

Synchronization of switched linear congruential pseudo-random generators

Gilles Millérioux, Lionel Rosier and Jamal Daafouz

Abstract—Pseudo-random generators are essential in many fields, especially in cryptography. Scalar linear congruential generators are ones of the most popular but, to enhance the statistical properties of the sequences, one may resort to vectorial (also called combined) and switched linear congruential generators. This paper deals with the problem of synchronizing two pseudo-random generators of this type. It is a central problem for many encryption schemes, in particular, for the so-called message-embedding which is the one considered here. From a control theory point of view, the synchronization issue is not trivial because we must cope with the specificity of the congruential generators, namely the use of \mathbb{Z} -valued matrices and modulo operations. The problem is tackled through the design of suitable unknown input observers.

I. INTRODUCTION

Pseudo-random generators are useful in many different kinds of applications such as simulation, sampling, numerical analysis or cryptography. In particular, they are essential in stream cipher-based cryptography [9]. Stream ciphers is an encryption mechanism which consists in “mixing” a sequence of informations called *plaintext* with a pseudo-random sequence. The “mixed” sequence, called *ciphertext*, is then secured and can be conveyed through a public channel. Most popular random number generators are special case of the so-called (scalar) *linear congruential generator* $x_{k+1} = ax_k + b \pmod{m}$ where $m \in \mathbb{N}^*$ is the *modulus*, x_k is an integer in the range $\mathbb{M} := [0, m-1]$, $a \in \mathbb{M}$ is the *multiplier* and $b \in \mathbb{M}$ is the *increment*. The sequence $(x_k)_{k \geq 0}$ is not really random but pseudo-random. Indeed, the cardinality of the set \mathbb{M} being finite, the congruential sequence will obviously get trapped into a loop, called a *cycle*, of finite period. We expect this period not to be too short and the degree of “randomness” of the sequence to be high. From this perspective, combination of linear congruential generators resulting in vectorial generators (that is $x_k \in \mathbb{M}^r$, $r > 1$) and switched generators have been proposed in the literature. When resorting to them, the period of the sequences can be rendered very large and their statistical properties (uniformity, independence) can be really improved.

G. Millérioux is with the University Henri Poincaré Nancy 1, Centre de Recherche en Automatique de Nancy (CRAN-UHP CNRS UMR 7039), ESSTIN, 2 rue Jean Lamour, 54519, Vandœuvre-les-Nancy, France. gilles.millieroux@esstin.uhp-nancy.fr

L. Rosier is with the University Henri Poincaré Nancy 1, Institut Elie Cartan de Nancy (IECN-UHP CNRS-INRIA UMR 7502), BP 239, 54506 Vandœuvre-lès-Nancy Cedex, France. rosier@iecn.u-nancy.fr

J. Daafouz is with the Institut National Polytechnique de Lorraine, Centre de Recherche en Automatique de Nancy (CRAN-INPL CNRS UMR 7039), ENSEM, 2 Avenue de la Forêt de Haye, 54516, Vandœuvre-les-Nancy, France. jamal.daafouz@ensem.inpl-nancy.fr

Having in mind this context, we can now motivate the present work. On one hand, it is worth noticing that a great deal of standard stream ciphers have the same structure and only differ on the nature of its pseudo-random generator. On the other hand, since 1993, a lot of methods of encryption involving nonlinear dynamics, in particular chaotic ones, have been proposed in the literature. There exist many encryption schemes (see [21] for a survey) but one of the most popular one is called *message-embedding*. Roughly speaking, it consists in, similar to the standard stream ciphers, “mixing” the plaintext with a chaotic sequence. However, the resulting ciphertext is not directly conveyed through the public channel but it is reinjected (embedded) in the chaotic dynamics. The recovering of the plaintext calls for reproducing, at the receiver side, the same chaotic sequence. The synchronization mechanism of the two chaotic sequences is known as *chaos synchronization*. Such a scheme appears as very appealing in terms of robustness against potential attacks. Nevertheless, chaotic sequences are aperiodic signals as long as an infinite accuracy encoding is used. In practice, chaotic recursions are unavoidably encoded on a finite accuracy machine. It follows that the chaotic map does not really produce random signals as it should be expected. The encryption setup is machine dependent with quite uncontrollable truncation effects. Recently, in [10] and [11], two powerful mechanisms of synchronization, based on unknown input observers, have been proposed for a general class of chaotic systems including switched linear systems. The purpose of this paper is to show how they can be adapted for switched vectorial linear congruential generators. The interest lies in the fact that we can then combine a safe encryption structure, namely the message-embedding, with the use of a pseudo-random generator having good statistical properties and besides, unlike chaotic ones, which exhibits reproducible and controllable behaviors (see [13], [14]). From a control theory point of view, the difficulty lies in the fact that we must cope with the specificity that those maps involve \mathbb{Z} -valued matrices. Besides, for practical reasons, we are interested in achieving a finite time synchronization.

Switched linear congruential generators under study here involve a switching rule denoted σ and defined as:

$$\sigma(j + pJ) = j + 1 \quad \forall j \in \{0, \dots, J-1\}, \forall p \geq 0. \quad (1)$$

The vectorial switched linear congruential generator associ-

ated to this rule reads:

$$x_{k+1} = A_{\sigma(k)}x_k + b_{\sigma(k)} \pmod{m} \quad (2)$$

where $x_k \in \mathbb{Z}^{N \times 1}$ is the state vector, $A_{\sigma(k)} \in \mathbb{Z}^{N \times N}$ and $b_{\sigma(k)} \in \mathbb{Z}^{N \times 1}$ belong respectively to the families of matrices $(A_j)_{1 \leq j \leq J}$ and $(b_j)_{1 \leq j \leq J}$, $m \in \mathbb{N}^*$ is the same modulus considered for each component of the state vector x_k .

