Synchronisation adaptative pour une classe de systèmes hyperchaotiques: application à la cryptanalyse

Estelle Cherrier, Mondher Farza, Mohammed M'Saad

Synchronisation adaptative pour une classe de systèmes hyperchaotiques : application à la cryptanalyse

Estelle Cherrier, Mondher Farza et Mohammed M'Saad

GREYC UMR CNRS 6072
Boulevard du Maréchal Juin
14050 Caen cedex, France

estelle.cherrier@greyc.ensicaen.fr, mondher.farza@greyc.ensicaen.fr, mohammed.msaad@greyc.ensicaen.fr

Résumé— **Cet article propose de réunir les travaux présentés dans les références [6] et [25]. Le premier détaille un schéma de communications sécurisées, dont l'émetteur est un système hyperchaotique à retard et développe quelques points de cryptanalyse. Le second article présente la synthèse d'un observateur adaptatif à grand gain pour une classe de systèmes non linéaires uniformément observables, dont l'état et l'entrée sont affectés par des retards. Nous proposons ici une synthèse de ces travaux afin de montrer comment l'observateur adaptatif construit dans [25] peut prolonger la cryptanalyse débutée dans [6]. De par la nature des signaux considérés, certaines hypothèses de convergence de l'observateur adaptatif peuvent être relaxées. Notamment, aucune entrée supplémentaire n'est requise pour garantir la condition d'excitation persistante vérifiée par le système lorsqu'il est en régime hyperchaotique. Des simulations numériques illustrent la cryptanalyse à la fin de l'article.**

Mots-clés— **Systèmes chaotiques à retard, synchronisation, observateur à grand gain, observateur adaptatif, cryptanalyse**

I. Introduction

Cet article propose de réunir les travaux présentés dans les articles [6] et [25]. Le premier détaille un schéma de communications sécurisées, dont l'émetteur est un système hyperchaotique à retard, le récepteur est un observateur non linéaire et la transmission d'information, de type transmission à deux voies, repose sur la modulation de la phase d'un signal hyperchaotique. Quelques points de cryptanalyse y sont abordés, afin de tester la sécurité du processus de chiffrement, ainsi que la force de la clé secrète. Le second article présente la synthèse d'un observateur adaptatif à grand gain pour une classe de systèmes non linéaires uniformément observables, dont l'état et l'entrée sont affectés par des retards. Nous proposons ici une synthèse de ces travaux afin de montrer comment l'observateur adaptatif construit dans [25] peut prolonger la cryptanalyse débutée dans [6].

Depuis les années 1990, les techniques de synchronisation du chaos ont connu un formidable essor. Les travaux novateurs de Pecora et Carroll [24] ont constitué une révolution dans l'étude de la synchronisation des systèmes chaotiques : ils ont prouvé que deux systèmes chaotiques identiques, de conditions initiales différentes, peuvent se synchroniser selon le principe appelé *maître-esclave*, ou *drive-response*, défiant ainsi la propriété de sensibilité aux conditions initiales caractéristique du chaos. Par la suite, [20] et [22] ont relié le processus de synchronisation à un problème classique d'estimation d'état non linéaire : le récepteur peut être conçu comme un observateur de l'émetteur. Une synthèse des différentes techniques de synchronisation du chaos se trouve dans les références [3] et [2]. L'une des motivations des recherches en cours sur la synchronisation du chaos provient de la variété des applications possibles, tant dans le domaine de la chimie, de la biologie, l'économie... que des communications sécurisées. Cette dernière application est l'objet d'une vaste littérature depuis une quinzaine d'années.

Les schémas de communications sécurisées reposant sur la synchronisation du chaos exploitent l'aspect aléatoire des signaux chaotiques, qui garantit une sécurité *a minima*. Plus précisément, l'information est noyée dans un signal qui ressemble à du bruit : il s'agit de stéganographie. Cependant, ce simple masquage est loin d'être suffisant, comme l'indique l'article d'Alvarez [1], qui est le premier à détailler les critères minimaux à vérifier avant de qualifier le schéma de communication de *sécurisé*. Il rappelle ainsi que l'étude de la sécurité doit suivre le principe de Kerckhoff, selon lequel tout le cryptosystème (ou système de chiffrement/déchiffrement) doit être public (c'est-à-dire la structure et les paramètres de l'émetteur, du récepteur, les fonctions de chiffrement et de déchiffrement), à l'exception de la clé de chiffrement. Complémentaire de la cryptographie, qui consiste à créer des algorithmes de chiffrement de données, la cryptanalyse doit permettre de juger le niveau de sécurité d'un cryptosystème et de savoir si le choix de la clé secrète est pertinent. Dans l'article [6], en suivant les différentes étapes proposées dans la référence [1], quelques points de cryptanalyse ont été vérifiés, notamment la force de la clé, les propriétés de confusion, de diffusion, les attaques spectrales. Il s'agit d'aspects de cryptanalyse dérivés de la cryptanalyse *classique*, dont le but est d'obtenir des informations sur le message chiffré sans connaissance sur la clé de chiffrement. Il existe un autre objectif de la cryptanalyse, à savoir obtenir la clé secrète, sans se préoccuper du message. C'est cet aspect que nous abordons dans cet article.

