Left invertibility, flatness and identifiability of switched linear dynamical systems: a framework for cryptographic applications

Phuoc Vo Tan, Gilles Millérioux, Jamal Daafouz

Left invertibility, flatness and identifiability of switched linear dynamical systems: a framework for cryptographic applications

Phuoc Vo Tan[a], Gilles Millérioux[a] and Jamal Daafouz[a]
[a] Nancy University, Research Center for Automatic Control of Nancy
(CRAN UMR CNRS 7039)
Corresponding author. Email: gilles.millerioux@esstin.uhp-nancy.fr

March 3, 2010

Abstract : The purpose of this paper is to illustrate the potential interest of the control theory framework for cryptographic applications. It is shown that under the properties of left invertibility and flatness, dynamical systems are structurally equivalent to some specific cryptographic primitives called self-synchronizing stream ciphers. After having motivated the interest of considering hybrid systems for such ciphers, the development is particularized for the special class of switched linear systems. We also show that identifiability is a necessary condition for security, describe an identification procedure as a possible attack and assess its complexity.

Hybrid systems have inspired a great deal of research from both control theory and theoretical computer science ([HSCC(2008)]). They provide a strong theoretical foundation which combines discrete-event and continuous-time systems in a manner that can capture software logic and physical dynamics in a unified modeling framework. The most well-known area of applicability of hybrid systems are naturally modeling, analysis and control design of embedded systems. From a theoretical point of view, stability, identifiability, controller or observer design are challenging problems widely studied in the literature ([Shorten et al.(2007), Bemporad et al.(2000), Juloski et al.(2005), Balluchi et al.(2002), Babaali and Egerstedt(2004)]).

In this paper, left invertibility, flatness and identifiability of discrete-time switched linear systems are investigated. The hybrid aspect is really taken into account insofar as the minimum "dwell-time" assumption is relaxed or in other words, since the switching rule is not restricted to the case when the modes are active during a sufficient large time. The conditions characterizing left invertibility ([Sain and Massey(1969)]) and flatness

([Levine and Nguyen(2003)]) of linear systems are no longer valid.

Next, it is shown that under the properties of left invertibility and flatness, dynamical systems are structurally equivalent to some specific cryptographic primitives called self-synchronizing stream ciphers. The consideration of hybrid systems is motivated by the fact that introducing heterogeneity in the ciphers sounds relevant. Indeed, in order to improve the security of a cipher, a general idea has been proposed and motivated by Shamir (see ([Klimov and Shamir(2004)]) as a pioneering work). Shamir suggests to mix algebraic domains and thereby to use combinations of boolean and arithmetic operations. And yet, switched systems are intrinsically heterogeneous in this sense since they involve several algebraic models which are switched in time according to some logical rules ([Liberzon(2003)]). The development is particularized here for switched linear systems. We further show that identifiability is a necessary condition for security, describe an identification procedure as a possible attack and assess its complexity.

The paper is organized as follows. Section 1 presents algebraic conditions under which switched linear discrete-time systems are left invertible and flat. A sequential left inversion procedure is provided. Next, identifiability and identification are addressed. In Section 2, a structural comparison between such dynamical systems and the special encryption schemes called self-synchronizing stream ciphers is brought out and illustrated through a simple numerical example. Further issues to be investigated in the perspective of designing fully-fledged cryptographic primitives are sketched.

1 Left invertibility, flatness and identification of switched linear systems

In this section, results on left invertibility, flatness and identification of switched linear systems are expressed in a form suitable to discuss their impact in secure communication applications. More general treatments can be found in ([Millerioux and Daafouz(2009)]) for left invertibility and flatness properties and in ([Vidal et al.(2003)]) for identification.

Before proceeding further, let us introduce some useful notation. Consider the switched linear dynamical system:

$$\left\{ \begin{array}{lcl} x_{k+1} & = & A_{\sigma(k)}x_k + B_{\sigma(k)}u_k \\ y_k & = & C_{\sigma(k)}x_k + D_{\sigma(k)}u_k \end{array} \right. \tag{1}$$

where $x_k \in \mathbb{R}^n$, $u_k \in \mathbb{R}$ and $y_k \in \mathbb{R}$. All the matrices, namely $A_{\sigma(k)} \in \mathbb{R}^{n\times n}$, $B_{\sigma(k)} \in \mathbb{R}^{n\times 1}$, $C_{\sigma(k)} \in \mathbb{R}^{1\times n}$ and $D_{\sigma(k)} \in \mathbb{R}$ belong to the respective finite sets $(A_j)_{1\leq j\leq J}$, $(B_j)_{1\leq j\leq J}$, $(C_j)_{1\leq j\leq J}$ and $(D_j)_{1\leq j\leq J}$. At a given time k, the

index j corresponds to the mode of the system and results from a switching function $\sigma : k \in \mathbb{N} \mapsto j = \sigma(k) \in \{1, \ldots, J\}$. $\{\sigma\}_{k_1}^{k_2}$ refers to the mode sequence $\{\sigma(k_1), \ldots, \sigma(k_2)\}$.
Let $\mathcal{U}$ be the space of input sequences over $[0, \infty)$ and $\mathcal{Y}$ the corresponding output space. At time k, for each initial state $x_k \in \mathbb{R}^n$, when the system (1) is driven by the input sequence $\{u\}_k^{k+T} = \{u_k, \ldots, u_{k+T}\} \in \mathcal{U}$, for a mode sequence $\{\sigma\}_k^{k+T}$, $\{x(x_k, \sigma, u)\}_k^{k+T}$ refers to the solution of (1) starting from x_k in the interval of time $[k, k+T]$ and $\{y(x_k, \sigma, u)\}_k^{k+T} \in \mathcal{Y}$ refers to the corresponding output sequence in the same interval of time $[k, k+T]$.

1.1 Left invertibility and left inversion

Before addressing the left invertibility property, the relative degree of a switched linear system must be defined. We first recall a general definition.