If e.g. $J = 2$ and $b_j = 0 \forall j$, the first terms of the sequence (x_k) read $x_1 = A_1x_0$, $x_2 = A_2x_1 = A_2A_1x_0$, $x_3 = A_1x_2 = A_1A_2A_1x_0$, etc.

Notations: Let $\mathbb{M} := [0, m-1]$, where $m \in \mathbb{N}^*$. We identify the set \mathbb{M} with the abelian group $\mathbb{Z}/m\mathbb{Z}$ through the map which, to any x_k in \mathbb{M} , associates its class modulo m . \mathbb{M} is a \mathbb{Z} -module and for any $A_{\sigma(k)} \in \mathbb{Z}^{N \times N}$ and $b_{\sigma(k)} \in \mathbb{M}^N$, $A_{\sigma(k)}x_k + b_{\sigma(k)}$ is a well-defined element in \mathbb{M}^N . Throughout the paper, most of the equations are then formulated in \mathbb{M}^N so that the expression $(\text{mod } m)$ can be omitted. According to the context, time-varying matrices or vectors will be either indexed by the discrete time k and so denoted with the underscript $\sigma(k)$, or indexed by the current mode j and so denoted with the underscript j . The i th component of a time-invariant vector v will be denoted by v^i while, for a time-varying vector $v_{\sigma(k)}$ (resp. v_j), it will be denoted by $v_{\sigma(k)}^i$ (resp. v_j^i). Finally, prime ' stands for transpose. $\mathbf{1}_N$ stands for the identity matrix.

II. ENCRYPTION SETUP

At each discrete time k , a symbol $m_k \in \mathbb{M}$ (the plaintext) of a sequence $(m_k)_{k \geq 0}$ is first encrypted by a (highly nonlinear) encrypting function e which ‘‘mixes’’ m_k and x_k and produces a ciphertext $u_k = e(x_k, m_k)$. In this context, the sequence (x_k) acts as a so-called running key. Then, the ciphertext u_k is embedded in the dynamics exhibited by the map (2). To the function e must correspond a decrypting function d such that $m_k = d(u_k, x_k)$. Two different embeddings are considered.

The encryption of type 1 obeys

$$(\Sigma_{A,b,M,C,\sigma}) \quad \begin{cases} x_{k+1} &= A_{\sigma(k)}(x_k + M_{\sigma(k)}u_k) + b_{\sigma(k)} \\ y_k &= C_{\sigma(k)}(x_k + M_{\sigma(k)}u_k) \end{cases} \quad (3)$$

and corresponds to an embedding of the ciphertext in both the dynamics and the output.

The encryption of type 2 obeys

$$(\Sigma_{A,b,B,C,\sigma}) \quad \begin{cases} x_{k+1} &= A_{\sigma(k)}x_k + b_{\sigma(k)} + B_{\sigma(k)}u_k \\ y_k &= C_{\sigma(k)}x_k \end{cases} \quad (4)$$

and corresponds to an embedding of the ciphertext in the dynamic only.

$A_{\sigma(k)} \in \mathbb{Z}^{N \times N}$, $b_{\sigma(k)} \in \mathbb{M}^N$, $B_{\sigma(k)} \in \mathbb{Z}^{N \times 1}$, $C_{\sigma(k)} \in \mathbb{Z}^{1 \times N}$, $M_{\sigma(k)} \in \mathbb{Z}^{N \times 1}$ are matrices belonging to the respective families $(A_j)_{1 \leq j \leq J}$, $(b_j)_{1 \leq j \leq J}$, $(B_j)_{1 \leq j \leq J}$, $(C_j)_{1 \leq j \leq J}$, and $(M_j)_{1 \leq j \leq J}$. σ is the switching signal as defined in (1). $B_{\sigma(k)}$

and $M_{\sigma(k)}$ are the ‘‘mixing’’ matrices. $y_k \in \mathbb{M}$ is the output conveyed to the receiver through the channel.

From the definition of the encrypting function e and the decrypting function d , it can be inferred that retrieving m_k at the decryption side requires the recovering of u_k , which in turn calls for reproducing a chaotic sequence (\hat{x}_k) synchronized with (x_k) , that is $\hat{x}_k = x_k \forall k$. To this end, for the two types of message-embedded encryption schemes, we propose two respective mechanisms based on some suitable switched unknown input observers. The observers that have been previously proposed respectively in [10] and [11] may be good candidates but they must be adapted for two reasons. First, the design must cope with the specificity of the maps proposed in the present paper which involves congruential operations and \mathbb{Z} -valued matrices. Secondly, for obvious practical reasons, we are interested in achieving a finite time synchronization.

