On the determination of an input-state-output realization of a secure McEliece-like cryptosystem based on convolutional codes

Joan-Josep Climent, Victoria Herranz, Carmen Perea and Virtudes Tomás

Abstract— **In this paper we present a public key cryptosystem based on the McEliece scheme, but using a convolutional code, instead of a block code. Firstly we present some conditions about the convolutional code $\mathcal{C}$ to construct the public key cryptosystem and then, starting with the parity check matrix H of a good block code, we find an input-state-output representation of $\mathcal{C}$ such that the controllability matrix of $\mathcal{C}$ is H^t. This cryptosystem is constructed so that any user can encrypt a message by introducing the largest number of possible errors.**

I. INTRODUCTION

Technological advances of recent years give us computers with very powerful processors. Due to this fact, many public or private key cryptosystems have become insecure or they have had to increase notoriously the key size in order to keep on being secure [9]. Error correcting codes based cryptosystems are the least influenced. One of the advantages of the code based cryptography is that the high coding and decoding speed helps to reduce the battery waste of cryptographic applications on mobile devices [5]. Another interesting characteristic is that we can build a complete infrastructure from it; one can find identification schemes, signature schemes, and pseudorandom number generators or hash functions [5].

One of these public keys cryptosystems based on error correcting codes is the McEliece cryptosystem. Until now no subexponential order attack to McEliece cryptosystem is know, nor with classic computers neither with quantum ones [5]. The security of this scheme is given by the NP-complexity of decoding general linear block codes [2], [7], [17].

In this paper, in order to introduce secure and efficient public key cryptosystems based on error correcting codes, we present one based on McEliece scheme where we obtain the generator matrix of the block code from the input-state-output representation of a convolutional code.

The rest of the paper is organized as follows. In Section II we introduce the necessary concepts related to convolutional codes, the basic steps for McEliece's cryptosystem, the algebraic decoding algorithm that we use in our cryptosystem and a partial realization problem, which we need to obtain a convolutional code to construct the cryptosystem. The construction of the cryptosystem and the encrypting and decrypting processes are explained in Section III. In Section IV we obtain matrices A and B of the input-state-output representation of a convolutional code to construct a McEliece-like cryptosystem. We analyze the cryptanalysis of the proposed McEliece-like cryptosystem in Section V. Finally in Section VI we show some conclusions and future research work.

II. PRELIMINARIES

A. McEliece cryptosystem

In 1978 McEliece developed a public key cryptosystem based on error correcting codes (see [10], [11]). Although in the beginning the McEliece public key cryptosystem was introduced using a Goppa code, we can describe it using a general block code in the following way:

- The receiver constructs a block code $\mathcal{C}$ with full rank generator matrix G of size $n \times k$ and high minimum distance, i.e., a code which can correct a high number of errors λ. The mathematical structure of the code will provide an efficient correcting algorithm.
- He computes $G' = PGQ$, where Q is an invertible matrix of size $k \times k$ and P is a permutation matrix of size $n \times n$. Then the $n \times k$ matrix G' is apparently the generator matrix of an arbitrary linear code $\mathcal{C}'$ for the one we do not known an efficient decoding algorithm.
- G' is the public key. The sender encrypts an information vector $\boldsymbol{u}$ of length k and gets a word $\boldsymbol{c} = G'\boldsymbol{u} + \boldsymbol{e}$ of length n, where $\boldsymbol{e}$ is an error vector chosen by the sender with $wt(\boldsymbol{e}) \leq \lambda$.
- The receiver knows that $\boldsymbol{c} = G'\boldsymbol{u}+\boldsymbol{e} = PGQ\boldsymbol{u}+\boldsymbol{e}$. He computes $P^{-1}\boldsymbol{c} = GQ\boldsymbol{u} + P^{-1}\boldsymbol{e}$ using the decoding algorithm of the original code $\mathcal{C}$. After eliminating the error vector $P^{-1}\boldsymbol{e}$ he recovers the vector $Q\boldsymbol{u}$ and finally, he recovers the message, which is obtained as $\boldsymbol{u} = Q^{-1}(Q\boldsymbol{u})$.

In 1986, Niederreiter proposed a different scheme which uses Generalized Reed Solomon codes, but Li, Deng and Wang [8] showed that this proposal is equivalent (dual) to McEliece's proposal if one substitute the Generalized Reed Solomon codes by Goppa codes. In 1992, Sidelnikov and Shestakov [16] showed that Niederreiter's proposal with Generalized Reed Solomon codes is insecure.

