Left invertibility of output-quantized systems: an application to cryptography

Nevio Dubbini, Anna Carluccio and Antonio Bicchi

Abstract— **In this paper a secure communication method is proposed, based on left invertibility of output-quantized dynamical systems. The sender uses an output-quantized linear system with a feedback function to encode messages, which are sequences of inputs of the system. So left invertibility property enables the receiver to recover the messages. The secret key is formed by the system's parameters, including the feedback function. The use of quantization makes the cryptographic system work exactly, and without asymptotic estimates. Simulations of encoding-decoding procedure and results about security of the method are finally shown.**

I. Introduction

Quantized control systems are an important class of hybrid systems. Hybrid systems have a great flexibility in modeling dynamic phenomena, since they combine a continuous state-space description associated with physical representation with a discrete-event description associated with software logic. In quantized systems the hybrid nature is given by the existence of both continuous variables (state-space variables), and discrete valued variables (input and output variables). Quantized control systems have been attracting increasing attention in recent years ([4], [6], [10], [24], [28]). The mathematical operation of quantization and the possibility of considering only finite inputs have practical and technological motivations in control with discrete sensors and/or actuators and control under communication constraints (in large-scale systems): see for example [5], [9], [18], [29], [30] and reference therein.

Left invertibility of control dynamical systems has to do with injectivity of the I/O map: roughly speaking a system is left invertible if the input sequence can be reconstructed on the basis of the output sequence. Invertibility of linear systems is a well understood problem, pioneered by [7], and then considered with algebraic approaches in [27], and frequency domain techniques ([19], [20]). More recent work has addressed the invertibility of nonlinear systems ([25], [26]). In [31], the left invertibility problem for a switched system is discussed. Left invertibility setting in relation with output-quantized systems, and results about contractive systems are given in ([12]).

In this paper a cryptographic system is proposed, based on left invertibility of output-quantized control systems. Messages are represented by sequences of inputs. An output-quantized linear system with a feedback function is used to generate the encoded messages, and left invertibility enables the receiver to recover the messages. The secret key is formed by the system's parameters, including the feedback function. Quantization makes the cryptosystem work in finite time.

The proposed cryptosystem model is based on chaotic behavior. Since chaotic signals are unpredictable in practice, noiselike and broadband, they have been proposed as a system to masking information. The main technique on which chaotic cryptosystems are based is synchronization, i.e. two chaotic systems reach equal states at each time step. Since the pioneering work [23], many methods to achieve secure communication relying on chaos synchronization have been proposed. Chaos synchronization is obtained by impulsive differential equations in [32], by unknown input observers in [17], [21], by left invertibility and flatness of switched system in [29]. In [32], [16] the reader may find a rather general treatment about chaos synchronization techniques.

The contribution of this paper is a framework to achieve a chaos communication method, using a system that generates chaos, based on left invertibility of *quantized* systems. Quantification gives a more likely setting for chaotic cryptosystems, since it avoids infinite precision (real numbers), which is normally needed in general treatments on chaotic synchronization, for theoretical results.

The paper is organized as follows: Section II contains definitions and results about left invertibility of output-quantized systems. In section III a cryptosystem is presented, which uses an output-quantized linear system for the enconding of a message, and a left invertibility procedure for the decoding. Section IV contains results about the security of the proposed cryptosystem, while section V shows an example of a practical implementation of the encoding/deconding procedure. Section V shows conclusions and future perspectives. The final appendix contains a more technical proof of a Theorem.

Notations: Throughout this paper we indicate with:

- π_p the canonical projection on the first p coordinate axes,
- ϖ_i the canonical projection on the $i-th$ coordinate axis,
- e_i the $i-th$ vector of the canonical basis,
- $\langle v_1, \dots, v_i \rangle$ the space generated by vectors $v_1, \dots, v_i$,
- $\setminus$ the set difference,
- $\lfloor \cdot \rfloor$ the floor function, acting componentwise.

N. Dubbini is with University of Pisa, Mathematics department "L. Tonelli", Pisa, Italy, dubbini@mail.dm.unipi.it.

A. Carluccio is with University of Pisa, Interdepartmental Research Center "E. Piaggio", Pisa, Italy.

A. Bicchi is with University of Pisa, Interdepartmental Research Center "E. Piaggio", Pisa, Italy.

II. Background: left invertibility and left D-invertibility

Definition 1: The uniform partition of rate δ of $\mathbb{R}^p$ is $\mathcal{P} = \{\mathcal{P}_i\} = \{[i_1\delta, (i_1+1)\delta[\times \ldots \times [i_p\delta, (i_p+1)\delta[\}$, where $i = i_1, \ldots, i_p \in \mathbb{Z}^p$. $\diamondsuit$