For the encryption of type 1 (see [10]), the decryption involves the following observer-like structure

$$(\hat{\Sigma}_{A,b,M,C,\sigma}) \quad \begin{cases} \hat{x}_{k+1} &= A_{\sigma(k)}\hat{x}_k + L_{\sigma(k)}(y_k - \hat{y}_k) + b_{\sigma(k)} \\ \hat{y}_k &= C_{\sigma(k)}\hat{x}_k \end{cases} \quad (5)$$

where $\hat{x}_k \in \mathbb{M}^N$ and $\hat{y}_k \in \mathbb{M}$ (\hat{x}_0 being an arbitrary point in \mathbb{M}^N). A first important specificity of the problem is that \hat{x}_{k+1} and \hat{y}_k are well defined provided that the observer gain $L_{\sigma(k)}$ is \mathbb{Z} -valued.

For the encryption of type 2 (see [11]), the decryption involves the following observer-like structure

$$(\hat{\Sigma}_{A,b,B,C,\sigma}) \quad \begin{cases} \hat{x}_{k+1} &= (P_{\sigma(k)}A_{\sigma(k)} - L_{\sigma(k)}C_{\sigma(k)})\hat{x}_k + \\ &L_{\sigma(k)}y_k + Q_{\sigma(k)}y_{k+1} + P_{\sigma(k)}b_{\sigma(k)} \\ \hat{y}_k &= C_{\sigma(k)}\hat{x}_k \end{cases} \quad (6)$$

with $P_{\sigma(k)} = \mathbf{1}_N - Q_{\sigma(k)}C_{\sigma(k)}$ and where $\hat{x}_k \in \mathbb{M}^N$, $\hat{y}_k \in \mathbb{M}$. (\hat{x}_0 being an arbitrary point in \mathbb{M}^N). In that case, \hat{x}_{k+1} and \hat{y}_k are well defined provided that $L_{\sigma(k)}$, $Q_{\sigma(k)}$ (and hence $P_{\sigma(k)}$) are \mathbb{Z} -valued.

Setting $e_k = x_k - \hat{x}_k$, when subtracting (5) from (3) we obtain that the error dynamics for the type 1 reads

$$e_{k+1} = (A_{\sigma(k)} - L_{\sigma(k)}C_{\sigma(k)})e_k + (A_{\sigma(k)} - L_{\sigma(k)}C_{\sigma(k)})M_{\sigma(k)}u_k \quad (7)$$

For the type 2, when subtracting (6) from (4), it can be easily shown that, under the necessary restriction $C_{\sigma(k)} = C$, a constant matrix for all k , the error reads

$$e_{k+1} = (P_{\sigma(k)}A_{\sigma(k)} - L_{\sigma(k)}C_{\sigma(k)})e_k + P_{\sigma(k)}B_{\sigma(k)}u_k \quad (8)$$

Because of this restriction, throughout the paper, $C_{\sigma(k)}$ will be systematically replaced by C for the encryption of type 2.

Before turning to the design of the observers, some definitions and preliminary results are first provided.

III. DEFINITIONS AND PRELIMINARY RESULTS

A. Definitions

Definition 1: A pair (A^b, C^b) is said to be in a *companion canonical form* if it takes the form

$$A^b = \begin{pmatrix} -\alpha^{N-1} & 1 & 0 & \cdots & 0 \\ -\alpha^{N-2} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -\alpha^1 & 0 & 0 & \cdots & 1 \\ -\alpha^0 & 0 & 0 & \cdots & 0 \end{pmatrix}, \quad (9)$$

$$C^b = (1 \ 0 \ \cdots \ 0 \ 0). \quad (10)$$

It is well known that the characteristic polynomial of A^b reads $\chi_{A^b}(\lambda) = \lambda^N + \alpha^{N-1}\lambda^{N-1} + \cdots + \alpha^1\lambda + \alpha^0$.

Definition 2: Two pairs (A, C) and (A^b, C^b) in $\mathbb{Z}^{N \times N} \times \mathbb{Z}^{1 \times N}$ are said to be *similar over \mathbb{Z}* if there exists a matrix $T \in \mathbb{Z}^{N \times N}$ with $\det T = \pm 1$ (hence $T^{-1} \in \mathbb{Z}^{N \times N}$ too) such that

$$A = T^{-1}A^bT, \quad C = C^bT.$$

B. Stability in the time-invariant case

Proposition 1: Let $A \in \mathbb{Z}^{N \times N}$ and $C \in \mathbb{Z}^{1 \times N}$, two time-invariant matrices. Assume that (A, C) is similar over \mathbb{Z} to a pair (A^b, C^b) in a companion canonical form (the first column of A^b reads $(-\alpha^{N-1} \ \cdots \ -\alpha^0)'$). Then there exists a unique matrix $L \in \mathbb{Z}^{N \times 1}$ such that the matrix $A - LC$ is Hurwitz (i.e. the spectrum of $A - LC$ lies in the set $\{z \in \mathbb{C}; |z| < 1\}$). $L = T^{-1}L^b$ with $L^b = (-\alpha^{N-1} \ \cdots \ -\alpha^0)'$. Furthermore, $(A - LC)^N = 0$.

