Invertibility, flatness and identifiability of switched linear dynamical systems: an application to secure communications

Phuoc Vo Tan, Gilles Millérioux, Jamal Daafouz

To cite this version:
Phuoc Vo Tan, Gilles Millérioux, Jamal Daafouz. Invertibility, flatness and identifiability of switched linear dynamical systems: an application to secure communications. 47th IEEE Conference on Decision and Control, CDC’08, Dec 2008, Cancun, Mexico. pp.CDROM. hal-00331829

HAL Id: hal-00331829
https://hal.science/hal-00331829
Submitted on 17 Oct 2008

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Invertibility, flatness and identifiability of switched linear dynamical systems: an application to secure communications

Phuoc Vo Tan, Gilles Millérioux and Jamal Daafouz

Abstract—This paper deals with invertibility, flatness and identifiability of switched linear dynamical systems. Based on these concepts, a framework which enables to test whether, from a structural point of view, a switched linear dynamical system can act as a cryptosystem for secure communications is proposed.

Hybrid systems have inspired a great deal of research from both control theory and theoretical computer science. 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. Switched systems are an important class of hybrid systems widely studied in the literature and stability, identifiability, controller or observer design are challenging problems related to. They are usually addressed for engineering applications.

The contribution of this paper is to provide results for an application related to secure communications. Let us briefly describe this context. Chaotic behavior is one of the most complex dynamics a nonlinear system can exhibit. Because the signals resulting from chaotic systems are broadband, noiselike, difficult to predict, the idea of using chaotic systems for information masking has received much attention since the pioneering work of [1]. Several ciphering methods for masking the information into a chaotic signal produced by a dynamical system have been proposed in the literature. An overview can be found according to the chronology in [2][3][4][5].

In this paper, we propose a framework, based on the concepts of control theory, which enables to test whether, from a structural point of view, a switched linear dynamical system can act as a cryptosystem. Such a class is interesting because it combines two advantages: capability of exhibiting complex dynamics and ease of implementation.

The paper is organized as follows. Section I aims at deriving algebraic conditions under which a switched linear discrete-time system is respectively invertible and flat. It is shown how these concepts are useful in the perspective of designing ciphers for secure communications, more precisely self-synchronizing stream ciphers. In Section II the security aspect is addressed and a connection between identification and algebraic attacks is brought out. An illustrative example is finally given.

I. INVERTIBILITY, FLATNESS AND IDENTIFIABILITY

Consider the switched linear dynamical system:

\[
\begin{cases}
    x_{k+1} = A_{\sigma(k)}x_k + B_{\sigma(k)}u_k \\
    y_k = C_{\sigma(k)}x_k + D_{\sigma(k)}u_k
\end{cases}
\] (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 \( \sigma: k \in \mathbb{N} \rightarrow j = \sigma(k) \in \{1, \ldots, J\} \). \( \{\sigma\}_{k_1} \) 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 \( \{u_k\}_{k=0}^{T} = \{u_0, \ldots, u_{k+T}\} \in \mathcal{U} \), for a mode sequence \( \{\sigma\}_{k=T} \), \( \{x(x_k,\sigma,u)\}_{k=T} \) refers to the solution of (1) starting from \( x_k \) in the interval of time \([k,k+T]\) and \( \{y(x_k,\sigma,u)\}_{k=T} \in \mathcal{Y} \) refers to the corresponding output sequence in the same interval of time \([k,k+T]\).

Two structural properties of (1) are now addressed: invertibility and flatness.

A. Invertibility

Before addressing the 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 the SISO switched linear system (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)

\[
y_{k+i} = C_{\sigma(k+i)}A_{\sigma(k+i-1)} \cdots A_{\sigma(k)}x_k + \sum_{j=0}^{i-1} \sum_{\sigma(k_j)} \mathcal{J}^{i-j} C_{\sigma(k_j)}D_{\sigma(k_j)}u_k + j
\] (2)
The existence of the inverse of \( \mathcal{F}(\sigma)(k) \) if \( (\sigma)_{\sigma}^{-1} \) holds and the input \( u \in \mathbb{R} \), indeed, 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 \( u \) can be deduced in a unique way. It reads:

\[
y_k = (\mathcal{F}_{\sigma}(k))^{-1}(y_{k+r} - C_{\sigma_{k+r}}A_{\sigma_{k+1}}^{-1}y_k)
\]

The existence of the inverse of \( \mathcal{F}_{\sigma}(k) \) is guaranteed since it is, by definition, always different from zero.