This work was partially supported by grants MTM2008-06674-C02-01 and MTM2008-06674-C02-02 of Spanish Government. The work of the last author was supported by a grant of the Vicerectorat d'Investigació, Desenvolupament i Innovació of the Universitat d'Alacant for PhD students.

J.J. Climent and V. Tomás are with Departament d'Estadística i Investigació Operativa, Universitat d'Alacant, Ap. Correus 99, E-03080 Alacant, Spain. jcliment@ua.es, vtomas@ua.es

V. Herranz and C. Perea are with the Centro de Investigación Operativa, Departamento de Estadística, Matemáticas e Informática, Universidad Miguel Hernández, Avenida del Ferrocarril, s/n. E-03202 Elche, Spain. mavi.herranz@umh.es, perea@umh.es

B. Convolutional codes

In the following we consider $\mathbb{F}$ as a finite field. We define an (n, k, δ) convolutional code $\mathcal{C}$ with rate k/n as a submodule of $\mathbb{F}^n[z]$, that we can describeb by the linear system

$$\left.\begin{array}{rcrcr} \boldsymbol{x}_{t+1} & = & A\boldsymbol{x}_t & + & B\boldsymbol{u}_t \\ \boldsymbol{y}_t & = & C\boldsymbol{x}_t & + & D\boldsymbol{u}_t \end{array}\right\}, \quad t = 0, 1, 2, \ldots \qquad (1)$$

$$\boldsymbol{v}_t = \begin{bmatrix} \boldsymbol{y}_t \\ \boldsymbol{u}_t \end{bmatrix}, \quad \boldsymbol{x}_0 = 0,$$

where A, B, C and D are matrices of sizes $\delta \times \delta$, $\delta \times k$, $(n-k) \times \delta$ and $(n-k) \times k$ respectively, $\boldsymbol{x}_t$ is the state vector, $\boldsymbol{y}_t$ is the parity vector, $\boldsymbol{u}_t$ is the information vector and $\boldsymbol{v}_t$ is the code vector. All of them, with entries in $\mathbb{F}$.

We say that the four matrices (A, B, C, D) are the input-state-output representation of the code $\mathcal{C}$. This representation was introduced by Rosenthal, York and Schumacher [14] and it has been widely used in the last years to analyze and construct convolutional codes [1], [3], [4], [6], [12], [13], [14], [18].

Let A, B, C be scalar matrices over $\mathbb{F}$ of sizes $\delta \times \delta$, $\delta \times k$ and $(n-k) \times \delta$, respectively. Let j be a positive integer and define

$$\Phi_j(A, B) = \begin{bmatrix} A^{j-1}B & A^{j-2}B & \cdots & AB & B \end{bmatrix}$$

and

$$\Omega_j(A, C) = \begin{bmatrix} C \\ CA \\ \vdots \\ CA^{j-2} \\ CA^{j-1} \end{bmatrix}.$$

Matrices $\Phi_j(A, B)$ and $\Omega_j(A, C)$ will be needed in the rest of the paper.

Remember that (A, B) is called a controllable pair if $\operatorname{rank}(\Phi_\delta(A, B)) = \delta$. Similarly, (A, C) is called an observable pair if $\operatorname{rank}(\Omega_\delta(A, C)) = \delta$. Moreover, we consider the matrix of the local description of trajectories

$$\mathcal{T}_j = \begin{bmatrix} D & O & \ldots & O & O \\ CB & D & \ldots & O & O \\ \vdots & \vdots & & \vdots & \vdots \\ CA^{j-2}B & CA^{j-3}B & \ldots & D & O \\ CA^{j-1}B & CA^{j-2}B & \ldots & CB & D \end{bmatrix}$$

for $j = 0, 1, 2, \ldots$.

Finally, given a matrix $X \in \mathbb{F}^{\delta \times \delta k}$ of $\operatorname{rank}(X) = \delta$, we say that X is realizable if there exist matrices A and B, of sizes $\delta \times \delta$ and $\delta \times k$, respectively such that $X = \Phi_\delta(A, B)$.

C. Algebraic decoding algorithm for convolutional codes

Rosenthal [12] propose an iterative algebraic decoding algorithm that decodes convolutional codes with a certain underlying algebraic structure. We use this algorithm to complete the decoding of the public key cryptosystem that we propose.