Definition 1 *The* relative degree *of a dynamical system with respect to its input u_k is the required number r of iterations of its output y_k so as y_{k+r} depends explicitly on u_k.*

Remark 1 *Hereafter, we only consider the case when the relative degree r is constant.*

We are checking for an algebraic interpretation of the relative degree for (1) in terms of its state space description matrices. To this end, we must write down the expression of y_{k+i} by iterating (1)

$$y_{k+i} = C_{\sigma(k+i)} A_{\sigma(k)}^{\sigma(k+i-1)} x_k + \sum_{j=0}^{j=i} \mathcal{T}_{\sigma(k)}^{i,j} u_{k+j} \tag{2}$$

with

$$\mathcal{T}_{\sigma(k)}^{i,j} = C_{\sigma(k+i)} A_{\sigma(k+j+1)}^{\sigma(k+i-1)} B_{\sigma(k+j)} \text{ if } j \leq i-1, \quad \mathcal{T}_{\sigma(k)}^{i,i} = D_{\sigma(k+i)} \tag{3}$$

and with the transition matrix defined as:

$$\begin{array}{rcl} A_{\sigma(k_0)}^{\sigma(k_1)} & = & A_{\sigma(k_1)} A_{\sigma(k_1-1)} \ldots A_{\sigma(k_0)} \text{ if } \ k_1 \geq k_0 \\ & = & \mathbf{1}_n \ \text{ if } \ k_1 < k_0 \end{array}$$

$\mathbf{1}_n$ is the identity matrix of dimension n.
According to the Definition 1, the relative degree r of (1) is

- $r = 0$ if $\mathcal{T}_{\sigma(k)}^{0,0} \neq 0$ for all k

- the least integer $r < \infty$ such that for all k

$$\begin{array}{l} \mathcal{T}^{i,j}_{\sigma(k)} = 0 \text{ for } \; i = 0, \ldots, r-1 \;\; \text{and} \;\; j = 0, \ldots, i \\ \mathcal{T}^{r,0}_{\sigma(k)} \neq 0 \end{array} \tag{4}$$

Let us notice that the product of matrices involved in $\mathcal{T}^{i,j}_{\sigma(k)}$ is the generalization of the well-known discrete-time Markov parameters CA^sB for a linear system described by the $4-$ uple (A, B, C, D) of state space matrices.

When (1) has relative degree r, its output reads at time $k + r$:

$$y_{k+r} = C_{\sigma(k+r)} A^{\sigma(k+r-1)}_{\sigma(k)} x_k + \mathcal{T}^{r,0}_{\sigma(k)} u_k \tag{5}$$

Definition 2 *The system (1) is* left invertible *if there exists a nonnegative integer $R < \infty$ such that, for two any inputs sequences $\{u\}_k^{k+R}, \{u'\}_k^{k+R} \in \mathcal{U}$, the following implication applies:*

$$\forall \sigma, \forall x_k \; \{y(x_k, \sigma, u)\}_k^{k+R} = \{y(x_k, \sigma, u')\}_k^{k+R} \;\; \Rightarrow \;\; u_k = u'_k \tag{6}$$

In other words, (1) is *left invertible* if the input u_k can be uniquely determined from an output sequence of finite length for any known initial condition and switching rule. It turns out that if (1) has a finite relative degree r, it is also left invertible with $R = r$. Indeed, if (1) has a finite relative degree r, (5) holds and the input u_k can be deduced in a unique way. It reads:

$$u_k = (\mathcal{T}^{r,0}_{\sigma(k)})^{-1} (y_{k+r} - C_{\sigma(k+r)} A^{\sigma(k+r-1)}_{\sigma(k)} x_k) \tag{7}$$

The existence of the inverse of $\mathcal{T}^{r,0}_{\sigma(k)}$ is guaranteed since, by definition (see Eq. (3)), it is always different from zero. Actually, let us notice that for (1), according to (7), only the last sample y_{k+R} of the sequence $\{y(x_k, \sigma, u)\}_k^{k+R}$ is required for recovering u_k. We are now concerned with a recursive left inversion of (1) achieving the recovery of u_k from y_k without any knowledge of x_k. Let us define the inverse transition matrix as

$$\begin{array}{rcl} P^{\sigma(k_1)}_{\sigma(k_0)} & = & P^r_{\sigma(k_1)} P^r_{\sigma(k_1-1)} \ldots P^r_{\sigma(k_0)} \text{ if } \; k_1 \geq k_0 \\ & = & \mathbf{1}_n \;\; \text{if} \;\; k_1 < k_0 \end{array}$$

with

$$P^r_{\sigma(k)} = A_{\sigma(k)} - B_{\sigma(k)} (\mathcal{T}^{r,0}_{\sigma(k)})^{-1} C_{\sigma(k+r)} A^{\sigma(k+r-1)}_{\sigma(k)} \tag{8}$$

Proposition 1 *Assume that (1) is left invertible and has relative degree r. The following dynamical system is a stable $r-$delayed inverter for (1)*

whenever the system $\nu_{k+1} = P^r_{\sigma(k)}\nu_k$ *is uniformly asymptotically stable*

$$\left\{\begin{array}{lcl} \hat{x}_{k+r+1} & = & P^r_{\sigma(k)}\hat{x}_{k+r} + B_{\sigma(k)}(\mathcal{T}^{r,0}_{\sigma(k)})^{-1}y_{k+r} \\ \hat{u}_{k+r} & = & -(\mathcal{T}^{r,0}_{\sigma(k)})^{-1}C_{\sigma(k+r)}A^{\sigma(k+r-1)}_{\sigma(k)}\hat{x}_{k+r} \\ & & +(\mathcal{T}^{r,0}_{\sigma(k)})^{-1}y_{k+r} \end{array}\right. \tag{9}$$

