Cryptanalysis of hybrid cryptosystems

Gilles Millérioux

CRYPTANALYSIS OF HYBRID CRYPTOSYSTEMS

G. MILLERIOUX
Université de Lorraine, Centre de Recherche en Automatique de Nancy (CRAN UMR 7039)
E-mail: gilles.millerioux@univ-lorraine.fr

June 21, 2013

An essential issue for the validation of ciphers is the cryptanalysis, that is the study of attacks in order to reveal possible weaknesses. In this paper, we propose a systematic and unified methodology for cryptanalyzing known chaos-based cryptosystems borrowed from the open literature, namely shift keying, discrete parameter modulation, switched message-embedding, time-varying delay-based schemes. It is shown that all of them have a hybrid feature. Based on this consideration, the cryptanalysis amounts to perform a specific parameter identification. The method is extended in straighforwad way for hybrid cryptosystems defined over finite fields, involving in particular Boolean functions. The complexity of the cryptanalysis is derived regardless of the exhibited dynamics and provides a new quantitative measure for security assessment. That allows to show by the way that most of the chaos-based cryptosystems proposed so far in the literature are weak.

Keywords: cryptanalysis, chaotic systems, hybrid systems

1. Introduction

Since the 90's, many methods involving chaotic dynamics have been proposed in the literature to scramble information. Most of them consist in "mixing" the confidential information being transmitted through an unsecured channel, with a chaotic analog or digital sequence. The most popular techniques based on chaotic systems for concealing information are additive masking, chaotic switching, discrete or continuous parameter modulation, two-channel transmission, message-embedding and time-varying-based schemes. An overview of the different methods devised so far can be found in the papers [Ogorzalek, 1993, Hasler, 1998, Yang, 2004, Millérioux *et al.*, 2008b] or in the book [Banerjee, 2010]. Additive masking was first suggested in [Cuomo *et al.*, 1993, Wu & Chua, 1993]. Chaotic switching is also referred to as chaotic modulation or chaos shift keying. Such a technique has been mostly proposed in the digital communications context. A description with deep insights can be found in [Kolumban *et al.*, 1998], even though the method was proposed a couple of years before, say, in 1993 [Dedieu *et al.*, 1993]. Basically, two kinds of parameter modulations can be distinguished: the discrete one [Parlitz *et al.*, 1993] and the continuous one [Fradkov & Markov, 1997, Huijberts *et al.*, 2000, Dedieu & Ogorzalek, 1997, Anstett *et al.*, 2004]. The two-channel transmission has been proposed, for example, in [Millérioux & Mira, 2008b, Jiang Z-P., 2002]. The message-embedded tech-

nique is given different names in the literature: embedding [Yang *et al.*, 1997, Lian & Liu, Millérioux & Daafouz, 2004], non autonomous modulation [Yang, 2004] or direct chaotic modulation [Hasler, 1998]. Finally and quite recently, a time-varying delay-based cryptosystems has been proposed in [Zheng *et al.*, 2008].

The main motivation of the present work stems from the fact that over the years, most of chaotic dynamical systems-based schemes for scrambling information have been proposed without any security study. Hence the terminology secure communication was really questionable. Indeed these cryptosystems mostly relied more on empirical researches than on substantial and well-established proofs of security. However, in the last decade, more formal approaches have been suggested and the studies have taken into account an issue which is essential for the validation of cryptosystems, namely the cryptanalysis. An overview of the relevant theoretical frameworks can be found in several papers or books [Kelber & Schwarz, 2005, Alvarez & Li,, 2006, Anstett *et al.*, 2006, Banerjee, 2010]. More particularly, the fundamental Kerkhoffs' principle first formulated in 1883 [Kerkhoff, 1883, Delfs & Knebl, 2002] has been considered. It states that the adversary is assumed to know 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 for the aforementioned cryptosystems, the dynamical system parameters play a central role because they are precisely expected to act as the secret key. Thus it is essential to address the issue of parameters recovery both from a methodological and complexity points of view.

In this paper, we propose a systematic and unified methodology for cryptanalyzing known chaos-based cryptosystems having a hybrid feature, namely shift keying, discrete parameter modulation, switched message-embedding, time-varying delay-based schemes. It enables to cope with cryptosystems involving not only intrinsic switched systems like the Tent map, the Lozi map, the Baker map, the Cat Map, ... but also cryptosystems with a switching architecture involving polynomial nonlinearities like the Logistic map, the Henon map, the Burger map, ... Motivated by digital application, an extension to systems operating over finite fields is also carried out, in particular those involving Boolean functions [Carlet, 2010].

The outline is the following. Section 2 is devoted to a strict necessary recall of some specific cryptosystems borrowed from the literature and under consideration here, namely the chaotic switching, the discrete parameter modulation, the switched message embedding and the time-varying delay-based scheme. It is shown how such cryptosystems can be generically modeled as hybrid systems. Section 3 is devoted to a general consideration on the cryptanalysis of hybrid cryptosystems. In Section 4, a detailed and technical method is proposed for cryptanalyzing hybrid cryptosystems. The underlying attack is called algebraic attack - the general principle was first suggested by Shannon [Shannon, 1949] - and works regardless of the dynamics. Its complexity is assessed to provide a new measure of security. As an extension of the method, a special treatment is carried out to cope with cryptosystems described over finite fields. Finally, illustrative examples are presented in Section 5.

Notation: $\mathbf{0}$ stands for the zero matrix of appropriate dimension. For any vector u, $u^{(i)}$ denoted the ith component of u. u^T stands for the transposition of u. A time-varying vector will be denoted u_k where $k \in \mathbb{N}$ stands for the discrete-time.

2. Cryptosystems under consideration

For all the cryptosystems under consideration in this paper, the transmitter is described by a state space model. It involves a state-transition function (also called dynamical function) and an output function. The corresponding state vector is denoted x_k.

2.1. Hybrid description

Hybrid systems are a special class of dynamical systems widely investigated during the past decade [Egerstedt & Mishra, 1997] in numerous engineering area. They are built from a family of subsystems having their own dynamics (possibly own output function as well) and at each discrete time k, only one of them is active.

The state vector x_k characterizing the internal state of the overall system is governed by the dynamics of the active subsystem. The switching rule orchestrates the way how a subsystem is activated or not. It corresponds to a function $\sigma : k \in \mathbb{N} \mapsto i = \sigma(k) \in \mathcal{I} = \{1, \ldots, I\}$. Such a function can be described by logical premises. The index i is called the discrete mode or merely the mode.

We show below that many chaos-based cryptosystems proposed in the literature can be modeled in a unified way as hybrid systems having the form

$$\left\{ \begin{array}{lcl} x_{k+1} & = & f_{\sigma(k)}^{\lambda_{\sigma(k)}}(x_k, m_k) \\ y_k & = & h_{\sigma(k)}^{\lambda_{\sigma(k)}}(x_k, m_k) \end{array} \right. \quad (1)$$

f is the dynamics which depends on the discrete mode $\sigma(k)$ at time k and $\lambda_{\sigma(k)}$ are parameters assigned to $f_{\sigma(k)}$. $m_k \in \mathbb{R}$ and $y_k \in \mathbb{R}$ are respectively the input, playing the role of the information to be scrambled, and the output, playing the role of the ciphered information.