Proof. Write $A = T^{-1}A^bT$, $C = C^bT$, with (A^b, C^b) as in (9) and $T \in \mathbb{Z}^{N \times N}$ with $\det T = \pm 1$. For any given matrix $L \in \mathbb{Z}^{N \times 1}$ we define the matrix $L^b = (l^{N-1} \ \cdots \ l^0)'$ by $L^b = TL$. Then, $A - LC = T^{-1}(A^b - L^bC^b)T$ with

$$A^b - L^bC^b = \begin{pmatrix} -\alpha^{N-1} - l^{N-1} & 1 & 0 & \cdots & 0 \\ -\alpha^{N-2} - l^{N-2} & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -\alpha^1 - l^1 & 0 & 0 & \cdots & 1 \\ -\alpha^0 - l^0 & 0 & 0 & \cdots & 0 \end{pmatrix},$$

Its characteristic polynomial reads $\chi_{A^b - L^bC^b}(\lambda) =$

$$\lambda^N + (\alpha^{N-1} + l^{N-1})\lambda^{N-1} + \cdots + (\alpha^1 + l^1)\lambda + (\alpha^0 + l^0).$$

If L is such that $A - LC$ is Hurwitz, then $A^b - L^bC^b = T(A - LC)T^{-1}$ is Hurwitz too, hence we may write $\chi_{A - LC}(\lambda) = \chi_{A^b - L^bC^b}(\lambda) = \lambda^p \chi(\lambda)$, where $p \in \{0, \dots, N\}$ and $\chi \in \mathbb{Z}[\lambda]$ has its roots $\lambda_1, \dots, \lambda_{N-p}$ in the set $\{z \in \mathbb{C}; 0 < |z| < 1\}$. Assume that $p < N$, and denote by d the constant coefficient of χ . Then $d \neq 0$ (since $\chi(0) \neq 0$), and $|d| = \prod_{i=1}^{N-p} |\lambda_i| < 1$, which is impossible, for $d \in \mathbb{Z}$. Therefore $p = N$ and $l^j = -\alpha^j$ for any $j \in \{0, \dots, N-1\}$ (hence L^b and L are unique). On the other hand

$$A^b - L^bC^b = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}. \quad (11)$$

For this choice of L , $\chi_{A - LC}(\lambda) = \lambda^N$ and $(A - LC)^N = 0$, according to Cayley-Hamilton theorem. ■

This proposition amounts to state that, for \mathbb{Z} -valued time invariant matrices, guaranteeing asymptotic stability is equivalent to guarantee finite time stability.

C. Stability in the time-variant case

Consider the switched system:

$$v_{k+1} = (A_{\sigma(k)} - L_{\sigma(k)}C_{\sigma(k)})v_k \quad (12)$$

The following result provides a sufficient condition guaranteeing that the state vector $v_k \in \mathbb{M}^N$ reaches zero in a finite time.

Lemma 1: Let $\mathcal{N}_1, \dots, \mathcal{N}_N$ be N nilpotent matrices in $\mathbb{C}^{N \times N}$. Assume that the Lie algebra spanned by these matrices is resolvable. Then $\mathcal{N}_1\mathcal{N}_2 \cdots \mathcal{N}_N = 0$.

Proof. Let $\text{Lie}(\mathcal{N}_1, \dots, \mathcal{N}_N)$ denote the Lie algebra spanned by the matrices $\mathcal{N}_1, \dots, \mathcal{N}_N$. Since $\text{Lie}(\mathcal{N}_1, \dots, \mathcal{N}_N)$ is resolvable, we infer from Lie theorem (see e.g. [18, Theorem 3.7.3]) that there exists an invertible matrix $T \in \mathbb{C}^{N \times N}$ such that each matrix $\mathcal{N}'_j := T^{-1}\mathcal{N}_jT$ is upper triangular with zeros on the diagonal. Now, a straightforward computation shows that $\mathcal{N}'_1 \cdots \mathcal{N}'_N = 0$. ■

Remark 1: This lemma states a central result when recalling that the product of N nilpotent matrices in $\mathbb{C}^{N \times N}$ may fail to be nilpotent without any additional assumption. (For instance, $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.) However, it is 0 when the matrices commute pairwise.

Remark 2: Relaxing the finite time convergence and checking for asymptotical convergence requires resorting to some specific stability conditions. Some conditions of first importance are based on the notion of polyquadratic stability introduced in [2]. They state necessary and sufficient conditions of the existence of Parameter Dependent Lyapunov Functions called Polyquadratic Lyapunov Functions, in the context of linear parameter varying systems (LPV) which include piecewise linear systems. The conditions are stated in the following Theorem.

Theorem 1: [3] The system (12) is poly-quadratically stable if and only if there exist definite positive matrices P_i and matrices G_i such that, for all (i, j) , the following set of Linear Matrix Inequalities is fulfilled :

$$\begin{bmatrix} P_i & (A_i - L_i C_i)' G_i' \\ G_i (A_i - L_i C_i) & G_i + G_i' - P_j \end{bmatrix} > 0 \quad (13)$$

As a result, $\lim_{k \rightarrow \infty} v_k = 0$.

Theorem 1 holds for any switched system, but it is worth highlighting the specificity of the case when the matrices are \mathbb{Z} -valued. The feasibility of the LMI's is equivalent to the existence of a Parameter Dependent Lyapunov Function decreasing along the trajectories of (12). In particular, the set of LMI's must be fulfilled for $i = j$ which corresponds to the

situation when $\sigma(k+1) = \sigma(k)$. Hence, it is necessary that each independent linear system associated to the dynamical matrix $A_j - L_j C_j$ be stable. That amounts to consider the time-invariant case, and yet, for \mathbb{Z} -valued matrices, from Proposition 1, it can be inferred that there exists a unique gain L_j such that $A_j - L_j C_j$ is stable and $(A_j - L_j C_j)^N = 0$. This condition is not sufficient for a finite time convergence of (12) as previously mentioned. However, Theorem 1 could be a useful alternative if Lemma 1 is not fulfilled. Indeed, Theorem 1 is less restrictive than Lemma 1 by noticing that resoluble implies that there exist a quadratic Lyapunov function which stabilizes the system. And yet, quadratic Lyapunov functions are special case of Polyquadratic Lyapunov functions.