Proof 1 *On one hand, substituting (5) into (9) yields:*

$$\begin{array}{rcl} \hat{x}_{k+r+1} & = & P^r_{\sigma(k)}\hat{x}_{k+r} + B_{\sigma(k)}(\mathcal{T}^{r,0}_{\sigma(k)})^{-1}C_{\sigma(k+r)}A^{\sigma(k+r-1)}_{\sigma(k)}x_k \\ & & +B_{\sigma(k)}(\mathcal{T}^{r,0}_{\sigma(k)})^{-1}\mathcal{T}^{r,0}_{\sigma(k)}u_k \end{array} \tag{10}$$

Taking into account (8) and noticing that $(\mathcal{T}^{r,0}_{\sigma(k)})^{-1}\mathcal{T}^{r,0}_{\sigma(k)} = 1$, $\epsilon_k = x_k - \hat{x}_{k+r}$ *fulfills the recursion:*

$$\begin{array}{rcl} \epsilon_{k+1} & = & (A_{\sigma(k)} - B_{\sigma(k)}(\mathcal{T}^{r,0}_{\sigma(k)})^{-1}C_{\sigma(k+r)}A^{\sigma(k+r-1)}_{\sigma(k)})\epsilon_k \\ & & = P^r_{\sigma(k)}\epsilon_k \end{array} \tag{11}$$

On the other hand, from the expression (7) of u_k *and the expression of* $\hat{u}_{k+r}$ *in (9), we get that:*

$$u_k - \hat{u}_{k+r} = -(\mathcal{T}^{r,0}_{\sigma(k)})^{-1}C_{\sigma(k+r)}A^{\sigma(k+r-1)}_{\sigma(k)}(x_k - \hat{x}_{k+r}) \tag{12}$$

From (12) we can infer that $\hat{u}_{k+r}$ *converges toward* u_k *as long as* $\hat{x}_{k+r}$ *converges toward* x_k*, that is provided that the system* $\nu_{k+1} = P^r_{\sigma(k)}\nu_k$ *with* $\nu_k = \epsilon_k$ *is uniformly asymptotically stable.*

1.2 Flatness

We first recall a general definition of *flat output* (for details about flatness, the reader can refer to ([Fliess et al.(1995)]) or the book ([Sira-Ramirez and Agrawal(2004)])).

Definition 3 *A* flat output *of a dynamical system is an output variable* y_k *such that all system variables can be expressed as a function of* y_k *and a finite number of its forward/backward iterates. In particular, there exists two functions* $\mathcal{F}$, $\mathcal{G}$ *and integers* $t_1 < t_2$, $t'_1 < t'_2$ *such that*

$$\begin{array}{rcl} x_k & = & \mathcal{F}(y_{k+t_1}, \cdots, y_{k+t_2}) \\ u_k & = & \mathcal{G}(y_{k+t'_1}, \cdots, y_{k+t'_2}) \end{array} \tag{13}$$

We derive an algebraic interpretation of flat outputs for (1).

Proposition 2 *The output y_k of (1), assumed to be left invertible and to have relative degree r, is a flat output if there exists a positive integer $0 < K < \infty$ such that for all $k \geq 0$*

$$P_{\sigma(k)}^{\sigma(k+K-1)} = \mathbf{0} \tag{14}$$

where $\mathbf{0}$ stands for the null matrix.

Proof 2 *The proof is based on the inverse system. If (1) is left invertible and has relative degree r, (9) exists. Iterating (9) $l-1$ times yields:*

$$\begin{array}{rcl} \hat{x}_{k+r+l} & = & P_{\sigma(k)}^{\sigma(k+l-1)} \hat{x}_{k+r} \\ & & + \sum_{i=0}^{l-1} P_{\sigma(k+i+1)}^{\sigma(k+l-1)} B_{\sigma(k+i)} \mathcal{T}_{\sigma(k+i)}^{r,0} y_{k+i+r} \end{array} \tag{15}$$

If (14) is fulfilled, (15) turns into

$$\hat{x}_{k+r+K} = \sum_{i=0}^{K-1} P_{\sigma(k+i+1)}^{\sigma(k+K-1)} B_{\sigma(k+i)} \mathcal{T}_{\sigma(k+i)}^{r,0} y_{k+i+r} \tag{16}$$

revealing that $\hat{x}_{k+r+K}$ is independent of $\hat{x}_{k+r}$. In particular, (16) holds for $\hat{x}_{k_0+r} = x_{k_0}$ for all $k_0 \geq 0$, that is for $\epsilon_{k_0} = 0$ with $k_0 \geq 0$. By virtue of (11), we infer that $\epsilon_k = 0$ for all $k \geq k_0$ and thus $\hat{x}_{k+r+K} = x_{k+K}$ for all $k \geq 0$. Therefore, after performing the change of variable $k \rightarrow k-K$, we obtain an explicit form for $\mathcal{F}$ involved in (13).

$$x_k = \sum_{i=0}^{K-1} P_{\sigma(k+i+1-K)}^{\sigma(k-1)} B_{\sigma(k+i-K)} \mathcal{T}_{\sigma(k+i-K)}^{r,0} y_{k+i+r-K} \tag{17}$$

On the other hand, substituting (17) into (7) yields an explicit form for $\mathcal{G}$ involved in (13) and then, we infer that y_k is a flat output according to the Definition 3.

1.3 Identification

Let θ be a parameter vector consisting of a subset of entries of $(A_j)_{1\leq j\leq J}$, $(B_j)_{1\leq j\leq J}$, $(C_j)_{1\leq j\leq J}$ and $(D_j)_{1\leq j\leq J}$ in the state space model (1). Having in mind the crytpographic context which will be further considered, we present an identification procedure of θ based on the input/output model of (1).