The idea is that with a received sequence of length T, a positive integer Θ and a known initial state vector $\boldsymbol{x}_\tau$, we can compute the state vector $\boldsymbol{x}_{\tau+T-\Theta}$ and the errors that occur between the instants τ and $\tau + T - \Theta$, recovering then the original sequence. Moreover, as in algebraic decoding algorithms for block codes, we need that the convolutional code holds certain conditions concerning to the algebraic structure. It can not be efficiently applied to arbitrary convolutional codes. Later on we will explain the steps with more detail. The conditions that the code must hold are the following:

1) $\Phi_{T-\Theta+1}(A, B)$ must have full rank δ. So, $\ker(\Phi_{T-\Theta+1}(A, B))$ is the block code whose parity check matrix is $\Phi_{T-\Theta+1}(A, B)$.
2) $d_1 = d(\ker(\Phi_{T-\Theta+1}(A, B))) > 3$, in order that the correcting error capability of the code $\ker(\Phi_{T-\Theta+1}(A, B))$ is at least 1.
3) $\Omega_\Theta(A, C)$ must have full rank δ.
4) $T > 2\Theta > 0$, in order to be able to introduce at least 1 error.
5) D must have no zero column.

We also need that $wt(\boldsymbol{e}) \leq \lambda$, where $\boldsymbol{e}$ is the error vector that occurs in a received sequence of length T and

$$\lambda = \min\left(\left\lfloor \frac{d_1 - 1}{2} \right\rfloor, \left\lfloor \frac{T}{2\Theta} \right\rfloor \right).$$

In this situation it is possible to recover the transmitted sequence $\left\{ \begin{bmatrix} \boldsymbol{y}_t \\ \boldsymbol{u}_t \end{bmatrix} \right\}_{t \geq 0}$ in a unique way.

We develop now the decoding process. Let us assume that the receiver has received the message $\widehat{\boldsymbol{v}}_0, \widehat{\boldsymbol{v}}_1, \ldots$ We take a part of the sequence $\widehat{\boldsymbol{v}}_\tau, \widehat{\boldsymbol{v}}_{\tau+1}, \ldots, \widehat{\boldsymbol{v}}_{\tau+T}$, and assume that we have correctly decoded the sequence up to instant $\tau - 1$, which allows us to know $\boldsymbol{x}_\tau$.

If we take the last Θ blocks of the received sequence, it must hold

$$\begin{bmatrix} \widehat{\boldsymbol{y}}_{\tau+T-\Theta+1} \\ \widehat{\boldsymbol{y}}_{\tau+T-\Theta+2} \\ \vdots \\ \widehat{\boldsymbol{y}}_{\tau+T} \end{bmatrix} - \mathcal{T}_{\Theta-1} \begin{bmatrix} \widehat{\boldsymbol{u}}_{\tau+T-\Theta+1} \\ \widehat{\boldsymbol{u}}_{\tau+T-\Theta+2} \\ \vdots \\ \widehat{\boldsymbol{u}}_{\tau+T} \end{bmatrix} = \Omega_\Theta(A, C)\boldsymbol{x}_{\tau+T-\Theta+1}.$$

Applying the decoding algorithm associated to the block code whose generator matrix is $\Omega_\Theta(A, C)$ we recover the state $\boldsymbol{x}_{\tau+T-\Theta+1}$. Once we have obtained $\boldsymbol{x}_{\tau+T-\Theta+1}$ we can compute the error sequence $\boldsymbol{e}_\tau$, $\boldsymbol{e}_{\tau+1}$,. . . $\boldsymbol{e}_{\tau+T-\Theta-1}$ using the decoding algorithm of the block code $\ker(\Phi_{T-\Theta+1}(A, B))$, according to the following relation

$$\Phi_{T-\Theta+1}(A, B) \begin{bmatrix} \widehat{\boldsymbol{u}}_\tau \\ \widehat{\boldsymbol{u}}_{\tau+1} \\ \vdots \\ \widehat{\boldsymbol{u}}_{\tau+T-\Theta} \end{bmatrix} - \boldsymbol{x}_{\tau+T-\Theta+1}$$

$$+ A^{T-\Theta+1}\boldsymbol{x}_\tau = \Phi_{T-\Theta+1}(A, B) \begin{bmatrix} \boldsymbol{e}_\tau \\ \boldsymbol{e}_{\tau+1} \\ \vdots \\ \boldsymbol{e}_{\tau+T-\Theta} \end{bmatrix}$$

and we can recover the original sequence since $\boldsymbol{u} = \widehat{\boldsymbol{u}} - \boldsymbol{e}$. Remember that this sequence will have weight lower than or equal to λ. Due to the fact that we know $\boldsymbol{x}_{\tau+T-\Theta+1}$ we can use this state as initial state to decode the following block.