### B. Inversion

We are now concerned with a recursive inversion of (1) achieving the recovering of \( u \) from \( y \) without any knowledge of \( x \). Let us define the inverse transition matrix as

\[
P_{\sigma(k)}^{r_0} = P_{\sigma(k_1)}^{r_0}P_{\sigma(k_{i-1})}^{r_0} \cdots P_{\sigma(k_0)}^{r_0}
\]

with

\[
P_{r_0}^{\sigma(k)} = A_{\sigma(k)} - B_{\sigma(k)}(\mathcal{F}_{\sigma}(k))^{-1}C_{\sigma_{k+r}}A_{\sigma_{k+1}}^{-1}
\]

### Proposition 1

The following dynamical system is a stable inverter whenever the system \( v_{k+1} = P_{r_0}^{\sigma(k)}v_k \) is uniformly asymptotically stable

\[
\begin{align*}
\dot{x}_{k+r+1} &= P_{r_0}^{\sigma(k)}x_{k+r} + B_{\sigma(k)}(\mathcal{F}_{\sigma}(k))^{-1}y_{k+r} \\
\dot{u}_{k+r} &= -(\mathcal{F}_{\sigma}(k))^{-1}C_{\sigma_{k+r}}A_{\sigma_{k+1}}^{-1}x_{k+r} + (\mathcal{F}_{\sigma}(k))^{-1}y_{k+r}
\end{align*}
\]

### Proof

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

\[
\dot{x}_{k+r+1} = P_{r_0}^{\sigma(k)}\hat{x}_{k+r} + B_{\sigma(k)}(\mathcal{F}_{\sigma}(k))^{-1}C_{\sigma_{k+r}}A_{\sigma_{k+1}}^{-1}x_k + B_{\sigma(k)}(\mathcal{F}_{\sigma}(k))^{-1}y_{k+r}uk
\]

Taking into account (8) and noticing that \( (\mathcal{F}_{\sigma}(k))^{-1}C_{\sigma_{k+r}}A_{\sigma_{k+1}}^{-1} = 1 \), \( \hat{x}_k = x_k - \hat{x}_{k+r} \) fulfills the recursion:

\[
\hat{e}_{k+1} = (A_{\sigma(k)} - B_{\sigma(k)}(\mathcal{F}_{\sigma}(k))^{-1}C_{\sigma_{k+r}}A_{\sigma_{k+1}}^{-1})(\hat{x}_k - x_k)
\]

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

\[
u_k - \hat{u}_{k+r} = -(\mathcal{F}_{\sigma}(k))^{-1}C_{\sigma_{k+r}}A_{\sigma_{k+1}}^{-1}(x_k - \hat{x}_{k+r})
\]

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 \( v_{k+1} = P_{r_0}^{\sigma(k)}v_k \) with \( v_k = \hat{x}_k \) is uniformly asymptotically stable.

### C. Flatness

We first recall a general definition of flat output (for details about flatness, the reader can refer to [6] or the book [7]).

### 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 exist two functions \( \mathcal{F}, \mathcal{G} \) and integers \( t_1 < t_2, t'_1 < t'_2 \) such that

\[
y_k = \mathcal{F}(y_{k+t_1}, \cdots, y_{k+t_2}) \\
u_k = \mathcal{G}(y_{k+t'_1}, \cdots, y_{k+t'_2})
\]

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

### Proposition 2

The output \( y_k \) of (1), assumed to be left invertible, is a flat output if there exists a positive integer \( 0 < K < \infty \) such that for all \( k \geq 0 \)

\[
P_{r_0}^{\sigma(k+K-1)} = 0
\]

where \( 0 \) stands for the null matrix.