When the switched system (1) is flat, its input/output model can be obtained in a systematic and convenient way. Indeed, if (1) is flat with flat

output y_k, the state vector x_k obeys (17). Substituting the expression (17) of x_k into (5) yields the input/output relation:

$$\begin{array}{l} y_{k+r} = C_{\sigma(k+r)} A^{\sigma(k+r-1)}_{\sigma(k)}. \\ (\sum_{i=0}^{K-1} P^{\sigma(k-1)}_{\sigma(k+i+1-K)} B_{\sigma(k+i-K)} \mathcal{T}^{r,0}_{\sigma(k+i-K)} y_{k+i+r-K}) + \mathcal{T}^{r,0}_{\sigma(k)} u_k \end{array} \tag{18}$$

Let $\{\sigma_1\}_{k+r-K}^{k+r-1}, \ldots, \{\sigma_N\}_{k+r-K}^{k+r-1}$ the N possible mode sequences $\{\sigma(k+r-K), \ldots, \sigma(k+r-1)\}$ over the interval of time $[k+r-K, k+r-1]$. The number N of all possible mode sequences is finite since the number J of modes of (1) is. These mode sequences will be respectively denoted for short $\sigma_1, \ldots, \sigma_N$ in the sequel. Thus, for $t = 1, \ldots, N$, the input/output relation (18) can be rewritten as

$$y_{k+r} = \sum_{j=0}^{K-1} a_j(\sigma_t) y_{k+j+r-K} + c(\sigma_t) u_k \tag{19}$$

where $c(\sigma_t)$ and the $a_j(\sigma_t)$'s ($j = 0, \ldots, K-1$) are coefficients depending, in different ways according to the sequence σ_t, on the entries of the matrices $(A_j)_{1 \leq j \leq J}$, $(B_j)_{1 \leq j \leq J}$, $(C_j)_{1 \leq j \leq J}$ and $(D_j)_{1 \leq j \leq J}$ of (1)
Based on (19), two identification procedures can be distinguished according to the assumption on the accessibility of σ_t.

First identification procedure

Let us first assume that σ_t is accessible. Since for each σ_t, the parameters $c(\sigma_t)$ and the $a_j(\sigma_t)$'s appear in a linear fashion in the input/output relation (19), they are obviously identifiable and the identification is easy. Indeed, for a given mode sequence σ_t, under the usual Persistently Exciting (PE) conditions, the identification can always be performed by iterating the relation (19) until a set of linear independent equations is obtained and can be solved. The solution is unique for each σ_t and gives $c(\sigma_t)$ and the $a_j(\sigma_t)$'s.

Second identification procedure

Conversely, let us assume that σ_t is not accessible. The previous procedure does no longer hold. Thus the identification procedure for recovering $c(\sigma_t)$ and the $a_j(\sigma_t)$'s must be substituted by another one. It turns out that it can be inspired from the method proposed in ([Vidal et al.(2003)]) for switched ARX systems. This method is summed up and adapted to our context.
Each input/output relation (19) can be rewritten for $t = 1, \ldots, N$

$$z_k^T b_t = 0 \tag{20}$$

- $z_k = [y_{k+r}, y_{k+r-1}, \cdots, y_{k+r-K}, u_k]^T \in \mathbb{R}^{K+2}$
- $b_t = [1, -a_0(\sigma_t), \ldots, -a_{K-1}(\sigma_t), -c(\sigma_t)]^T \in \mathbb{R}^{K+2}$

z_k is the *regressor vector* while b_t is the *parameter vector* corresponding to the mode sequence σ_t.
We can thereby define N hyperplanes S_t, $t = 1 \ldots, N$

$$S_t = \{z_k : z_k^T b_t = 0\}$$

The key idea rests on the fact that the so-called *Hybrid Decoupling Constraint* equation is fulfilled regardless of the switching sequences:

$$p_N(z_k) = \prod_{t=1}^{N} (z_k^T b_t) = \nu_N(z_k)^T h_N = 0 \tag{21}$$

$h_N \in \mathbb{R}^{M_N}$ is the coefficient of the *Hybrid Decoupling Polynomial* and $\nu_N : z_k \in \mathbb{R}^{K+2} \mapsto \xi_k \in \mathbb{R}^{M_n}$ is a *Veronese map* of degree N, the components of ξ_k corresponding to all the M_N monomials (product of the components of z_k) sorted in the degree-lexicographic order. The quantity M_N is given by

$$M_N = \begin{pmatrix} N+K-1 \\ N \end{pmatrix} = \frac{(N+K-1)!}{N!(K-1)!} \tag{22}$$

For the identification of the b_t's in (20), it is first needed to compute the coefficients h_N of (21). To this end, let $\mathcal{L}_N$ denote an embedded data matrix involving N mapped regressor vectors z_k through ν_N

$$\mathcal{L}_N = \begin{bmatrix} \nu_N(z_{k_1}) \\ \nu_N(z_{k_2}) \\ \ldots \\ \nu_N(z_{k_N}) \end{bmatrix}^T \in \mathbb{R}^{N \times M_N}$$

The following relation applies:

$$\mathcal{L}_N h_N = \mathbf{0} \tag{23}$$

If the mapped regressor vectors $\nu_N(z_{k_i})$ are *sufficiently exciting* (PE conditions), the existence of an integer N' such that the $\nu_{N'}(z_{k_i})$'s $(i = 1, \ldots, N')$ can span a $M_N - 1$ dimensional vector space, i.e

$$rank(\mathcal{L}_{N'}) = (M_N - 1) \tag{24}$$

is guaranteed. The lower bound of N' is $M_N - 1$. If (24) is fulfilled, the coefficient h_N can be retrieved by

$$h_N = Ker(\mathcal{L}_{N'}) \tag{25}$$

Ker stands for the null space.
If w_t is a point lying on the t^{th} hyperplane S_t, we can obtain, for $t = 1, \ldots, N$, the b_t's from the knowledge of h_N by performing:

$$b_t = \frac{Dp_N(w_t)}{eDp_N(w_t)} \tag{26}$$

where e stands for the vector $[1\ 0\cdots 0] \in \mathbb{R}^{K+2}$ and $Dp_N(w_t)$ stands for the derivative $Dp_N(z_k)$ of $p_N(z_k)$ with $z_k = w_t$. $Dp_N(z_k)$ reads

$$Dp_N(z_k) = \frac{\partial p_N(z_k)}{\partial z_k} = \frac{\partial}{\partial z_k}\prod_{t=1}^{N}(z_k^T b_t) = \sum_{t=1}^{N} b_t \prod_{l\neq t}(z_k^T b_l) \tag{27}$$