D. On a partial realization problem

As we have defined in Section II-B, a matrix $X \in \mathbb{F}^{n \times nm}$ is realizable if there exist matrices A and B, of sizes $n \times n$ and $n \times m$, respectively, such that the pair (A, B) is controllable and $X = \Phi_n(A, B)$. So, if we consider

$$X = \left[\begin{array}{cccc} X_1 & X_2 & \cdots & X_n \end{array}\right], \quad X_i \in \mathbb{F}^{n\times m} \qquad (2)$$

then X is realizable if and only if $X_i = A^{n-i}B$, for some controllable pair (A, B).

In order to get conditions ensuring the existence of these matrices, we need the following definition. Given a matrix X of size $n \times nm$ as (2), we define its Hankel structure as $(\mathcal{H}_1(X), \mathcal{H}_2(X), \ldots, \mathcal{H}_n(X))$, where $\mathcal{H}_i(X)$ is the $(n-i+1)n \times im$ matrix given by

$$\mathcal{H}_i(X) = \left[\begin{array}{cccc} X_n & X_{n-1} & \cdots & X_{n-i+1} \\ X_{n-1} & X_{n-2} & \cdots & X_{n-i} \\ \vdots & \vdots & & \vdots \\ X_i & X_{i-1} & \cdots & X_1 \end{array}\right]$$

In the rest of the paper, we adopt the following notation. Given a matrix Y of size $p \times q$, we denote by $Y(:, j : l)$ the submatrix of size $p \times (l - j + 1)$ obtaining from Y taking all files and columns between column j-th and column l-th.

In order to determine the input-state-output representation of a convolutional code to construct a McEliece-like cryptosystem, we need the following result, which ensure us the existence and uniqueness of matrices A and B such that $X = \Phi_n(A, B)$.

Theorem 1 (Proposition 1 of [19]): *Let $X \in \mathbb{F}^{n\times nm}$ and assume that*

$$(\mathcal{H}_1(X), \mathcal{H}_2(X), \ldots, \mathcal{H}_n(X))$$

is the Hankel structure of X. Then X is realizable if and only if there exist non-negative integers $r_1, r_2, \ldots, r_n$ and, for $i = 1, 2, \ldots, n$, index sets $J_i \subseteq \{1, 2, \ldots, m\}$ with $|J_i| = r_i$ such that

1) $J_{i+1} \subseteq J_i$, $i = 1, 2, \ldots, n - 1$.
2) $\operatorname{rank} \mathcal{H}_i(X) = \operatorname{rank} \big(\mathcal{H}_i(X)(:, J_1 \cup (m + J_2) \cup \cdots \cup ((i-1)m+J_i))\big) = r_1+r_2+\cdots+r_i$, *for* $i = 1, 2, \ldots, n$.

The pairs realizing X are controllable if and only if $r_1 + r_2 + \cdots + r_n = n$. Moreover, if $X \in \mathbb{F}^{n\times nm}$ is realizable and $\operatorname{rank}(X) = n$, *then it is realizable by a unique (A, B) if and only if* $\operatorname{rank}(X(:, 1 : m)) = \operatorname{rank} X_1 > 1$.

III. CRYPTOSYSTEM BASED ON MCELIECE SCHEME

In this section we detail the construction of the cryptosystem. The core of the proposal is to construct a convolutional code and structure the message in such a way that the convolutional code can be used in the McEliece scheme similarly to a block code. Next we develop both the encryption process and the decryption process.

Let us take a controllable and observable convolutional code given by its input-state-output representation (A, B, C, D). We construct the local description of trajectories matrix $\mathcal{T}_{T-\Theta}$. If at an instant τ we have $\boldsymbol{x}_\tau = \boldsymbol{0}$, then

$$\left[\begin{array}{c} \boldsymbol{y}_\tau \\ \boldsymbol{y}_{\tau+1} \\ \vdots \\ \boldsymbol{y}_{\tau+T-\Theta} \end{array}\right] = \mathcal{T}_{T-\Theta} \left[\begin{array}{c} \boldsymbol{u}_\tau \\ \boldsymbol{u}_{\tau+1} \\ \vdots \\ \boldsymbol{u}_{\tau+T-\Theta} \end{array}\right]. \qquad (3)$$

In order to be able to use equation (3) when we encrypt a sequence we must ensure that each iteration begins at state $\boldsymbol{x}_\tau = \boldsymbol{0}$. That is, the word encrypted in the previous iteration leaded the system to the zero state. To ensure it, we need to consider only codewords with finite weight.