Les méthodes de synthèse d'observateurs adaptatifs ont largement été utilisées dans la synchronisation des sys-

tèmes chaotiques. L'une des premières techniques de chiffrement par le chaos consistait à moduler (à multiplier) un paramètre de l'émetteur en fonction du message (voir par exemple [13], [28]). Un contrôleur adaptatif était associé au récepteur afin de maintenir la synchronisation, puis le message était déchiffré. Cette technique de chiffrement, réservée aux messages variant lentement dans le temps, a été cassée par la suite, notamment dans l'article [29]. Les techniques adaptatives ont été exploitées pour l'identification des paramètres des systèmes chaotiques dans [10], [9], ou combinées à la propriété d'autosynchronisation des systèmes chaotiques dans [23]. La synchronisation adaptative est également utilisée dans les articles [14], [4], dans le cas où les paramètres du système maître sont inconnus ou incertains. Les contrôleurs adaptatifs sont également utilisés à des fins de synchronisation dans [17]. Concernant la cryptanalyse, certains articles (*cf.* [15] et les références mentionnées) ont fait appel à la synchronisation adaptative afin d'estimer les paramètres du système de Lorenz principalement. Il s'agit en général de paramétrisation linéaire, pour des systèmes chaotiques sans retard.

Peu de travaux ont été consacrés à la synchronisation adaptative pour les systèmes chaotiques à retard. Cette classe de systèmes chaotiques de dimension infinie, étudiée en détails dans [19], [7], possède un comportement hyperchaotique, plus complexe que celui des systèmes chaotiques (lié à la présence de plusieurs exposants de Lyapunov positifs), qui pourrait, *a priori*, renforcer la sécurité. Parmi les articles récents consacrés à ce sujet, on peut citer [18], [27]. Le premier utilise la théorie du contrôle adaptatif pour stabiliser des systèmes chaotiques comportant un retard connu. Le second fait appel à des techniques récentes d'optimisation multi-dimensionnelle pour estimer les paramètres - dont le retard - du système, mais la méthode proposée nécessite la connaissance de tout l'état du système à chaque instant.

Dans cet article, nous verrons comment utiliser les résultats de l'article [25] pour approfondir la cryptanalyse du cryptosystème présenté dans [6]. Dans [25], la synthèse d'un observateur adaptatif à grand gain pour une classe de systèmes non linéaires à retard (retard affectant l'état du système ainsi que son entrée) est détaillée. Nous montrerons que les hypothèses établies peuvent être relaxées dans le cas d'un système hyperchaotique à retard, et qu'il est possible de réaliser la synthèse d'un observateur de type grand gain afin d'estimer (avec une convergence exponentielle) simultanément l'état de l'émetteur ainsi que certains paramètres, intervenant de façon non linéaires dans sa dynamique. La synthèse de l'observateur, dont le gain est donné explicitement, repose sur la résolution d'une équation de Lyapunov algébrique. La possibilité ou non d'estimer certains paramètres sera utilisée ensuite pour guider le choix de la clé de chiffrement.

L'organisation de cet article est la suivante. La partie II est consacrée à la synthèse d'un observateur adaptatif à grand gain pour la classe de systèmes considérée. En particulier, on rappellera le contexte des techniques grand gain et des techniques adaptatives, puis les résultats de [25] seront adaptés au cadre des systèmes hyperchaotiques à retard. Ensuite le lien avec la cryptanalyse sera fait dans la partie III. Des simulations numériques en lien avec le cryptosystème décrit dans [6] seront réalisées.

Notations: Tout au long de cet article, on adoptera les notations suivantes.

- $x_\tau(t)$ représente $x(t-\tau)$
- $\lambda_m(M)$ et $\lambda_M(M)$ représentent respectivement les valeurs propres minimale et maximale de la matrice carrée M.

II. Synchronisation adaptative

Dans cet article, on considère la classe suivante de systèmes chaotiques à retard :

$$\left\{\begin{array}{l} \dot{x}(t) = Ax(t) + \phi(x(t), x_\tau(t), \rho) \\ y(t) = Cx(t) = x_1(t) \\ x(s) = \psi(s),\ \forall s \in [-\tau, 0] \end{array}\right. \tag{1}$$

avec $x = \left(\begin{array}{ccc} x_1 & \dots & x_n \end{array}\right)^T$; $\rho = \left(\begin{array}{ccc} \rho_1 & \dots & \rho_m \end{array}\right)^T$;

$$A = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ \vdots & \ddots & 1 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & & & \ddots & 1 \\ 0 & \dots & \dots & \dots & 0 \end{pmatrix}; \tag{2}$$

$$C = \left(\begin{array}{cccc} 1 & 0 & \dots & 0 \end{array}\right) \tag{3}$$

où $x \in \mathbf{R^n}$, $y \in \mathbf{R}$ et $\rho \in \mathbf{R^m}$ représentent respectivement l'état, le signal transmis au récepteur et le vecteur de paramètres constants inconnus.