### Proof

The proof is based on the inverse system. Iterating (9) \( I - 1 \) times yields:

\[
\dot{x}_{k+r+1} = P_{r_0}^{\sigma(k+I)}\hat{x}_{k+r} + \sum_{i=0}^{I-1} P_{r_0}^{\sigma(k+i)}B_{\sigma_{k+i}}(\mathcal{F}_{\sigma}(k+i))^{-1}y_{k+i+r}
\]

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

\[
\dot{x}_{k+r+K} = \sum_{i=0}^{K-1} P_{r_0}^{\sigma(k+K-i)}B_{\sigma_{k+i}}(\mathcal{F}_{\sigma}(k+i))^{-1}y_{k+i+r}
\]

revealing that \( \hat{x}_{k+r+K} \) is independent of \( \hat{x}_{k+r} \). In particular, (16) holds for \( \hat{x}_{k+r+K} = x_{k+r} \) for all \( k_0 \geq 0 \), that is for \( \hat{x}_{k_0} = 0 \) with \( k_0 \geq 0 \). By virtue of (11), we infer that \( \hat{x}_k = 0 \) for all \( k \geq k_0 \) and thus \( \hat{x}_{k+r+K} = x_{k+r} \) 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).

\[
x_k = \sum_{i=0}^{K-1} \rho^{(k-1)}_{\sigma(k+i+1-K)} B_{\sigma(k+i-K)} \mathcal{F} r_{0}^{(k+i-K)} y_{k+i+K}
\]

(17)

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

D. Connection with usual stream ciphers in secure communication

Secure communications requires cryptographic algorithms called ciphers (see the book of Menezes [8] for details). Among a variety of ciphers, symmetric-key ciphers are very efficient for secure transmission requiring high throughput. We focus here on self-synchronous stream ciphers which is an interesting class of symmetric ciphers owing to their inherent ability to self-synchronizing without requiring any synchronization flags or interactive protocols for recovering lost synchronization induced for instance by bit slips. At the transmitter side, the self-synchronous stream cipher admits a flat output, then (1) is a self-synchronizing stream cipher.

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

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

\[
\begin{align*}
x_k &= \sum_{i=0}^{K-1} \rho^{(k-1)}_{\sigma(k+i+1-K)} B_{\sigma(k+i-K)} \mathcal{F} r_{0}^{(k+i-K)} y_{k+i+K} \\
y_{k+r} &= C_{\sigma(k+r-1)} A_{\sigma(k)}^{\sigma(k+r-1)} x_k + \mathcal{F} r_{0}^{(k)} y_k
\end{align*}
\]

(19)

and the result follows from the identification of (19) with (18), the correspondences being:

- \( u_k \leftrightarrow m_k \) (plaintext)
- \( y_k \leftrightarrow c_k \) (ciphertext)
- \( x_k \leftrightarrow K_k \) (keystream)
- \( \mathcal{F} \leftrightarrow \sigma_0^{\sigma_k} \) (keystream generator)
- \( (x_k, u_k) \leftrightarrow C_{\sigma(k+r-1)} A_{\sigma(k)}^{\sigma(k+r-1)} x_k + \mathcal{F} r_{0}^{(k)} y_k \leftrightarrow e \) (encryption function)
- \( r \leftrightarrow b_t \) (number of stages of the pipeline)

II. IDENTIFICATION, ALGEBRAIC ATTACKS AND SECURITY

An essential issue for the validation of cryptosystems is the cryptanalysis, that is the study of attacks against cryptographic schemes in order to reveal their possible weakness. A fundamental assumption in cryptanalysis, first stated by A. Kerckhoff in [10], is that the eavesdropper knows all the details of the cryptosystem, including the algorithm and its implementation, except the secret key, on which the security of the cryptosystem must be entirely based. As a result, the security is directly related to the complexity of the parameters recovering task and so, on the complexity of the underlying identification procedure. The identification is nothing but what is called in the cryptographic context an algebraic attack. The consideration of the possible attacks and their complexity will dictate the way how the secret key of (1) must be defined as detailed below.