Remark 2 *An algebraic solution to determine the N distinct points w_t that lie on the N hyperplanes S_t can be found in ([Vidal et al.(2003)]).*

The unicity of the solution of an identification procedure is directly related to the notion of parametric identifiability ([Nõmm and Moog(2004)])([Anstett et al.(2008)]). Indeed, let us recall that a parameter of a discrete-time dynamical system is *identifiable* if it can be rewritten as a unique function of the input, the output and their iterates. For (1), it turns out that the aforementioned identification procedures provide $c(\sigma_t)$ and the $a_j(\sigma_t)$'s ($j = 0,\ldots,K-1,\ t = 1,\ldots,N$) of (19) in a unique way and that they depend on the input, the output and their iterates. Indeed, observe that b_t (and so $c(\sigma_t)$ and the $a_j(\sigma_t)$'s ($j = 0,\ldots,K-1,\ t = 1,\ldots,N$)) are inferred from (26) which involves p_N, p_N depending in turn on h_N through (21). Finally, h_N depends on the input, the output and their iterates of (1) through (25). On the other hand, the rank condition (24) and the normalization of b_t in (26) guarantee unicity. Thus, recalling that θ is a subset of entries of $(A_j)_{1\leq j\leq J}$, $(B_j)_{1\leq j\leq J}$, $(C_j)_{1\leq j\leq J}$ and $(D_j)_{1\leq j\leq J}$ of (1), the unicity of θ is guaranteed provided that θ can be deduced from $c(\sigma_t)$ and the $a_j(\sigma_t)$'s in a unique way.

2 Application to secure communication

The aim of this Section is to show and to illustrate the potential interest, for cryptographic applications, of the control theory framework developed in Section 1.

2.1 Generalities on stream ciphers

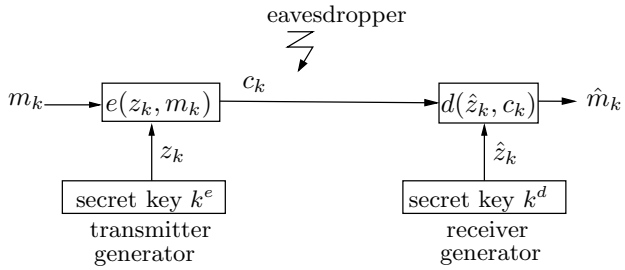

Figure 1: General encryption mechanism

A general stream cipher mechanism is illustrated in Fig. 1. We are given an alphabet A, that is, a finite set of basic elements named symbols. On the *transmitter* part, a plaintext (also called information or message) $m \in \mathcal{M}$ ($\mathcal{M}$ is called the message space) consisting of a string of symbols $m_k \in A$ is encrypted according to an encryption function e which depends on a so-called running key z_k. Consequently, for stream ciphers, the encryption function can change for each symbol. The sequence $\{z_k\}$ is called the *keystream*. The resulting ciphertext $c \in \mathcal{C}$ ($\mathcal{C}$ is called the ciphertext space), a string of symbols c_k from an alphabet B usually (and assumed hereafter) identical to A, is conveyed through a public channel to the *receiver*. At the receiver side, the ciphertext c is decrypted according to a decryption function d which depends on the running key $\hat{z}_k$. For a prescribed z_k, the function e must be invertible. The running keys z_k and $\hat{z}_k$ are delivered by generators which are identical at the transmitter and receiver sides. They are respectively parametrized at the transmitter side by a secret key $k^e \in \mathcal{K}$, ($\mathcal{K}$ being the key space) and parametrized at the receiver side by $k^d \in \mathcal{K}$. For proper decryption, the equality $k^d = k^e$ must be fulfilled. In the sequel, the secret key will be denoted $k^d = k^e = \theta$.
Stream ciphers are generally well appropriate and their use can even be compulsory when buffering is limited or when only one symbol can be processed at a time: the field of telecommunications often include such constraints.
Next we detail the special class of stream ciphers called self-synchronizing stream ciphers.

2.2 Self-synchronizing stream ciphers

Self-synchronizing stream ciphers admit the following recursion, written with the usual notation encountered in the literature:

$$\begin{cases} z_k = \sigma_\theta^{ss}(c_{k-l}, \ldots, c_{k-l'}) \\ c_{k+b_s} = e(z_k, m_k) \end{cases} \tag{28}$$

m_k is the plaintext and c_k is the the ciphertext. σ_θ^{ss} is the function of the keystream generator and is parameterized by a vector θ which acts as the secret key. σ_θ^{ss} depends on c_{k-i} $(i = l, \ldots, l')$ that is a fixed number of past values of c_k. Let us notice that, for computational reasons, there may exist a delay $b_s \geq 0$ between the plaintext m_k and the corresponding ciphertext c_{k+b_s}.
The equations (28) reveal the following merits and shortcomings of SSSC. First, if a ciphertext is deleted, inserted or flipped, the SSSC will automatically resume proper decryption after a short, finite and predictable transient time. Hence, SSSC does not require any additional synchronization flags or interactive protocols for recovering lost synchronization. Secondly, the self-synchronizing mechanism also enables the receiver to switch at any time into an ongoing enciphered transmission. Third, any modification of ciphertext

symbols by an active eavesdropper causes incorrect decryption for a fixed number of next symbols. As a result, an SSSC prevents active eavesdroppers from undetectable tampering with the plaintext: message authenticity is possible.

