Message-Embedded Cryptosystems: Cryptanalysis and Identifiability

Floriane Anstett, Gilles Millérioux, Gérard Bloch

Message-Embedded Cryptosystems: Cryptanalysis and Identifiability

Floriane Anstett, Gilles Millerioux and Gérard Bloch*

Abstract

The aim of this paper is to compare two encryption schemes, the standard stream cipher and a so-called message-embedded cryptosystem. The comparison is based on two main aspects. The first aspect deals with the synchronization of the time-varying keys at the transmission side and at the reception side. The second aspect focuses on the cryptanalysis of the encryption algorithms. The cryptanalysis focuses on the system parameter retrieving. For message-embedded cryptosystems, the cryptanalysis is thus treated as a parametric identifiability issue. Two methods, the local state isomorphism approach and the Gröbner bases method, are presented for systems including polynomial nonlinearities. It is shown that these systems are weak against algebraic attack.

1 INTRODUCTION

Since 1993, a lot of methods involving nonlinear dynamic systems in order to mask an information have been proposed, because these systems can exhibit complex behaviors. In particular, the chaotic behaviors can be distinguished by their extreme sensitivity to initial conditions and to model parameters changes. Thus, the signals resulting from chaotic systems are broadband, long-term unpredictable and present random-like statistical properties although they are generated by deterministic systems. That is why, there is likely a connection between the random-look behaviors exhibited by chaotic systems and the required properties like confusion and diffusion of cryptosystems. The chaotic masking [1], the parametric modulation [2], the approach by inclusion [3] (and references therein) have been proposed. An overview of these different methods can be found in [4]. However, very few works have really established the connection between the standard encryption algorithms and those based on the generation of chaotic sequences, except for deep comparative studies in [5][6]. In particular, the cryptanalysis of the chaos-based encryption algorithms is really missing today, although it constitutes an essential step of their validations.

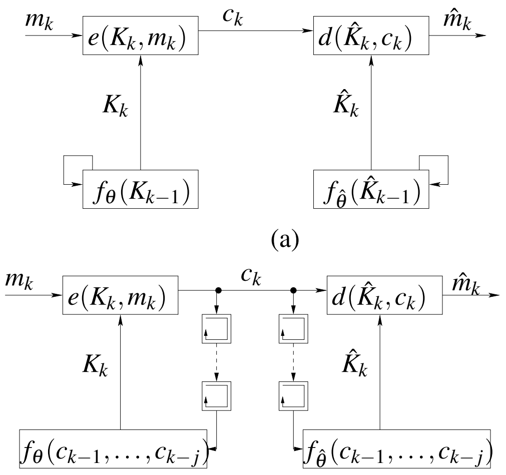
The aim of this paper is to compare two encryption schemes, the standard stream cipher and a so-called message-embedded cryptosystem. The comparison is based on the synchronization of the time-varying keys, also called running keys, at the transmission and at the reception and on the cryptanalysis of the encryption algorithms, studied through the particular problem of the static key reconstruction. In the case of the message-embedded cryptosystem, the cryptanalysis is treated here as a parametric identifiability problem, borrowed from the control theory. Note that the parametric identifiability has been evoked and illustrated for the first time in [7], but, until now, has never been really formalized. The paper is organized as follows. In Section 2.1, we recall the principle of usual stream cipher. Then, in Section 2.2, we present the message-embedded cryptosystem, its principle and the information reconstruction based on observers. Finally, the Section 3 deals with the static key reconstruction problem and with the parametric identifiability. The local state isomorphism approach and the Gröbner bases method are presented for testing the parametric identifiability for the suitable choice of the static key, in the case of systems including polynomial nonlinearities. In Section 4, two examples emphasize the weakness of such systems.

[*] The corresponding authors are with Centre de Recherche en Automatique de Nancy, Université Henri Poincaré - Nancy 1, CRAN - ESSTIN, 2 Rue Jean Lamour 54519 Vandoeuvre Les Nancy Cedex, France, Email : floriane.anstett@esstin.uhp-nancy.fr, gilles.millerioux@esstin.uhp-nancy.fr, gerard.bloch@esstin.uhp-nancy.fr

2 Principles of Encryption: Comparison

2.1 Usual Stream Cipher

There exists two common classes of stream cipher, one is called synchronous and the other self-synchronous [8]. They are respectively illustrated on the Figures 1(a) and 1(b).



m_k
$e(K_k,m_k)$
c_k
$d(\hat{K}_k,c_k)$
$\hat{m}_k$
K_k
$\hat{K}_k$
$f_\theta(K_{k-1})$
$f_{\hat{\theta}}(\hat{K}_{k-1})$
$f_\theta(c_{k-1},\dots,c_{k-j})$
$f_{\hat{\theta}}(c_{k-1},\dots,c_{k-j})$