2.2. Modulation

2.2(A). Chaotic switching

Chaotic switching (see [Dedieu *et al.*, 1993] for pioneering works) is also referred to as chaotic modulation or chaos shift keying. For each symbol $m_k = m^i$ to be concealed and belonging to a finite set $\{m^1, \ldots, m^I\}$, it is assigned a parameter vector λ_i which parametrizes a dynamics f_i with output function h_i $(i = 1, \ldots, I)$. The assignment is performed by means of a bijective function $l : m_k \in \mathbb{R} \mapsto i = l(m_k) \in \mathcal{I} = \{1, \ldots, I\}$. During the interval of time $[jK, (j+1)K-1]$, m_k is assumed to be constant. This being the case, according to the current value of the symbol m_k at times $k = jK$ $(j \in \mathbb{N})$, a switch is periodically triggered on every K samples. The chaotic signal y_k of the system which has been switched on is conveyed through the channel. Therefore, the chaotic switching cryptosystem can be described at the transmitter side by

$$\left\{ \begin{array}{lcl} x_{k+1} & = & f_i^{\lambda_i}(x_k) \\ y_k & = & h_i^{\lambda_i}(x_k) \end{array} \right. \quad (2)$$

This is typically a hybrid system of the form (1) with $\sigma(k) = i = l(m_k)$.

2.2(B). Discrete parameter modulation

For discrete parameter modulation (see [Parlitz *et al.*, 1993] for pioneering works), to each symbol $m_k = m^i$ belonging to a finite set $\{m^1, \ldots, m^I\}$, it is assigned a chaotic signal emanating from a unique dynamics f and a unique output function h. Similarly to the chaotic switching, the assignment is performed by means of a bijective function $l : m_k \in \mathbb{R} \mapsto i = l(m_k) \in \mathcal{I} = \{1, \ldots, I\}$. The dynamics only differ from each other in the parameter vector λ_i where i depends on m_k. During the interval of time $[jK, (j+1)K-1]$, m_k is assumed to be constant and the chaotic signal y_k is conveyed through the channel. Hence, the transmitter obeys the following equations.

$$\left\{ \begin{array}{lcl} x_{k+1} & = & f^{\lambda_i}(x_k) \\ y_k & = & h^{\lambda_i}(x_k) \end{array} \right. \quad (3)$$

Again, this is typically a hybrid system of the form (1) with $\sigma(k) = i = l(m_k)$ and with $f_{\sigma(k)} = f$ for all $\sigma(k) \in \mathcal{I}$.

2.3. Switched message-embedding

Message-embedding is a scheme for which a special attention has been paid over the years [Yang *et al.*, 1997, Lian & Liu, Millérioux & Daafouz, 2004, Yang, 2004, Hasler, 1998]. At the transmitter part of a message-embedded setup, the information m_k is directly injected (or, as it is also usually said, embedded) into the dynamics. Injecting m_k into the dynamics can be considered as a "modulation" of the phase space. Switched message-embedded cryptosystems may be designed from piecewise linear maps like, to mention a few, the Tent map, the Lozi map, the Baker map, the Cat Map. For such maps, the state space is partitioned into a finite number I of regions. At each time k, according to the region which is visited by x_k, it is assigned a dynamics f_i, an output function h_i and a parameter vector λ_i $(i = 1, \ldots, I)$. The assignment is performed by means of a bijective function $l' : x_k \in \mathbb{R} \mapsto i = l'(x_k) \in \mathcal{I} = \{1, \ldots, I\}$. The output y_k of the system is transmitted through the channel. Hence, a switched message-embedded cryptosystem obeys

$$\left\{ \begin{array}{lcl} x_{k+1} & = & f_i^{\lambda_i}(x_k, m_k) \\ y_k & = & h_i^{\lambda_i}(x_k, m_k) \end{array} \right. \quad (4)$$

This is typically a hybrid system of the form (1) with $\sigma(k) = i = l'(x_k)$.

2.4. Time-varying delay-based scheme

Such a scheme has never been really proposed as is so far but the use of delays has been proposed in [Zheng *et al.*, 2008]. The time-varying delay-based scheme consists of two cascaded systems: a system with a time-varying delay $\tau(k)$ resulting from a complex sequence of symbols c_k delivered by an external system. Every symbol c_k results from successive compositions (rounds) of a next-state transition function of a chaotic map with itself. The initial condition is the information m_k to be ciphered and such an operating mode follows the same lines as a block cipher. The quantity $\tau(k)$ is an integer taking values in a bounded and known range $\{1, \ldots, \alpha\}$. The assignment between a symbol c_k and the delay $\tau(k)$ is performed by means of a bijective function $l'' : c_k \in \mathbb{R} \mapsto \tau(k) = l''(c_k) \in \{1, \ldots, \alpha\}$. Then, $\tau(k)$ is injected in a second dynamical system. Finally, the transmitter obeys the following equations.

$$\left\{ \begin{array}{lcl} \bar{x}_{k+1} & = & \bar{f}^{\lambda}(\bar{x}_k, \bar{x}_{k-\tau(k)}) \\ y_k & = & \bar{h}^{\lambda}(\bar{x}_k, \bar{x}_{k-\tau(k)}) \end{array} \right. \quad (5)$$

where $\bar{x}$ is the state vector, $\bar{f}$, $\bar{h}$ are respectively the state-transition function and the output function, λ is the parameter which parametrizes $\bar{f}$ and $\bar{h}$. The recovery of m_k requires a two-stages procedure: the recovery of the sequence of delays $\tau(k)$ followed by the recovery of the initial condition which has generated, after successive rounds, c_k assigned to $\tau(k)$ through the bijective function l''. By introducing an extended state vector $x_k = [\bar{x}_k, \bar{x}_{k-1}, \cdots, \bar{x}_{k-\alpha}]^T$, we can define a function f_i as $f_i(x_k) = \bar{f}(\bar{x}_k, \bar{x}_{k-i})$ and a function h_i as $h_i(x_k) = \bar{h}(\bar{x}_k, \bar{x}_{k-i})$. Therefore, the system (5) can be rewritten as

$$\left\{ \begin{array}{lcl} x_{k+1} & = & f_{\tau(k)}^{\lambda_{\tau(k)}}(x_k) \\ y_k & = & h_{\tau(k)}^{\lambda_{\tau(k)}}(x_k) \end{array} \right. \quad (6)$$

where $\lambda_{\tau(k)}$ is the reconsideration of λ for each value of $\tau(k)$. Clearly, (5) is of the form (1) with $\sigma(k) = \tau(k)$.