The equations of the decryption part obey:

$$\left\{ \begin{array}{l} \hat{z}_k = \sigma_\theta^{ss}(c_{k-l}, \ldots, c_{k-l'}) \\ \hat{m}_{k+b_s} = d(c_{k+b_s}, \hat{z}_k) \end{array} \right. \tag{29}$$

with, according to the principle of symmetric ciphers explained above, the decryption function d obeying the rule:

$$\hat{m}_{k+b_s} := d(c_{k+b_s}, \hat{z}_k) = m_k \text{ if } \hat{z}_k = z_k \tag{30}$$

Since the generators function σ_θ^{ss} share, at the transmitter and receiver sides, the same quantities, namely the past ciphertexts, it is clear that the generators synchronize automatically after a finite transient time of length M, that is $\hat{z}_k = z_k$ for $k \geq M$. That explains the terminology self-synchronizing stream ciphers.

Actually, (28) is a conceptual model, called canonical representation, that may correspond to numerous different architectures and may result from different design approaches ([Maurer(1991)])([Daemen and Kitsos(2005)]). We show in the next section, with a special treatment on switched linear systems, that under the properties of left invertibility and flatness, dynamical systems are structurally equivalent to self-synchronizing stream ciphers.

2.3 The role of left invertibility and flatness in the design of SSSC

Proposition 3 *If (1) has a finite relative degree r and y_k is a flat output, then (1) is structurally equivalent to a self-synchronizing stream cipher.*

Proof 3 *By virtue of (5) and (17), the system (1) can be rewritten in the following equivalent form:*

$$\left\{ \begin{array}{lcl} x_k & = & \sum_{i=0}^{K-1} P_{\sigma(k+i+1-K)}^{\sigma(k-1)} B_{\sigma(k+i-K)} \mathcal{T}_{\sigma(k+i-K)}^{r,0} y_{k+i+r-K} \\ y_{k+r} & = & C_{\sigma(k+r)} A_{\sigma(k)}^{\sigma(k+r-1)} x_k + \mathcal{T}_{\sigma(k)}^{r,0} u_k \end{array} \right. \tag{31}$$

and the result follows from the identification of (31) with (28), the correspondences being:

- $u_k \leftrightarrow m_k$ *(plaintext)*
- $y_k \leftrightarrow c_k$ *(ciphertext)*

- $x_k \leftrightarrow z_k$ *(keystream)*
- $\mathcal{F} \leftrightarrow \sigma_\theta^{ss}$ *(keystream generator)*
- $(x_k, u_k) \mapsto C_{\sigma(k+r)} A_{\sigma(k)}^{\sigma(k+r-1)} x_k + \mathcal{T}_{\sigma(k)}^{r,0} u_k \leftrightarrow e$ *(encryption function)*
- $r \leftrightarrow b_s$ *(delay)*

2.4 Identification and security

An essential issue for the validation of ciphers is the cryptanalysis, that is the study of attacks against cryptographic schemes in order to reveal their possible weakness. A fundamental assumption in cryptography first stated by A. Kerkhoff in ([Delfs and Knebl(2002)]), is that any unauthorized person (called adversary or eavesdropper) knows all the details of the cipher, including the algorithm and its implementation, except the secret key. As a result, insofar as the parameters of (1) are expected to act as the secret key, the security is directly related to the complexity of retrieving the parameters θ.
It is usual assuming that the eavesdropper has the opportunity of controlling the input of the cipher, namely the plaintext, and analyzing the corresponding ciphertext (the attack is called chosen plaintext attack). In our context, if the dynamical system (1) is considered as a cipher, that means that the pair (u_k, y_k) is assumed to be known by the eavesdropper. The recovery of θ can only be based on the input/output model of (1).
Besides, it worth emphasizing that a cipher must face at least the most basic attack, i.e. the brute force attack. This attack consists in trying exhaustively every possible parameter value in the parameter space of the secret key (which is in practice a finite space). The quicker the brute force attack, the weaker the cipher. Consequently, the worst situation for the eavesdropper and the best for the security arises when, for known plaintexts and corresponding ciphertext sequences, only one solution in the parameters of the cipher exists. As explained in Subsection 1.3, the unicity is directly related to the notion of parametric identifiability. As a result, we conclude that the most relevant parameters of a system to act as the secret key are the ones which are identifiable. Such a result might appear as paradoxical at first glance because of a possible misunderstanding on the meaning of "identifiable". Actually, identifiability means unicity in the parameters. Such a paradox has been highlighted in ([Anstett et al.(2006)]).

Thus, according to the above discussion and Subsection 1.3, we infer the following Proposition:

Proposition 4 *The secret key θ must be the set of entries of $(A_j)_{1\leq j\leq J}$, $(B_j)_{1\leq j\leq J}$, $(C_j)_{1\leq j\leq J}$ and $(D_j)_{1\leq j\leq J}$ of (1) which can be deduced from $c(\sigma_t)$ and the $a_j(\sigma_t)$'s in a unique way.*

Actually, the security is related to the complexity of the underlying identification procedure. The recovery of the secret parameters can be performed through the identification procedures described in Subsection 1.3. Clearly the identification procedure is much more complex when σ_t is not accessible. Thus the secret key θ must be determined so that the eavesdropper has no other choice than resorting to the second identification procedure. As a result, σ_t must not be directly accessible and the following Proposition must be thereby fulfilled:

Proposition 5 *The switching rule σ must depend on θ.*

We can assess the security in terms of the complexity of the required algebraic computations to identify θ. The most important task in the second identification procedure is the computation of the coefficients h_N through (25). In practice, the kernel (null space) is obtained through a Singular Values Decomposition (SVD) of which complexity is $O(min(N'M_N^2, N'^2M_N))$. The lower bound of N' being $M_N - 1$, when M_N is large enough, the complexity can be approximated by $O(M_{N^3})$. The increasing rate of M_N is depicted on Figure 2.

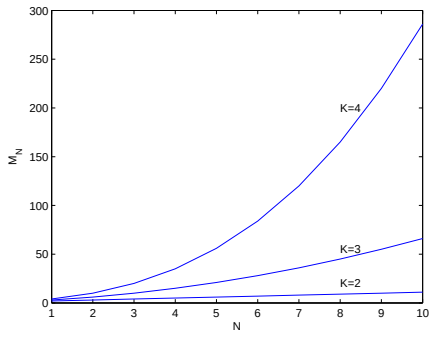

Figure 2: M_N versus N for different values of K.

