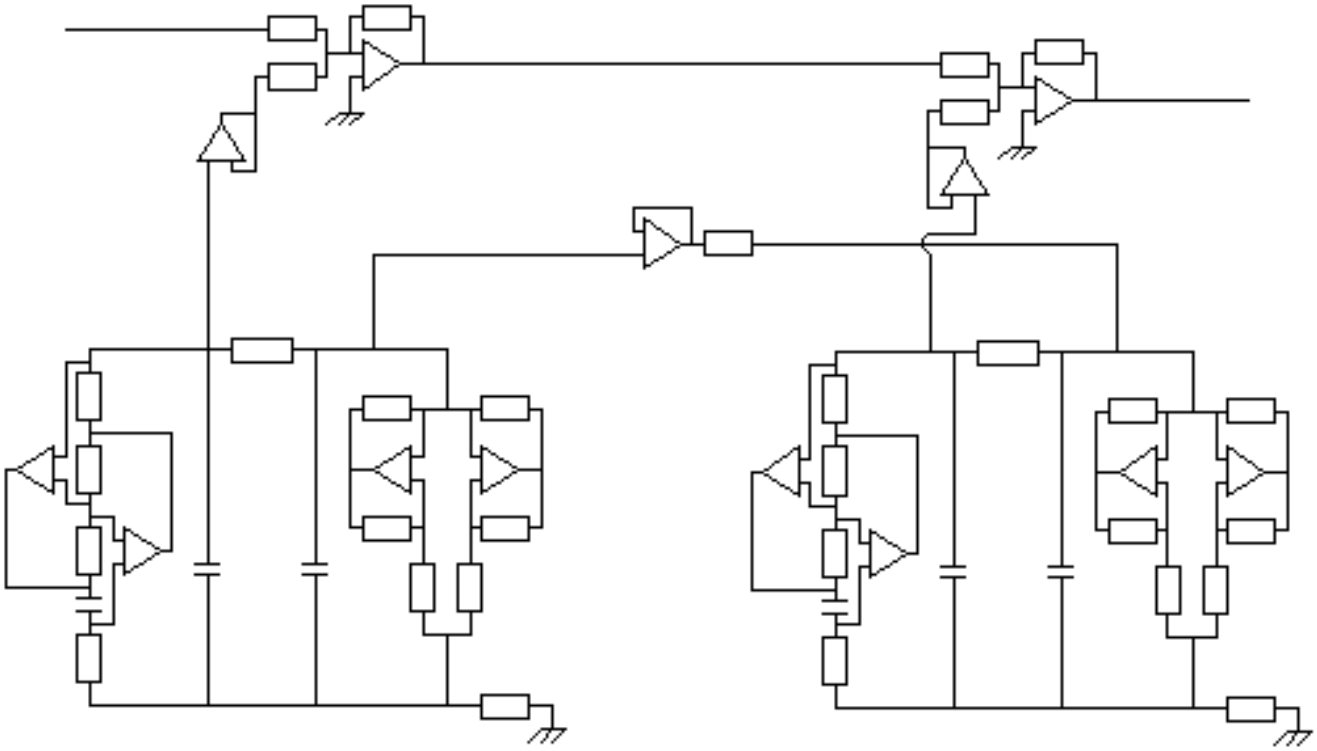
TRANSFERT ET CHAOS

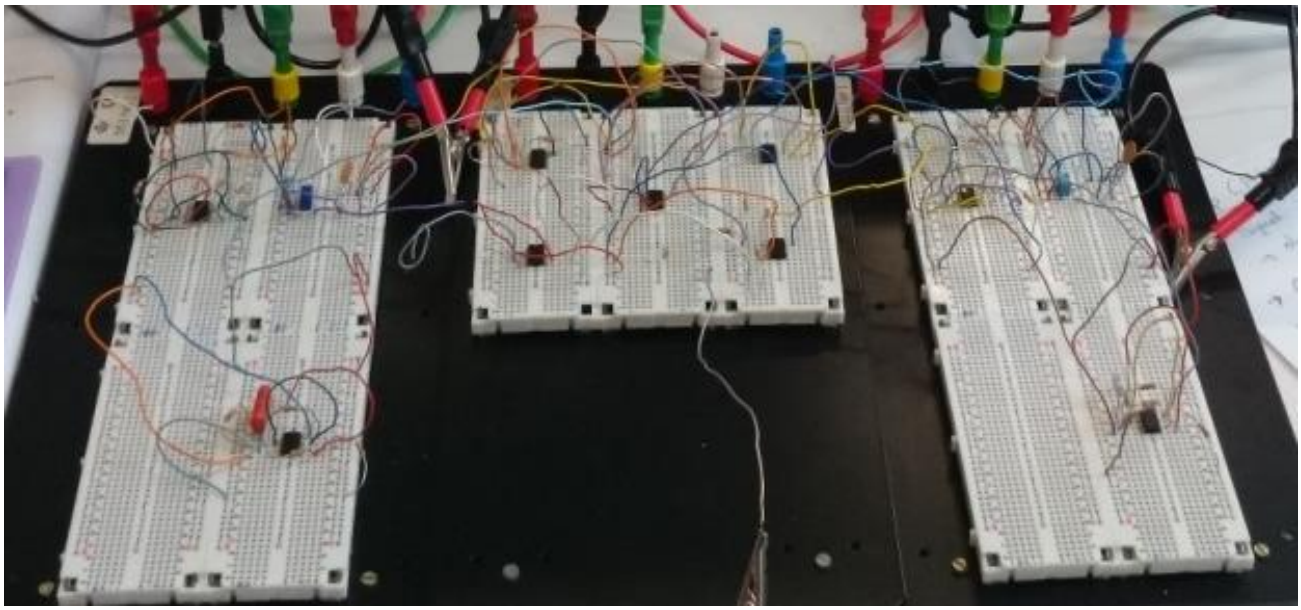
-Cryptographie d'un message par synchronisation de deux oscillateurs chaotiques de Chua-