On suppose que la nonlinéarité ϕ a une structure triangulaire par rapport à $x_1, \dots, x_n$ et $x_{\tau,1}, \dots, x_{\tau,n}$, c'est-à-dire :

$$\phi(x, x_\tau, \rho) = \begin{pmatrix} \phi_1(x_1, x_{\tau,1}, \rho) \\ \phi_2(x_1, x_2, x_{\tau,1}, x_{\tau,2}, \rho) \\ \vdots \\ \phi_n(x, x_\tau, \rho) \end{pmatrix} \tag{4}$$

Remarque 1 : En l'absence de retard dans la dynamique de l'état, la classe de systèmes considérée (1) coïncide avec la classe des systèmes uniformément observables, définie dans l'article [11]).

Remarque 2 : Nous soulignons ici que les paramètres pouvant être estimés doivent être constants. S'ils sont variables dans le temps, les techniques adaptatives ne sont pas appropriées, il faut recourir à d'autres méthodes, par exemple un observateur à entrées inconnues.

La synthèse de l'observateur adaptatif nécessite les hypothèses suivantes.

(H1) La fonction ϕ est globalement lipschitzienne par rapport à x, x_τ et ρ.

(H2) La fonction de paramétrisation non linéaire $\phi(x, x_\tau, .)$ est injective de $\mathbf{R^m}$ dans $\mathbf{R^n}$.
Remarque 3 : L'hypothèse (H1) est devenue classique dans le cadre des techniques à grand gain. En effet, si la fonction ϕ ne vérifie pas (H1), sous l'hypothèse que l'état et les paramètres inconnus sont bornés, il est possible de définir une extension de ϕ qui soit globalement lipschitzienne sur $\mathbf{R^n} \times \mathbf{R^n} \times \mathbf{R^m}$. Nous renvoyons le lecteur à la référence [26] pour une démonstration détaillée. Notons que le système étudié est chaotique, dont les variables d'état sont naturellement bornées. Il n'est donc pas nécessaire de formuler d'hypothèse supplémentaire, et on considère, sans perte de généralité.
Soit l'observateur adaptatif candidat suivant :

$$\begin{aligned}
\dot{\hat{x}}(t) &= A\hat{x}(t) + \phi(\hat{x}(t), \hat{x}_\tau(t), \hat{\rho}) \\
&\quad -\theta\Delta_\theta^{-1}\left(S^{-1} + \Gamma(t)P(t)\Gamma^T(t)\right)C^TC(\hat{x}(t) - x(t)) \qquad (5a)\\
\dot{\hat{\rho}}(t) &= -\theta P(t)\Gamma^T(t)C^TC(\hat{x}(t) - x(t)) \qquad (5b)\\
\dot{\Gamma}(t) &= \theta(A - S^{-1}C^TC)\Gamma + \Delta_\theta\frac{\partial\phi}{\partial\rho}(\hat{x}(t), \hat{x}_\tau(t), \hat{\rho}) \qquad (5c)\\
\dot{P}(t) &= -\theta P(t)\Gamma^T(t)C^TC\Gamma(t)P(t) + \theta P(t) \qquad (5d)
\end{aligned}$$

avec les notations et définitions suivantes :

- Δ_θ est la matrice diagonale définie par

$$\Delta_\theta = diag\begin{pmatrix} 1 & \frac{1}{\theta} & \dots & \frac{1}{\theta^{n-1}} \end{pmatrix} \qquad (6)$$

où θ est un paramètre de synthèse strictement positif.
Après quelques simplifications, on obtient les égalités ci-dessous :

$$\begin{array}{c} \Delta_\theta A\Delta_\theta^{-1} = \theta A \\ C\Delta_\theta = C \end{array} \qquad (7)$$

- S est la solution unique de l'équation de Lyapunov algébrique suivante :

$$S + A^TS + SA = C^TC \qquad (8)$$

Il a été montré dans l'article [11] que la matrice S est symétrique, définie positive, dont l'expression peut être donnée explicitement. En particulier, on a :

$$S^{-1}C^T = \begin{pmatrix} C_q^1 & C_q^2 & \dots & C_q^q \end{pmatrix}^T$$

où $C_n^p = \dfrac{n!}{p!(n-p)!}$.
On suppose également que l'hypothèse suivante est vérifiée.

(H3) Quelle que soit la trajectoire du système (5) de conditions initiales $(\hat{x}(0), \hat{\rho}(0))$, la matrice $C\Gamma(t)$ est à *excitation persistante, i.e.* il existe $\delta_1, \delta_2 > 0$ et $T \geq 0$ tels que :

$$\delta_1 I_m \leq \int_t^{t+T} \Gamma(s)^TC^TC\Gamma(s)ds \leq \delta_2 I_m \qquad (9)$$

Remarque 4 : Cette condition d'excitation persistante est intrinsèque aux techniques adaptatives, *cf.* le livre [21]. En général, elle impose de choisir une entrée suffisamment "riche", de telle sorte que la sortie du système contienne suffisamment d'informations pour pouvoir estimer les paramètres inconnus. Etant donné la classe de systèmes hyperchaotiques considérés, aucune entrée n'est nécessaire car les trajectoires des états sont intrinsèquement "riches" pour certaines valeurs des paramètres : il faut que le comportement du système soit effectivement hyperchaotique, si on se trouve dans une fenêtre d'ordre (*i.e.* si le comportement est périodique), cette condition ne peut évidemment pas être remplie sans entrée supplémentaire. Cette propriété des systèmes hyperchaotiques, abordée dans [16], est en cours d'étude.