A. Connection between identification and algebraic attacks

One of the most powerful attack is the chosen plaintext attack. For such an attack, the eavesdropper is assumed to control the input of the cipher, namely the plaintext, and to analyze the corresponding ciphertext. In our context, since the cipher is the dynamical system (1), it means that the eavesdropper is supposed to control both the input \( u_k \) and the output \( y_k \). As a result, the pair \( (u_k, y_k) \) is supposed to be known by the eavesdropper and the cryptanalytic reasoning must be 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 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

\[
y_{k+r} = C_{\sigma(k+r-1)} A_{\sigma(k)}^{\sigma(k+r-1)} + \sum_{i=0}^{K-1} \rho^{(k-1)}_{\sigma(k+i+1-K)} B_{\sigma(k+i-K)} \mathcal{F} r_{0}^{(k+i-K)} y_{k+i+K}
\]

(20)

Let \( \{ \sigma_1, \sigma_2, \ldots, \sigma_N \} \) be 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

\[
C_{\sigma(k+r-1)} A_{\sigma(k)}^{\sigma(k+r-1)} + \sum_{i=0}^{K-1} \rho^{(k-1)}_{\sigma(k+i+1-K)} B_{\sigma(k+i-K)} \mathcal{F} r_{0}^{(k+i-K)} y_{k+i+K}
\]

(20)
The key idea rests on the fact that the so-called hybrid switching sequences will be respectively denoted by \( \sigma \) (for short \( \sigma(1) \) is. These mode sequences will be respectively denoted \( (A_j)_{1 \leq j \leq J} \), \( (B_j)_{1 \leq j \leq J} \), \( (C_j)_{1 \leq j \leq J} \) and \( (D_j)_{1 \leq j \leq J} \) of (1).

Let us first assume that \( \sigma_t \) is accessible. Since for each \( \sigma_t \), the parameters \( c(\sigma_t) \) and the \( a_j(\sigma_t) \)'s appear in a linear fashion in the input/output relation (21), they are obviously identifiable. Indeed, for a given mode sequence \( \sigma_t \), under the usual Persistently Exciting (PE) conditions, the identification can be always performed by iterating the relation (21) until a set of linear independent equations is obtained. The solution is unique for each \( \sigma_t \) and gives \( c(\sigma_t) \) and the \( a_j(\sigma_t) \)'s.

Conversely, let us assume that \( \sigma_t \) is not accessible. The previous procedure does no longer hold. An alternative identification procedure (and so algebraic attack) for recovering \( c(\sigma_t) \) and the \( a_j(\sigma_t) \)'s attack can follow the method proposed in [11] for switched ARX systems. This method is summed up and adapted to our context. Each input/output relation (21) can be rewritten for \( t = 1, \ldots, N \)

\[
z_k^T b_t = 0 \tag{22}
\]

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

\( z_k \) is the regressor vector while \( b_t \) is the parameter vector corresponding to the mode sequence \( \sigma_t \).

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 Decoding Constraint* equation is fulfilled regardless the switching sequences:

\[
p_N(z_k) = \prod_{t=1}^{N} (z_k^T b_t) = v_N(z_k)^T h_N = 0 \tag{23}
\]

\( h_N \in \mathbb{R}^{M_N} \) is the coefficient of the Hybrid Decoding Polynomial and \( v_N : z_k \in \mathbb{R}^{K+2} \mapsto \xi_k \in \mathbb{R}^{M_N} \) is a Veronese map of degree \( N \), the components of \( \xi_k \) 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

\[
M_N = \binom{N+K-1}{N} = \frac{(N+K-1)!}{N!(K-1)!} \tag{24}
\]

For the identification of the \( b_t \)'s in (22), it is needed to compute the coefficients \( h_N \) of (23). To this end, let \( \mathcal{L}_N \) denote an embedded data matrix involving \( N \) mapped regressor vectors \( z_k \) through \( v_N \)

\[
\mathcal{L}_N = \begin{bmatrix}
v_N(z_{k_1}) \\
v_N(z_{k_2}) \\
\vdots \\
v_N(z_{k_N})
\end{bmatrix}^T \in \mathbb{R}^{N \times M_N}
\]

The following relation applies:

\[
\mathcal{L}_N h_N = 0 \tag{25}
\]

If the mapped regressor vectors \( v_N(z_k) \)'s are *sufficiently exciting*, the existence of an integer \( N' \) such that the \( v_N(z_k) \)'s \( (i = 1, \ldots, N') \) span a \( M_N - 1 \) dimensional vector space, i.e

\[
\text{rank}(\mathcal{L}_N) = (M_N - 1) \tag{26}
\]

is guaranteed. The lower bound of \( N' \) is \( M_N - 1 \). If (26) is fulfilled, the coefficient \( h_N \) can be retrieved by

\[
h_N = \ker(\mathcal{L}_N) \tag{27}
\]