Definition 2: The map $q_{\mathcal{P}} : \mathbb{R}^p \to \mathbb{Z}^p$ such that $q_{\mathcal{P}}(x) = i \Leftrightarrow x \in \mathcal{P}_i$ will be referred as to the quantizer induced by the uniform partition $\mathcal{P}$. $\diamondsuit$

With regards to left invertibility results in this paper we consider discrete-time systems of the form

$$\left\{ \begin{array}{l} x(k+1) = Ax(k) + Bu(k) \\ y(k) = q_{\mathcal{P}}\big(Cx(k)\big) \end{array} \right. \tag{1}$$

where $x(k) \in \mathbb{R}^d$ is the state, $y(k) \in \mathbb{Z}^p$ is the output, and $u(k) \in \mathcal{U} \subset \mathbb{R}^m$ is the input. We assume that $\mathcal{U}$ is a finite set of cardinality n. A, B, C are matrices of appropriate dimensions. Without loss of generality, with a change of bases, in the system (1) we can suppose $\delta = 1$, $C = \pi_p$. Therefore only output–quantized linear systems of the following form are considered:

$$\left\{ \begin{array}{l} x(k+1) = Ax(k) + Bu(k) \\ y(k) = \lfloor \pi_p x(k) \rfloor. \end{array} \right. \tag{2}$$

Notations: $H_{k_1}^{k_2}\big(x(0), u(1), \ldots, u(k_2)\big)$ will denote the sequence of outputs $\big(y(k_1), \ldots, y(k_2)\big)$ generated by the system (2) with initial condition $x(0)$ and inputs $\big(u(1), \ldots, u(k_2)\big)$. $\diamondsuit$

Definition 3: A pair of input strings $\{u(i)\}_{i\in\mathbb{N}}, \{u'(i)\}_{i\in\mathbb{N}}$ is uniformly distinguishable in k steps, if there exists l such that $\forall x(0), x'(0) \in \mathbb{R}^d$ and $\forall m > l$ the following holds:

$$\begin{gathered} u(m) \neq u'(m) \\ \Downarrow \\ H_m^{m+k}\Big(x(0), u(1), \ldots, u(m+k)\Big) \neq \\ \neq H_m^{m+k}\Big(x'(0), u'(1), \ldots, u'(m+k)\Big). \end{gathered} \tag{3}$$

Outputs $y(i)$ are referred to the system with initial condition $x(0)$ and inputs $u(i)$, while outputs $y'(i)$ are referred to the system with initial condition $x'(0)$ and inputs $u'(i)$. k is called the distinguishability time. $\diamondsuit$

Definition 4: A system of type (2) is uniformly left invertible (ULI) in k steps if every pair of distinct input sequences is uniformly distinguishable in k steps after a finite time l, where k and l are constant. $\diamondsuit$

For a ULI system, it is possible to recover the input string until instant m observing the output string until instant $m+k$. A simple trick shows left invertibility properties in a different perspective: roughly speaking a system is left invertible if the state exits a particular "diagonal" set.

Definition 5: The quantization-diagonal set relative to the system (2) is

$$Q = \bigcup \underbrace{\Big\{[i_1, i_1+1[\times \ldots [i_p, i_p+1[\times \langle e_{p+1}, \ldots, e_d\rangle\Big\}}_{\subset \langle e_1, \ldots, e_d\rangle} \times \underbrace{\Big\{[i_1, i_1+1[\times \ldots [i_p, i_p+1[\times \langle e_{d+p+1}, \ldots, e_{2d}\rangle\Big\}}_{\subset \langle e_{d+1}, \ldots, e_{2d}\rangle} \subset \mathbb{R}^{2d},$$

where the union is taken over $i_1, \ldots, i_p \in \mathbb{Z}$. $\diamondsuit$

In other words, Q contains all pairs of states that are in the same element of the partition $\mathcal{P}$, and to address left invertibility, from the point of view of the quantization-diagonal set, we are interested in studying the following system on $\mathbb{R}^{2d}$.

Definition 6: The doubled system relative to the system (2) is

$$X(k+1) = \left[\begin{array}{c} Ax(k) + Bu(k) \\ Ax'(k) + Bu'(k) \end{array} \right] \tag{4}$$

where $X(k) = \left(\begin{array}{c} x(k) \\ x'(k) \end{array} \right) \in \mathbb{R}^{2d}$; $U(k) = \left(\begin{array}{c} u(k) \\ u'(k) \end{array} \right) \in \mathcal{U} \times \mathcal{U}$. $\diamondsuit$

If it is possible to find an initial state in Q and an appropriate choice of the strings $\{u(k)\}, \{u'(k)\}$ such that the orbit of (4) remains in Q, it means that the two strings of inputs give rise to the same output for the system (2). Conditions ensuring that the state is outside Q for some k will be sought to guarantee left invertibility.