Les propriétés suivantes, établies dans [8], seront nécessaires à dans la suite.
1) La norme de la matrice $\Gamma(t)$ est bornée, et cette borne ne dépend pas de θ, pourvu que $\theta \geq 1$:il existe $\gamma > 0$ tel que, pour tout $t \geq 0$:

$$\|\Gamma(t)\| \leq \gamma \qquad (10)$$

2) Sous l'hypothèse (H3), la matrice $P(t)$, définie par l'équation (5d), est symétrique, définie positive et bornée indépendamment de θ, dès lors que $\theta \geq 1$.

Le théorème suivant établit la synchronisation adaptative de l'observateur candidat (5) avec le système (1). Il est adapté du résultat principal de l'article [25] concernant une classe de systèmes non linéaires, à retard, avec une entrée à excitation persistante.

Théorème 5 : Sous les hypothèses (H1) à (H2), le système (5) *est un observateur adaptatif exponentiel du système* (1).

Les étapes-clés de la démonstration sont données. Pour une démonstration plus détaillée, nous renvoyons le lecteur à l'article [25].

Preuve: On définit les vecteurs d'erreur d'estimation : $\tilde{x}(t) = \hat{x}(t) - x(t)$, $\bar{x} = \Delta_\theta\tilde{x}$, $\tilde{\rho}(t) = \hat{\rho}(t) - \rho$.
On rappelle que le vecteur de paramètres inconnus ρ étant constant, on a $\dot{\rho} = 0$ et par suite $\dot{\tilde{\rho}} = \dot{\hat{\rho}}$.
En utilisant (7), la dynamique de $\bar{x}$ est donnée par :

$$\dot{\bar{x}} = \theta A\bar{x} + \Delta_\theta\phi(\hat{x}, \hat{x}_\tau, \hat{\rho}) - \Delta_\theta\phi(x, x_\tau, \rho) - \theta S^{-1}C^TC\bar{x} + \Gamma\dot{\tilde{\rho}} \qquad (11)$$

D'après le théorème de la valeur moyenne pour les fonctions à valeurs vectorielles (voir [30] par exemple) et la propriété de Lipschitz vérifiée par ϕ, après quelques majorations on obtient :

$$\begin{aligned}
\dot{\bar{x}} = \quad & \theta A\bar{x} - \theta S^{-1}C^TC\bar{x} + \Delta_\theta\frac{\partial\phi}{\partial\rho}(\hat{x}, \hat{x}_\tau, \hat{\rho})\tilde{\rho} + \Gamma\dot{\tilde{\rho}} \\
& + \Delta_\theta\frac{\partial\phi}{\partial x}(\xi_x, x_\tau, \rho)\Delta_\theta^{-1}\bar{x} + \Delta_\theta\frac{\partial\phi}{\partial x_\tau}(\hat{x}, \xi_\tau, \rho)\Delta_\theta^{-1}\bar{x}_\tau \\
& + \Delta_\theta\left(\frac{\partial\phi}{\partial\rho}(\hat{x}, \hat{x}_\tau, \xi_\rho) - \frac{\partial\phi}{\partial\rho}(\hat{x}, \hat{x}_\tau, \hat{\rho})\right)\tilde{\rho}
\end{aligned} \qquad (12)$$

Posons le changement de variable suivant :

$$\eta(t) = \bar{x} - \Gamma(t)\tilde{\rho}(t) \qquad (13)$$

En utilisant l'équation (5c), la dynamique de $\eta(t)$ est donnée par :

$$\begin{aligned}\dot{\eta}(t) &= \dot{\bar{x}}(t) - \Gamma(t)\dot{\tilde{\rho}}(t) - \dot{\Gamma}(t)\tilde{\rho}(t) \\ &= \theta A\eta + \theta S^{-1}C^TC\Gamma\tilde{\rho} - \theta S^{-1}C^TC\bar{x} \\ &\quad +\Delta_\theta \frac{\partial\phi}{\partial x}(\xi_x, x_\tau, \rho)\Delta_\theta^{-1}(\eta + \Gamma\tilde{\rho}) \\ &\quad +\Delta_\theta \frac{\partial\phi}{\partial x_\tau}(\hat{x}, \xi_\tau, \rho)\Delta_\theta^{-1}(\eta_\tau + \Gamma_\tau\tilde{\rho}_\tau) \\ &\quad +\Delta_\theta \left(\frac{\partial\phi}{\partial\rho}(\hat{x}, \hat{x}_\tau, \xi_\rho) - \frac{\partial\phi}{\partial\rho}(\hat{x}, \hat{x}_\tau, \hat{\rho})\right)\tilde{\rho}\end{aligned} \tag{14}$$