Theorem 2 (Proposition 2.4 of [15]): $\left\{ \left[\begin{array}{c} \boldsymbol{y}_t \\ \boldsymbol{u}_t \end{array}\right] \in \mathbb{F}^n \mid t = 0, 1, \ldots, \gamma \right\}$ *represents a codeword with finite weight if and only if*

$$\left[\begin{array}{c|c} O & \Phi_{\gamma+1}(A, B) \\ \hline -I & \mathcal{T}_\gamma \end{array}\right] \left[\begin{array}{c} \boldsymbol{y}_0 \\ \boldsymbol{y}_1 \\ \vdots \\ \boldsymbol{y}_\gamma \\ \hline \boldsymbol{u}_0 \\ \boldsymbol{u}_1 \\ \vdots \\ \boldsymbol{u}_\gamma \end{array}\right] = \boldsymbol{0}.$$

In order to get this condition we will transforms the original message into codewords of the block code $\ker(\Phi_{T-\Theta+1}(A, B))$. So, we need a $k(T - \Theta + 1) \times (k(T - \Theta + 1) - \delta)$ generator matrix G of the block code $\ker(\Phi_{T-\Theta+1}(A, B))$.

In addition, we need to check if the necessary conditions 1, 2, 3, 4 and 5 (in page 2) to apply the decoding algorithm proposed in [12] hold. The assumption on the errors must hold as well. In our case, we suppose that there are no errors due to the channel and only the sender can introduce them. Then we control the number of errors that occur and we can apply the algorithm.

The private key of the cryptosystem is given by (P, Q, G, A, B, C, D), where P is a permutation matrix of order $n(T - \Theta + 1)$ and Q is an invertible matrix of order $k(T - \Theta + 1) - \delta$. The public key is given by (E, λ), where E is an $\alpha \times \beta$ matrix, with $\alpha = n(T - \Theta + 1)$ and $\beta = k(T - \Theta + 1) - \delta$. The matrix E is computed by the receiver in the following way $E = P \left[\begin{array}{c} \mathcal{T}_{T-\Theta} \\ I_{(T-\Theta+1)k} \end{array}\right] GQ$.

A. Encrypting process

In order to encrypt a message the sender divides it in blocks of length β. At instant i the sender computes $\mathfrak{v}_i = E\boldsymbol{m}_i$. Then he adds an error vector $\mathfrak{e}$ such that $wt(\mathfrak{e}) \leq \lambda$. Thus $\widetilde{\mathfrak{v}}_i = \mathfrak{v}_i + \mathfrak{e}$ is the sent word.

B. Decrypting process

The receiver recovers the message following the same steps as in the McEliece cryptosystem. The receiver receives the word $\widetilde{\mathfrak{v}}_i$. He can compute

$$\begin{aligned}
\widehat{\mathfrak{v}}_i &= \begin{bmatrix} \widehat{\boldsymbol{v}}_{i(T-\Theta+1)} \\ \widehat{\boldsymbol{v}}_{i(T-\Theta+1)+1} \\ \vdots \\ \widehat{\boldsymbol{v}}_{i(T-\Theta+1)+T-\Theta-1} \\ \widehat{\boldsymbol{v}}_{i(T-\Theta+1)+T-\Theta} \end{bmatrix} = P^{-1}\widetilde{\mathfrak{v}}_i \\
&= P^{-1} \begin{bmatrix} \widetilde{\boldsymbol{v}}_{i(T-\Theta+1)} \\ \widetilde{\boldsymbol{v}}_{i(T-\Theta+1)+1} \\ \vdots \\ \widetilde{\boldsymbol{v}}_{i(T-\Theta+1)+T-\Theta-1} \\ \widetilde{\boldsymbol{v}}_{i(T-\Theta+1)+T-\Theta} \end{bmatrix} \\
&= \begin{bmatrix} \mathcal{T}_{T-\Theta} \\ I_{(T-\Theta+1)k} \end{bmatrix} GQ\boldsymbol{m}_i + P^{-1}\mathfrak{e} \\
&= \begin{bmatrix} \mathcal{T}_{T-\Theta} \\ I_{(T-\Theta+1)k} \end{bmatrix} \widetilde{\boldsymbol{u}} + P^{-1} \begin{bmatrix} \boldsymbol{e}_{i(T-\Theta+1)} \\ \boldsymbol{e}_{i(T-\Theta+1)+1} \\ \vdots \\ \boldsymbol{e}_{i(T-\Theta+1)+T-\Theta-1} \\ \boldsymbol{e}_{i(T-\Theta+1)+T-\Theta} \end{bmatrix} \\
&= \begin{bmatrix} \widehat{\boldsymbol{y}}_{i(T-\Theta+1)} \\ \widehat{\boldsymbol{y}}_{i(T-\Theta+1)+1} \\ \vdots \\ \widehat{\boldsymbol{y}}_{i(T-\Theta+1)+T-\Theta-1} \\ \widehat{\boldsymbol{y}}_{i(T-\Theta+1)+T-\Theta} \\ \widehat{\boldsymbol{u}}_{i(T-\Theta+1)} \\ \widehat{\boldsymbol{u}}_{i(T-\Theta+1)+1} \\ \vdots \\ \widehat{\boldsymbol{u}}_{i(T-\Theta+1)+T-\Theta-1} \\ \widehat{\boldsymbol{u}}_{i(T-\Theta+1)+T-\Theta} \end{bmatrix}.
\end{aligned}$$