Definition 7: The difference system associated with the system (2) is

$$z(k+1) = Az(k) + Bv(k) \tag{5}$$

where $z(k) \in \mathbb{R}^d$, $v(k) \in \mathcal{Z} = \mathcal{U} - \mathcal{U} = \{u - u' : u \in \mathcal{U},\ u' \in \mathcal{U}\}$. $\diamondsuit$

Remark 1: The difference system represents at any instant the difference between the two states $z(k) = x(k) - x'(k)$ when the input symbols $u(k) - u'(k) = v(k)$ are performed. Let $\mathcal{S} = (]-1,1[)^p \times \langle e_{p+1}, \ldots, e_d\rangle$. We are interested in understanding the conditions under which

$$\{z(k)\} \ \cap \ \mathcal{S} = \emptyset.$$

Indeed, this implies that $y(k) \neq y'(k)$. The converse is obviously not true. $\diamondsuit$

Notations: $D_{k_1}^{k_2}\big(z(0), v(1), \ldots, v(k_2)\big)$ will denote the sequence $(\pi_p z(k_1), \ldots, \pi_p z(k_2))$ generated by the system (5) with initial condition $z(0)$ and inputs $(v(1), \ldots, v(k_2))$. $\diamondsuit$

Definition 8: A pair of input strings $\{u(i)\}_{i\in\mathbb{N}}, \{u'(i)\}_{i\in\mathbb{N}}$ is uniformly D-distinguishable in k steps if there exists $l \in \mathbb{N}$ such that $\forall x(0), x'(0) \in \mathbb{R}^d$ and $\forall m > l$ the following holds:

$$\begin{gathered} v(m) \neq 0 \ \Rightarrow \\ D_m^{m+k}\big(z(0), v(1), \ldots, v(m+k)\big) \notin \underbrace{]-1,1[^p \times \ldots \times]-1,1[^p}_{k+1 \ times} \end{gathered}$$

where $z(0) = x(0) - x'(0)$ and $v(i) = u(i) - u'(i)$. k is called the distinguishability time. $\diamondsuit$

Definition 9: A system of type (2) is uniformly left D-invertible (ULDI) in k steps if every pair of distinct input sequences is uniformly D-distinguishable in k steps after a finite time l, where k and l are constant. $\diamondsuit$

Left D-left invertibility implies left invertibility, but the viceversa is not true in general (see [13]). The (first) key point dealing with the introduction of left D-invertibility is the fact that there exists an algorithmic procedure to check it. Precisely it holds:

Theorem 1: [13] Consider the system (2) and suppose that

- if λ is an eigenvalue of the matrix A, then $|\lambda| \neq 1$;
- A does not have an eigenvector in $\langle e_{p+1}, \dots, e_d \rangle$.

Then, there exists an algorithmic procedure to check left D-invertibility and find out the invertibility time. $\diamondsuit$

III. Chaos Communication Method Using Uniform Left Invertibility

In this section a cryptosystem is presented, with symmetric key, based on of left invertibility of output-quantized linear systems. The encoding of this communication method uses such a system (see figure 1), where inputs are divided in known and unknown. The known inputs are obtained by a feedback function of the system's parameters and the unknown inputs are arbitrary sequences of symbols in a finite alphabet. Therefore the plaintext, i.e. the information to be transmitted, is the unknown input sequence, and the ciphertext, which has to be transmitted on a unsafe channel, is the output sequence. The decoding is performed by a left inversion algorithm. The secret key is made of the system's parameters, his invertibility time and the feedback function. Our encoding strategy is performed by the following system:

$$\begin{cases} x(k+1) = Ax(k) + Bu(k) + Nv(k) \\ y(k) = q_{\mathcal{P}}[Cx(k)] \end{cases} \tag{6}$$

where $u(k) \in \mathcal{U}$ ($\sharp\mathcal{U} < \infty$, where $\sharp$ denotes the cardinality) is the unknown input, $v(k) \in \mathcal{V}$ is the known input, $y(k) \in \mathbb{Z}^p$ is the output, A, B, N, C are matrices with appropriate dimensions. The known input signal $v(k)$ is generated by a function f, whose arguments are the system's parameters (they can be A, B, C, N, k, y, but not necessarily all).

The decoding scheme (see figure 1) is obtained by an inversion algorithm based on ULDI. The information signal is reconstructed by left D-invertibility, assuming that the system (6) satisfies the hypotheses of Theorems 1.

Remark 2: It's important to recall that ULDI of output-quantized linear systems is algorithmically checkable. But another fundamental fact is that ULDI is not affected by the introduction of known inputs: indeed the reader can easily check that systems (2) and (6) give rise to the same difference system. $\diamondsuit$

Before getting into details of the inversion algorithm, it might be useful to highlight the relation between ULDI and ULI of systems of type (6): they are indeed equivalent for a full measure set.

