THEORIE DU CONTROLE ET SYSTEMES HYBRIDES DANS LE CONTEXTE CRYPTOGRAPHIQUE

Gilles Millérioux
Centre de Recherche en Automatique de Nancy (CRAN UMR 7039)
CNRS, Nancy Université

Dans les années 1990 ont émergées, pour la sécurisation des communications, des techniques de ``brouillage'' de l'information basées sur l'utilisation de dynamiques complexes et plus particulièrement chaotiques. Ces comportements, exhibés par des systèmes dynamiques non linéaires, se distinguent par leur sensibilité aux conditions initiales. Cette sensibilité se manifeste par le fait qu'une faible perturbation puisse engendrer des changements notoires au niveau du comportement dynamique. Les phénomènes chaotiques ont fait l'objet d'une attention toute particulière depuis de nombreuses années. En réalité, la terminologie ``chaos'' a été introduite tardivement, en 1975, dans le papier maintenant célèbre intitulé ``Period Three Implies Chaos'' de Li et Yorke [1]. Mais il n'a pas fallu attendre les années 1975 pour constater l'intérêt qu'ont suscité les dynamiques complexes. Dès la fin du 19e siècle, le mathématicien français Henri Poincaré (1854-1912) s'intéressant à la dynamique des corps célestes avaient fait apparaître des solutions d'équations différentielles à forte sensibilité aux conditions initiales. Plus tard, en 1963, Edward Lorenz avait illustré ce phénomène expérimentalement sur des problèmes de convection propres à la météorologie. Depuis les années 90, le développement d'applications liées aux phénomènes chaotiques a été considérable: circuits électriques, mécanique, physique, avionique ont fait l'objet d'études liées au chaos. En raison de leurs propriétés, ils possèdent en particulier en effet des spectres étendues et s'apparentant à des signaux aléatoires, les signaux chaotiques, bien que générés par des systèmes de nature parfaitement déterministe, sont très difficiles à prédire. Ceci explique les raisons qui ont motivé les chercheurs à exploiter de telles séquences pour concevoir des schémas de communications sécurisées. En effet, il y a tout lieu de penser qu'il existe un lien entre ces caractéristiques et les propriétés de Shannon, à savoir confusion et diffusion, usuellement rencontrées en cryptographie. L'année 1990 a été marquée par un éminent papier [2] de Pecora et Carroll proposant un schéma de communication sécurisée. Bien que relativement basique, ce fut le point de départ d'un nombre impressionnant de travaux portant sur l'élaboration d'architectures de communications sécurisées. Cependant, la plupart des algorithmes proposés relèvent plus de la stéganographie que du chiffrement au sens de la cryptographie classique où on distingue typiquement deux grandes classes d'algorithmes: les algorithmes à clé publique et ceux à clé secrète. Les algorithmes à clé publique sont principalement basés sur des problèmes mathématiques difficiles à résoudre du point de vue calculatoire, le problème de la factorisation première en est un exemple. Un algorithme célèbre appartenant à cette classe est le RSA. Les algorithmes à clé symétrique dits par flot sont quant à eux basés sur la synchronisation de séquences complexes générés par des systèmes dynamiques prenant la forme d'automates à états finis.

Au cours de cet exposé, on développe une étude effectuée dans [3] qui établit une connexion entre certains cryptosystèmes chaotiques et des algorithmes de chiffrement symétriques classiques. On montre en quoi les propriétés structurelles des systèmes dynamiques telles que l'inversibilité, la platitude ou l'identifiabilité peuvent jouer un rôle majeur pour la conception d'algorithmes de chiffrement et ainsi permettre de développer des approches alternatives de synthèse. On montre dans le même temps en quoi les systèmes hybrides peuvent constituer une classe particulière intéressante de systèmes dynamiques dans le contexte cryptographique. La raison essentielle est qu'un chiffreur par flot doit être rapide et avoir une simplicité d'implantation. Dans cette perspective, des études intéressantes et pionnières en la matière ont été menées par Shamir [4]. Ce dernier suggère le recours à des primitives mêlant à la fois des opérations booléennes et des opérations arithmétiques. Ainsi, définit-il la classe des T-fonctions résultant de la composition d'opérations élémentaires telles que l'addition, la soustraction, la multiplication, le ou, le et, le ou exclusif, ces opérations étant faites sur des mots binaires. Cela confère aux chiffreurs associés une résistance aux attaques exclusivement

algébriques ou purement booléennes. En d'autres termes, il semble opportun d'introduire de l'hétérogénéité et les systèmes hybrides sont particulièrement intéressants dans cette perspective car intrinsèquement hétérogènes. Les conditions algébriques [5] caractérisant l'inversibilité à gauche et la platitude pour la classe particulière des systèmes linéaires à commutations seront rappelées au cours de l'exposé

Références bibliographiques :

[1] T. Y. LI and J. A. YORKE, 1975, *Period Three Implies Chaos, Amer. Math. Monthly, Vol. 82, pp. 985-992*

[2] L. M. PECORA and T. L. CARROLL, 1990, *Synchronization in Chaotic Systems, Phys. Rev. Letters,, Vol. 64, pp. 821-824*

[3] G. MILLERIOUX, J. M. AMIGO and J. DAAFOUZ, 2008, *A connection between chaotic and conventional cryptography , IEEE Trans. Circuits and Systems I: Regular Papers, Vol. 55, N. 6, pp. 1695-1703*

[4] A. SHAMIR, 2004, New cryptographic primirives based on multiword T-functions, Chapter 1, Springer Berlin / Heidelberg, Vol. 2004, pp. 1-15

[5] G. MILLERIOUX and J. DAAFOUZ, 2009, *Flatness of switched linear discrete-time systems , IEEE Trans. On Automatic Control, Vol. 54, N.3, March.*