(a)

(b)

Figure 1: Stream cipher: (a) synchronous, (b) self-synchronous

2.1.1 Transmitter and encryption

The synchronous stream cipher obeys, at the transmitter side:

$$\left\{\begin{array}{l} K_k = f_\theta(K_{k-1}) \\ c_k = e(K_k,m_k) \end{array}\right. \tag{1}$$

In this encryption scheme, the information signal, also called the *plaintext*, is divided into blocks of same length, called symbols and denoted by m_k. The encryption transformation e can change for each symbol since e depends on a time-varying key K_k which is called *keystream*. The keystream K_k is generated by a function f_θ, parameterized by a constant θ. Usually, the plaintext m_k and the ciphertext c_k are binary words, the function e is a simple XOR operation. If the running key K_k is randomly chosen and never used again, the encryption scheme is called *"one-time pad"*. Generally, the running key is generated iteratively by feedback shift registers which produce pseudo-random sequences, as, for instance, the Linear Feedback Shift Registers (LFSR). The ciphertext c_k is available at the transmitter output.

The self-synchronous stream cipher obeys, at the transmitter side:

$$\left\{\begin{array}{l} K_k = f_\theta(c_{k-1},\dots,c_{k-l}) \\ c_k = e(K_k,m_k) \end{array}\right. \tag{2}$$

f_θ is a function parameterized by the constant parameter θ, which generates the keystream K_k. Unlike the synchronous stream cipher, K_k does not depend on an internal dynamic but only on a fixed number of past values of c_k. However, as previously, c_k is generated by the encryption transformation e which combines the running key K_k and the plaintext m_k.

2.1.2 Receiver and reconstruction of the plaintext

For the usual stream cipher, the reconstruction of the plaintext requires the synchronization of the sequences of the running keys at the transmission and at the reception. At the receiver side, the decryption process is described, in the synchronous case, by:

$$\left\{\begin{array}{l} \hat{K}_k = f_{\hat{\theta}}(\hat{K}_{k-1}) \\ \hat{m}_k = d(\hat{K}_k,c_k) \end{array}\right. \tag{3}$$

and, in the self-synchronous case, by:

$$\left\{\begin{array}{l} \hat{K}_k = f_{\hat{\theta}}(c_{k-1},\dots,c_{k-l}) \\ \hat{m}_k = d(\hat{K}_k,c_k) \end{array}\right. \tag{4}$$

In both cases, the decryption transformation d is such that $\hat{m}_k = m_k$ if $\hat{K}_k = K_k$. For the synchronous stream cipher, the sequence $\{K_k\}$ resulting from autonomous recurrences, the key generators f_θ at both sides have to be initialized at the same value ($\hat{K}_0 = K_0$). This initial value K_0 can be considered as a static key. At the contrary, for the self-synchronous stream cipher, the sequences of the running key synchronize automatically.

2.2 Message-Embedded Cryptosystem

2.2.1 Transmitter and encryption

Generally, the message-embedded cryptosystem [3] obeys, at the transmitter side:

$$\Sigma_\theta \left\{ \begin{array}{l} x_{k+1} = f_\theta(x_k, m_k) \\ y_k = h_\theta(x_k, [m_k]) \end{array} \right. \qquad (5)$$

where $x_k \in \mathbb{R}^n$, $m_k \in \mathbb{R}$ and $y_k \in \mathbb{R}$. $[m_k]$ means that h_θ can depend on m_k but not necessary. The principle of the message embedded cryptosystem is illustrated on Figure 2.

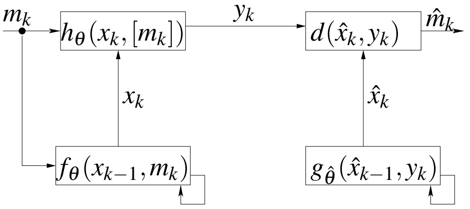


Figure 2: Message-Embedded Cryptosystem

Each symbol m_k is embedded in a sequence $\{x_k\}$ generated by a nonlinear chaotic map f_θ, where $\theta \in \Theta$ is a constant parameter. The most common nonlinearities f_θ are of polynomial type (Henon map, Logistic map, ...), or of linear piecewise type (Markov map). Only the quantity y_k is available at the transmitter output, x_k being an internal state which is not directly transmitted to the receiver.