3 Illustrative example

We consider a switched linear system in the form (1) with

$$A_{\sigma(k)} = \begin{pmatrix} q^1_{\sigma(k)} & 1 \\ q^3 & 0 \end{pmatrix}, \quad B_{\sigma(k)} = \begin{pmatrix} 0 \\ q^2_{\sigma(k)} \end{pmatrix}$$

and with $C_{\sigma(k)} = (1\ 0)$ and $D_{\sigma(k)} = 0$ for any k.
We consider any switching rule σ with $J = 2$ modes where the time-varying entries fulfill $q^1_1 = 1.7$, $q^1_2 = -1.7$, $q^2_1 = -0.01$, $q^2_2 = 0.01$ and $q^3 = 0.5$.

i) The relative degree is $r = 2$ according to (4) since $\mathcal{T}^{i,j}_{\sigma(k)} = 0$ for $i = 0, 1$ and $j = 0, \ldots, i$ while $\mathcal{T}^{2,0}_{\sigma(k)} = C_{\sigma(k+2)} A_{\sigma(k+1)} B_{\sigma(k)} \neq 0$ for all k.
ii) The computation of (14) gives $\mathbf{0}$ with $K = 2$ and reveals that y_k is a flat output.

From *i)* and *ii)*, we can infer that, according to the Proposition 3, the system is structurally equivalent to a self-synchronizing stream cipher.

iii) Let us examine the setting $\theta = (\theta^{(1)}\ \theta^{(2)}\ \theta^{(3)}\ \theta^{(4)}\ \theta^{(5)}) = (q^1_1\ q^1_2\ q^3\ q^2_1\ q^2_2) = (1.7\ \ -\ 1.7\ \ 0.5\ \ -\ 0.01\ \ 0.01)$. The dimension L of θ is $L = 5$. Let us check whether θ would be an admissible choice for the secret key in terms of identifiability.
The computation of (18) allows us to obtain an input/output relation in the form (19)

$$\begin{array}{rcl} y_{k+2} & = & q^3 y_k + q^1_{\sigma(k+1)} y_{k+1} + q^2_{\sigma(k)} u_k \\ & = & a_0(\sigma_t) y_k + a_1(\sigma_t) y_{k+1} + c(\sigma_t) u_k \end{array} \tag{32}$$

In the time interval $[k, k+1]$, to the $N = 4$ possible modes sequences $\sigma_1 = \{1, 1\}$, $\sigma_2 = \{1, 2\}$, $\sigma_3 = \{2, 1\}$, $\sigma_4 = \{2, 2\}$, correspond four respective input/output equations

$$\begin{array}{lrcl} t = 1, & y_{k+2} & = & \theta^{(3)} y_k + \theta^{(1)} y_{k+1} + \theta^{(4)} u_k \\ t = 2, & y_{k+2} & = & \theta^{(3)} y_k + \theta^{(2)} y_{k+1} + \theta^{(4)} u_k \\ t = 3, & y_{k+2} & = & \theta^{(3)} y_k + \theta^{(1)} y_{k+1} + \theta^{(5)} u_k \\ t = 4, & y_{k+2} & = & \theta^{(3)} y_k + \theta^{(2)} y_{k+1} + \theta^{(5)} u_k \end{array}$$

with the following relations

$$\begin{array}{l} \theta^{(1)} = a_1(\sigma_1) \text{ or } \theta^{(1)} = a_1(\sigma_3) \\ \theta^{(2)} = a_1(\sigma_2) \text{ or } \theta^{(2)} = a_1(\sigma_4) \\ \theta^{(3)} = a_0(\sigma_t) \text{ for any } t = 1, \ldots, 4 \\ \theta^{(4)} = c(\sigma_1) \text{ or } \theta^{(4)} = c(\sigma_2) \\ \theta^{(5)} = c(\sigma_3) \text{ or } \theta^{(5)} = c(\sigma_4) \end{array} \tag{33}$$

From (33), we infer that θ can be recovered in a unique way from the knowledge of $(a_0(\sigma_t), a_1(\sigma_t), c(\sigma_t))$ $(t = 1, \ldots, 4)$ and then Proposition 4 is fulfilled. Consequently θ could act as the secret key and must also be involved in the switching rule σ according to the Proposition 5. We can define for example a switching rule σ in the form,

$$\sigma(k) = Int(\sum_{i=1}^{L} \theta^{(i)} y_{k-i}) + 1 \ (\text{mod } J)$$

where Int stands for the integer part and mod stands for the congruential operation.

iv) Let us illustrate the second identification procedure described in Subsection 1.3. It consists in injecting known inputs u_k into (1) and collecting the corresponding outputs y_k. We iterate (1) until the matrix $\mathcal{L}_{N'}$ fulfills the rank condition (24). After computing h_N from (25), we derive $b_1, \ldots, b_4$ by (26)

$$\begin{array}{rcccc} b_1 = & [1 & \text{-}0.5 & -1.7 & 0.01]^T \\ b_2 = & [1 & \text{-}0.5 & 1.7 & 0.01]^T \\ b_3 = & [1 & \text{-}0.5 & -1.7 & -0.01]^T \\ b_4 = & [1 & \text{-}0.5 & 1.7 & -0.01]^T \end{array}$$

and then recover the $c(\sigma_t)$'s and the $a_j(\sigma_t)$'s ($j = 0, \ldots, K-1,\ t = 1, \ldots, N$) and finally the $\theta^{(i)}$'s by (33).