IV. SYNCHRONIZATION AND INFORMATION RECOVERING

A. Encryption of type 1

As mentioned before, for practical reasons, it should also be expected that the synchronization of (3) and (5) might be achieved in a finite time and regardless of the initial condition \hat{x}_0 of (5). To this end, the following theorem provides some sufficient conditions.

Theorem 2: Let us consider (3) and (5). Assume that the following conditions are fulfilled for each $j = 1, \dots, J$:

- 1) the pair (A_j, C_j) is similar over \mathbb{Z} to a pair (A_j^b, C^b) in a companion canonical form through $T_j \in \mathbb{Z}^{N \times N}$ with $\det T_j = \pm 1$;
- 2) the matrix T_j may be written in the form $T_j = S_j T$ with S_j being upper triangular of determinant ± 1 , T being any square matrix in $\mathbb{Z}^{N \times N}$ with $\det T = \pm 1$;
- 3) the matrix $M_j \in \mathbb{Z}^{N \times 1}$ is such that $M_j = T_j^{-1} M^b$ with

$$M^b = (1, 0, \dots, 0)'; \quad (14)$$

- 4) the matrix $L_j \in \mathbb{Z}^{N \times 1}$ is such that $L_j = T_j^{-1} L_j^b$ with

$$L_j^b = (-\alpha_j^{N-1} \dots -\alpha_j^0)'. \quad (15)$$

Then the error (7) fulfills $e_k = 0$ for $k \geq N$ and for any \hat{x}_0 in (5). Furthermore, $\hat{u}_k := y_k - C_{\sigma(k)} \hat{x}_k = u_k$ for $k \geq N$.

Proof. On one hand, if 1) and 4) are fulfilled, a simple computation leads to

$$A_j - L_j C_j = T_j^{-1} (A_j^b - L_j^b C^b) T_j = T_j^{-1} \mathcal{N} T_j \quad (16)$$

with

$$\mathcal{N} = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}.$$

\mathcal{N} is clearly a nilpotent, upper triangular matrix. Moreover, from 1) and 3), $(A_j - L_j C_j) M_j = T_j^{-1} \mathcal{N} M_j^b$ and $\mathcal{N} M_j^b = 0$. As a result, $(A_j - L_j C_j) M_j = 0$ and (7) does no

longer depend on u_k and for any $p \geq 0$ and any $j \in \{1, \dots, J\}$, integrating (7) yields $e_{j+pJ} =$

$$(A_j - L_j C_j) \cdots (A_1 - L_1 C_1) \{(A_j - L_j C_j) \cdots (A_1 - L_1 C_1)\}^p e_0. \quad (17)$$

with, from 1) and 2), $A_j - L_j C_j = T^{-1} (S_j^{-1} \mathcal{N} S_j) T$.

Now, let \mathcal{T} denote the set of upper triangular complex matrices. It is well-known that \mathcal{T} is a resoluble Lie algebra (see [18, p. 201]). As each matrix $S_j^{-1} \mathcal{N} S_j$ is upper triangular, the Lie algebra $\text{Lie}(S_1^{-1} \mathcal{N} S_1, S_2^{-1} \mathcal{N} S_2, \dots, S_J^{-1} \mathcal{N} S_J)$ is a Lie subalgebra of \mathcal{T} , hence it is resoluble.

The same property holds true for $\text{Lie}(A_1 - L_1 C_1, \dots, A_J - L_J C_J) = T^{-1} \text{Lie}(S_1^{-1} \mathcal{N} S_1, S_2^{-1} \mathcal{N} S_2, \dots, S_J^{-1} \mathcal{N} S_J) T$. It follows then from Lemma 1 that $e_k = 0$ for all $k \geq N$.

On the other hand, according to (3),

$$y_k = C_{\sigma(k)} (x_k + M_{\sigma(k)} u_k) = C_{\sigma(k)} e_k + C_{\sigma(k)} \hat{x}_k + C_{\sigma(k)} M_{\sigma(k)} u_k$$

hence

$$\hat{u}_k := y_k - C_{\sigma(k)} \hat{x}_k = C_{\sigma(k)} e_k + u_k = u_k \quad \forall k \geq N. \quad \blacksquare$$

Remark 3: The choice $S_j = \mathbf{1}_N$ in 2) for all j corresponds to the case when the matrices T_j are identical and equal to T . For this choice, the result is obvious.

B. Encryption of type 2

For the encryption of type 2, it is recalled that the restriction $C_{\sigma(k)} = C$ is required. Likewise, for practical reasons, it should also be expected that the synchronization of (4) and (6) might be achieved in a finite time and regardless of the initial condition \hat{x}_0 of (6).

To this end, the following theorem provides some sufficient conditions.