Theorem 2: Consider the system (6), and suppose $B, C, N, \mathcal{U}, \mathcal{P}$ fixed. Define $\mathbb{S}_D$ to be the set of matrices $A \in \mathbb{R}^{d \times d}$ such that the system (6) is uniformly left D-invertible. Define $\mathbb{S}$ to be the set of matrices $A \in \mathbb{R}^{d \times d}$ such that the system (6) is uniformly left invertible. Then $\mathbb{S} \setminus \mathbb{S}_D$ has Lebesgue measure zero in $\mathbb{R}^{d \times d}$. Here $\setminus$ denotes the set difference.

Proof: See appendix. $\diamondsuit$

We now describe the left inversion algorithm. It assumes the *a priori* knowledge of the invertibility time of the system (6), which is denoted with inv_time. It is worth noting that Theorem 1 provide an algorithmic procedure to check left D-invertibility and find out the invertibility time of the system (6).

Definition 10: A convex polytope in $\mathbb{R}^d$ is a set that can be described as

$$\left\{ x \in \mathbb{R}^d : \; Mx \leq K \right\},$$

where $M \in \mathbb{R}^{m \times d}$, $K \in \mathbb{R}^{1 \times m}$, and $\leq$ is intended to act componentwise. $\diamondsuit$

Note that a polytope can be empty or unbounded. For a general reference on convex polytopes see [14].

Given the sequence of outputs $\{y(k)\}_{k \in \mathbb{N}}$, the algorithm recovers the input symbol $u(k)$ reading the outputs $\big((y(k), \dots, y(k + inv\_time)\big)$. The following are the main steps of the algorithm.

1) For every $i = k, \dots, k + inv\_time$, compute the polytope $P(i)$ that contains the states that give rise to the output $y(i)$:

$$P(i) = \big[y_1(i), y_1(i)+1\big[\; \times \ldots \times \; \big[y_p(i), y_p(i)+1\big[\; \times$$
$$\times \langle e_{p+1}, \dots, e_d \rangle;$$

where p is the dimension of the output.

2) For $i = k, \dots, k + inv\_time$, compute the polytopes $\mathcal{R}(i)$ representing the possible reached states compatible with the observed outputs. This is done iteratively, at each step computing the image of $\mathcal{R}(i)$ under the dynamics of the system (6) given by every $u \in \mathcal{U}$, and successively intersecting with the polytope $P(i+1)$, that represents the observed output:

$$\mathcal{R}(k) = P(k)$$

$$\mathcal{R}(i{+}1) = \Big[\cup_{u \in \mathcal{U}} A(\mathcal{R}(i)) {+} Bu {+} Nv(i)\Big] \bigcap P(i{+}1).$$

3) Since the system is left invertbile in time inv_time, all input strings that generates the polytopes $\mathcal{R}(inv\_time)$ begins with the same input symbols, i.e. the input $u(k)$ is recovered.

IV. Security considerations

In this section we give some results about the security of the proposed communication method. A fundamental issue for the validation of a cryptographic system is the cryptanalysis, that is the study of cryptographic schemes in order to reveal their possible weakness. An essential

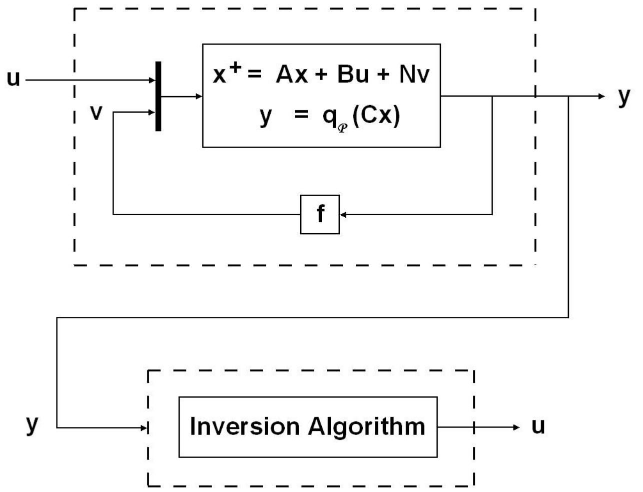


Fig. 1. Communication method based on left invertibility of output-quantized systems proposed in this paper.

hypothesis in cryptanalysis ([11]) is that every detail about the cryptographic system must be known, except the secret key, on which the security of the cryptosystem should be entirely based. Far from being a complete analysis this section provides indications about the choice of the secret key, and shows that, once assigned a plaintext and a ciphertext of arbitrary length, there are *infinite* choices of the secret key parameters that realizes the coupling, of which only *one* represents the secret key.