2.2.2 Receiver and reconstruction of the plaintext

At the receiver side, the decryption process is described by:

$$\left\{ \begin{array}{l} \hat{x}_{k+1} = g_{\hat{\theta}}(\hat{x}_k, y_k) \\ \hat{m}_k = d(\hat{x}_k, \underline{y_k}) \end{array} \right. \qquad (6)$$

where $\underline{y_k}$ denotes a "window" of delayed outputs and of length to be determined.

The decryption transformation d is such that $\hat{m}_k = m_k$ if $\hat{x}_k = x_k$. However, it is not necessary here that the key generators at both sides are initialized to the same initial state x_0. Indeed, g is chosen such that, if $\hat{\theta} = \theta$, then $\hat{x}_k = x_k$, for all $\hat{x}_0$ and independently of m_k. More precisely, we ensure either an asymptotic convergence:

$$\lim_{k\to\infty} \|x_k - \hat{x}_k\| = 0 \quad \forall \hat{x}_0, \forall m_k \qquad (7)$$

or a finite-time convergence:

$$\exists k_f, \|x_k - \hat{x}_k\| \quad \forall \hat{x}_0, \forall m_k, \forall k > k_f \qquad (8)$$

Particular structures of g ensuring a so-called *Information Independent Global Synchronization* (IIGS) have been introduced for encryption purposes in [3][9][10]. In [3][10], the synchronization of x_k and $\hat{x}_k$ is formulated as a state reconstruction problem. An unknown input observer is proposed for g in (6). Its design is recalled below.

We consider a particular structure for the system (5), where f_θ and h_θ are some functions charaterized by the matrices, $\mathscr{A}_\theta \in \mathbb{R}^{n\times n}$, $B_\theta \in \mathbb{R}^{n\times 1}$ and $C_\theta \in \mathbb{R}^{1\times n}$, such that:

$$\left\{ \begin{array}{l} x_{k+1} = \mathscr{A}_\theta(\rho_k)x_k + B_\theta m_k \\ y_k = C_\theta x_k \end{array} \right. \qquad (9)$$

where $\rho_k = q(y_k)$ with q a nonlinear function of y_k. These systems are known as LPV (*Linear Parameter Varying*) systems and ρ_k is assumed to be available through the output. The matrices depend on a constant parameter vector $\theta = [\theta_1, \ldots, \theta_L]^T \in \Theta$. Actually, this structure is not very conservative because a specificity of usual chaotic systems including a nonlinearity of polynomial or linear piecewise type is that $\mathscr{A}_\theta$ can always be expressed in the following polytopic form [3]:

$$\left\{ \begin{array}{l} \mathscr{A}_\theta(\rho_k) = \sum_{i=1}^N \xi_k^{(i)}(\rho_k) A_\theta^{(i)} \\ \\ \sum_{i=1}^N \xi_k^{(i)}(\rho_k) = 1 \\ \\ \xi_k^{(i)}(\rho_k) \geq 0, \forall i, \forall k \end{array} \right. \qquad (10)$$

where the $A_\theta^{(i)}$'s are constant matrices.
In order to ensure the reconstruction of the internal state x_k, the function g has a structure of an unknown input polytopic observer, described by:

$$\hat{x}_{k+1} = (P\mathscr{A}_\theta - \mathscr{K}C_\theta)\hat{x}_k + \mathscr{K}y_k + Qy_{k+1} \qquad (11)$$

where P, $\mathscr{K}$ and Q are gain matrices which have to fulfill (7) or (8).
The stability conditions of the scheme (9)-(11) are given by the following theorem:

Theorem 1 *[3] The encryption scheme (9)-(11) is IIGS whenever the following conditions are satisfied:*

- *rank(CB) = rank(B) = 1*

- *there exists $S_i > 0$, $S_j > 0$, G_i and F_i, such that the following set of linear matrix inequalities:*

$$\begin{bmatrix} G_i + G_i^T - S_i & G_i^T P A_\theta^{(i)} - F_i^T C_\theta \\ (PA_\theta^{(i)})^T G_i - C_\theta^T F_i & S_j \end{bmatrix} > 0 \qquad (12)$$

is feasible $\forall (i,j) \in \{1,\ldots,N\} \times \{1,\ldots,N\}$.

Remark 1 *The rank condition means that the relative degree of (9) has to be equal to 1, which is not conservative in practice.*

In [11], it has been proved that the conservatism of the stability conditions (12) can be reduced by considering the vertices $A_\theta^{(i)}$ of the minimal polytope including ρ_k, which are functions of the chaotic attractor. Thus, this polytopic observer can be an alternative, for example, to the well-known Extended Kalman Filter which does not take into account the chaos specificities.