Finally, to recover the parameter vectors \( b_t \) from the knowledge of \( h_N \), let’s consider the derivative \( Dp_N(z_k) \) of \( p_N(z_k) \):

\[
\frac{\partial p_N(z_k)}{\partial z_k} = \frac{\partial}{\partial z_k} \prod_{t=1}^{N} (z_k^T b_t) = \sum_{t=1}^{N} b_t \prod_{t \neq t} (z_k^T b_t) \tag{28}
\]

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 by performing:

\[
b_t = \frac{Dp_N(w_t)}{eDp_N(w_t)} \tag{29}
\]

\( e \) stands for the vector \([1, 0 \ldots 0] \in \mathbb{R}^{K+2} \).

**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 [11].

**B. Complexity and security**

We recall that the parameters \( c(\sigma_t) \) and \( a_j(\sigma_t) \)'s of the input/output model of (1) depend 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 \( (D_j)_{1 \leq j \leq J} \) and on the switching rule \( \sigma \). The objective of this section is to determine the relevant entries of the matrices which can be involved in the secret key denoted hereafter \( \theta \).

To this end, it worth emphasizing that a cryptosystem 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 cryptosystem. Consequently, the worst situation for the eavesdropper and the best for the security arises when, for known plaintexts (because accessible to eavesdropper in the chosen plaintext attack) and corresponding ciphertext sequences, only one solution in the parameters of the cipher exists.

And yet, we recall that a component \( \theta_i \) of a parameter vector \( \theta \) of a discrete-time dynamical system is identifiable
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 (a result which could seem paradoxical at first glance without the previous reasoning).

From the identification procedures described above, it turns out that \( c(\sigma_i) \) and the \( a_j(\sigma_i) \)'s \((j = 0, \ldots, K - 1, \ t = 1, \ldots, N)\) can always be expressed in a unique way as a function of the input, the output and their iterates. Thus we have the following result:

\[ \theta^{(i)} = \varphi(y_k, \ldots, y_{k+M}, u_k, \ldots, u_{k+M'}) \]  

with \( M < \infty \) and \( M' < \infty \) some positive integers.

Proposition 4: The secret key \( \theta \) 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 \( c(\sigma_i) \) and the \( a_j(\sigma_i) \)'s in a unique way.

Besides, it has been seen that if \( \sigma_i \) is accessible, recovering the parameters \( c(\sigma_i) \) and \( a_j(\sigma_i) \)'s of the input/output model is quite simple by solving a set of linear equations. Thus to force the eavesdropper resorting to the second approach and so to complexify the identification, one must imagine a configuration for which \( \sigma_i \) is not directly accessible. One solution is to render the switching rule \( \sigma \) dependent on \( \theta \) as well.

We are now in position of assessing the security in terms of the complexity of the required algebraic computations to identify \( \theta \). The most important task in the algebraic procedure related to the case \( \sigma_i \) not accessible and described above is the computation of the coefficients \( h_{xy} \) through (27). In practice, the kernel (null space) is obtained through a Determination of the secret key

\[ \text{Determination of the secret key} \]

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

\[ A_{\sigma(k)} = \begin{pmatrix} q_{0}^{4}(k) & 1 \\ 0.5 & 0 \end{pmatrix}, \quad B_{\sigma(k)} = \begin{pmatrix} 0 \\ q_{0}^{5}(k) \end{pmatrix} \]

and with \( C_{\sigma(k)} = (1, 0) \) and \( D_{\sigma(k)} = 0 \) for any \( k \).

The number of modes of the switching rule \( \sigma \) is \( J = 4 \). The time-varying entries fulfill \( q_{0}^{1} = q_{0}^{2} = 1.7, \quad q_{0}^{3} = q_{0}^{4} = -1.7, \quad q_{0}^{5} = q_{0}^{6} = -0.01, \quad q_{0}^{7} = q_{0}^{8} = 0.01 \).