On introduit la fonctionnelle de Lyapunov-Krasovskii candidate suivante :

$$V(t, \eta, \tilde{\rho}) = V_1(t, \eta) + V_2(t, \tilde{\rho}) \tag{15}$$

avec

$$V_1(t, \eta) = \eta^T S\eta + \theta^{-\frac{t}{2\tau}} \int_{t-\tau}^{t} \theta^{-\frac{s}{2\tau}} \eta^T(s)\eta(s)ds \tag{16}$$

et

$$V_2(t, \tilde{\rho}) = \tilde{\rho}^T P^{-1}\tilde{\rho} + \theta^{-\frac{t}{2\tau}} \int_{t-\tau}^{t} \theta^{-\frac{s}{2\tau}} \tilde{\rho}^T(s)\tilde{\rho}(s)ds \tag{17}$$

Dans un premier temps on établit la dynamique de V_1, le long des trajectoires de (14) :

$$\dot{V}_1 = 2\eta^T S\dot{\eta} - \frac{\ln(\theta)}{2\tau}(V_1 - \eta^T S\eta) + \eta^T\eta \tag{18}$$

Après quelques simplifications, si $\theta > 1$ on arrive à :

$$\begin{aligned}\dot{V}_1 + \frac{\ln(\theta)}{2\tau} &\leq -c(\theta)\eta^T S\eta + \theta\eta^T C^TC\eta \\ &\quad +2\theta\eta^T C^TC\Gamma\tilde{\rho} - 2\theta\eta^T C^TC\bar{x} \\ &\quad +k\tilde{\rho}^T P^{-1}\tilde{\rho} + k_3\eta^T\eta_\tau + k_3'\eta^T\tilde{\rho}_\tau\end{aligned} \tag{19}$$

avec

$$c(\theta) = \theta - 2k_1 - \frac{\ln(\theta)}{2\tau} - \frac{1}{\lambda_m(S)} \tag{20}$$

Dans un second temps, on considère la dynamique de V_2 le long des trajectoires de (5b).

$$\begin{aligned}\dot{V}_2 &= 2\tilde{\rho}^T P^{-1}\dot{\tilde{\rho}} - \frac{\ln(\theta)}{2\tau_M}(V_2 - \tilde{\rho}^T P^{-1}\tilde{\rho}) + \tilde{\rho}^T\tilde{\rho} \\ &\quad -(1-\dot{\tau})\theta^{\frac{-\tau}{2\tau_M}}\tilde{\rho}_\tau^T\tilde{\rho}_\tau - \tilde{\rho}^T P^{-1}\dot{P}P^{-1}\tilde{\rho}\end{aligned} \tag{21}$$

On arrive, après quelques simplifications, à la majoration suivante

$$\begin{aligned}\dot{V}_2 + \frac{\ln(\theta)}{2\tau}V_2 \leq\ & -2\theta\tilde{\rho}^T\Gamma^T C^TC\bar{x} + \frac{\ln(\theta)}{2\tau}\tilde{\rho}^T P^{-1}\tilde{\rho} \\ & +\tilde{\rho}^T\tilde{\rho} + \theta\tilde{\rho}^T\Gamma^T C^TC\Gamma\tilde{\rho} - \theta\tilde{\rho}^T P^{-1}\tilde{\rho}\end{aligned} \tag{22}$$

En regroupant (19) et (22), on aboutit à :

$$\begin{aligned}\dot{V} + \frac{\ln(\theta)}{2\tau}V &\leq -c(\theta)\eta^T S\eta + \theta\eta^T C^TC\eta \\ &\quad +2\theta\eta^T C^TC\Gamma\tilde{\rho} - 2\theta\eta^T C^TC\bar{x} \\ &\quad +k\tilde{\rho}^T P^{-1}\tilde{\rho} + k_3\eta^T\eta_\tau + k_3'\eta^T\tilde{\rho}_\tau \\ &\quad -2\theta\tilde{\rho}^T\Gamma^T C^TC\bar{x} + \frac{\ln(\theta)}{2\tau}\tilde{\rho}^T P^{-1}\tilde{\rho} \\ &\quad +\tilde{\rho}^T\tilde{\rho} + \theta\tilde{\rho}^T\Gamma^T C^TC\Gamma\tilde{\rho} - \theta\tilde{\rho}^T P^{-1}\tilde{\rho}\end{aligned} \tag{23}$$

On définit

$$c_1(\theta) = \theta - k - \frac{\ln(\theta)}{2\tau} - \frac{1}{\lambda_m(P^{-1})} \tag{24}$$

L'équation (23) peut se mettre sous la forme :

$$\begin{aligned}\dot{V} + \frac{\ln(\theta)}{2\tau}V &\leq -c(\theta)\eta^T S\eta - \theta\bar{x}^T C^TC\bar{x} \\ &\quad -c_1(\theta)\tilde{\rho}^T P^{-1}\tilde{\rho} + k_3\eta^T\eta_\tau + k_3'\eta^T\tilde{\rho}_\tau\end{aligned} \tag{25}$$

Si on pose $k(\theta) = \dfrac{\ln(\theta)}{4\tau}$, on obtient finalement l'expression :

$$V \leq e^{-2k(\theta)t} \max_{s\in[-\tau_M, 0]} V \tag{26}$$

D'après [12], cette majoration de V implique la convergence exponentielle vers zero des variables η et $\tilde{\rho}$, puis celle de $\bar{x}$ et de $\tilde{x}$, ce qui termine la démonstration. ■

III. Application à la cryptanalyse

Dans cette partie, on utilise l'observateur adaptatif précédent dans le but de guider le choix de la clé de chiffrement : tous les paramètres du système émetteur qui peuvent être estimés grâce à l'observateur adaptatif sont éliminés.