The reconstruction of the information m_k at each iteration k is then given by:

$$\hat{m}_k = (C_\theta B_\theta)^{-1}(y_{k+1} - C\mathscr{A}_\theta \hat{x}_k) \qquad (13)$$

and $\hat{m}_k = m_k$ if $\hat{x}_k = x_k$.

According to (13), the reconstruction of the plaintext m_k requires the knowledge of the internal state vector x_k although it is not transmitted. Since x_k is essential to retrieve m_k, x_k plays the role of a running key. To reconstruct x_k, from (11), it is clear that the system parameter θ is necessary and θ is considered as the static key.

An advantage of this method compared to the usual stream cipher is that whenever the synchronization is lost accidentally, an automatic resynchronization is ensured.

3 Cryptanalysis

Cryptanalysis is the science of studying attacks against cryptosystems in order to reveal their possible weakness.

For the standard stream cipher, according to (3) for the synchronous case and to (4) for the self-synchronous case, the plaintext m_k reconstruction requires the synchronization of the sequences $\{K_k\}$ and $\{\hat{K}_k\}$ acting as the running keys.

The generation of these sequences by LFSR is a common mecanism for synchronous stream cipher. Nevertheless, Massey [12] has proved that the reconstruction of a whole sequence can be achieved from the knowledge of a fragment whose length is fixed and linked to the linear complexity of the LFSR. This is an example of weakness. Indeed, the pseudo-random sequence can be retrieved by carrying out a known plaintext attack, which consists in choosing a segment of the plaintext m_k and in analysing the corresponding ciphertext c_k. Thus, it is worth noting that forcing m_k to 0 in (1) or in (2), e being the XOR operation, we obtain $K_k = c_k$ which is available at the output. The analysis of the sequence $\{K_k\}$ can then allow to retrieve the initial condition K_0 of K_k (see 2.1.2), which is the static key.

For the message-embedded cryptosystem, we consider the so-called known plaintext attack, i.e, the eavesdropper is supposed to know a sequence of $\{m_k\}$ and the corresponding $\{y_k\}$. To retrieve m_k, an eavesdropper cannot analyse the sequence $\{x_k\}$ since, even if $m_k = 0$, x_k does not appear at the output. We admit that the eavesdropper has no other strategy than trying all the possible static keys θ (brute force attack or exhaustive search) and analyzing the corresponding pairs (m_k, y_k). Thus, the most difficult situation for the eavesdropper is that there exists a unique θ that generates y_k from m_k. The unicity of θ can be formulated in terms of the parametric identifiability whose some basics are recalled below.

The following definition is borrowed from [13].

Definition 1 *The system* Σ_θ *is* structurally globally identifiable *if for almost any* $\hat{\theta} \in \Theta$, $\Sigma_{\hat{\theta}} = \Sigma_\theta \Rightarrow \hat{\theta} = \theta$.

The system Σ_θ *is* structurally locally identifiable *if for almost any* $\hat{\theta} \in \Theta$*, there exists a neighbourhood* $v(\theta)$ *such that* $\hat{\theta} \in v(\theta)$ *and* $\Sigma_{\hat{\theta}} = \Sigma_\theta \Rightarrow \hat{\theta} = \theta$.

The system Σ_θ *is* structurally unidentifiable *if for almost any* $\hat{\theta} \in \Theta$*, there is no neighbourhood* $v(\theta)$ *such that* $\hat{\theta} \in v(\theta)$ *and* $\Sigma_{\hat{\theta}} = \Sigma_\theta \Rightarrow \hat{\theta} = \theta$.

Several methods for testing the parametric identifiability exist as the Taylor series expansion [14], the local state isomorphism approach [15] and the Gröbner bases method [16]. We only describe here the local state isomorphism approach and the Gröbner bases method.

3.1 Local state isomorphism approach

Consider the general system expressed as:

$$\begin{cases} x_{k+1} = f_\theta^{(1)}(x_k) + m_k f_\theta^{(2)}(x_k) \\ y_k = h(x_k) \end{cases} \tag{14}$$

where $f_\theta^{(1)}$ and $f_\theta^{(2)}$ are nonlinear functions of x_k and $\theta = [\theta_1, \ldots, \theta_L]^T \in \Theta$. The initial condition of x_k is denoted by $x_0(\theta)$.

Remark 2 *For the systems of the form (9) considered in the Section 2.2.2, $f_\theta^{(2)} = B_\theta$ where B_θ is a constant matrix.*

Consider the system (14). Assume that Σ_θ is locally reduced at $x_0(\theta)$ for almost any $\theta \in \Theta$, that is, it satisfies both the controllability rank condition and the observability rank condition [17]. The following proposition establishes a *condition* for global identifiability of system (14), as a discrete counterpart of the theorem found in [15].