3. Attacks and security

3.1. Generalities

According to Kerkhoffs' principle mentioned in the introduction, any unauthorized party is assumed to know all the details of the cipher, including the algorithm and its implementation, except the secret key. Here, the expected secret key is a selection of L components of the λ_i $(i = 1, \ldots, I)$. They are collected in a L-dimensional vector denoted θ. The most unfavorable situation for the security corresponds to the case when the adversary is able to control the input sequences of the transmitter (sequences $\{m_k\}$ of plaintexts) and to analyze the corresponding output sequences (sequences $\{y_k\}$ of ciphertexts). It is the assumption that we will consider hereafter.

This being the case, an attempt to recover θ can be performed by a so-called algebraic attack of which general principle was first suggested by Shannon [Shannon, 1949]. It consists in an identification procedure which requires first, lumping together inputs m_k, outputs y_k and their iterates considered over a finite interval of time, then deriving a set of algebraic equations of which indeterminates are the components of θ. The security is directly related to the complexity of finding out the solution. This attack can be very effective insofar as it works regardless of the complexity of the dynamics which is exhibited by the system. It differs from attacks based on statistical considerations of the ciphered sequence or approaches based on time series prediction.

Appropriate equations involving the inputs and the outputs, as required for algebraic attacks, can be derived from the input/output model of the state space representation (6). Since such a model plays a central role and deserves a special treatment for hybrid systems, it is detailed in the next subsection.

3.2. Input/output model for general hybrid systems

An input/output model for a dynamical system is a relation where the state does not appear and which only involves the input m_k, the output y_k and a finite number of their iterates.

Hence, to derive an input/output model from the state space model, a number of iterations must be performed to obtain a set of equations from which x_k can be eliminated. Let s be the integer corresponding to the number of required iterations. The peculiarity due to the hybrid nature of the systems lies in that some of the parameters of the state space equations depend on the mode and so are time-varying. Hence, we get different input/output models according to the different mode sequences $\{\sigma(k), \ldots, \sigma(k+s)\}$ over the interval of time $[k, \ldots, k+s]$. Let us notice that the maximum number of mode sequences over an interval of time of finite length is finite since the number I of modes delivered by the switching function σ is finite too. Actually, it is equal to I^{s+1}. Let N be the number of derived input/output models. They can implicitly be written by means of functions $\mathcal{L}_n$ for each $n = 1, \ldots, N$

$$\mathcal{L}_n(\mu_n, y_{k+s}, \ldots, y_k, m_{k+s'}, \ldots, m_k) = 0 \quad (7)$$

where s and s' are positive integers and clearly $s \geq s'$. The components $\mu_n^{(i)}$ $(n = 1, \ldots, N)$ of the vector μ_n consists of the parameters involved in $\mathcal{L}_n$. They depend on the parameters λ_i $(i = 1, \ldots, I)$ of the state space model since they result from operations on the state space models performed to eliminate the state vector x_k. Consequently some (or all) of them depend on the $\theta^{(i)}$. Indeed, we recall that the secret key θ is a selection of L components of the λ_i $(i = 1, \ldots, I)$. The number of parameters $\mu_n^{(i)}$ is not necessarily equal to the number of $\theta^{(i)}$.

As highlighted in the introduction, chaotic maps involved in the literature are essentially switched linear systems and systems with polynomial nonlinearities. Thus, in the next subsection, we concentrate and provide the expressions of the input/output relations for those classes of dynamical systems.

3.2(A). Switched linear dynamical systems

Switched linear dynamical systems are governed by

$$\left\{ \begin{array}{rcl} x_{k+1} & = & A_{\sigma(k)} x_k + B_{\sigma(k)} m_k \\ y_k & = & C_{\sigma(k)} x_k + D_{\sigma(k)} m_k \end{array} \right. \quad (8)$$

All the matrices, namely $A_{\sigma(k)}$, $B_{\sigma(k)}$, $C_{\sigma(k)}$ and $D_{\sigma(k)}$ belong to the respective finite sets $\{A_i\}_{1 \leq i \leq I}$, $\{B_i\}_{1 \leq i \leq I}$, $\{C_i\}_{1 \leq i \leq I}$ and $\{D_i\}_{1 \leq i \leq I}$.

Remark 3.1. It is worth emphasizing that we could consider, with little further efforts, piecewise affine systems, by adding constant matrices $E_{\sigma(k)}$ and $E'_{\sigma(k)}$ in both equations of (8).

Equation (8) is of the form (1) where the parameters $\lambda_{\sigma(k)}$ correspond here to the entries of the matrices. Hence, for the switched message-embedding, the parameter vector θ consists of L selected entries of the matrices $A_{\sigma(k)}$, $B_{\sigma(k)}$, $C_{\sigma(k)}$ and $D_{\sigma(k)}$. For the chaotic switching, the discrete parameter modulation or the time-varying delay-based scheme, the matrices $B_{\sigma(k)}$ and $D_{\sigma(k)}$ are zero and the parameter vector θ consists of L selected entries of the matrices $A_{\sigma(k)}$ and $C_{\sigma(k)}$.

It can be shown (see [Paoletti *et al.*, 2008]) that, for (8), there generically exist two positive integers s and s' such that the corresponding input/output model reads for $n = 1, \ldots, N$

$$\mathcal{L}_n = \sum_{i=0}^{s} \mu_n^{(i+s'+1)} y_{k+i} + \sum_{i=0}^{s'} \mu_n^{(i)} m_{k+i} = 0 \quad (9)$$

Hereafter, it will be assumed without any restriction that $\mu_n^{(s)} = 1$ after a normalization. For convenience, we define the quantity K as a positive integer corresponding to number of terms involved in (9). Hence, we have that $K = s + s' + 2$. If no term involving m_k or its iterate appears in $\mathcal{L}_n$ (a situation which typically occurs for cryptosystems (2), (3) and (6)), by convention, we will take $s' = -1$.

A simple example

Consider a one-dimensional switched dynamical system of the form (8) with $A_{\sigma(k)} = a_{\sigma(k)}$, $B_{\sigma(k)} = 1$ for any $\sigma(k)$, $C_{\sigma(k)} = c_{\sigma(k)}$ and $D_{\sigma(k)} = 0$ for any $\sigma(k)$. Assume that the switching function $\sigma(k)$ delivers $I = 2$ modes ($\sigma(k) = 1$ or $\sigma(k) = 2$). Hence, the corresponding parameters are a_1, a_2, c_1 and c_2. Let us define the L-dimensional ($L = 4$) parameter vector θ of the state space model $\theta = [\theta^{(1)}, \theta^{(2)}, \theta^{(3)}, \theta^{(4)}] = [a_1, a_2, c_1, c_2]$. It is expected to act as the secret key.

From the state space model, it's a simple matter to derive the input/output model which obeys

the form (9) and reads

$$y_{k+1} - \frac{c_{\sigma(k+1)}a_{\sigma(k)}}{c_{\sigma(k)}}y_k - c_{\sigma(k+1)}m_k = 0 \qquad (10)$$

with $s = 1, s' = 0$.