Plan de la présentation :

Annexes :

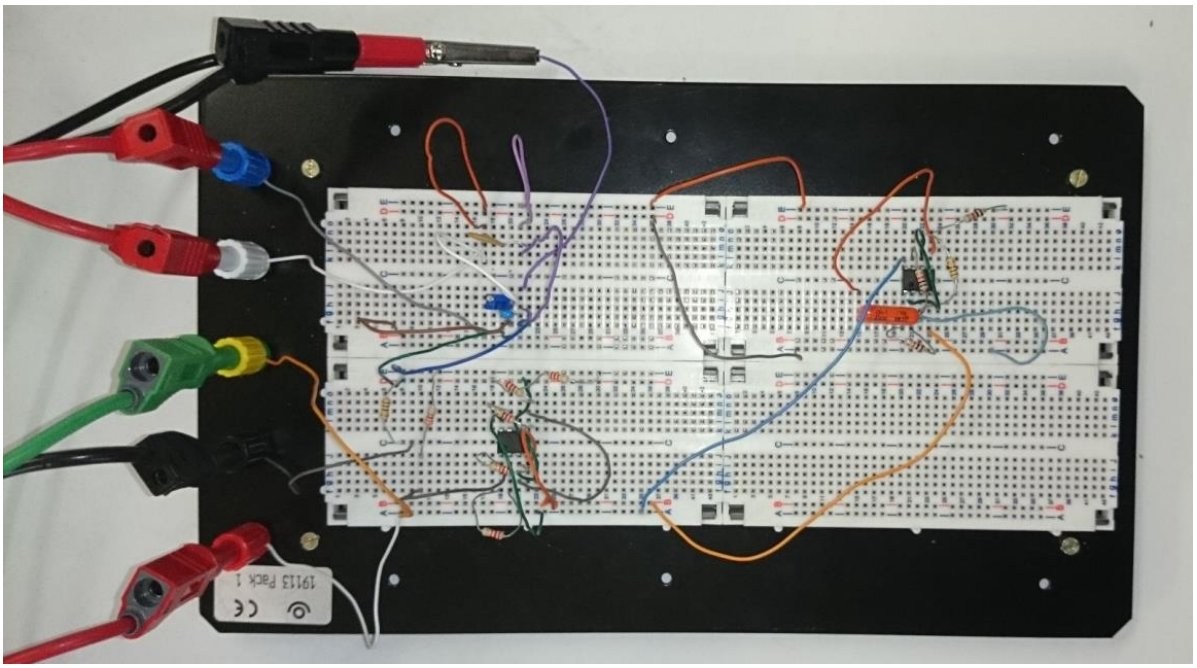
SCHEMA DU MONTAGE



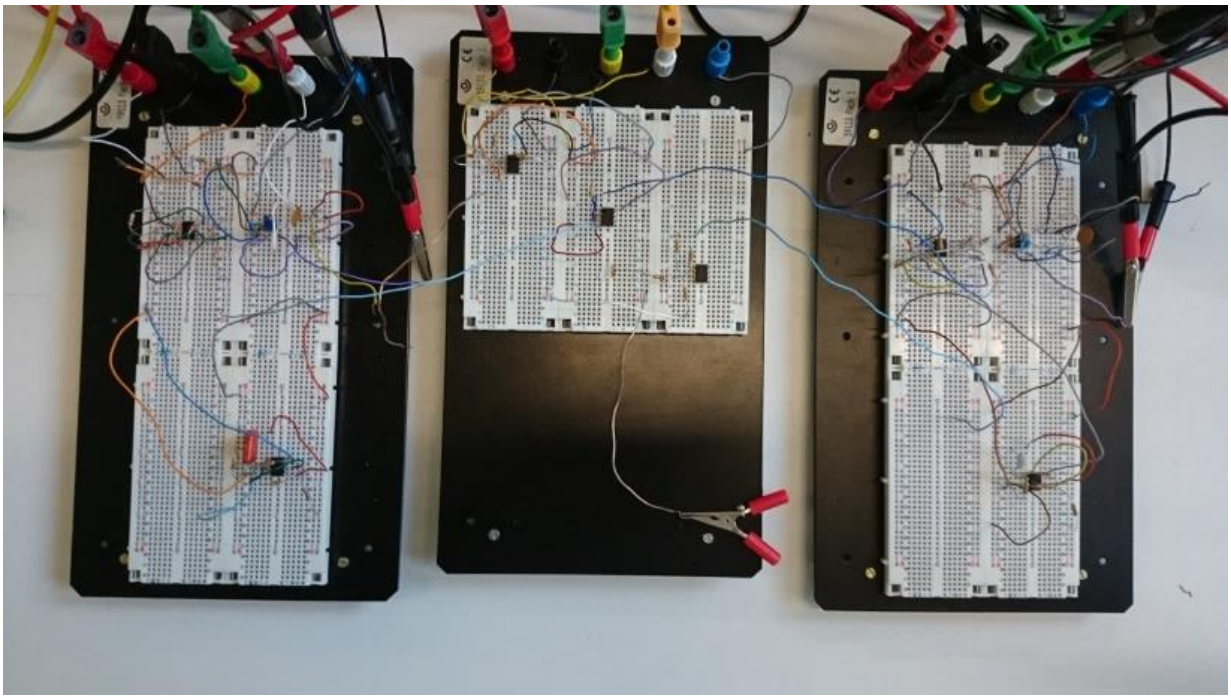


PHOTOS DU DISPOSITIF EXPERIMENTAL