Proposition 1 *Σ_θ and $\Sigma_{\hat\theta}$ have the same input-output behavior for any m_k if and only if there exists a local state isomorphism ϕ, defined by $x_k \in v(x_0) \mapsto \phi(x_k) \in \mathbb{R}^n$, such that, for any x_k in the neighborhood $v(x_0)$, the following conditions are satisfied:*

$$\begin{aligned} &(i) && rank(\tfrac{\partial\phi(x_k)}{\partial x_k^T}) = n, \\ &(ii) && \phi(x_0(\hat\theta)) = x_0(\theta), \\ &(iii) && f_{\hat\theta}^{(1)}(\phi(x_k)) = \tfrac{\partial\phi(x_k)}{\partial x_k^T} f_\theta^{(1)}(x_k), \\ &(iv) && f_{\hat\theta}^{(2)}(\phi(x_k)) = \tfrac{\partial\phi(x_k)}{\partial x_k^T} f_\theta^{(2)}(x_k), \\ &(v) && h_{\hat\theta}(\phi(x_k)) = h_\theta(x_k). \end{aligned} \tag{15}$$

These conditions express that ϕ is a diffeomorphism (i), the initial states coincide (ii), the dynamic terms coincide (iii), the control terms coincide (iv) and the observation terms coincide (v).

After checking that Σ_θ is locally reduced at $x_0(\theta)$, one can look for all solutions for $\hat\theta$ and ϕ of (15). If, for almost any θ, the only possible solution is $\hat\theta = \theta$ and $\phi(x_k) = x_k$, then Σ_θ is globally identifiable.

In the case $f_\theta^{(1)}$ and $f_\theta^{(2)}$ are polynomials in x_k, parameterized by θ, and $h_\theta(x_k) = C_\theta x_k$, ϕ can directly be written as a linear transformation $\phi(x_k) = Tx_k$, which simplifies the calculations. Hence, the Proposition 1 turns into:

Proposition 2 *Σ_θ and $\Sigma_{\hat\theta}$ have the same input-output behavior for any m_k if and only if there exists a linear transformation T such that the following conditions are satisfied:*

$$\begin{aligned} &(i) && det(T) \neq 0, \\ &(ii) && Tx_0(\hat\theta) = x_0(\theta), \\ &(iii) && f_{\hat\theta}^{(1)}(Tx_k) = Tf_\theta^{(1)}(x_k), \\ &(iv) && f_{\hat\theta}^{(2)}(Tx_k) = Tf_\theta^{(2)}(x_k), \\ &(v) && C_{\hat\theta}T = C_\theta. \end{aligned} \tag{16}$$

If, for almost any θ, the only possible solution is $\hat\theta = \theta$ and $T = I$ where I is the identity matrix of dimension n, then Σ_θ is globally identifiable.

Note that Propositions 1 and 2 are just conjectures.

Another approach to test the parametric identifiability is the Gröbner bases method, exposed in the next section.

3.2 Gröbner bases approach

In order to test the parameter identifiability, we want to obtain an input/output relation, with the general form:

$$\mathscr{L}_\theta(y_k, y_{k+1}, \ldots, m_k, m_{k+1}, \ldots) = 0 \tag{17}$$

with $\mathscr{L}_\theta$, a function parameterized by θ.

To this end, the internal state x_k must be eliminated and hence is considered as indeterminate. The elimination can be achieved thanks to the method of the Gröbner bases, borrowed from algebra. The first algorithm of this type is due to [16]. Some notions of differential algebra can be found in [18] for continous-time systems. However, they can equally be defined with the derivative operator (continous-time case) or with the delay operator (discrete-time case). Some recalls in the case of discrete-time systems are carried out below.

Consider a system Σ_θ of the polynomial ring, denoted by $\mathbb{A} = \mathbb{R}[x_k^{(1)}, \ldots, x_k^{(n)}]$ where the indeterminates are $x_k^{(1)}, \ldots, x_k^{(n)}$ and the coefficients are real numbers.