C. Illustrative example

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

\[ y_{k+2} = 0.5y_{k} + q_{0}^{1}(\sigma_{k+1})y_{k+1} + q_{0}^{2}(\sigma_{k})u_{k} \]

\[ y_{k+2} = a_{0}(\sigma_{k})y_{k} + a_{1}(\sigma_{k})y_{k+1} + c(\sigma_{k})u_{k} \]  

\[ \text{In the time interval} \ [k, k + 1], \ \text{the} \ N = 4 \ \text{possible modes sequences} \ \sigma_{1} = \{1, 1\}, \ \sigma_{2} = \{1, 2\}, \ \sigma_{3} = \{2, 1\}, \ \sigma_{4} = \{2, 2\}, \ \text{correspond four respective input/output equations} \]

\[ t = 1, \quad y_{k+2} = \theta^{(1)}y_{k} + \theta^{(1)}y_{k+1} + \theta^{(4)}u_{k} \]

\[ t = 2, \quad y_{k+2} = \theta^{(1)}y_{k} + \theta^{(2)}y_{k+1} + \theta^{(4)}u_{k} \]

\[ t = 3, \quad y_{k+2} = \theta^{(1)}y_{k} + \theta^{(1)}y_{k+1} + \theta^{(5)}u_{k} \]

\[ t = 4, \quad y_{k+2} = \theta^{(3)}y_{k} + \theta^{(2)}y_{k+1} + \theta^{(5)}u_{k} \]
with the following relations
\[
\begin{align*}
\theta^{(1)} &= a_1(\sigma_1) \quad \text{or} \quad \theta^{(1)} = a_1(\sigma_3) \\
\theta^{(2)} &= a_1(\sigma_2) \quad \text{or} \quad \theta^{(2)} = a_1(\sigma_4) \\
\theta^{(3)} &= a_0(\sigma_t) \quad \text{for any } t = 1, \ldots, 4 \\
\theta^{(4)} &= c(\sigma_1) \quad \text{or} \quad \theta^{(4)} = c(\sigma_2) \\
\theta^{(5)} &= c(\sigma_3) \quad \text{or} \quad \theta^{(5)} = c(\sigma_4)
\end{align*}
\]
From (32), we infer that \( \theta \) can be recovered in a unique way from the knowledge of \( (a_0(\sigma_t), a_i(\sigma_j), c(\sigma_j)) \) \( (t = 1, \ldots, 4) \) and then Proposition 4 is fulfilled. Consequently \( \theta \) can act as the secret key.

**Attack and related complexity**

Let us perform the algebraic attack described in Subsect. II-B and assess its complexity. To this end, we inject known plaintexts \( u_k \) into (1) and collect the corresponding ciphertexts \( y_k \). We then iterate (1) until a sufficient number of regressor vectors \( z_t \) are obtained for the matrix \( \mathcal{L}_N \) to fulfill the rank condition (26). After computing \( h_N \) from (27), we derive \( b_1, \ldots, b_4 \) by (29)
\[
\begin{align*}
b_1 &= [1 -0.5 -1.7 \quad 0.01]^T \\
b_2 &= [1 -0.5 1.7 \quad 0.01]^T \\
b_3 &= [1 -0.5 -1.7 -0.01]^T \\
b_4 &= [1 -0.5 1.7 -0.01]^T
\end{align*}
\]

and then recover the \( c(\sigma_j) \)'s and the \( a_j(\sigma_t) \)'s \( (j = 0, \ldots, K - 1, \; t = 1, \ldots, N) \) and finally the \( \theta^{(i)} \)'s by (32). According to the discussion of Subsect. II-B, it is worth emphasizing that since \( M_4 = 35 \), the minimal complexity of the attack is \( 35^3 = 42875 \), a complexity which would have required a dimension 35 if we would have resorted to a linear system.

**III. Conclusion**

In this paper, it is presented a framework which enables to test whether a switched linear system may act as a self-synchronizing cryptosystem from a structural point of view. Invertibility and flatness are the two properties which allow the dynamical system to be structurally equivalent to a self-synchronizing stream cipher. Identifiability is the necessary required property such that the parameters may be involved in the secret key. Identification consists of an algebraic attack in the context of secure communication. For switched linear systems, the complexity to identify the parameters increases significantly with the number of modes and let us expect that switched linear systems could be good candidates for ciphering. Further consideration are needed for validation in particular the vulnerability against statistical attacks.

**Acknowledgement** This work is partially funded by a grant from the Agence Nationale pour la Recherche in France (Ref. ANR-05-JCJC-0112-01)

**REFERENCES**