Consider for example the brute force attack and the known-plaintext attack. Brute force attack consists essentially in trying exhaustively every possible parameter value in the parameter space of the secret key. In the known-plaintext attack instead the eavesdropper is supposed to know both the plaintext and the ciphertext: in our setting a finite number of pair of (finite) sequences $\{u(k), y(k)\}$ is supposed to be known. The following Theorem 3 shows that both in brute force and in known-plaintext attack the eavesdropper cannot identify the system's parameters, since in any case it remains an ambiguity given by an infinite number of possibilities.

Theorem 3: Consider the system (6), and fix any pair of sequences $\{v(k), y(k)\}_{k=1}^{T}$, for $T \in \mathbb{N}$. Then there exists an infinite number of choices of the matrices A, B, C, N and the function f such that the pair $\{v(k), y(k)\}_{k=1}^{T}$ is an input/output pair.

Proof: We describe two possible strategies in such a way that there exists an infinite number of choices of parameters of the system (6) that realizes $\{v(k), y(k)\}_{k=1}^{T}$ as an input/output pair. It is clearly sufficient to prove the theorem.

1) Suppose that the matrices A, B, C, N are fixed (though they are unknown parameters of the secret key). Then define a function

$$f = f(A, B, C, N, y)$$

such that

$$y(i) \neq y(j) \quad \forall\ i, j = 1, \ldots, T,\ i \neq j.$$

This can be done for instance in the following way: consider the image of any element of the partition $\mathcal{P}$ under the map

$$F : x \mapsto \bigcup_{u \in \mathcal{U}} Ax + Bu + Nf(y),$$

and choose f such that

$$x \in \mathcal{P}_i \ \Rightarrow\ F(x) \notin \mathcal{P}_i.$$

Note that such an f can be defined in an infinite number of ways.

2) Choose $f = f(y(k), k)$. Clearly there is an infinite number of choices of f, thanks to the time-dependence, that realizes any input/output pair. $\diamondsuit$

Another issue concerning the security of the proposed cryptographic system is the choice of the secret key, which is formed by the matrices A, B, N, C, the partition $\mathcal{P}$, the alphabet $\mathcal{U}$, and the feedback function f in the system (6). A fundamental requirement of the cryptosystem is the chaotic behavior of the system (6). The reader can see how many properties of chaotic systems have counterparts in cryptographic systems in the introduction of [2]). For reasons of space we cannot go into further details on this topic, and future investigation will be directed to a precise characterization of the system's parameters that influence the dynamics (i.e. the matrices A, B, C, N and the feedback function f) to have chaotic behavior, and in particular to obtain positive Lyapunov exponents and the mixing property. Here we just observe that the fundamental ingredient for chaos is the feedback function f, which gives the nonlinearity of the system (without which chaos is not possible). For a survey on chaos theory, and many examples of chaotic maps, see for example [1].

V. An Example

In order to evaluate the performance of the proposed communication method, a simulation experiment is carried out to serve as an example. We can consider the system:

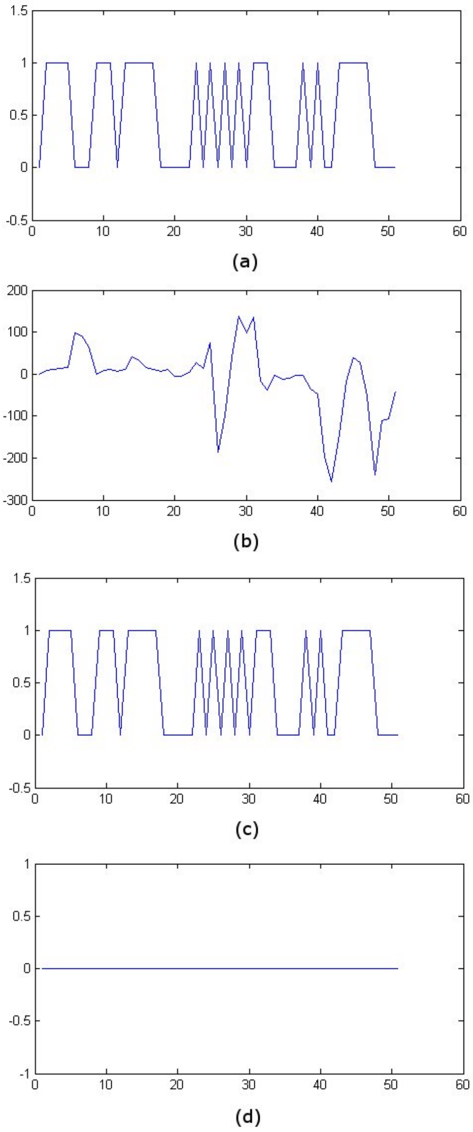
$$\begin{cases} x(k+1) = \frac{1}{2}x(k) + \pi u(k) + \sqrt{71}v(k) \\ y(k) = \lfloor x(k) \rfloor \end{cases} \tag{7}$$