Definition 2 *An* ideal *of $\mathbb{A}$ is a subset I of $\mathbb{A}$, such that:*

$$\begin{aligned} &- \quad \forall p \in I, \forall q \in I, p+q \in I \\ &- \quad \forall p \in I, \forall g \in I, pg \in \mathbb{A} \end{aligned} \tag{18}$$

Definition 3 *The ideal, generated by the system with polynomial nonlinearities Σ_θ (5), in $\mathbb{A}$, is the set of all linear combinations of the elements of Σ_θ with any elements of $\mathbb{A}$ for coefficients.*

Definition 4 *A* lexicographic order *is a ranking according to the names of the variables and their iterates such that:*

$$\begin{aligned} &- \quad x_k^{(i)} < x_{k+l}^{(i)}, \forall l \in \mathbb{N}^+, \\ &- \quad x_k^{(i)} < x_{k+l}^{(i)} \Rightarrow x_{k+l}^{(i)} < x_{k+l+t}^{(i)}, \forall l \in \mathbb{N}^+, \forall t \in \mathbb{N}^+, \\ &- \quad x_k^{(i)} < x_k^{(j)} \Rightarrow (x_k^{(i)})^\alpha < (x_k^{(j)})^\beta, \forall \alpha \in \mathbb{N}^+, \forall \beta \in \mathbb{N}^+ \end{aligned} \tag{19}$$

The variables to be eliminated are considered as the greatest.

If a given pair (m_k, y_k) satisfies (5), it will also satisfy equations that are obtained by addition and by multiplication of (5), that is the ideal generated by (5). For a given lexicographic order, it then suffices to find a basis of this ideal whose expressions do no longer contain the variables x_k, but only contain y_k, m_k, their iterates and θ. These expressions of the basis are of the required form (17). Such a basis is called a *Gröbner basis*. A more formal definition of the Gröbner bases can be found in [16] and a theorem of variable elimination based on this method is detailed in [19]. After obtaining the relation (17) thanks to the Gröbner basis method, the following theorem formulates a *necessary and sufficient condition* for parameter global identifiability.

Theorem 2 *[20] The parameter vector θ is globally identifiable if and only if the equations (17) can be rearranged in a linear regression such that, parameter by parameter:*

$$P_i(y_k, m_k)\theta_i - Q_i(y_k, m_k) = 0 \quad i = 1, \ldots, L \tag{20}$$

where P_i and Q_i are polynomials depending only on y_k, m_k, and on their iterates, and L =dim(θ).

Discussion

3.2.1 Brute force attack

If the equation (17) admits several possible solutions for the parameter θ_i, θ_i is not identifiable. In this case, an eavesdropper has a favorable chance to find θ_i by a brute force attack because several solutions are possible for θ_i. Thus, the parameter θ_i is a bad candidate to play the role of the static key.
If the equation (17) admits a unique solution for θ_i, then it is more difficult for the eavesdropper to find θ_i from (17) by an exhaustive search. Consequently, the parameter θ_i may be a good candidate to play the role of the static key against a brute force attack.

3.2.2 Algebraic attack

Contrarily to the brute force attack, if the eavesdropper knows the structure of the algorithm, (20) highlights the fact that he is able to retrieve easily the parameters. Indeed, he must solve a system with L linear equations with L unknowns. Solving (20) is a kind of algebraic attack.

A fundamental conclusion derived from this analysis is that cryptosystems involving only polynomial nonlinearities (for which Gröbner bases are dedicated) are weak against algebraic attacks.

4 Illustrative examples

4.1 Example 1

Consider the message-embedded cryptosystem which obeys, at the transmitter side:

$$\begin{cases} x_{k+1}^{(1)} = ax_k^{(1)} - bx_k^{(2)} \\ x_{k+1}^{(2)} = bx_k^{(1)} + \theta_1 x_k^{(2)} + \theta_2 (x_k^{(2)})^2 + \theta_3 (x_k^{(2)})^3 + m_k \\ y_k = x_k^{(2)} \end{cases} \tag{21}$$

where m_k represents the plaintext.

4.1.1 Local state isomorphism approach

It can be shown that system (21) is locally reduced at $x_0(\theta)$ for all $\theta \in \Theta$. The system (21) has polynomial nonlinearities and $h_\theta(x_k) = x_k^{(2)}$. Hence, the local state isomorphism ϕ can be written as a linear transformation $\phi(x_k) = Tx_k$. Let define the matrix T, with $t_i \in \mathbb{R}$, as:

$$T = \begin{bmatrix} t_1 & t_2 \\ t_3 & t_4 \end{bmatrix} \tag{22}$$

with det(T)$\neq 0$. The conditions (16)-(v) and (16)-(iv) implies respectively that $t_3 = 0$, $t_4 = 1$ and, $t_2 = 0$. Condition (16)-(iii) implies:

$$at_1 x_k^{(1)} - bx_k^{(2)} = t_1(ax_k^{(1)} - bx_k^{(2)}) \tag{23}$$

$$\begin{aligned} &bx_k^{(1)} + \hat{\theta}_1 x_k^{(2)} + \hat{\theta}_2 (x_k^{(2)})^2 + \hat{\theta}_3 (x_k^{(2)})^3 = \\ &bx_k^{(1)} + \theta_1 x_k^{(2)} + \theta_2 (x_k^{(2)})^2 + \theta_3 (x_k^{(2)})^3 \end{aligned} \tag{24}$$