Theorem 3: Let us consider (4) and (6). Assume that the following conditions are fulfilled for each $j = 1, \dots, J$:

- 1) the pair (A_j, C) is similar over \mathbb{Z} to a pair (A_j^b, C^b) in a companion canonical form through $T_j \in \mathbb{Z}^{N \times N}$ with $\det T_j = \pm 1$;
- 2) the matrix T_j may be written in the form $T_j = S_j T$ with S_j being upper triangular of determinant ± 1 , T being any square matrix in $\mathbb{Z}^{N \times N}$ with $\det T = \pm 1$;
- 3) the matrices $Q_j \in \mathbb{Z}^{N \times 1}$ and $B_j \in \mathbb{Z}^{N \times 1}$ are such that $Q_j = T_j^{-1} Q^b$ and $B_j = T_j^{-1} B^b$ with

$$Q^b = B^b = (1 \ 0 \ \dots \ 0)'; \quad (18)$$

- 4) the matrix $L_j \in \mathbb{Z}^{N \times 1}$ is such that $L_j = T_j^{-1} L_j^b$ with

$$L_j^b = (0 \ -\alpha_j^{N-2} \ \dots \ -\alpha_j^0)'. \quad (19)$$

Then the error (8) fulfills $e_k = 0$ for $k \geq N$ and for any \hat{x}_0 in (6). Furthermore, $\hat{u}_k := y_{k+1} - C A_{\sigma(k)} \hat{x}_k - C B_{\sigma(k)} = u_k$ for $k \geq N$.

Proof. On one hand, since $P_j = \mathbf{1}_N - Q_j C$, it follows that $P_j B_j = B_j - Q_j C B_j$ and taking into account 1), $P_j B_j = T_j^{-1} (B^b - Q^b C^b B^b)$. In view of 3), it is easy to see that

$Q^b C^b B^b = B^b$ which induces $P_j B_j = 0$. Besides, defining P^b as $P^b = \mathbf{1}_N - Q^b C^b$, from 4) one has

$$P_j A_j - L_j C = T_j^{-1} (P^b A_j^b - L_j^b C^b) T_j = T_j^{-1} \mathcal{A} T_j \quad (20)$$

with

$$\mathcal{A} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

\mathcal{A} is a nilpotent, upper triangular matrix.

Then, (8) does no longer depend on u_k and for any $p \geq 0$ and any $j \in \{1, \dots, J\}$, integrating (8) yields

$$e_{j+pJ} = (P_j A_j - L_j C) \cdots (P_1 A_1 - L_1 C) \{(P_j A_j - L_j C) \cdots (P_1 A_1 - L_1 C)\}^p e_0. \quad (21)$$

with $P_j A_j - L_j C = T^{-1} (S_j^{-1} \mathcal{A} S_j) T$ when considering 2).

Let \mathcal{T} denote again the set of all the upper triangular complex matrices. As each matrix $S_j^{-1} \mathcal{A} S_j$ is upper triangular, the Lie algebra $\mathcal{T}' := \text{Lie}(S_1^{-1} \mathcal{A} S_1, S_2^{-1} \mathcal{A} S_2, \dots, S_J^{-1} \mathcal{A} S_J)$ is a Lie subalgebra of \mathcal{T} , hence it is resoluble. The same property holds true for $\text{Lie}(P_1 A_1 - L_1 C, \dots, P_J A_J - L_J C) = T^{-1} \text{Lie}(S_1^{-1} \mathcal{A} S_1, S_2^{-1} \mathcal{A} S_2, \dots, S_J^{-1} \mathcal{A} S_J) T$. It follows then from Lemma 1 that $e_k = 0$ for all $k \geq N$. On the other hand, noticing that $C B_{\sigma(k)} = C^b B^b = 1$, premultiplying the dynamics of (4) by C gives:

$$u_k = y_{k+1} - C A_{\sigma(k)} x_k - C b_{\sigma(k)} \quad (22)$$

Hence,

$$\begin{aligned} \hat{u}_k &:= y_{k+1} - C A_{\sigma(k)} \hat{x}_k - C b_{\sigma(k)} \\ &= C A_{\sigma(k)} e_k + y_{k+1} - C A_{\sigma(k)} x_k - C b_{\sigma(k)} \\ &= u_k \quad \forall k \geq N \end{aligned}$$

Remark 4: If $a := C^b B^b \neq 1$, we obtain instead of (22)

$$a u_k = y_{k+1} - C A_{\sigma(k)} x_k - C b_{\sigma(k)}.$$

Clearly, the map $u \in \mathbb{Z}/m\mathbb{Z} \mapsto a u \in \mathbb{Z}/m\mathbb{Z}$ is bijective if and only if $(a, m) = 1$ (i.e. the integers a and m are relatively prime). Therefore, the condition $C^b B^b = 1$ might be relaxed in $(C^b B^b, m) = 1$.

Remark 5: Assume for simplicity that $C^b B^b = 1$. Then the condition $B^b = Q^b$ of 3) is needed for the convergence. Indeed, the convergence can be guaranteed only if the term involving u_k in (8) vanishes, so that the error equation becomes independent from u_k . That requires $P_j B_j = 0$ for each j ($j = 1, \dots, J$), i.e. $P^b B^b = 0$ or equivalently $B^b = Q^b C^b B^b = Q^b$.