A. Système hyperchaotique

On considère le système hyperchaotique décrit dans l'article [6]:

$$\dot{x}(t) = Fx(t) + \phi\left(x(t), x_\tau(t), \rho\right) \tag{27}$$

avec

$$F = \begin{pmatrix} 0 & \alpha & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \tag{28}$$

$$\phi(x, x_\tau) = \begin{pmatrix} -\alpha x_1(t) - \alpha\delta\tanh(x_1(t)) \\ x_1(t) - x_2(t) \\ -\beta x_2(t) - \gamma x_3(t) + \varepsilon\sin(\sigma x_1(t-\tau)) \end{pmatrix} \tag{29}$$

et ρ est le vecteur de paramètres inconnus qui jouent le rôle de la clé de chiffrement dans cette partie.
La première étape consiste à mettre la dynamique de l'émetteur (27) sous la forme canonique (1), grâce au changement de variable suivant :

$$z = \Lambda x = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \alpha \end{pmatrix} x \tag{30}$$

Par conséquent la dynamique de $z(t)$ est la suivante :

$$\begin{cases} \dot{z}_1(t) = z_2(t) + (-\alpha z_1(t) - \alpha\delta\tanh(z_1(t))) \\ \dot{z}_2(t) = z_3(t) + (\alpha z_1(t) - z_2(t)) \\ \dot{z}_3(t) = (\beta z_2(t) - \gamma z_3(t) + \alpha\varepsilon\sin(\sigma z_1(t-\tau))) \end{cases} \tag{31}$$

Il apparaît clairement que le système dans ces nouvelles coordonnées est sous la forme canonique (1) (dans le membre de droite, la partie entre parenthèses définit la fonction ϕ). Les résultats du théorème 5 sont appliqués à l'émetteur, dans les nouvelles coordonnées. On obtient ensuite la dynamique de l'observateur dans les coordonnées initiales (on remarquera que $C\Lambda = C$) :

$$\begin{aligned}
\dot{\hat{x}}(t) &= F\hat{x}(t) + \phi(\hat{x}(t), \hat{x}_\tau(t), \hat{\rho}) \\
&\quad -\theta\Lambda^{-1}\Delta_\theta^{-1}\left(S^{-1} + \Gamma(t)P(t)\Gamma^T(t)\right)C^TC\tilde{x}(t) \\
\dot{\hat{\rho}}(t) &= -\theta P(t)\Gamma^T(t)C^TC\tilde{x}(t) \\
\dot{\Gamma}(t) &= \theta(A - S^{-1}C^TC)\Gamma + \Delta_\theta\Lambda\frac{\partial\phi}{\partial\rho}(\hat{x}(t), \hat{x}_\tau(t), \hat{\rho}) \\
\dot{P}(t) &= -\theta P(t)\Gamma^T(t)C^TC\Gamma(t)P(t) + \theta P(t)
\end{aligned} \tag{32}$$

B. *Cryptanalyse*

D'après les résultats du théorème 5, l'observateur (32) converge exponentiellement si les hypothèses (H1)-(H3) sont vérifiées. L'hypothèse (H1) est toujours remplie, l'hypothèse (H2) dépend du choix du paramètre choisi pour tenir le rôle de la clé et l'hypothèse (H3) dépend des valeurs choisies pour l'ensemble des paramètres de l'émetteur : si l'émetteur est en régime chaotique, (H3) est vérifiée. Si l'émetteur est dans une fenêtre d'ordre (qui correspond à un retour à un comportement périodique après une phase chaotique), particulièrement visible sur un diagramme de bifurcations tracé dans l'article [6], alors la condition d'excitation persistante (9) ne peut être vérifiée. Il a été montré dans [6] que les paramètres de l'émetteur doivent justement être choisis pour garantir un comportement réellement hyperchaotique, ce qui définit l'espace des clés. On supposera donc que l'ensemble des paramètres appartient à cet espace des clés, et par conséquent la condition (H3) est vérifiée.

Les simulations suivantes montrent qu'un intrus, connaissant le cryptosystème, à l'exception d'un paramètre, peut se synchroniser avec l'émetteur, et estimer ce paramètre. On donne deux exemples : le premier estime un paramètre linéaire γ, le second estime le retard τ.

Les paramètres γ et τ sont fixés au niveau de l'émetteur, et ils sont inconnus au niveau du récepteur (32). Dans la suite, ρ représente le vecteur $(\gamma\ \tau)^T$.
On calcule la dérivée partielle de ϕ par rapport au vecteur ρ :

$$\frac{\partial\phi}{\partial\rho}(\hat{x}, \hat{x}_\tau, \hat{\rho}) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ \hat{x}_3(t) & -\varepsilon\sigma\dot{\hat{x}}_1(t-\hat{\rho})\cos(\sigma\hat{x}_1(t-\hat{\rho})) \end{pmatrix} \tag{33}$$

Les simulations sont réalisées avec Matlab-Simulink, avec un algorithme d'intégration numérique de Runge-Kutta d'ordre quatre, de pas fixe égal à 1 ms.
Les valeurs suivantes sont choisies afin de garantir un comportement hyperchaotique (cf. [6]).