Moreover, let $\mathcal{U} = \{0, 1\}$ be the inputs alphabet and define

$$f(k, y(k)) = 110 \cdot \sin k \cdot \sin y(k) \cdot \sin y(k-1) \cdot \sin y(k-2) \cdot \sin y(k-3)$$

to be the feedback function. We can observe, besides, that ($\sharp$ denotes the cardinality)

$$\forall u,\ u' \in \mathcal{U}, \qquad |u - u'| > \frac{|a| + 1}{\sharp\mathcal{U}}$$



(a)

(b)

(c)

(d)

Fig. 2. Simulation of the cryptosystem (7) (a) information signal $u(k)$ (plaintext), (b) transmitted signal $y(k)$ (ciphertext), (c) recovered signal, (d) difference between the plaintext and the recovered signal: the signal is recovered exactly.

so (7) is ULDI and has invertibility time equal to one ([13]).

Therefore, if the information signal is

$$v = [1\,1\,1\,1\,0\,0\,0\,1\,1\,1\,0\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,1\,0\,1\,0 \\ 1\,0\,1\,0\,1\,1\,1\,0\,0\,0\,0\,1\,0\,1\,0\,0\,1\,1\,1\,1\,1\,0\,0\,0\,0\,1]$$

as shown in figure 2 (a), then the encoded signal is shown in figure 2 (b), and the recovered signal is shown in figure 2 (c). The (null) error is shown in figure 2 (d) (the implementation of the algorithm can be found in [8]).

VI. Conclusions

In this paper a secure communication method based on left invertibility of output-quantized linear system, with finite inputs, is presented. Plaintext is represented by sequences of inputs on a finite alphabet. The ciphertext is the output of a quantized linear system with a feedback function and a left invertibility algorithm allows the recovery of the message. The secret key is formed by the system's parameters, including the feedback function.

We emphasize two main advantages of the proposed cryptographic system. First, the use of quantization is more realistic when digital data transmission is used, and makes the cryptosystem reproduce the plaintext exactly in finite time. Secondly, the feedback function adds an *infinite-dimensional* degree of freedom in the secret key, which is a distinct advantage with respect to methods where guessing a finite, albeit large, number of parameters would allow an eavesdropper to break the code.

Notwithstanding the apparent advantages, a quantitative assessment of the vulnerability of the proposed cryptographic system in the face of specific threat models is missing at this point, and will be the subject of further investigations.

Appendix

Proof of Theorem 2

Definition 11: Indicate with $\mathbb{Q}[\zeta_1, \ldots, \zeta_N]$ the ring of polynomials in the variables ζ_i with coefficients in $\mathbb{Q}$. The set of numbers $\alpha_1, \ldots, \alpha_N \in \mathbb{C}$ is said to be algebraically independent if

$$0 \neq p(\zeta_1, \ldots, \zeta_N) \in \mathbb{Q}[\zeta_1, \ldots, \zeta_N] \;\Rightarrow\; p(\alpha_1, \ldots, \alpha_N) \neq 0. \diamondsuit$$

We will show that, if in the output-quantized system (6) the set of elements of the matrix A is algebraically independent, then the system is uniformly left D-invertible if and only if it is uniformly left invertible. This implies that $\mathbb{S} \setminus \mathbb{S}_D$ has Lebesgue measure zero in $\mathbb{R}^{d \times d}$ for every $B, C, N, \mathcal{U}, \mathcal{P}$: this implication is proved final part of the proof.

Let us parametrize the possible pairs of states $(x, x') \in \mathbb{R}^{2d}$ such that $x' - x \in \mathcal{S}$ with the set

$$I = \Big\{ (t_1, \ldots, t_d, t_1 + s_1, \ldots, t_p + s_p, t_{d+p+1}, \ldots, t_{2d}) \\ \textit{such that } t_i, \in \mathbb{R},\; s_k \in]-1, 1[\Big\}.$$

Moreover we define the 2-dimensional plane P_i to be

$$P_i = \{X \in \mathbb{R}^{2d} :\; \varpi_j X = 0, \;\; j \neq i, i+d\},$$

i.e. P_i is the 2-dimensional plane generated by the $i-th$ and the $i+d-th$ component of vectors in $\mathbb{R}^{2d}$. If $X = (t_1, \ldots, t_d, t_1 + s_1, \ldots, t_p + s_p, t_{d+p+1}, \ldots, t_{2d}) \in I$, for

$i = 1, \ldots, p$, define $d_i(X)$ to be the distance, measured along the line

$$\{t_1, \ldots, \underbrace{\tau_i}_{varies}, \ldots, t_d, t_1 + s_1, \ldots$$
$$\ldots, \underbrace{\tau_i}_{varies} + s_i, \ldots, t_p + s_p, t_{d+p+1}, \ldots, t_{2d} : \ \tau_i \in \mathbb{R}\}$$

from the set Ω_i obtained by the union of the $i - th$ and $i + d - th$ coordinate axes.