Let us consider the distinct mode sequences over the time interval $[k, k+1]$. Since there are $I = 2$ modes, the different mode sequences are $\{1,1\}$, $\{1,2\}$, $\{2,1\}$ and $\{2,2\}$ and there are $N = 4$ distinct input/output models of the form (9) with

$$\begin{array}{ll} \mu_1^{(1)} = -\theta^{(1)} & ,\mu_1^{(0)} = -\theta^{(3)} \\ \mu_2^{(1)} = -\frac{\theta^{(4)}\theta^{(1)}}{\theta^{(3)}} & ,\mu_2^{(0)} = -\theta^{(4)} \\ \mu_3^{(1)} = -\frac{\theta^{(3)}\theta^{(2)}}{\theta^{(4)}} & ,\mu_3^{(0)} = -\theta^{(3)} \\ \mu_4^{(1)} = -\theta^{(2)} & ,\mu_4^{(0)} = -\theta^{(4)} \end{array} \qquad (11)$$

Finally, $\mu_n^{(2)} = 1$ for $n = 1, \ldots, 4$.

3.2(B). Switched systems with polynomial nonlinearities

Systems with polynomial nonlinearities obey (1) with the peculiarity that $f_{\sigma(k)}^{\lambda_{\sigma(k)}}$ and $h_{\sigma(k)}^{\lambda_{\sigma(k)}}$ are functions of a linear combination of monomials involving $x_k^{(i)}$, m_k, the products, their iterates and their powers. Eliminating x_k can be achieved by techniques based, for example, on Gröbner basis [Banerjee, 2010]. It yields N input/output relations, according to the different mode sequences, in the form of a linear combination of monomials involving y_k, m_k, the products, their iterates and their powers. Thus, for $n = 1, \ldots, N$, the input/output relation reads

$$\mathcal{L}'_n = \sum_{i=0}^{K-1} \mu_n^{(i)} \sum_{p_j, p'_j} y_k^{p_1} \cdots y_{k+s}^{p_s} m_k^{p'_1} \cdots m_{k+s'}^{p'_{s'}} = 0 \qquad (12)$$

with the p_j and the p'_j depending on n and i. The quantity K is compliant with the one introduced before. It is a positive integer corresponding to number of terms involved in (12). Likewise for switched linear systems, the subscript n in the $\mu_n^{(i)}$ means that the $\mu_n^{(i)}$ depend in different ways on the parameters of the state space model according to the sequence of modes and consequently some (or all) of them depend on the $\theta^{(i)}$. It is also assumed that $\mu_n^{(s)}$, weighting the term of higher degree, equals 1 after normalization.

Remark 3.2. It is worth pointing out that (9) is a particular case of (12). Indeed, (12) reduces to (9) when the exponents $p_1,\ldots,p_s,p'_1,\ldots,p'_{s'}$ of the monomials $y_k^{p_1} \cdots y_{k+s}^{p_s} m_k^{p'_1} \cdots m_{k+s'}^{p'_{s'}}$ are all zero expect one which equals 1.

3.3. Conclusion on attacks

If the mode sequences were accessible, it means that $\sigma(k), \sigma(k+1), \ldots$ over a given time horizon is known. Hence, we can assign, for every input/output model n, the input-output pairs of the data set and the unknown $\mu_n^{(i)}$ having the same index n. Thus, for a given n, the identification could be performed by iterating the model (9) or (12) until a set of independent equations is obtained and can be solved to find out θ. Since the $\mu_n^{(i)}$ appear in a linear fashion in the input/output model (9) or (12), the identification procedure would be rather straightforward. Nevertheless, the modes may not be directly accessible to the eavesdropper, the switching rule σ being likely to be also parametrized by the secret key. The purpose of next section is to show that, despite this favorable situation, the eavesdropper can successfully achieve an algebraic attack by resorting to a specific identification procedure. The technique is inspired from [Vidal *et al.*, 2003] dedicated to the identification of switched ARX systems but revisited here for our context.

4. Identification procedure

4.1. Technical aspects

The input/output relation (9) can be rewritten for each $n = 1, \ldots, N$

$$z_k^T b_n = 0 \qquad (13)$$

with

$$z_k = [y_{k+s}, \ldots, y_k, m_{k+s'}, \ldots, m_k]^T \in \mathbb{R}^K \qquad (14)$$

$$b_n = [1, \mu_n^{(K-2)}, \ldots, \mu_n^{(0)}]^T \in \mathbb{R}^K \qquad (15)$$

The vector z_k is called the *regression vector* while the vector b_n is called the *parameter vector* assigned to the input/output model number n.

According to Remark 3.2, the equality (13) still holds for systems with polynomial nonlinearities

and so for (12) with the same parameter vector (15) and with

$$z_k = [\ldots, y_k^{p_1} \cdots y_{k+s}^{p_s} m_k^{p'_1} \cdots m_{k+s'}^{p'_{s'}}, \ldots]^T \in \mathbb{R}^K \tag{16}$$

As it turns out, the following equation applies for $n = 1, \ldots, N$

$$p_N(z_k) = \prod_{n=1}^{N} (z_k^T b_n) = 0 \tag{17}$$

since there always exists an integer $n \in \{1, \ldots, N\}$ such that (13) is fulfilled. Let ξ_k be the vector which components consists of all the products of the components $z_k^{(i)}$ of z_k ordered in a lexicographic way. Let M_N be the number of components of ξ_k. As a result, (17) can be rewritten as

$$p_N(z_k) = \nu_N(z_k)^T h_N = 0 \tag{18}$$

By definition, the function $\nu_N : z_k \in \mathbb{R}^K \mapsto \xi_k \in \mathbb{R}^{M_N}$ is a map of degree N and corresponds to the so-called *Veronese map* [Harris, 1995]. The components of the vector $h_N \in \mathbb{R}^{M_N}$ are the coefficients of p_N and h_N is the vector representation of the symmetric tensor product of the individual system parameters b_n $(n = 1, \ldots, N)$. It is known that the quantity M_N depends on K as

$$M_N(K) = \frac{(N + K + 1)!}{N!(K + 1)!} \tag{19}$$

For shortness, $M_N(K)$ will sometimes be merely written M_N in the sequel.

Remark 4.1. The first component $h_N^{(0)}$ of h_N equals 1 since the first component of the b_n equals 1.

This being the case, the issue of retrieving the secret key θ of the state space model is equivalent to the problem of recovering the μ_n, and so the b_n in the N corresponding input/output models (13). Indeed, it is recalled that the $\theta^{(i)}$ are assumed to be deduced from the $\mu_n^{(i)}$.

The identification of the b_n in (13) requires first of all to compute the coefficients h_N of (18).

Computing h_N

Let $\mathcal{L}_N$ denote the embedded data matrix involving N' mapped regression vectors $\nu_N(z_{k_i})$ through ν_N

$$\mathcal{L}_N = \begin{bmatrix} \nu_N(z_{k_1})^T \\ \nu_N(z_{k_2})^T \\ \vdots \\ \nu_N(z_{k_{N'}})^T \end{bmatrix} \in \mathbb{R}^{N' \times M_N} \tag{20}$$

The following relation applies

$$\mathcal{L}_N h_N = \mathbf{0} \tag{21}$$

If there exists an integer N' large enough so that the $\nu_N(z_{k_i})$ $(i = 1, \ldots, N')$ can span a $M_N - 1$ dimensional vector space, *i. e.*

$$\text{rank}(\mathcal{L}_N) = M_N - 1 \tag{22}$$

then h_N is one-dimensional and according to Remark 4.1 is unique after normalization. The lower bound of N' is clearly $M_N - 1$.