4 Conclusion

In this paper, we have discussed and illustrated the potential interest of the control theory framework for cryptographic applications. It has been shown that invertibility and flatness are two properties which allow a dynamical system to be structurally equivalent to a self-synchronizing stream cipher. Identifiability is related to the notion of unicity in the parameters, a necessary required property of any ciphers when parameters act as the secret key. Involving hybrid systems is motivated by the relevance of introducing heterogeneity in the ciphers. In this paper, switched linear systems have been investigated. Nevertheless, if a fully specified cipher is thought, the security aspect deserves a deeper investigation.
Indeed, identification consists of a so-called algebraic attack in the context of cryptography. It could be expected that the linearity of the modes is a weakness and that nonlinearities should be introduced, while keeping heterogeneity through hybrid models and a similar control theory framework. Besides, others kinds of attacks should be considered, to mention a few, linear and differential cryptanalysis, distinguisher-based attacks, side channels attacks. Those kinds of issues are naturally out of the scope of the present paper.

References

[Anstett et al.(2008)] Anstett, F., Bloch, G., Millérioux, G., and Denis-Vidal, L. (2008), "Identifiability of discrete-time nonlinear systems: the local isomorphism approach," *Automatica*, 44, 2884–2889.

[Anstett et al.(2006)] Anstett, F., Millérioux, G., and Bloch, G. (2006), "Chaotic Cryptosystems: Cryptanalysis and Identifiability," *IEEE Trans. on Circuits and Systems : Regular papers*, 53, 2673–2680.

[Babaali and Egerstedt(2004)] Babaali, M., and Egerstedt, M. (2004), "Observability for Switched Linear Systems," *Lectures Notes on Hybrid Systems: Computation and Control*, Philadelphia, PA: Springer-Verlag.

[Balluchi et al.(2002)] Balluchi, A., Benvenuti, L., Benedetto, M.D.D., and Sangiovanni-Vincentelli, A.L. (2002), Vol. 2289 of *Lecture Notes in Computer Science: Hybrid Systems: Computation and ControlDesign of Observers for Hybrid Systems*, Berlin Heidelberg New York: Springer-Verlag, pp. 76–89.

[Bemporad et al.(2000)] Bemporad, A., Ferrari-trecate, G., and Morari, M. (2000), "Observability and controllability of piecewise affine and hybrid systems," *IEEE Trans. Aut. Control*, 45, 1864–1876.

[Daemen and Kitsos(2005)] Daemen, J., and Kitsos, P. (2005), "The self-synchronizing stream cipher MOUSTIQUE," *eSTREAM, ECRYPT Stream Cipher Project*, Available online at http://www.ecrypt.eu.org/stream.

[Delfs and Knebl(2002)] Delfs, H., and Knebl, H., *Introduction to cryptography*, Berlin: Springer-Verlag (2002).

[Fliess et al.(1995)] Fliess, M., Levine, J., Martin, P., and Rouchon, P. (1995), "Flatness and defect of non-linear systems: introductory theory and examples," *Int. Jour. of Control*, 61, 1327–1361.

[HSCC(2008)] HSCC, (2008), "Hybrid Systems: Computation and Control," in *Proceeding of the 11th International Workshop, HSCC 2008, LNCS 4981, Springer*, April 22-24, St. Louis, MO, USA.

[Juloski et al.(2005)] Juloski, A.L., Heemels, W., Ferrari-Trecate, G., Vidal, R., Paoletti, S., and Niessen, J. (2005), "Comparision of four procedures for the identification of hybrid systems," in *In Proc. 8th International Workshop on Hybrid Systems: Computation and Control*, eds. M. Morari and L. Thiele, Vol. 3414, Springer-Verlag Berlin Heideberg 2005, pp. 354–369.

[Klimov and Shamir(2004)] Klimov, A., and Shamir, A. (2004), Vol. 3017, "1," *New cryptographic primitives based on multiword T-functions*, Springer Berlin / Heidelberg, pp. 1–15.

[Levine and Nguyen(2003)] Levine, J., and Nguyen, D.V. (2003), "Flat output characterization for linear systems using polynomial matrices," *Systems and control Letters*, 48, 69–75.

[Liberzon(2003)] Liberzon, D. (2003)*Switching in systems and control*, Birkhauser.

[Maurer(1991)] Maurer, U.M. (1991), "New approaches to the design of self-synchronizing stream cipher," *Advance in Cryptography, In Proc. Eurocrypt '91, Lecture Notes in Computer Science*, pp. 548–471.

[Menezes et al.(1996)] Menezes, A.J., Oorschot, P.C., and Vanstone, S.A., *Handbook of Applied Cryptography*, CRC Press (1996).

[Millerioux and Daafouz(2009)] Millerioux, G., and Daafouz, J. (2009), "Flatness of Switched Linear Discrete-Time Systems," *IEEE Transactions on Automatic Control*, 54, 615–619.

[Nõmm and Moog(2004)] Nõmm, S., and Moog, C.H. (2004), "Identifiability of discrete-time nonlinear systems," in *Proc. of the 6th IFAC Symposium on Nonlinear Control Systems, NOLCOS*, September 1-3, Stuttgart, Germany, pp. 477–489.

[Sain and Massey(1969)] Sain, M.K., and Massey, J.L. (1969), "Invertibility of Linear Time-Invariant Dynamical Systems," *IEEE Trans. Automatic Control*, 14, 141–149.

[Shorten et al.(2007)] Shorten, R., Wirth, F., Mason, O., Wulff, K., and King., C. (2007), "Stability criteria for switched and hybrid systems," *SIAM Review*, 49, 545592.

[Sira-Ramirez and Agrawal(2004)] Sira-Ramirez, H., and Agrawal, S.K., *Differentially Flat Systems*, New York: Marcel Dekker (2004).

[Vidal et al.(2003)] Vidal, R., Ma, Y., and Sastry, S. (2003), "An algebraic geometric approach to the identification of a class of linear hybrid systems," *42nd IEEE Conference on Decision and Control 2003 (CDC'03)*.

[Vu and Liberzon(2008)] Vu, L., and Liberzon, D. (2008), "Invertibility of switched linear systems," *Automatica*.