Using the decoding algorithm introduced in Section II-A he can recover $\widetilde{\boldsymbol{u}} = GQ\boldsymbol{m}$ and finally he can compute $\boldsymbol{m}$.

Notice that in our particular case we do not need to have correctly decoded any previous sequence. The purpose of this condition is to know an initial state $\boldsymbol{x}_t$ to start the decoding process, but we know that for every iteration the initial state is $\boldsymbol{x}_t = \boldsymbol{0}$. In addition, after decoding a block we can always compute the next states and start the following iteration from any of them.

IV. INPUT-STATE-OUTPUT REPRESENTATION OF A CONVOLUTIONAL CODE OBTAINED FROM AN MDS BLOCK CODE

In order that the sender can introduce as many errors as possible, matrix $\Phi_{T-\Theta+1}(A,B)$ has to be the parity check matrix of a MDS block code, as the decoding algorithm of Section II-C shows. Reed-Solomon codes are MDS and hence have the largest possible minimum distance for codes of their size and dimension. The following result shows that, given a parity check matrix H of any Reed Solomon code, there exist matrices A and B such the pair (A,B) is controllable and $H^t = \Phi_{T-\Theta+1}(A,B)$.

Theorem 3: *Let $\mathbb{F}$ be the Galois field of q elements. Let H be the parity-check matrix of a $[(T-\Theta+1)k, (T-\Theta+1)(k-1)]$-Reed-Solomon code (so $(T-\Theta+1)k = q-1$). Then there exist a unique controllable pair (A,B), with $A \in \mathbb{F}^{(T-\Theta+1)\times(T-\Theta+1)}$ and $B \in \mathbb{F}^{(T-\Theta+1)\times k}$, such that*

$$\Phi_{T-\Theta+1}(A,B) = H^t$$

Proof: Let α be a primitive element of $\mathbb{F}$, then the Reed-Solomon code of length $(T-\Theta+1)k$ and dimension $(T-\Theta+1)(k-1)$ is the code defined by the parity-check matrix

$$H = \begin{bmatrix} 1 & \cdots & 1 \\ \alpha^b & \cdots & \alpha^{b+T-\Theta} \\ \alpha^{2b} & \cdots & \alpha^{2(b+T-\Theta)} \\ \vdots & & \vdots \\ \alpha^{((T-\Theta+1)k-1)b} & \cdots & \alpha^{((T-\Theta+1)k-1)(b+T-\Theta)} \end{bmatrix}$$

For $i = 1, 2, \dots, T-\Theta+1$, let X_i be the $(T-\Theta+1)\times k$ submatrix of H^t defined by $X_i = H^t(:, (i-1)k+1 : ik)$ and η be the integer verifying

$$T-\Theta+1 = \left\lfloor \frac{T-\Theta+1}{k} \right\rfloor k + \eta, \quad 0 \leq \eta < k.$$

In order to apply Theorem 1, we have to identify the non-negative integers r_i and the index sets J_i, for $i = 1, 2, \dots, T-\Theta+1$.

We define the index sets J_i, $i = 1, 2, \dots, T-\Theta+1$, by

$$J_i = \begin{cases} \{1, 2\dots, k\}, & \text{if } i = 1, 2, \dots, \left\lfloor \frac{T-\Theta+1}{k} \right\rfloor \\ \{1, 2\dots, \eta\}, & \text{if } i = \left\lfloor \frac{T-\Theta+1}{k} \right\rfloor + 1 \\ \emptyset, & \text{if } i = \left\lfloor \frac{T-\Theta+1}{k} \right\rfloor + 2, \dots, T-\Theta+1 \end{cases}$$

Observe that $J_{i+1} \subseteq J_i$, for $i = 1, 2\dots, T-\Theta$. Now, let $r_1, r_2, \dots, r_{T-\Theta+1}$ be the non-negative integers defined as follows

$$r_i = \begin{cases} k, & \text{if } i = 1, 2, \dots, \left\lfloor \frac{T-\Theta+1}{k} \right\rfloor \\ \eta, & \text{if } i = \left\lfloor \frac{T-\Theta+1}{k} \right\rfloor + 1 \\ 0, & \text{if } i = \left\lfloor \frac{T-\Theta+1}{k} \right\rfloor + 2, \dots, T-\Theta+1 \end{cases}$$