We provide conditions such that $\forall \epsilon > 0$, $\forall m \in \mathbb{N}$, $\forall s_1, \ldots, s_p \in]-1, 1[$, there exists $t_1, \ldots, t_d \in \mathbb{R}$ such that, if $\{X(j)\}_{j=0}^{m}$ is the orbit of the $2d$-dimensional system with $X(0) = (t_1, \ldots, t_d, t_1 + s_1, \ldots, t_p + s_p, \tilde{t}_{p+1}, \ldots, \tilde{t}_d)$, then the following holds

$$frac\Big(d_i(X(j))\Big) < \epsilon, \tag{8}$$

for every $i = 1, \ldots, p$, $j = 1, \ldots, m$. Here $frac(\cdot)$ denotes the fractional part, acting componentwise. If conditions (8) are satisfied, the system is not uniformly left invertible (see [13]). These conditions will be verified by a full measure set. Consider the set

$$\mathbb{S}' = \left\{A \in \mathbb{R}^{d \times d} : \{a_{ij}\}_{i,j=1}^{d} \ alg. \ independent \ set\right\}.$$

Set $A \in \mathbb{S}'$. For $i = 1, \ldots, p$, simple (but boring) calculations show that $\varpi_{\langle e_i, e_{d+i}\rangle} X(j)$ has the form

$$\left(\begin{array}{c} \varpi_i X(j) \\ \varpi_{i+d} X(j) \end{array}\right) = \varpi_{\langle i, i+d\rangle} \left[\left(\begin{array}{cc} A & 0 \\ 0 & A \end{array}\right)^{j} X(0) + \right.$$
$$+ \left(\begin{array}{cc} A & 0 \\ 0 & A \end{array}\right)^{j-1} BU(1) + \ldots + BU(j) +$$
$$\left. + \left(\begin{array}{cc} A & 0 \\ 0 & A \end{array}\right)^{j-1} NV(1) + \ldots + NV(j) \right] =$$
$$= \left(\begin{array}{l} c_{i1}^{(j)} \ t_1 + \ldots + c_{id}^{(j)} \ t_d \\ \\ c_{i1}^{(j)} t_1 + \ldots + c_{ip}^{(j)} t_p + c_{i(p+1)}^{(j)} t_{d+p+1} + \ldots + c_{id}^{(j)} t_{2d} \end{array}\right)$$
$$+ constant \ terms,$$

where $c_{il}^{(j)}$ is the entry (i, l) of the matrix A^j. The set $\left\{a_{il}^{(j)} : \ i, l = 1, \ldots d; \ j = 1, \ldots N\right\}$ is a linearly independent set, thanks to the algebraic independence hypothesis on the elements of the matrix A (see [13]), so, by Kronecker's Theorem ([15]) there exists a choice of $(t_1 \ldots, t_d, t_{d+p+1}, \ldots, t_{2d})$ such that equation (8) is satisfied. Therefore the system (6) is not ULI.

To prove that the set of matrices with algebraically independent entries are a full measure set, first observe that the set of polynomial $P \in \mathbb{Q}[\zeta_1, \ldots, \zeta_{d^2}]$ is countable. For a single polynomial P the set

$$0_P = \left\{(x_1, \ldots, x_{d^2}) \in \mathbb{R}^{d^2} : \ P(x_1, \ldots, x_{d^2}) = 0\right\}$$

is a finite union of manifolds of dimension at most $d^2 - 1$. So the measure of 0_P is zero. Moreover

$$\mathbb{S}' = \bigcup_{P \in \mathbb{Q}[\zeta_1, \ldots, \zeta_{d^2}]} 0_P,$$

i.e. $\mathbb{S}'$ is a countable union of sets of measure zero, which in turn implies that the measure of $\mathbb{S}'$ is zero. ♢

References

[1] Alligood T.K., Sauer T, Yorke J.A., *Chaos: an introduction to dynamical systems,* Springer-Verlag New York Inc., (1996).

[2] Alvarez G., Li S., *Some basic cryptographic requirements for chaos-based cryptosystems,* International Journal of Bifurcation and Chaos, 16(8), pages: 2129-2151, (2006).

[3] Amigó J.M., Kocarev L., Szczepanski J., *Theory and practice of chaotic cryptography,* Physics Letters, A(366), pages: 211-216, (2007).

[4] Bicchi A., Marigo A., Piccoli B., *On the reachability of quantized control sytems,* IEEE Transactions on Automatic Control, 47(4), pages: 546-563, (2002).