Remark 6: The conditions $B^b = (1 \ 0 \ \dots \ 0)'$ and $L_j^b = (0 \ -\alpha_j^{N-2} \ \dots \ -\alpha_j^0)'$ are needed for $P_j A_j - L_j C$ to be similar to a nilpotent upper triangular matrix. Indeed, writing $Q^b =$

$B^b = (1 \ b^{N-2} \ \dots \ b^0)'$ and $L_j^b = (l_j^{N-1} \ \dots \ l_j^0)'$ yields

$$P^b A_j^b - L_j^b C^b = \begin{pmatrix} -l_j^{N-1} & 0 & 0 & \cdots & 0 \\ b^{N-2} \alpha_j^{N-1} - \alpha_j^{N-2} - l_j^{N-2} & -b^{N-2} & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b^1 \alpha_j^{N-1} - \alpha_j^1 - l_j^1 & -b^1 & 0 & \cdots & 1 \\ b^0 \alpha_j^{N-1} - \alpha_j^0 - l_j^0 & -b^0 & 0 & \cdots & 0 \end{pmatrix}. \quad (23)$$

And yet, rendering $P^b A_j^b - L_j^b C^b$ nilpotent is equivalent to ensure that $\chi_{P^b A_j^b - L_j^b C^b}(\lambda) = \lambda^N$. From (23), the characteristic polynomial being $\chi_{P^b A_j^b - L_j^b C^b}(\lambda) = (\lambda + l_j^{N-1})(\lambda^{N-1} + b^{N-2} \lambda^{N-2} + \dots + b^1 \lambda + b^0)$, that imposes $l_j^{N-1} = 0$ and $b^i = 0$ for $i = 0, \dots, N-2$ which gives B^b . The roots of $\lambda^{N-1} + b^{N-2} \lambda^{N-2} + \dots + b^1 \lambda + b^0$ correspond to the $N-1$ invariant zeros of the system. $P^b A_j^b - L_j^b C^b$ turns into an upper triangular matrix if, besides, $l_j^i = -\alpha_j^i$ for $i = 0, \dots, N-2$ which gives L_j^b .

Remark 7: The fact that $S_j^{-1} \mathcal{A} S_j$ is an upper triangular matrix for each j is a sufficient condition for the Lie subalgebra \mathcal{T}' to be resoluble, which, combined to the nilpotence property, guarantees a global finite time convergence.

V. NUMERICAL SIMULATIONS

Hereby, a numerical simulation is conducted to illustrate the message-embedded encryption of type 2 and its corresponding decryption mechanism. The design of such an encryption scheme may obey the following procedure. First, we choose a switching rule for the system $\Sigma_{A,B,C,\sigma}$. For this example, we define the switching as a periodic function $\sigma: \mathbb{N} \rightarrow \{1, 2\}$ ($J = 2$) for which $\sigma(k) = 1$ if k is even and $\sigma(k) = 2$ if k is odd. We set arbitrarily $b_{\sigma(k)}$ to 0 for all k . Secondly, we must choose matrices which fulfill the points 1) to 4) of Theorem 3. To this end, we choose two pairs (A_j^b, C^b) in companion canonical form:

$$A_1^b = \begin{pmatrix} -1 & 1 & 0 & 0 \\ 7 & 0 & 1 & 0 \\ -3 & 0 & 0 & 1 \\ -4 & 0 & 0 & 0 \end{pmatrix}, \quad A_2^b = \begin{pmatrix} 1 & 1 & 0 & 0 \\ -2 & 0 & 1 & 0 \\ 3 & 0 & 0 & 1 \\ 5 & 0 & 0 & 0 \end{pmatrix}$$

and

$$C^b = (1 \ 0 \ 0 \ 0)$$

Then, we choose two upper triangular matrices S_1, S_2 and a matrix T whose determinants are ± 1 .

$$S_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 3 & 1 \\ 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad S_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & -4 & 1 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

and

$$T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 11 & 1 & 1 \\ 0 & 1 & 5 & -2 \\ 0 & 1 & -2 & 1 \end{pmatrix}$$

They define two similarity transformations T_1 and T_2 fulfilling $T_1 = S_1 T$ and $T_2 = S_2 T$. Then, the matrices A_j 's ($j = 1, 2$) can be computed.

$$A_1 = T_1^{-1} A_1^b T_1 = \begin{pmatrix} -1 & -7 & 12 & -6 \\ 17 & 1 & -9 & 4 \\ -70 & -2 & 25 & -11 \\ -161 & -5 & 59 & -26 \end{pmatrix}$$

and

$$A_2 = T_2^{-1} A_2^b T_2 = \begin{pmatrix} 1 & -14 & -23 & 8 \\ 21 & -10 & 13 & -7 \\ -60 & 31 & -41 & 22 \\ -136 & 72 & -95 & 51 \end{pmatrix}$$

and the matrix $C = C^b T_1 = C^b T_2 = (1 \ 0 \ 0 \ 0)$. It is recalled that for the encryption of type 2, the output matrix must be the same whatever j is. As a result, the pairs (A_j, C) are similar over \mathbb{Z} to the pairs (A_j^b, C^b) in companion canonical form. Finally, the matrices B_j , Q_j (hence P_j), and L_j are computed according to the points 3) and 4) of Theorem 3. They read $B_1 = B_2 = Q_1 = Q_2 = (1 \ 0 \ 0 \ 0)'$, $L_1 = (0 \ 17 \ -70 \ -161)'$, $L_2 = (0 \ 21 \ -60 \ -136)'$. The design is now complete and a numerical simulation for the encryption/decryption setup can be conducted. The information to be masked is a sequence of integers ranging from 0 to 255 and corresponding for instance to ASCII characters, pixels in a video, samples of an acoustic signal, ... The data are embedded into the dynamics of $\Sigma_{A,b,B,C,\sigma}$ according to (3) through an encryption function e which consists in a permutation of the digits of m_k (the rule is not detailed here) depending on the current value of x_k . Results are reported on Fig 1. The original information m_k is depicted on Fig 1A, while the recovered information \hat{m}_k is depicted on Fig 1B. After a finite transient time corresponding to $N = 4$, namely the dimension of the system, the information is successfully retrieved, which is consistent with the theoretical results.