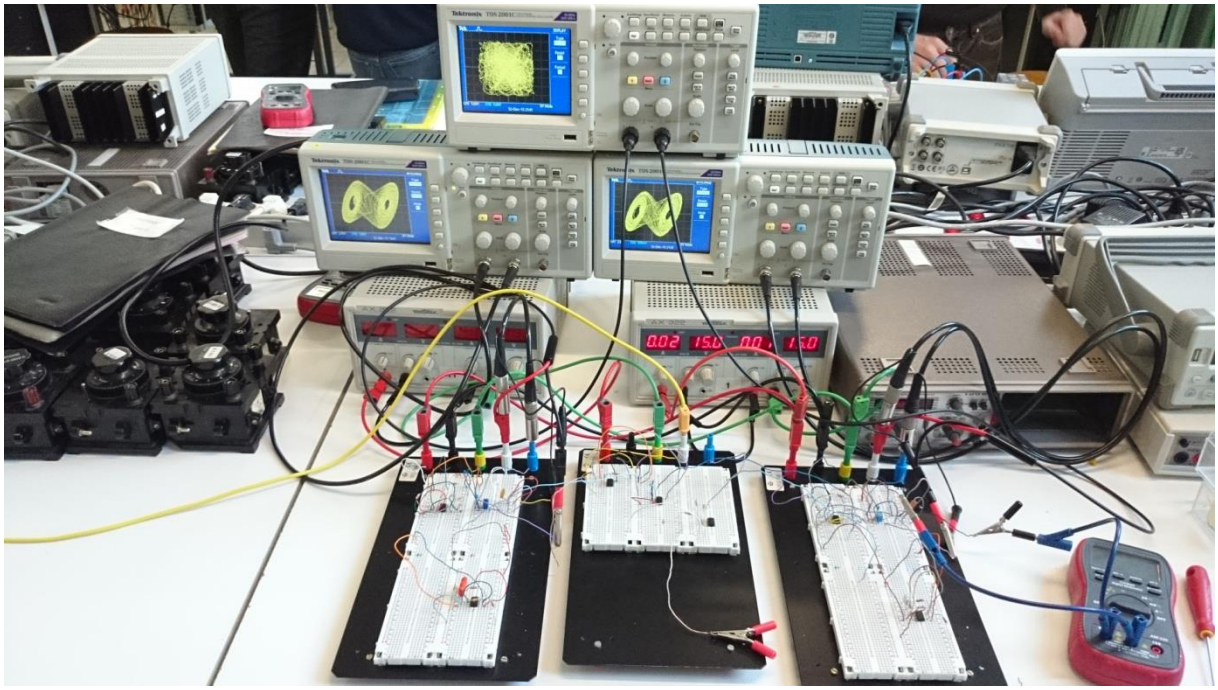
Oscillateur de Chua sur plaque à soudures sèches



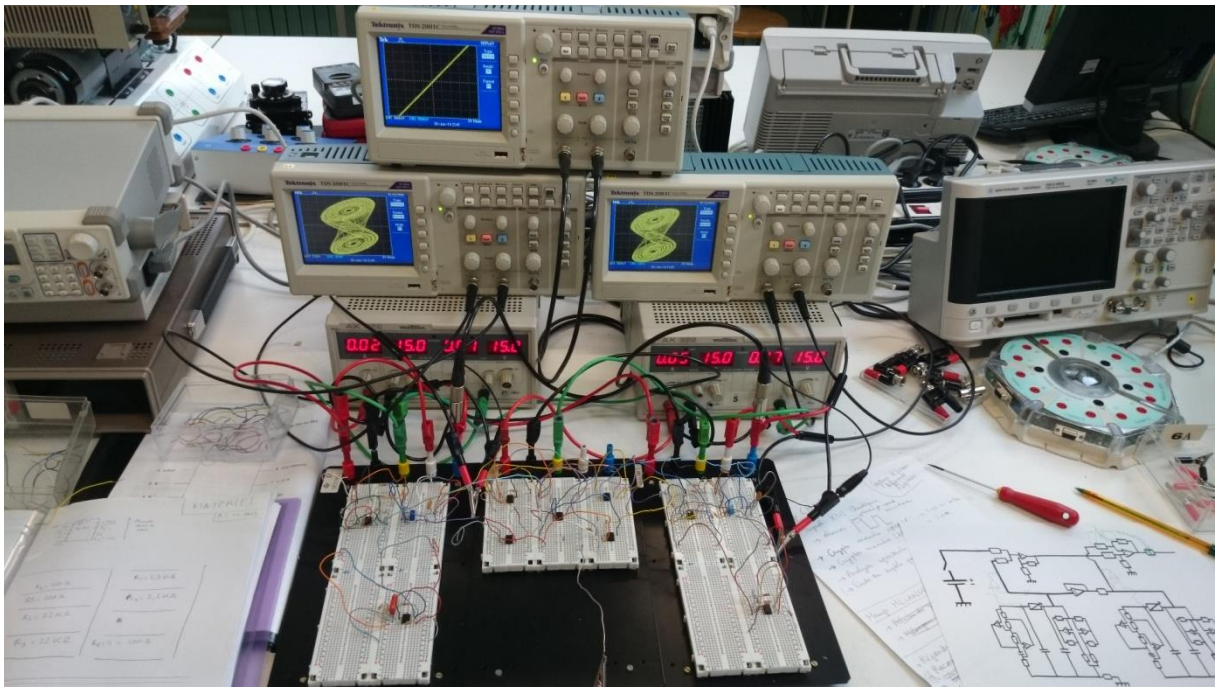
Circuit maître, montage suiveur et circuit esclave