If (22) is fulfilled, h_N can be retrieved by

$$h_N = \ker(\mathcal{L}_N) \tag{23}$$

where ker stands for the kernel (also called the null space) of $\mathcal{L}_N$.

Computing b_n

It can be shown, (see [Vidal *et al.*, 2003] for details), that

$$b_n = (D^{(0)} p_N(w_n))^{-1} \frac{\partial p_N(z_k)}{\partial z_k} | w_n \tag{24}$$

$$w_n = \rho_n v + w_0 \tag{25}$$

with ρ_n the roots of

$$p_N(\rho v + w_0) = 0 \tag{26}$$

and v and w_0 two arbitrary vectors fulfilling the constraint $p_N(v) \neq 0$.

It can be convenient to give here a geometrical interpretation.

For $n = 1, \ldots, N$, (13) defines N hyperplanes S_n

$$S_n = \{z_k | z_k^T b_n = 0\}$$

The roots ρ_n of (26) are the N intersections of the hyperplanes S_n with the parametrized line $\mathcal{D}$ defined as

$$\mathcal{D} : \rho v + w_0, \ \rho \in \mathbb{R}$$

The constraint $p_N(v) \neq 0$ guarantees that $\mathcal{D}$ is not parallel with any of the hyperplanes S_n. A graphical interpretation is given on Figure 1 in the three-dimensional case.

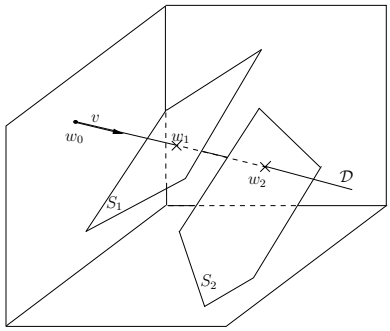

Fig. 1: The intersection of an arbitrary line $\mathcal{D}$ with two planes S_1, S_2 in a three-dimensional space

4.2. Summary of the identification procedure

The identification procedure for cryptanalyzing the hybrid cryptosystems (2), (3), (4) and (6) and so retrieving the secret key θ, can be summed up in 7 steps:

- From the state space description, derive the N input/output models involving the time-invariant parameters $\mu_n^{(i)}$ by considering the mode sequences over the time interval $[k, \ldots, k+s]$. The input/output models obey (9) if a switched linear system is considered or (12) if a system with polynomial nonlinearities is considered.
- Extract from the input/output model (9) or (12) the regression vector z_k and the corresponding parameter vector b_n to rewrite the input/output models in the form (13). Express the $\mu_n^{(i)}$ with respect to the components $\theta^{(i)}$ of the secret key θ.
- Express (18) involving the Veronese map, apply a sufficiently long sequence of inputs m_k to the state space model in order to build the embedded data matrix $\mathcal{L}_N$ (20)
- Compute the vector h_N from the kernel of $\mathcal{L}_N$ (23)
- By solving (26), find out the points w_n expressed by (25) lying on the hyperplanes S_n
- Retrieve the parameter vectors b_n from (24)
- Retrieve the secret key, that is the $\theta^{(i)}$ from the $\mu_n^{(i)}$ which are the components of b_n (see (15))

4.3. Complexity and security

Now we are in position of assessing the complexity of the identification procedure or equivalently the algebraic attack. Such an issue is particularly relevant because it delivers an interesting indicator for assessing the security of the cryptosystems. The most important task of the procedure is the computation of the coefficients of h_N through (23). Usually, the kernel is obtained with, for instance, a Gaussian algorithm, a Singular Value Decomposition or a QR decomposition. Since the complexity of these algorithms is $O(min(N'M_N^2, N'^2 M_N))$ and the lower bound of N' is $M_N - 1$, the complexity is lower bounded by $O(M_N^3)$. The expansion rate of M_N and the complexity for different values of N and K are respectively depicted in Fig. 2 and Fig. 3. A cryptosystem is considered as secure if the eavesdropper has no other alternative than resorting to a brute force attack. Such an attack consists in trying exhaustively every possible parameter value in the parameter space of the secret key. Conversely, a cryptosystem suffers from weakness if an eavesdropper can successfully perform an attack which complexity lower than the exhaustive search. Hence, such a quantity is a measure of security regarding the algebraic attacks.

Based on this consideration, it can be claimed that most of the chaos-based cryptosystems involving classical chaotic systems like Cat map, Burger map, Henon map, ... are definitively weak. Indeed, for those systems, the dimension is usually low. Take a dimension equal to 4. We can show that K is of the same order of the dimension. Take $K = 4$. N depends on the number of modes. According to the cryptosystem, it may correspond to the number

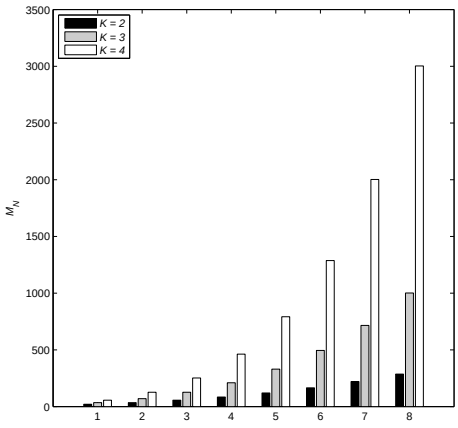

Fig. 2: M_N versus N for different values of K

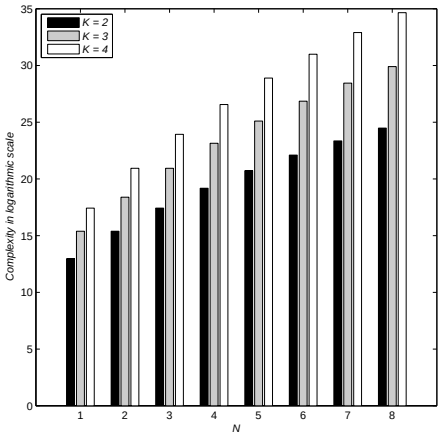

Fig. 3: The evolution of the complexity M_N^3 with respect to N for different values of K

of regions of the piecewise linearity, the cardinality of the set where the information takes value, the number of time-varying delays, ... Take $N = 10$. With these values, M_N is of order 1000 and so M_N^3 is of order 10^9. Assume that a computer takes 10^{-9} seconds to perform one operation. In all, it will take 1 second to retrieve the secret key!

4.4. Extension to finite fields

If a digital application is sought (hardware implementation in e.g. FPGA or DSP), the data to be encrypted are either intrinsically digital or digitalized and so lie in a finite set. It is clear that resorting to a map which takes value in a dense set (for example the set of real values for chaotic maps) will cause the output (the corresponding encrypted information) to also take value in a dense set. When implemented in a finite state machine, the output is automatically quantized and rounded, but clearly, this is a poor solution regarding the throughput because the amount of output data is larger than the one corresponding to the original information. Besides the result of the encryption is likely to be machine dependent. Undoubtedly, resorting to a dynamical system whose state and output directly take value in a finite set whose range is identical to the one of the input data is a better solution. This is precisely the case in classical cryptography which usually considers Boolean functions [Carlet, 2010] and so the field of two elements $\{0, 1\}$.