The equation (23) leads to $t_1 = 1$. The equation (24) is equivalent to:

$$(\hat{\theta}_1 - \theta_1)x_k^{(2)} + (\hat{\theta}_2 - \theta_2)(x_k^{(2)})^2 + (\hat{\theta}_3 - \theta_3)(x_k^{(2)})^3 = 0 \tag{25}$$

which implies that $\hat{\theta}_1 = \theta_1$, $\hat{\theta}_2 = \theta_2$ and $\hat{\theta}_3 = \theta_3$, assuming that $x_k^{(2)} \neq 0$. Consequently, the matrix T reduces to the identity matrix of dimension 2. Hence, θ_1, θ_2 and θ_3 are globally identifiable.

4.1.2 Gröbner bases approach

Since $x_k^{(1)}$ is not directly transmitted through the signal y_k, it is chosen to be the greatest and the corresponding lexicographic order is:

$$x_k^{(2)} < x_{k+1}^{(2)} < x_{k+2}^{(2)} < x_k^{(1)} < x_{k+1}^{(1)} < x_{k+2}^{(1)} \tag{26}$$

The ideal of the Gröbner basis generated by the system (21), with the lexicographic order (26), is:

$$\begin{aligned} &y_{k+2} + \theta_1(ay_k - y_{k+1}) + \theta_2(ay_k^2 - y_{k+1}^2) + \theta_3(ay_k^3 - y_{k+1}^3) - \\ &ay_{k+1} - b^2 y_k + am_k - m_{k+1} = 0 \end{aligned} \tag{27}$$

By iterating the equation (27), we get a system of linear equations with three unknowns θ_1, θ_2 and θ_3. We can then write three expressions of the form:

$$\begin{aligned} P_1(y_k, m_k)\theta_1 - Q_1(y_k, m_k) = 0 \\ P_2(y_k, m_k)\theta_2 - Q_2(y_k, m_k) = 0 \\ P_3(y_k, m_k)\theta_3 - Q_3(y_k, m_k) = 0 \end{aligned} \tag{28}$$

So, Theorem 2 is fulfilled for each parameter and the same conclusion is reached as with the local state isomorphism approach: the parameters θ_1, θ_2 and θ_3 are globally identifiable. Hence, against brute force attack, θ_1, θ_2 and θ_3 may play the role of the static key. On the other hand, it is easy to solve the system (28), highlighting the weakness of the cryptosystem (21) against algebraic attack.

4.2 Example 2

Consider now the message-embedded cryptosystem where the plaintext m_k is embedding in the Henon map:

$$\begin{cases} x_{k+1}^{(1)} = \theta_1 (x_k^{(1)})^2 + \theta_2 x_k^{(2)} + m_k \\ x_{k+1}^{(2)} = \theta_3 x_k^{(1)} + \theta_4 m_k \\ y_k = x_k^{(1)} \end{cases} \tag{29}$$

This example is only treated through the Gröbner bases method.
Since $x_k^{(2)}$ is not directly transmitted through the signal

y_k, it is chosen to be the greatest and the corresponding lexicographic order is:

$$x_k^{(1)} < x_{k+1}^{(1)} < x_{k+2}^{(1)} < x_k^{(2)} < x_{k+1}^{(2)} < x_{k+2}^{(2)} \qquad (30)$$

The ideal of the Gröbner basis generated by the system (29), with the lexicographic order (30), is:

$$\theta_1 y_{k+1}^2 + \theta_2\theta_3 y_k - y_{k+2} + m_{k+1} + \theta_2\theta_4 m_k = 0 \qquad (31)$$

By iterating the equation (31), we get three expressions of the form:

$$\begin{aligned} P_1(y_k, m_k)\theta_1 - Q_1(y_k, m_k) = 0 \\ P_2(y_k, m_k)\theta_2\theta_3 - Q_2(y_k, m_k) = 0 \\ P_3(y_k, m_k)\theta_2\theta_4 - Q_3(y_k, m_k) = 0 \end{aligned} \qquad (32)$$

Theorem 2 is satisfied for θ_1 and the products $\theta_2\theta_3$ and $\theta_2\theta_4$. θ_1, the products $\theta_2\theta_3$ and $\theta_2\theta_4$ are globally identifiable, but not the parameters θ_2, θ_3 and θ_4 themselves. As there is several possible solutions for θ_2, θ_3 and θ_4, they are bad candidates for the static key against brute force attacks.