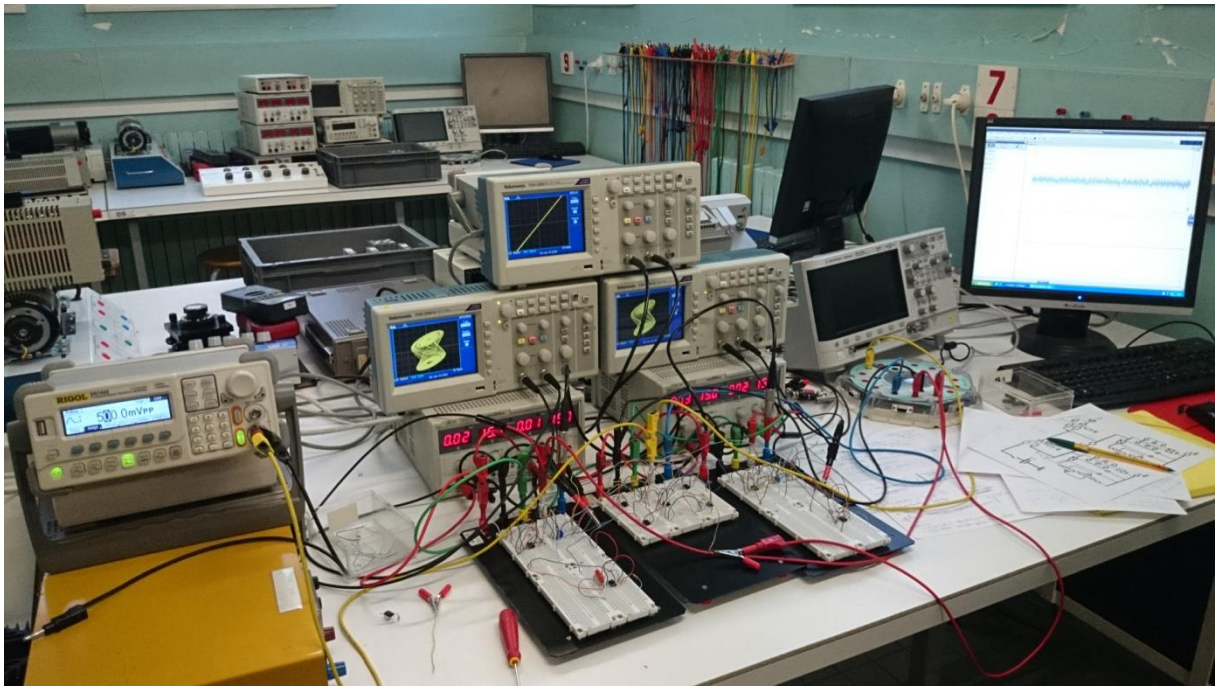
Oscillateurs non synchronisés



Oscillateurs synchronisés



Transfert d'un signal



SYNCRONISATION THEORIQUE

Le système d'équations différentielles $(S1)$ qui caractérise l'oscillateur de Chua est :

$$(\boldsymbol{S1})\begin{cases}\dfrac{\boldsymbol{dU_1}}{\boldsymbol{dt}} = -\dfrac{\boldsymbol{1}}{\boldsymbol{RC_1}}\boldsymbol{U_1} + \dfrac{\boldsymbol{1}}{\boldsymbol{RC_1}}\boldsymbol{U_2} - \dfrac{\boldsymbol{1}}{\boldsymbol{C_1}}\boldsymbol{f(U_1)} \\ \dfrac{\boldsymbol{dU_2}}{\boldsymbol{dt}} = -\dfrac{\boldsymbol{1}}{\boldsymbol{RC_2}}\boldsymbol{U_2} + \dfrac{\boldsymbol{1}}{\boldsymbol{RC_2}}\boldsymbol{U_1} + \dfrac{\boldsymbol{1}}{\boldsymbol{C_2}}\boldsymbol{i_L} \\ \dfrac{\boldsymbol{di_L}}{\boldsymbol{dt}} = -\dfrac{\boldsymbol{1}}{\boldsymbol{L}}\boldsymbol{U_2}\end{cases}$$

Le changement de variable $\boldsymbol{\xi = \dfrac{t}{RC_2}}$ permet d'établir le système (S) équivalent à $(S1)$:

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

Avec : $x_1 = \dfrac{U_1}{E}$; $x_2 = \dfrac{U_2}{E}$; $x_3 = \dfrac{Ri_L}{E}$; $\alpha = \dfrac{C_2}{C_1}$; $\beta = R^2\dfrac{C_2}{L}$

On pose $X(t)$ (respectivement $\hat{X}(t)$) le vecteur caractérisant le circuit maître (respectivement esclave).

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

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

Où k est le vecteur de rétroaction qui permet la synchronisation.

<u>Théorème de synchronisation</u>

On suppose que le vecteur de rétroaction dans la réponse du circuit esclave est choisi ainsi :

$$k = \begin{pmatrix}k_1\\k_2\\k_3\end{pmatrix} = \begin{bmatrix}-1 & -\dfrac{1}{\beta} & -\dfrac{1}{\beta}\\ 0 & -\dfrac{1}{\beta} & 0\\ 1 & 0 & 0\end{bmatrix}\begin{bmatrix}3\theta\\3\theta^2\\\theta^3\end{bmatrix}$$

Si le paramètre θ (qui dépend des valeurs des composants des circuits) est assez grand, alors le circuit maître et le circuit esclave seront globalement synchronisés de façon asymptotique, au sens où :

$$\forall\left(X(0), \hat{X}(0)\right), \qquad \boldsymbol{\lim_{t\to\infty}\hat{X}(t) - X(t) = 0}$$

Démonstration

On pose :

$$z = H(X) = \begin{pmatrix} x_3 \\ \dot{x}_3 \\ \ddot{x}_3 \end{pmatrix} = \begin{pmatrix} x_3 \\ -\beta x_2 \\ -\beta x_1 + \beta x_2 - \beta x_3 \end{pmatrix}$$

$$\hat{z} = H(\hat{X}) = \begin{pmatrix} \hat{x}_3 \\ -\beta \hat{x}_2 \\ -\beta \hat{x}_1 + \beta \hat{x}_2 - \beta \hat{x}_3 \end{pmatrix}$$

Avec $M = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -\beta & 0 \\ -\beta & \beta & -\beta \end{pmatrix}$ la matrice de l'application H dans la base canonique de $\mathcal{M}_{3,1}(\mathbb{R})$.