This section is mainly dedicated to this important aspect and shows that the proposed cryptanalyzing method can be directly extended to hybrid cryptosystems defined over finite fields [Lidl & Niederreiter, 2008].

A field is a 3-uplet $(\mathbb{F},+,\cdot)$ where $\mathbb{F}$ is a set, $+$ an operation usually called *addition* and $\cdot$ an operation usually called *multiplication*. The following properties apply

1. For all a and b in $\mathbb{F}$ both $a+b$ and $a\cdot b$ are $\mathbb{F}$,
2. For all a, b and c in $\mathbb{F}$, associativity holds: $a+(b+c) = (a+b)+c$ and $a\cdot(b\cdot c) = (a\cdot b)\cdot c$,
3. For all a and b in $\mathbb{F}$, commutativity holds: $a + b = b + a$ and $a \cdot b = b \cdot a$,
4. There exists an element of $\mathbb{F}$, called the additive identity element and denoted by 0 such

that for all a in $\mathbb{F}$, $a+0=a$. Likewise, there is an element called the multiplicative identity element and denoted by 1, such that for all a in $\mathbb{F}$, $a\cdot 1=a$. The identity elements 0 and 1 have to be different,

5. For every a in $\mathbb{F}$, there exists an element $-a$ in $\mathbb{F}$ such that $a+(-a)=0$. Similarly, for any a in $\mathbb{F}$ other than 0, there exists an element a^{-1} in $\mathbb{F}$ such that $a\cdot a^{-1}=1$,

6. For all a, b and c in $\mathbb{F}$ distributivity of the multiplication over the addition holds: $a\cdot(b+c)=(a\cdot b)+(a\cdot c)$.

A finite field is a field with a finite number of elements. The set of integers modulo a prime p, that is the structure $\mathbb{Z}/p\mathbb{Z}$ also denoted $\mathbb{F}_p$, is a usual finite field.

The required operations for the identification procedure provided in Section 4 are addition, multiplication, inversion and differentiation. The identification can therefore be applied to any (possibly finite) set over which similar operations still hold. It turns out that these requirements match the definition of the mathematical structure like a field. Indeed, addition and multiplication are directly involved in the definition of a field. Furthermore the definition of a field implies the existence of an inverse element for the addition (it corresponds to the subtraction) and also implies the existence of a multiplicative inverse for non-zero elements. Hence inversion is well-defined. As it turns out, the notion of derivative also exists.

5. Examples

Two simple examples are detailed throughout this section. Each of them illustrates the cryptanalysis in some specific cases. Example 1 illustrates the discrete parameter modulation with polynomial chaotic maps. To show that the method still applies for finite fields, the second example addresses a switched linear system described over the field of two elements $\{0,1\}$. The different steps of the cryptanalysis follow the summary of Section 4.2. The first example details all the steps whereas the second one is described in a more compact way.

5.1. Example 1: discrete parameter modulation with polynomial chaotic maps

Let us consider the two-dimensional discrete parameter modulation system of the form (3) involving the chaotic Burger map

$$x_{k+1}=f_{\sigma(k)}^{\lambda_{\sigma(k)}}(x_k)=\begin{cases}(1+0.73)x_k^{(1)}+x_k^{(1)}x_k^{(2)}\\(1-a_{\sigma(k)})x_k^{(2)}-x_k^{(1)}x_k^{(1)}\end{cases} \tag{27}$$

and

$$y_k=h_{\sigma(k)}^{\lambda_{\sigma(k)}}(x_k)=x_k^{(1)} \tag{28}$$

$\lambda_{\sigma(k)}$ involves all the parameters of the map. Actually the indexation with $\lambda_{\sigma(k)}$ of h could be omitted since the output function does not depend on σ. However, the generic notation (1) has been kept. To each binary value m_k assumed to belong to the finite set $\{0,1\}$, a switching rule σ assigns the respective values $a_1=2$ or $a_2=2.1$. Consequently, the cryptosystem has a hybrid feature with $I=2$ modes. The parameter vector θ is of dimension $L=3$ and is defined as $[\theta^{(1)},\theta^{(2)},\theta^{(3)}]=[0.73,a_1,a_2]=[0.73,2,2.1]$. The vector θ acts as the secret key.

An example of the time evolution of m_k and the corresponding $a_{\sigma(k)}$ is depicted in Figure 4. The attractor of the resulting switched system is depicted in Figure 5.

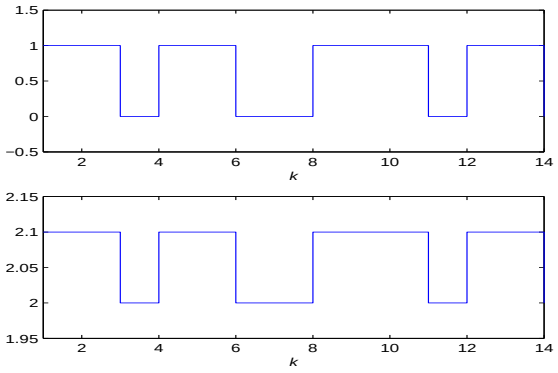

Fig. 4: The evolution of m_k (up) and $a_{\sigma(k)}$ (bottom)

Input/output models

By iterating (27) and (28) twice ($s=2$), it turns

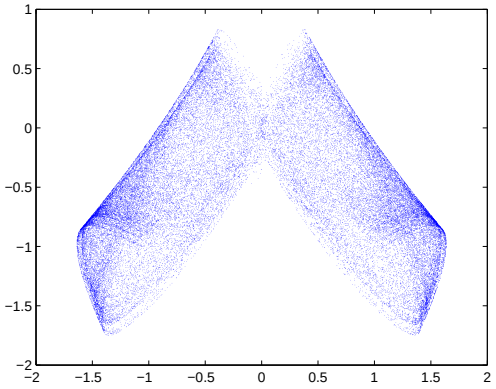

Fig. 5: Attractor of the switched Burger map in the two-dimensional state space

out that x_k can be eliminated and that the input/output model reads

$$y_k^3 y_{k+1} - y_{k+1}^2 + y_k y_{k+2} + a_{\sigma(k)}(y_{k+1}^2 - y_k y_{k+1}) \\ -\theta^{(1)} a_{\sigma(k)} y_k y_{k+1} = 0 \tag{29}$$

Since there are $I = 2$ modes, it is clear that there are here $N = 2$ distinct input/output models of the form (12). They read respectively for $n = 1$ and $n = 2$

$$y_k^3 y_{k+1} - y_{k+1}^2 + y_k y_{k+2} + a_1(y_{k+1}^2 - y_k y_{k+1}) \\ -\theta^{(1)} a_1 y_k y_{k+1} = 0 \tag{30}$$

$$y_k^3 y_{k+1} - y_{k+1}^2 + y_k y_{k+2} + a_2(y_{k+1}^2 - y_k y_{k+1}) \\ -\theta^{(2)} a_2 y_k y_{k+1} = 0 \tag{31}$$