Then, by the structure of matrix H^t, we have that

$$\begin{aligned} \operatorname{rank}(\mathcal{H}_i(H)) &= \operatorname{rank}\big(\mathcal{H}_i(H)(:, J_1 \cup (k+J_2) \cup \cdots \\ &\qquad \cup ((i-1)k + J_i))\big) \\ &= r_1 + r_2 + \cdots + r_i, \\ &\qquad \text{for } i = 1, 2, \dots, T-\Theta+1. \end{aligned}$$

So applying Theorem 1, there exist matrices A and B, of sizes $(T-\Theta+1)\times(T-\Theta+1)$ and $(T-\Theta+1)\times k$, respectively, such that

$$\begin{aligned} H^t &= \Phi_{T-\Theta+1}(A,B) \\ &= \begin{bmatrix} A^{T-\Theta}B & \cdots & AB & B \end{bmatrix}. \end{aligned} \tag{4}$$

Moreover, since

$$\begin{aligned} r_1 + r_2 + \cdots + r_{T-\Theta+1} &= \left\lfloor \frac{T-\Theta+1}{k} \right\rfloor k + \eta \\ &= T - \Theta + 1, \end{aligned}$$

the pair (A, B) is controllable. Finally, since

$$\operatorname{rank}(H^t(:, 1:k)) > 1,$$

we have that the matrices verifying condition (4) are unique by Theorem 1. ■

So, beginning from a parity-check matrix of a Reed-Solomon code, we obtain the matrices A and B verifying the relation (4). Now, let C be an $(n-k) \times (T - \Theta + 1)$ matrix such that $\operatorname{rank}(\Omega_\Theta(A, C)) = T - \Theta + 1$ and let D be an $(n-k) \times k$ matrix with nonzero column. Using the $(n, k, T - \Theta + 1)$ convolutional code described by (A, B, C, D) to construct the McEliece-like cryptosystem of section III, the sender can introduce $\lfloor \frac{T-\Theta}{2} \rfloor$ errors. Observe that parameters T and Θ must satisfy $T > 2\Theta > 0$ in order to be able to introduce at least 1 error.

V. CRYPTANALYSIS OF THE PROPOSED MCELIECE-LIKE CRYPTOSYSTEM

One of the guidelines to cryptanalyze cryptosystems based on error-correcting codes is recover the secret code or alternatively, constructing an equivalent code that can be efficiently decoded. We use this technique to analyze the cryptanalysis of the proposed cryptosystem.

Depending on the permutation matrix P, we distinguish three cases:

- If $P = I$, then the public key is given by (E, λ), where E is the $n(T - \Theta + 1) \times k(T - \Theta + 1) - \delta$ matrix
$$E = \begin{bmatrix} \mathcal{T}_{T-\Theta} GQ \\ GQ \end{bmatrix}.$$
The attacker can thus recover the matrix GQ, but previously it must verify the value of the parameter $(T - \Theta + 1)k$. Since the local description of trajectories matrix $\mathcal{T}_{T-\Theta}$ is a block lower triangular matrix, the attacker has to solve a system of $k(T - \Theta + 1) - \delta$ linear equations with k unknowns in order to compute each submatrix of $\mathcal{T}_{T-\Theta}$. So, cryptosystem security increases with the difference $k - (k(T - \Theta + 1) - \delta)$. Observe that $\operatorname{rank}(\Phi_{T-\Theta+1}(A, B)) = \delta$ implies $\delta \leq (T - \Theta + 1)k$. Then, the attacker can compute the local description of trajectories matrix and, therefore, the private key, by solving some linear equations.
- If $P = \begin{bmatrix} P_{11} & O \\ O & P_{22} \end{bmatrix}$, with P_{11} and P_{22} permutation matrices of sizes $(n-k)(T - \Theta + 1) \times (n-k)(T - \Theta + 1)$ and $k(T - \Theta + 1) \times k(T - \Theta + 1)$, respectively, then the matrix E has the form
$$E = \begin{bmatrix} P_{11} \mathcal{T}_{T-\Theta} GQ \\ P_{22} GQ \end{bmatrix}.$$
The difficult for the attacker in this case is to verify the value of the parameter $(T - \Theta + 1)k$ and then recover permutation matrices P_{11} and P_{22} in order to compute matrix $\mathcal{T}_{T-\Theta} GQ$. Once he obtains this matrix, he compute the local description of trajectories matrix by solving a system of $k(T - \Theta + 1) - \delta$ linear equations with k unknowns, as in the previous case.
- If $P = \begin{bmatrix} P_1 & P_2 \end{bmatrix}$, with P_1 and P_2 matrices of sizes $n(T - \Theta + 1) \times (n-k)(T - \Theta + 1)$ and $n(T - \Theta + 1) \times k(T - \Theta + 1)$, respectively, then the matrix
$$E = (P_1 \mathcal{T}_{T-\Theta} + P_2) GQ$$
has no structure as in previous cases. Then, it is impossible for the attacker to recover the private key of the cryptosystem.