On pose $e(t) = \hat{z}(t) - z(t)$

On introduit la fonction de Lyapunov :

$$V = e^T \cdot P(\theta) \cdot e\,, \qquad avec\ P(\theta) = \begin{pmatrix} \theta^{-1} & -\theta^{-2} & \theta^{-3} \\ -\theta^{-2} & 2\theta^{-3} & -3\theta^{-4} \\ \theta^{-3} & -3\theta^{-4} & 6\theta^{-5} \end{pmatrix}$$

On pose $\dddot{x}_3 = h(X) = c_1 x_1 + c_2 x_2 + c_3 x_3 - \alpha\beta f(x_1)$

Alors, d'après la définition de z :

$$\dot{z} = \begin{pmatrix} \dot{x}_3 \\ \ddot{x}_3 \\ \dddot{x}_3 \end{pmatrix} = \begin{pmatrix} \dot{x}_3 \\ \ddot{x}_3 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ h(X) \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} x_3 \\ \dot{x}_3 \\ \ddot{x}_3 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ h(X) \end{pmatrix}$$

$$ie\ \dot{z} = Az + \begin{pmatrix} 0 \\ 0 \\ h(X) \end{pmatrix}, \qquad avec\ A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

De même, en posant $\dddot{\hat{x}}_3 = h(\hat{X}) = c_1 \hat{x}_1 + c_2 \hat{x}_2 + c_3 \hat{x}_3 - \alpha\beta f(\hat{x}_1)$, on a :

$$\dot{\hat{z}} = A\hat{z} + \begin{pmatrix} 0 \\ 0 \\ h(\hat{X}) \end{pmatrix} + Mk(x_3 - \hat{x}_3)$$

Alors on a :

$$\left|h(\hat{X}) - h(X)\right| = \left|c_1(\hat{x}_1 - x_1) + c_2(\hat{x}_2 - x_2) + c_3(\hat{x}_3 - x_3) - \alpha\beta\left(f(\hat{x}_1) - f(x_1)\right)\right|$$

D'où, d'après l'inégalité triangulaire et l'inégalité de Cauchy-Schwarz :

$$\left|h(\hat{X}) - h(X)\right| \leq \eta\left\|\hat{X} - X\right\|, \qquad avec\ \eta = ({c_1}^2 + {c_2}^2 + {c_3}^2)^{\frac{1}{2}} - a\alpha\beta$$

On a : $M^{-1} = \begin{pmatrix} -1 & -\frac{1}{\beta} & -\frac{1}{\beta} \\ 0 & -\frac{1}{\beta} & 0 \\ 1 & 0 & 0 \end{pmatrix}$ et $P(\theta)^{-1} = \begin{pmatrix} 3\theta & 3\theta^2 & \theta^3 \\ 3\theta^2 & 5\theta^3 & 2\theta^4 \\ \theta^3 & 2\theta^4 & \theta^5 \end{pmatrix}$

D'où : $k = M^{-1}P(\theta)^{-1}\begin{pmatrix}1\\0\\0\end{pmatrix}$

Donc :

$$\dot{\hat{z}} = A\hat{z} + \begin{pmatrix}0\\0\\h(\hat{X})\end{pmatrix} + P(\theta)^{-1}B(z-\hat{z}), \qquad avec\ B = \begin{pmatrix}1\\0\\0\end{pmatrix}\cdot\begin{pmatrix}1\\0\\0\end{pmatrix}^T = \begin{pmatrix}1&0&0\\0&0&0\\0&0&0\end{pmatrix}$$

Finalement,

$$\dot{e} = \dot{\hat{z}} - \dot{z} = A\hat{z} + \begin{pmatrix}0\\0\\h(\hat{X})\end{pmatrix} + P(\theta)^{-1}B(z-\hat{z}) - Az - \begin{pmatrix}0\\0\\h(X)\end{pmatrix}$$

$$\text{ie } \dot{e} = (A + P(\theta)^{-1}B)e + \begin{pmatrix}0\\0\\h(\hat{X}) - h(X)\end{pmatrix}$$

$$\dot{V} = e^T(A^TP(\theta) + P(\theta)A - 2B)e + 2e^TP(\theta)\begin{pmatrix}0\\0\\h(\hat{X}) - h(X)\end{pmatrix}$$

On vérifie que :

$A^TP(\theta) + P(\theta)A - B = -\theta P(\theta)$

$$\text{D'où : } \dot{V} = -\theta e^TP(\theta)e - \begin{pmatrix}(1&0&0)e\end{pmatrix}^2 + 2e^TP(\theta)\begin{pmatrix}0\\0\\h(\hat{X}) - h(X)\end{pmatrix}$$

On pose : $\|e\|_{P(\theta)} = \sqrt{e^TP(\theta)e}$ (car P(θ) est définie positive), et $P(\theta) = \sum_{i,j=1}^{3} p_{i,j}(\theta)$

Alors on a :

$\dot{V} \le -\theta\|e\|^2_{P(\theta)} + 2\|e\|_{P(\theta)}\sqrt{p_{33}(\theta)}\left|h(\hat{X}) - h(X)\right|$