α	β	γ	δ	ε	σ	τ
9	14	5	-1	100	10	1

TABLE I
PARAMÈTRES DE L'ÉMETTEUR (27)

Les conditions initiales suivantes ont été fixées :
$x(0) = \begin{pmatrix} 0.1 & 0.1 & 0.1 \end{pmatrix}^T$, $\hat{x}(0) = -x(0)$,

$$P(0) = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \Gamma(0) = \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 1 \end{pmatrix}, \hat{\rho}(0) = 0.$$

La valeur du paramètre θ est fixée à 15. S'agissant d'un observateur de type grand gain, plus la valeur du paramètre θ est élevée, plus la convergence est rapide. Cela est quantifié par l'équation (26).
Les figures ci-dessous illustrent ces simulations.

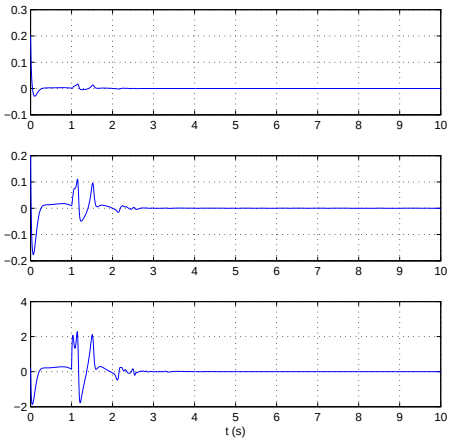

Fig. 1. Erreurs de synchronisation : $x_1 - \hat{x}_1$ (en haut), $x_2 - \hat{x}_2$ (au milieu), $x_3 - \hat{x}_3$ (en bas)

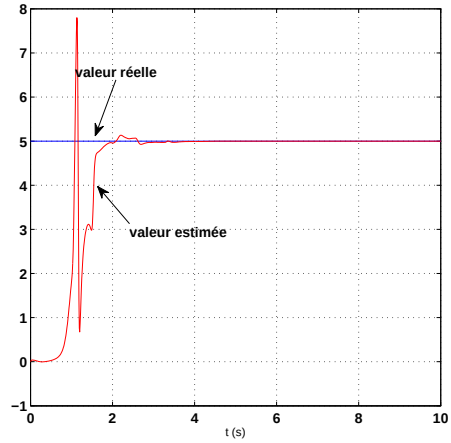

Fig. 2. Estimation de γ

L'observateur adaptatif détaillé dans la partie précédente permet donc d'approfondir la cryptanalyse des cryptosystèmes hyperchaotiques considérés ci-dessus : un paramètre *seul* que l'observateur (5) permet d'estimer, même intervenant de façon non linéaire dans la dynamique de l'émetteur, ne peut tenir le rôle de la clé de chiffrement. Il faut donc trouver une combinaison de paramètres qui sont qualifiés d'*anti-adaptatifs* dans [5], [15].

IV. Conclusion

Dans cet article, nous avons étendu les résultats de [25] à une classe de systèmes hyperchaotiques à retard. Les hypothèses de convergence de l'observateur adaptatif proposé dans cet article sont relaxées, dans le sens où les états

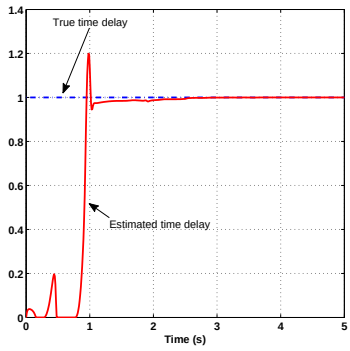

Fig. 3. Estimation du retard

des systèmes hyperchaotiques sont naturellement bornés. En outre, la condition d'excitation persistante indissociable des techniques adaptatives ne nécessite pas l'ajout d'une entrée *riche*, car les signaux hyperchaotiques sont déjà à excitation persistante. Nous avons appliqué ces résultats dans le cadre de la cryptanalyse, pour compléter les résultats présentés dans l'article [6] : les paramètres qui peuvent être estimés par l'observateur adaptatif ne peuvent être choisis comme clé de chiffrement. Il en résulte qu'un paramètre -constant- seul, même intervenant de façon non linéaire dans la dynamique de l'émetteur ne peut tenir le rôle de la clé.

Références

[1] G. Alvarez and S. Li. Some basic cryptographic requirements for chaos-based cryptosystems. *Int. J. Bifurc. Chaos*, 16(8):2129–2151, 2006.

[2] M.A. Aziz-Alaoui. Synchronization of chaos. *Encyclopedia of Mathematical Physics*, 5:213–226, 2006.

[3] S. Boccaletti, J. Kurths, G. Osipov, D.L. Valladares, and C.S. Zhou. The synchronization of chaotic systems. *Physics Reports*, 366:1–101, 2002.