Regression and parameter vector
From (30) and (31), it is inferred that the regression vector is given by

$$z_k = \begin{bmatrix} z_k^{(1)} \\ z_k^{(2)} \\ z_k^{(3)} \end{bmatrix} = \begin{bmatrix} y_k^3 y_{k+1} - y_{k+1}^2 + y_k y_{k+2} \\ y_{k+1}^2 - y_k y_{k+1} \\ -y_k y_{k+1} \end{bmatrix} \tag{32}$$

Besides, there are two distinct parameter vectors b_1 and b_2 related to the input/output models $n = 1$ and $n = 2$.

$$b_1 = [1, \mu_1^{(1)}, \mu_1^{(0)}]^T = [1, \theta^{(2)}, \theta^{(1)}\theta^{(2)}]^T \\ b_2 = [1, \mu_2^{(1)}, \mu_2^{(0)}]^T = [1, \theta^{(3)}, \theta^{(2)}\theta^{(3)}]^T \tag{33}$$

Veronese map
Since $N = 2$, the Hybrid Decoupling Constraint polynomial (18) reads

$$p_N(z_k) = (z_k^T b_1)(z_k^T b_2) = \nu_N(z_k)^T h_N \tag{34}$$

with

$$\nu_N(z_k)^T = [(z_k^{(1)})^2, z_k^{(1)} z_k^{(2)}, z_k^{(1)} z_k^{(3)}, (z_k^{(2)})^2, \\ z_k^{(2)} z_k^{(3)}, (z_k^{(3)})^2] \tag{35}$$

and

$$h_N = [1, \mu_1^{(1)} + \mu_2^{(1)}, \mu_1^{(0)} + \mu_2^{(0)}, \mu_1^{(1)}\mu_2^{(1)}, \\ \mu_1^{(0)}\mu_2^{(1)} + \mu_1^{(1)}\mu_2^{(0)}, \mu_1^{(0)}\mu_2^{(0)}] \tag{36}$$

Computing h_N
After applying a sufficiently long input sequence m_k, it turns out that the kernel of $\mathcal{L}_N$ is one-dimensional meaning that the resulting embedded data matrix $\mathcal{L}_N$ fulfills the rank condition (22). The kernel h_N numerically reads after normalization (see Remark 4.1)

$$h_N = [1, 4.09981, 2.9925, 4.1196, 6.1315, 2.2378]^T \tag{37}$$

From (34), the derivative $Dp_N(z_k)$ of $p_N(z_k)$ reads

$$Dp_N(z_k) = \begin{bmatrix} 2z_k^{(1)} + 4.1z_k^{(2)} + 2.993z_k^{(3)} \\ 4.1z_k^{(1)} + 8.4z_k^{(2)} + 6.315z_k^{(3)} \\ 2.993z_k^{(1)} + 6.1315z_k^{(2)} + 4.4756z_k^{(3)} \end{bmatrix} \tag{38}$$

Computing w_n
Consider a line with an arbitrary direction $v = [0.1935, -1.1025, -0.1661]$ and an arbitrary base point $w_0 = [-0.0186, -0.5884, -0.1441]^T$.

Solving (26) yields $\rho_1 = -0.6237$ and $\rho_2 = -0.6207$ and the two corresponding intersections are
$w_1 = [-0.13926, 0.099214, -0.040525]^T$ and
$w_2 = [-0.13869, 0.095984, -0.041012]^T$.

Computing b_n
According to (24), the parameter vectors b_n are

$$\begin{array}{ll} b_1 & = [1, \quad 2, \quad 1.46]^T \\ b_2 & = [1, \quad 2.1, \quad 1.533]^T \end{array} \tag{39}$$

Recovery of the secret key θ
From (33) and (39), the following relations apply

$$\begin{array}{lll} \mu_1^{(1)} & = \theta^{(2)} & = 2 \\ \mu_1^{(0)} & = \theta^{(1)}\theta^{(2)} & = 1.46 \\ \mu_2^{(1)} & = \theta^{(3)} & = 2.1 \\ \mu_2^{(0)} & = \theta^{(2)}\theta^{(3)} & = 1.53 \end{array} \tag{40}$$

and the secret key $\theta^{(1)} = 0.73,\ \theta^{(2)} = a_1 = 2,\ \theta^{(3)} = a_2 = 2.1$ is properly recovered.

Let us assess the complexity. Here, $N = 4$ and $K = 3$. Thus, $M_N = 70$ and $M_n^3 = 343.10^3$ which is very small. That reveals a dramatic weakness if such a map would have been expected to act as a cipher (see the discussion in Subsection 4.3)

5.2. Example 2

Consider a three-dimensional switched dynamical system over the finite field $\mathbb{F}_2$ ($p = 2$) of the form (8) with

$$A_{\sigma(k)} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & a_{\sigma(k)} & 1 \end{bmatrix},\ B_{\sigma(k)} = B = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

$$C_{\sigma(k)} = C = [1 \ \ 0 \ \ 0],\ D_{\sigma(k)} = D = 0$$

The switching function $\sigma(k)$ delivers two modes ($I = 2$) and the corresponding parameters are $a_1 = 0$ and $a_2 = 1$.

The parameter vector θ is defined as $\theta = [\theta^{(1)}, \theta^{(2)}] = [a_1, a_2] = [0, 1]$. It is supposed to act as the secret key.

Input/output relations
From the state space model, it can be shown that the input/output model reads

$$y_{k+3} - y_{k+2} - a_{\sigma(k)} y_{k+1} - y_k - m_k = 0 \tag{41}$$

Again, following the same reasoning as in the previous examples, we conclude that there are $N = 2$ distinct input/output relations of the form (9).

Regression and parameter vector
From (41) it is inferred that the regression vector is given by

$$z_k = [y_{k+3}, y_{k+2}, y_{k+1}, y_k, m_k]^T$$

and there are two distinct parameter vectors b_1 and b_2 related to the input/output models $n = 1$ and $n = 2$.

$$\begin{array}{l} b_1 = [1, \mu_1^{(3)}, \ldots, \mu_1^{(0)}]^T = [1, 1, -\theta^{(1)}, 1, 1]^T \\ b_2 = [1, \mu_2^{(3)}, \ldots, \mu_2^{(0)}]^T = [1, 1, -\theta^{(2)}, 1, 1]^T \end{array} \tag{42}$$

Let us note that we have taken into account that $-1 = 1$ over $\mathbb{F}_2$.