Or $\dot{V} = 2\|e\|_{P(\theta)}\frac{d}{dt}\left(\|e\|_{P(\theta)}\right)$

D'où :

$\frac{d}{dt}\left(\|e\|_{P(\theta)}\right) \le -\frac{\theta}{2}\|e\|_{P(\theta)} + \sqrt{p_{33}(\theta)}\left|h(\hat{X}) - h(X)\right|$

On note :

$\mu = \|M^{-1}\|$

On a montré que :

$\left|h(\hat{X}) - h(X)\right| \le \eta\left\|\hat{X} - X\right\|$

De plus, $\left\|\hat{X} - X\right\| \le \mu\|e\|$

On note λ_1 la valeur propre de $P(1)$ la plus petite $\left(\lambda_1 = 4 - \sqrt{15}\right)$.

Alors, d'après le théorème de Courant-Fischer,

$\|e\| \leq \frac{1}{\sqrt{\lambda_1}} \|e\|_{P(1)}$

De plus, $\|e\|_{P(1)}^2 = \sum_{i,j=1}^{3} e_i p_{i,j}(\theta)\, e_j$

D'où, pour $\theta \geq 1$, $\|e\|_{P(1)}^2 \leq \theta^5 \sum_{i,j=1}^{3} e_i p_{i,j}(\theta)\, e_j \frac{1}{\theta^{i+j-1}}$

ie pour $\theta \geq 1$, $\|e\|_{P(1)}^2 \leq \theta^5 \|e\|_{P(\theta)}^2$

Finalement :

$$\frac{d}{dt}\left(\|e\|_{P(\theta)}\right) \leq -\left(\frac{\theta}{2} - \eta\mu\sqrt{\frac{p_{33}(1)}{\lambda_1}}\right)\|e\|_{P(\theta)}$$

On pose $\eta\mu\sqrt{\frac{p_{33}(1)}{\lambda_1}} = \rho$ (ρ est une constante indépendante du temps).

On suppose $\theta \geq \rho$, alors :

$$\|e(t)\|_{P(\theta)} \leq \|e(0)\|_{P(\theta)} exp\left(-\frac{1}{2}(\theta - \rho)t\right)$$

Or $\left\|\hat{X}(t) - X(t)\right\| \leq \mu\|e(t)\|$

Et en notant λ_θ la valeur propre la plus petite de $P(\theta)$, le théorème de Courant-Fischer donne : $\|e(t)\| \leq {\lambda_\theta}^{-1/2} \|e(t)\|_{P(\theta)}$

Puis :

$$\left\|\hat{X}(t) - X(t)\right\| \leq \mu {\lambda_\theta}^{-1/2} \|e(0)\|_{P(\theta)} exp\left(-\frac{1}{2}(\theta - \rho)t\right)$$

D'où :

$\left\|\hat{X}(t) - X(t)\right\| \to 0$

Finalement,

$\forall \left(X(0), \hat{X}(0)\right),\ lim_{t\to\infty}\, \hat{X}(t) - X(t) = 0,$

donc les deux oscillateurs sont bien synchronisés.

```
restart;
with(plots) :
```

 # GRANDEURS CARACTERISTIQUES DU DIPOLE PASSIF MASTER (1)

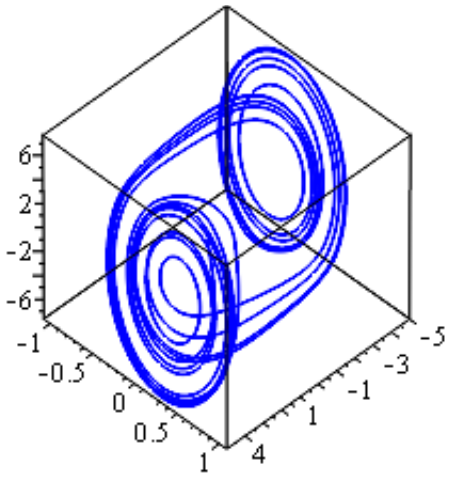
```
C11 := 4.7·10^-9 :
C21 := 47·10^-9 :
R0 := 0 :
L1 := 10·10^-3 :
```

 # VALEUR DE LA RESISTANCE VARIABLE (1)

```
R1 := 1850 :
```

SIMULATION

```
alpha1 := C21/C11 :
beta1 := R1^2·C21/L1 :
g1 := R1·R0·C21/L1 :
mb := -0.411 :
ma := -0.767 :
b1 := R1·mb·10^-3 :
a1 := R1·ma·10^-3 :
f1 := x→b1·x + 1/2·(a1 - b1)·(abs(x + 1) - abs(x - 1)) :
Ini1 := x(0) = 1, y(0) = 0, z(0) = 0 :
E11 := -diff(x(t), t) + alpha1·(y(t) - x(t) - f1(x(t))) :
E21 := -diff(y(t), t) + x(t) - y(t) + z(t) :
E31 := -diff(z(t), t) - beta1·y(t) - g1·z(t) :
Sol1 := dsolve({E11, E21, E31, Ini1}, numeric) :
graphe1 := [seq([subs(Sol1(k/100), x(t)), subs(Sol1(k/100), y(t)), subs(Sol1(k/100),
    z(t))], k = 0..4000)] :
spacecurve(graphe1);
```



> **# GRANDEURS CARACTERISTIQUES DU DIPOLE PASSIF SLAVE (2)**

> $C12 := 4.7 \cdot 10^{-9}$:
$C22 := 47 \cdot 10^{-9}$:
$R0 := 0$:
$L2 := 10 \cdot 10^{-3}$:
$alpha2 := \frac{C22}{C12}$:
$beta2 := \frac{R2^2 \cdot C22}{L2}$:

$g2 := \frac{R2 \cdot R0 \cdot C22}{L2}$:

> $alpha2 := \frac{C22}{C12}$:
$beta2 := \frac{R2^2 \cdot C22}{L2}$:
$g2 := \frac{R2 \cdot R0 \cdot C22}{L2}$:
$mb := -0.411$:
$ma := -0.767$:
$b2 := R2 \cdot mb \cdot 10^{-3}$:
$a2 := R2 \cdot ma \cdot 10^{-3}$:

> $f2 := x \rightarrow b2 \cdot x + \frac{1}{2} \cdot (a2 - b2) \cdot (\mathrm{abs}(x+1) - \mathrm{abs}(x-1))$:

> **# VALEUR DE LA RESISTANCE VARIABLE (2)**

> **$R2 := 1900$:**

SYNCHRONISATION

```
> theta :='theta':
> theta := 20 :
```

$$> K := \left\langle \left\langle -1 - \frac{g2}{beta2}, -\frac{g2}{beta2}, 1 \right\rangle \middle| \left\langle -\frac{1+g2}{beta2}, -\frac{1}{beta2}, 0 \right\rangle \middle| \left\langle -\frac{1}{beta2}, 0, 0 \right\rangle \right\rangle . \left\langle 3\cdot \mathrm{theta}, 3\cdot\theta^2, \theta^3 \right\rangle;$$

$$K := \begin{bmatrix} -\frac{10218020}{16967} \\ -\frac{1200000}{16967} \\ 60 \end{bmatrix} \quad (1)$$

```
> k1 := K[1] :
  k2 := K[2] :
  k3 := K[3] :
```

$$> EE1 := -diff(xss(t), t) + alpha2\cdot(-xss(t) + yss(t) - f2(xss(t))) + k1\cdot(z(t) - zss(t));$$
$$EE2 := -diff(yss(t), t) + xss(t) - yss(t) + zss(t) + k2\cdot(z(t) - zss(t));$$
$$EE3 := -diff(zss(t), t) - beta2\cdot yss(t) - g2.zss(t) + k3\cdot(z(t) - zss(t));$$

$$EE1 := -\left(\frac{d}{dt} xss(t)\right) - 2.191000000\, xss(t) + 10.00000000\, yss(t) + 3.382000000\, |xss(t) + 1|$$
$$- 3.382000000\, |xss(t) - 1| - \frac{10218020}{16967} z(t) + \frac{10218020}{16967} zss(t)$$

$$EE2 := -\left(\frac{d}{dt} yss(t)\right) + xss(t) - yss(t) + \frac{1216967}{16967} zss(t) - \frac{1200000}{16967} z(t)$$

$$EE3 := -\left(\frac{d}{dt} zss(t)\right) - \frac{16967}{1000} yss(t) + 60\, z(t) - 60\, zss(t) \quad (2)$$

```
> Iniss := xss(0) = 1, yss(0) = 0, zss(0) = 0 :
```

$$> Solsynchr := dsolve(\{E11, E21, E31, Ini1, EE1, EE2, EE3, Iniss\}, numeric, maxfun = 0, method = classical);$$

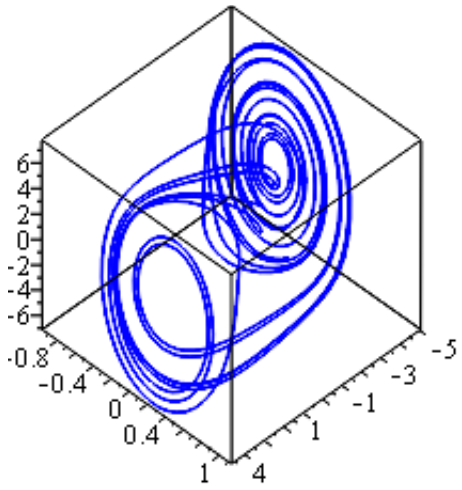
$$Solsynchr := \mathbf{proc}(x\_classical) \ \ldots \ \mathbf{end\ proc} \quad (3)$$

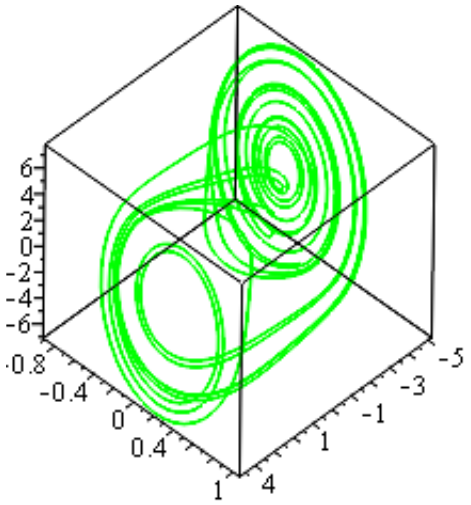
```
> Solsynchr(10) :
```

$$> graphe1 := \left[seq\left(\left[subs\left(Solsynchr\left(\frac{k}{20}\right), x(t)\right), subs\left(Solsynchr\left(\frac{k}{20}\right), y(t)\right), subs\left(Solsynchr\left(\frac{k}{20}\right), z(t)\right)\right], k = 100..1000\right)\right] :$$