[4] S. Bowong. Adaptive synchronization between two different chaotic dynamical systems. *Commun. Nonlinear Sci. Numer. Simulat.*, 12(6):976–985, 2007.

[5] S. Čelikovský and G. Chen. Secure synchronization of a class of chaotic systems from a nonlinear observer approach. 50(1):76–82, 2005.

[6] E. Cherrier, M. Boutayeb, and J. Ragot. Observers based synchronization and input recovery for a class of nonlinear systems. *IEEE Trans. Circuit Syst. I*, 53(9), 2006.

[7] J.D. Farmer. Chaotic attractors of an infinite-dimensional dynamical system. *Physica D*, 4:366–393, 1982.

[8] M. Farza, M. M'Saad, T. Maatoug, and M. Kamoun. Adaptive observers for nonlinearly parameterized class of nonlinear systems. *Automatica*, pages 2292–2299, 2009.

[9] A.L. Fradkov, B. Andrievsky, and R.J. Evans. Adaptive observer-based synchronization of chaotic systems with first-order coder in the presence of information constraints. *IEEE Trans. Circuit Syst. I*, 55(6):1685–1694, 2008.

[10] A.L. Fradkov and A.Yu. Markov. Adaptive synchronization of chaotic systems based on speed gradient method and passification . *IEEE Trans. Circuit Syst. I*, 44(10):905 – 912, 1997.

[11] J.P. Gauthier, H. Hammouri, and S. Othman. A simple obsever for nonlinear systems: Application to bioreactors. *IEEE Trans. Automatic Control*, 37(6):875–880, 1992.

[12] K. Gu, V.L. Kharitonov, and J. Chen. *Stability of time-delay systems*. Birkhäuser, 2003.

[13] K.S. Halle, C.W. Wu, M. Itoh, and L.O. Chua. Spread spectrum communication through modulation of chaos. *Int. J. Bifurc. Chaos*, 3(2):469–477, 1993.

[14] L.L. Huang, M. Wang, and R.P. Feng. Parameters identification based synchronization for a class of chaotic systems with unknown parameters. *Phys. Lett. A*, 342:299–304, 2005.

[15] Y. Liu and W.K.-S. Tang. *Adaptive synchronization of chaotic systems and its uses in cryptanalysis*, volume 254 of *Recent advances in nonlinear dynamics and synchronization*. Springer, Berlin, 2009.

[16] A. Loria, E. Panteley, and A. Zavala-Rio. Adaptive observers with persistency of excitation for synchronization of chaotic systems. *IEEE Trans. Circuit Syst. I*, 2009, Accepted for future publication.

[17] A. Loria and A. Zavala-Rio. Adaptive tracking control of chaotic systems with applications to synchronization. *IEEE Trans. Circuit Syst. I*, 54(9):2019–2029, 2007.

[18] J. Lu, J. Cao, and D.W.C. Ho. Adaptive Stabilization and Synchronization for Chaotic Lur'e Systems With Time-Varying Delay . *IEEE Trans. Circuit Syst. I*, 55(5):1347 – 1356, 2008.

[19] MC. Mackey and L. Glass. Oscillation and chaos in physiological control systems. *Science*, 197:287–289, 1977.

[20] O. Morgül and E. Solak. Observer based synchronization of chaotic systems. *Physical Review E*, 54(5):4803–4811, 1996.

[21] K.S. Narendra and A. Annaswamy. *Stable adaptive systems*. Prentice Hall Int., NJ, 1989.

[22] H. Nijmeijer and I.M.Y. Mareels. An observer looks at synchronization. *IEEE Trans. Circuit Syst. I*, 44(10):882–890, 1997.

[23] U. Parlitz. Estimating model parameters from times series by autosynchronization. *Phys. Rev. Lett.*, 76:1232–1235, 1996.

[24] L.M. Pecora and T.L. Carroll. Synchronization in chaotic systems. *Phys. Rev. Lett.*, 64(8):821–824, 1990.

[25] A. Sboui, M. Farza, E. Cherrier, and M. M'Saad. Adaptive observer for a class of nonlinear time delay systems. In *15th IFAC Symposium on System Identification*, Saint-Malo, France, July 2009.

[26] H. Shim. *A passivity-based nonlinear observer and a semi-global separation principle*. PhD thesis, School of Electrical Engineering, Seoul National University, 2001.

[27] Y. Tang and X. Guan. Parameter estimation of chaotic system with time-delay: A differential evolution approach. *Chaos, Solitons and Fractals*, 42:3132–3239, 2009.

[28] T. Yang and L.O. Chua. Secure communication via chaotic parameter modulation. *IEEE Trans. Circuit Syst. I*, 43(9):817–819, 1996.

[29] T. Yang, L.-B. Yang, and C.-M. Yang. Cryptanalysing chaotic secure communications using return maps. *Phys. Lett. A*, 245:495–510, 1998.

[30] A. Zemouche, M. Boutayeb, and G. I. Bara. Observer design for nonlinear systems : An approach based on the differential mean value theorem. In *Proceedings of the Joint 44th IEEE Conference on Decision and Control and European Control Conference, Seville, Spain*, 2005.