[5] Bertram J.E., *The effect of quantization in sampled feedback systems*, AIEE Transactions on Applied Industry , Part. II volume 77, pages: 177-181, (1958).

[6] Brockett R. Liberzon D., *Quantized feedback stabilization of linear systems*, IEEE Transactions on Automatic Control, 45(7), pages: 1279-1289, (2000).

[7] Brockett R.W., Mesarovic M.D., *The reproducibility of multivariable control systems*, Journal of Mathenatical Analalysis and Applications, 11, pages: 548-563, (1965).

[8] Carluccio A., *Crittosistema a chiave simmetrica basato sulla comunicazione caotica: modello e simulazione*, Laurea degree thesis, (2009).

[9] Curry R.E., *Estimation and control with quantized measurements*, Research Monograph, M.I.T. Press, (1970).

[10] Delchamps D.F., *Stabilizing a linear system with quantized state feedback*, IEEE Transactions on Automatic Control, 35(8), pages: 916-924, (1990).

[11] Delfs H., Knebl H., *Introduction to cryptography*, CRC Press, (1996).

[12] Dubbini N., Piccoli B., Bicchi A., *Left invertibility of discrete systems with finite inputs and quantised output*, International Journal of Control, 83(4), pages: 798-809 (2010).

[13] Dubbini N., Piccoli B., Bicchi A., *Left invertibility of discrete-time output-quantized systems: the linear case with finite inputs*, Mathematics of Control Signals and Systems, note: submitted, (2010).

[14] Branko Grünbaum, *Convex polytopes*, Springer-Verlag NewYork Inc, (2003).

[15] Hardy G.H., Wright E.M., *An introduction to the theory of numbers*, Oxford Science Publications, (1979).

[16] Hasler M., *Synchronization of chaotic systems and transmission of information*, International Journal of Bifurcation and Chaos, 8(4), pages: 647-659, (1998).

[17] Inoue E., Ushio T., *Chaos communication using unknown input observer*, Electronic and Comunication in Japan, Part 3, 84, pages 21-27 (2001).

[18] Kalman R.E. *Nonlinear aspects of sampled-data control systems*, In Proceedings of the Symposium on Nonlinear Circuit Theory, vol. VII, Brooklyn, NY: Polytechnic Press, (1956)

[19] Massey J.L., Sain M.K., *Invertibility of linear time-invariant dynamical systems*, IEEE Transactions on Automatic Control, AC-14(2), pages: 141-149, (1969).

[20] Massey J.L., Sain M.K., *Inverses of linear sequential circuits*, IEEE Transactions on Computers, C-17, pages: 330-337, (1968).

[21] Nijmeijer H., Mareels I.M.Y., *An observer look at synchronization,* IEEE Transactions on Circuits and Systems I, 44, pages: 882-890, (1997).

[22] Parlitz U., Chua L.O., Kocareva L.J., Halle K.S., Shang A., *Trasmission of digital signals by chaotic synchronization,* International Journal of Bifurcation and Chaos, 2, pages: 973-977, (1992).

[23] Pecora L.M., Carrol T.L., *Synchronization in chaotic systems*, Physical Review Letters, 64, pages: 821-824, (1991).

[24] Picasso B., Bicchi A., *On the stabilization of linear systems under assigned I/O quantization*, IEEE Transactions on Automatic Control, 52(10), pages: 1994-2000, (2007).

[25] Respondek W., *Right and Left Invertibility of Nonlinear Control Systems*, Nonlinear Controllability and Optimal Control, New York, pages: 133-176, (1990).

[26] Respondek W., *Geometry of static and dynamic feedback*, Lecture notes.

[27] Silverman L.M., *Inversion of multivariable linear systems*, IEEE Transactions on Automatic Control, 14(3), pages: 270-276, (1969).

[28] Szanier M., Sideris, A., *Feedback control of quantized constrained systems with applications to neuromorphic controller design*, IEEE Transactions on Automatic Control, 39(7), 1497-1502, (1994).

[29] Vo Tan P., Millerioux G., Daafouz J., *Control under communication constraints,* Proceedings of the 47th IEEE Conference on Decision and Control, pages: 959-964, (2008)

[30] Tatikonda S.C., Mitter S., *Control under communication constraints,* IEEE Transactions on Automatic Control, 49(7), pages: 1056-1068, (2004).

[31] Vu L., Liberzon D., *Invertibility of switched linear systems*, Proceedings of the 45th IEEE Conference on Decision and Control, pages: 4081-4086, (2006).

[32] Yang T., *A survey of chaotic secure communication systems*, International Journal of Computational Cognition (http://www.YangSky.com/yangijcc.htm), 2(2), 81-130, (2004)