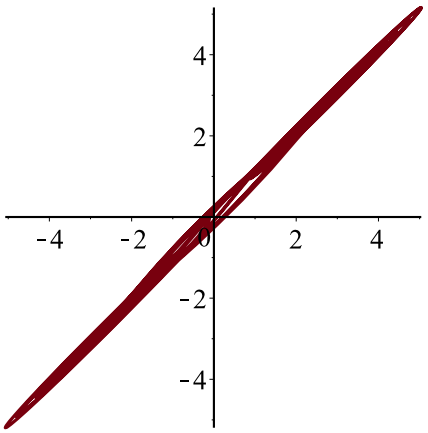
$$> graphe2 := \left[seq\left(\left[subs\left(Solsynchr\left(\frac{k}{20}\right), xss(t)\right), subs\left(Solsynchr\left(\frac{k}{20}\right), yss(t)\right), subs\left(Solsynchr\left(\frac{k}{20}\right), zss(t)\right)\right], k = 100..1000\right)\right] :$$

```
> spacecurve(graphe1, color = blue);
  spacecurve(graphe2, color = green);
```

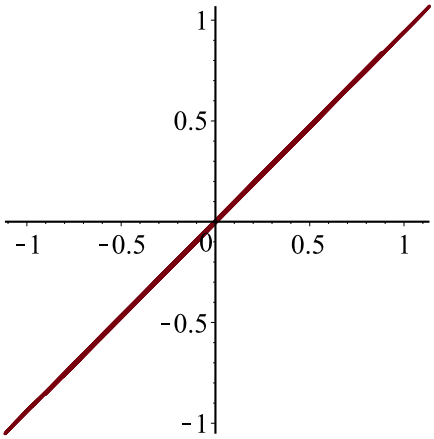




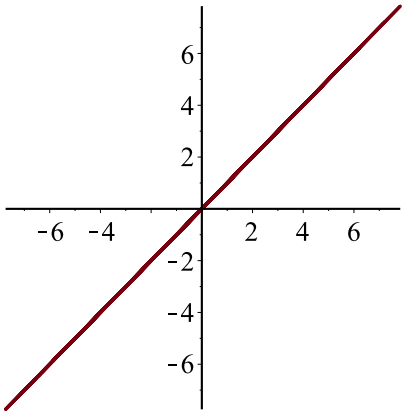

```
> plot([seq([[subs(Solsynchr(k/20), x(t)), subs(Solsynchr(k/20), xss(t))], k = 3000..4000)]]);
```



> $plot\left(\left[seq\left(\left[subs\left(Solsynchr\left(\frac{k}{20} \right), y(t) \right), subs\left(Solsynchr\left(\frac{k}{20} \right), yss(t) \right) \right], k = 3000 \ldots 4000 \right) \right] \right);$



> $plot\left(\left[seq\left(\left[subs\left(Solsynchr\left(\frac{k}{20} \right), z(t) \right), subs\left(Solsynchr\left(\frac{k}{20} \right), zss(t) \right) \right], k = 3000 \ldots 4000 \right) \right] \right);$



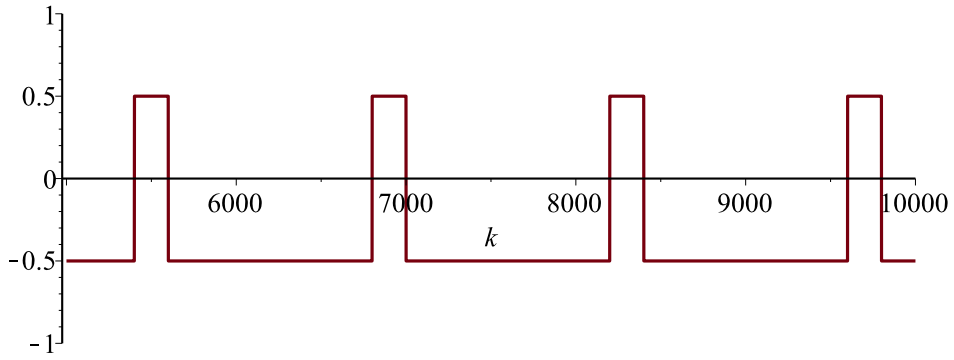
CRYPTAGE

```
> randseq := [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0,
      0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1,
      1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0,
      0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, ] :
```

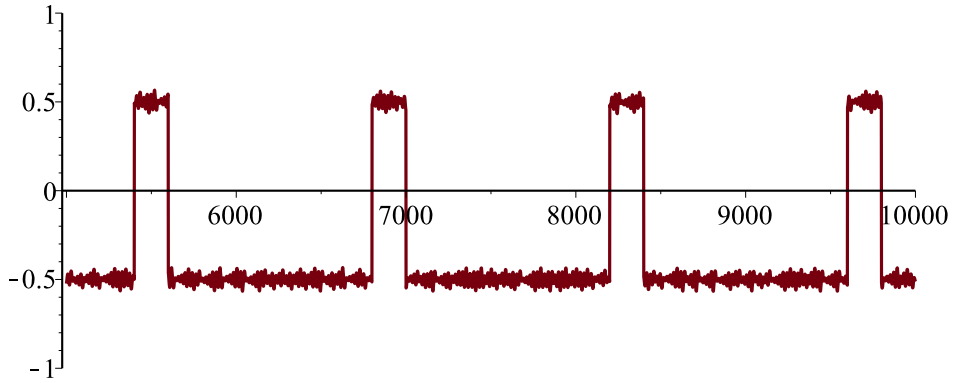
```
> message := proc (k) local i;
    i := eval(floor(k/100) + 1);
    randseq[i]
  end proc;
```

$$message := \mathbf{proc}(k)\ \mathbf{local}\ i;\ i := eval(\mathrm{floor}(1/100 * k) + 1);\ randseq[i]\ \mathbf{end\ proc} \qquad (4)$$

```
> message(4.5) :
> plot(message(k) - 0.5, k = 5000..10000, (-1)..(1));
```




```
> plot([seq([k, subs(Solsynchr(k/10), y(t)) + message(k) - subs(Solsynchr(k/10), yss(t)) - 0.5], k = 5000..10000)], 5000..10000, (-1)..(1));
```




```
>
```