Computing h_N
After applying a sufficiently long input sequence m_k, it turns out that the kernel of $\mathcal{L}_N$ is one-dimensional meaning that the resulting embedded data matrix $\mathcal{L}_N$ fulfills the rank condition (22). The kernel h_N numerically reads after normalization (see Remark 4.1)

$$h_N = [1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0]^T$$

Computing w_n, b_n and the secret key θ
We compute $N = 2$ points w_n so that $w_n^T b_n = 0$. For this example, we do not provide details of the computation. From the kernel vector h_N, we can find out, according to (24), the corresponding parameter vector b_n which numerically reads for $n = 1$ and $n = 2$

$$\begin{array}{l} b_1 = [1, 1, 0, 1, 1]^T \\ b_2 = [1, 1, 1, 1, 1]^T \end{array} \tag{43}$$

From (42) and (43), the secret key $\theta^{(1)} = 0$ and $\theta^{(2)} = 1$ is properly recovered.

6. Conclusion

In this paper, we have proposed a systematic and unified methodology for cryptanalyzing well-known cryptosystems having a hybrid feature, namely chaotic switching, discrete parameter modulation, message-embedding and time-varying delay-based schemes. The proposed approach consists of a specific parameter identification. It applies both for switched systems described over the field of real numbers, as it is the case for chaotic maps, or

over finite fields, in particular for Boolean dynamical systems which are commonly used in the context of digital applications. The complexity of the cryptanalysis has been worked out and provides a new quantitative measure for security assessment. Based on this criterion and having in mind that security is always a question of trade-off between complexity, time analysis and availability of data, we can argue that the existing cryptosystems based on classical chaotic systems are certainly not safe for most of real world applications, at least without any further improvements.

References

Alvarez, G. & Li, S. [2006] "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. of Bifurcations and Chaos* **16**, 2129–2151.

Anstett F., Millérioux G. & Bloch G. [2004] "Global adaptive synchronization based upon polytopic observers," Proc. of the IEEE International symposium on circuit and systems (ISCAS'04), Vancouver, Canada, May.

Anstett F., Millérioux G. & Bloch G. [2006] "Chaotic cryptosystems: Cryptanalysis and identifiability," *IEEE Trans. on Circuits and Systems : Regular papers* **53**, 2673–2680.

Banerjee S. [2010] *Chaos Synchronization and Cryptography for Secure Communications: Applications for Encryption* (IGI Global).

Buchberger B. [1965] *An algorithm for finding a basis for the residue class ring of zero-dimensional polynomial ideal* (PhD thesis, Math. Inst. Univ. of Innsbrück, Austria).

Carlet C. [2010] *Boolean Models and Methods in Mathematics, Computer Science, and Engineering* (Cambridge Press).

Cuomo K. M., Oppenheim A. V. & Strogatz S. H. [1993] "Synchronization of lorenz-based chaotic circuits with applications to communications," *IEEE Trans. Circuits. Syst. II: Anal. Digit. Sign. Process* **40**, 626–633.

Dedieu H., Kennedy M. P. & Hasler M. [1993] "Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing chua's circuits," *IEEE Trans. Circuits. Syst. II: Anal. Digit. Sign. Process* **40**, 634–642.

Dedieu H. & Ogorzalek M. [1997] "Identification of chaotic systems based on adaptive synchronization," Proc. of the European Conference on Circuit Theory and Design (ECCTD'97), Budapest, Hungary, September.

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

Egerstedt M. & Mishra B. [2008] *Proc. of the 11th International Workshop on Hybrid Systems: Computation and Control (HSCC 2008)* (LNCS, Springer).

Fradkov A. L. & Markov A. Y. [1997] "Adaptive synchronization of chaotic systems based on speed-gradient method and passification," *IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl* **44**, 905–912.

Harris J. [1995] *Algebraic Geometry: A First Course* (Berlin, New York: Springer-Verlag).

Hasler M. [1998] "Synchronization of chaotic systems and transmission of information," *International Journal of Bifurcation and Chaos* **8**, 647–659.

Huijberts H. J. C., Nijmeijer H. & Willems R. [2000] "System identification in communication with chaotic systems," *IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl* **47**, 800–808.

Jiang Z-P. [2002] "A note on chaotic secure communication systems," *IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl* **49**, 92–96.

Kelber K. & Schwarz W. [2005] "General design rules for chaos-based encryption systems," 2005 International Symposium on Nonlinear Theory and its Applications (NOLTA 2005), Bruges, Belgium, October.

Kerkhoff A. [1883] "La cryptographie militaire," *Journal des Sciences Militaires* **9**, 161–191.

Kolumban G., Kennedy M. P. & Chua L. O. [1998] "The role of synchronization in digital communications using chaos - part II: Chaotic modulation and chaotic synchronization," *IEEE Trans.*

Circuits. Syst. I: Fundamental Theo. Appl **45**, 1129–1140.

Lian K-Y. & Liu P. [2000] "Synchronization with message embedded for generalized lorenz chaotic circuits and its error analysis," *IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl* **47**, 1418–1424.

Lidl R. & Niederreiter H. [2008] *Finite fields* (Cambridge University Press).

Millérioux G. & Daafouz J. [2004] "Unknown input observers for message-embedded chaos synchronization of discrete-time systems," *International Journal of Bifurcation and Chaos* **14**, 1357–1368.

Millérioux G., Amigo J. M. & Daafouz J. [2008] "A connection between chaotic and conventional cryptography," *IEEE Trans. on Circuits and Systems I: Regular Papers* **55**, 1695–1703.

Millérioux G. & Mira C. [1998] "Coding scheme based on chaos synchronization from noninvertible maps," *International Journal of Bifurcation and Chaos* **10**, 2019–2029.

Ogorzalek M. J. [1993] "Taming chaos - part I: synchronization," *IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl* **40**, 693–699.

Paoletti S., Garulli A., Roll J. & Vicino A. [2008] "A necessary and sufficient condition for input-output realization of switched affine state space models," Proc. of the IEEE Conf. on Dec. and Control (CDC 2008), Cancún, México, December.

Parlitz U., Chua L. O., Kocarev L., Halle K. S. & Shang A. [1993] "Transmission of digital signals by chaotic synchronization," *International Journal of Bifurcation and Chaos* **2**, 973–977.

Shannon C. E [1949] "Communication theory of secrecy systems," *Bell Systems Tech. Journ.* **28**, 657–715.

Vidal R., Ma Y. & Sastry S. [2003] "An algebraic geometric approach to the identification of a class of linear hybrid systems," Proc. of the 42th IEEE Conference on Decision and Control (CDC 2003), Maui, Hawaii, USA, December.

Wu C. W. & Chua L. O [1993] "A simple way to synchronize chaotic systems with applications to secure communications systems," *International Journal of Bifurcation and Chaos* **3**, 1619–1627.

Yang T., Wu C. W. & Chua L. O. [1993] "Cryptography based on chaotic systems," *IEEE Trans. Circuits. Syst. I: Fundamental Theo. Appl* **44**, 469–472.

Yang T. [2004] "A survey of chaotic secure communication systems," *Int. J. of Computational Cognition* , (available at `http://www.YangSky.com/yangijcc.htm`).

Zheng G., Boutat D., Floquet T. & Barbot J. P. [2008] "Secure data transmission based on multi-input multi-output delayed chaotic system," *International Journal of Bifurcation and Chaos* **18**, 2063–2072.