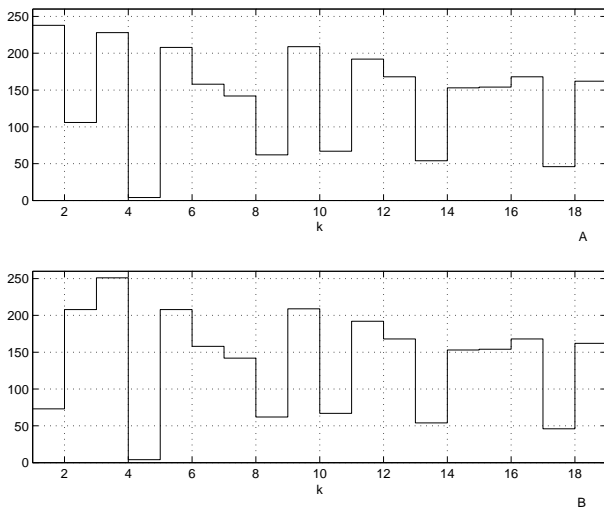


Fig. 1. A : information m_k vs k . B : recovered information \hat{m}_k vs k .

VI. CONCLUDING REMARKS

This paper has been concerned with the synchronization issue of congruential generators in a cryptographic context. The interest of the results lies in that they allow to combine a safe encryption structure, namely the message-embedding, with the use of a pseudo-random generator having good statistical properties and without machine dependent behaviors. From a control theory point of view, the interest lies in that, by now, few results have been stated for dynamical systems involving \mathbb{Z} -valued matrices. Let us notice that the results still hold for a modulus $m = 2$, i.e. for binary sequences. Assessing the security of such an encryption scheme will certainly deserve special attention but it is out of the scope of the present note.

REFERENCES

- [1] J. Banks, G. Cairns, G. Davis, P. Stacey, *On Devaney's definition of chaos*, Am. Math. Monthly 99 4 (1992) 332-334.
- [2] J. Daafouz and J. Bernussou. Parameter dependent lyapunov functions for discrete time systems with time varying parametric uncertainties. *Systems and Control Letters*, 43:355–359, 2001.
- [3] J. Daafouz, G. Millerioux, and C. Iung. A poly-quadratic stability based approach for switched systems. *International Journal of Control*, 75:1302–1310, November 2002.
- [4] R. L. Devaney, *An introduction to chaotic dynamical systems*, 2nd ed., Addison Wesley Publishing Company, Reading, MA, 1989.
- [5] W. H. Greub, *Linear Algebra*, third edition, Springer, Berlin 1967.
- [6] A. Katok and B. Hasselblatt, *Introduction to the modern theory of dynamical systems*, Cambridge University Press.
- [7] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, John Wiley & Sons, 1974.
- [8] R. Mané, *Ergodic Theory and Differentiable Dynamics*, Springer.
- [9] A. J. Menezes, P. C. Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, October 1996.
- [10] G. Millerioux and J. Daafouz. An observer-based approach for input independent global chaos synchronization of discrete-time switched systems. *IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl*, pages 1270–1279, October 2003.
- [11] G. Millerioux and J. Daafouz. Input independent chaos synchronization of switched systems. *IEEE Trans. on Automatic Control*, 49(7):1182 – 1187, July 2004.
- [12] G. Rauzy, *Propriétés statistiques de suites arithmétiques*, Presses Universitaires de France, Paris, 1976.
- [13] L. Rosier, G. Millérioux, G. Bloch, *Chaos synchronization on the N-torus and cryptography*, C.R.A.S. Méc., N.332, pp 969-972, 2005
- [14] L. Rosier, G. Millérioux, and G. Bloch. Synchronization of chaos for a class of dynamical systems on the N -torus (in preparation).
- [15] R. Schmitz, *Use of chaotic dynamical systems in cryptography*, Journal of the Franklin Institute **338** (2001) 429-441.
- [16] E. D. Sontag, *Mathematical Control Theory - Deterministic Finite Dimensional Systems*, 2nd ed., Texts Appl. Math. **6**, Springer, New York, 1998.
- [17] M. A. van Wyk and W.-H. Steeb, *Chaos in Electronics*, series Mathematical Modelling: Theory and Applications, Vol. 2, Kluwer Academic Publishers, Dordrecht, The Netherlands, 1997.
- [18] V. S. Varadarajan. *Lie groups, Lie algebras, and their representations*, volume 102 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1984. Reprint of the 1974 edition.
- [19] E. Vesentini, *An introduction to topological dynamics in dimension 1*, Rend. Sem. Mat. Univ. Pol. Torino, **55**, No. 4 (1997).
- [20] P. Walters, *An Introduction to Ergodic Theory*, Springer Verlag, New York, 1975.
- [21] T. Yang. A survey of chaotic secure communication systems. *Int. J. of Computational Cognition*, 2004. (available at <http://www.YangSky.com/yangijcc.htm>).