5 Conclusion

This paper has carried out a comparison between two encryption schemes, the standard stream cipher and the message-embedded cryptosystem. The comparison was focused, on one hand, on the synchronization of the running key sequences and, on the other hand, on the cryptanalysis of the encryption algorithms. The cryptanalysis has been studied through the reconstruction of the transmitter static parameter. A formalism based on the parametric identifiability has been proposed in the case of the message-embedded cryptosystem. As a result, the identifiable parameters are good candidates to play the role of the static key against brute force attack. However, they can easily be retrieved by performing an algebraic attack. A fundamental conclusion is that the cryptosystems involving only polynomial nonlinearities are weak against algebraic attacks.

References

[1] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, “Synchronization of Lorenz-based chaotic circuits with applications to communications,” *IEEE Trans. Circuits Syst. II: Anal. Digit. Sign. Process.*, vol. 40, no. 10, pp. 626–633, 1993.

[2] H. Dedieu, M. P. Kennedy, and M. Hasler, “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.*, vol. 40, pp. 634–642, 1993.

[3] G. Millérioux and J. Daafouz, “Unknown input observers for message-embedded chaos synchronization of discrete-time systems,” *International Journal of Bifurcation and Chaos*, vol. 14, no. 4, pp. 1357–1368, April 2004.

[4] T. Yang, “A survey of chaotic secure communication systems,” *International Journal of Computational Cognition*, vol. 2, no. 2, pp. 81–130, 2004, disponible à http://www.YangSky.com/yangijcc.htm.

[5] F. Dachselt, K. Kelber, J. Vandewalle, and W. Schwarz, “Chaotic versus classical stream ciphers – a comparative study,” in *Proc. of International Symposium on Circuits and Systems, ISCAS’98*, vol. IV, Monterey. 31 May - 3 June, June 1998, pp. 518–521.

[6] L. Kocarev, “Chaos-based cryptography: a brief overview,” *IEEE Circuits Syst. Mag.*, vol. 1, no. 3, pp. 6–21, 2001.

[7] H. Dedieu and M. Ogorzalek, “Identifiability and identification of chaotic systems based on adaptive synchronization,” *IEEE Trans. Circuits Syst. I: Fund. Theo. Appl*, vol. 44, no. 10, pp. 948–962, October 1997.

[8] A. Menezes, P. V. Oorschot, and S. Vanstone, *Handbook of applied cryptography*. CRC Press, October 1996.

[9] U. Feldmann, M. Hasler, and W. Schwarz, “Communication by chaotic signals: the inverse system

approach," *Int. J. of Circuit Theo. Appl.*, vol. 24, pp. 551–579, 1996.

[10] G. Millérioux and J. Daafouz, "An observer-based approach for input independent global chaos synchronization of discrete-time switched systems," *IEEE Trans. Circuits Syst. I: Fund. Theo. Appl*, pp. 1270–1279, October 2003.

[11] G. Millérioux, F. Anstett, and G. Bloch, "Considering the attractor structure of chaotic maps for observer-based synchronization problems," *Mathematics and Computers in Simulation*, vol. 68, no. 1, pp. 67–85, February 2005.

[12] J. L. Massey, "Shift register synthesis and BCH decoding," *IEEE Trans. Inform. Theory*, vol. 15, pp. 122–127, 1969.

[13] E. Walter and L. Pronzato, *Nonlinear Systems*. London, England: Chapmann and Hall, 1993.

[14] H. Pohjanpalo, "System identifiability based on the power series expansion of the solution," *Mathematical Biosciences*, vol. 41, pp. 21–33, 1978.

[15] S. Vajda and H. Rabitz, "State isomorphism approach to global identifiability of nonlinear systems," *IEEE Trans. Automat. Contr.*, vol. 34, no. 2, pp. 220–223, 1989.

[16] B. Buchberger, "An algorithm for finding a basis for the residue class ring of zero-dimensional polynomial ideal," Ph.D. dissertation, Math. Inst. Univ. of Innsbrück, Austria, 1965.

[17] R. Hermann and A. J. Krener, "Nonlinear controllability and observability," *IEEE Trans. on Automatic Control*, vol. 22, no. 5, pp. 728–740, 1977.

[18] F. Boulier, "Etude et implantation de quelques algorithmes en algèbre différentielle," Ph.D. dissertation, Université Lille 1, Laboratoire d'Informatique Fondamentale de Lille, France, 1994.

[19] E. Frisk, "Residual generation for fault diagnosis," Ph.D. dissertation, Linköpings Universitet, Sweden, Nov. 2001.

[20] L. Ljung and T. Glad, "On global identifiability for arbitrary model parametrizations," *Automatica*, vol. 30, no. 2, pp. 265–276, 1994.