Finally, note that we cannot begin from a parity check matrix of a Generalized Reed-Solomon code, because these codes does not verify conditions of Theorem 1. So the Sidelnikov-Shestakov attack [16] can not be applied to our cryptosystem.

VI. CONCLUSIONS AND FUTURE WORKS

A. Conclusions

In this paper we have presented a public key cryptosystem based on convolutional codes following McEliece's scheme and we give a input-state-output representation of a convolutional code to the sender can introduce as many errors as possible. This opens a new door to the introduction of these codes into this kind of cryptosystems.

B. Future Works

As future research work in order to keep on developing this purpose we want to apply different decoding algorithms to obtain an optimum performance cryptosystem and check which are the values of the parameters that can lead us to the most efficient possible situation. As well, we will study different ways of cryptanalysis for this particular case.

REFERENCES

[1] B. M. Allen, "Linear systems analysis and decoding of convolutional codes," Ph.D. dissertation, Department of Mathematics, University of Notre Dame, Indiana, USA, Jun. 1999.

[2] A. Canteaut and F. Chabaud, "A new algorithm for finding minimum-weight words in a linear code: application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511," *IEEE Transactions on Information Theory*, vol. 44, no. 1, pp. 367–378, 1998.

[3] J.-J. Climent, V. Herranz, and C. Perea, "A first approximation of concatenated convolutional codes from linear systems theory viewpoint," *Linear Algebra and its Applications*, vol. 425, pp. 673–699, 2007.

[4] J.-J. Climent, V. Herranz, and C. Perea, "Linear system modelization of concatenated block and convolutional codes," *Linear Algebra and its Applications*, vol. 429, pp. 1191–1212, 2008.

[5] D. Engelbert, R. Overbeck, and A. Schmidt, "A summary of McEliece-type cryptosystems and their security," Cryptology ePrint Archive, Report 2006/162, 2006, http://eprint.iacr.org/.

[6] R. Hutchinson, J. Rosenthal, and R. Smarandache, "Convolutional codes with maximum distance profile," *Systems & Control Letters*, vol. 54, no. 1, pp. 53–63, 2005.

[7] H. Janwa and O. Moreno, "McEliece public key cryptosystems using algebraic-geometric codes," *Designs, Codes and Cryptography*, vol. 8, pp. 293–307, 1996.

[8] Y. X. Li, R. H. Deng, and X. M. Wang, "On the equivalence of McEliece's and Niederreiter's public-key cryptosystems," *IEEE Transactions on Information Theory*, vol. 40, no. 1, pp. 271–273, 1994.

[9] P. Loidreau and N. Sendrier, “Weak keys in the McEliece public-key cryptosystem,” *IEEE Transactions on Information Theory*, vol. 47, no. 3, pp. 1207–1211, 2001.

[10] R. J. McEliece, “A public-key cryptosystem based on algebraic coding theory,” DNS Progress Report 42–44, Jet Propulsion Laboratory, 1978.

[11] R. J. McEliece, *Finite Fields for Computer Scientists and Engineers*. Norwell, MA, USA: Kluwer Academic Publishers, 1987.

[12] J. Rosenthal, “An algebraic decoding algorithm for convolutional codes,” *Progress in Systems and Control Theory*, vol. 25, pp. 343–360, 1999.

[13] J. Rosenthal, “Connections between linear systems and convolutional codes,” in *Codes, Systems and Graphical Models*, ser. The IMA Volumes in Mathematics and its Applications, B. Marcus and J. Rosenthal, Eds. New York: Springer-Verlag, 2001, vol. 123, pp. 39–66.

[14] J. Rosenthal, J. Schumacher, and E. V. York, “On behaviors and convolutional codes,” *IEEE Transactions on Information Theory*, vol. 42, no. 6, pp. 1881–1891, 1996.

[15] J. Rosenthal and E. V. York, “BCH convolutional codes,” *IEEE Transactions on Information Theory*, vol. 45, no. 6, pp. 1833–1844, 1999.

[16] V. M. Sidelnikov and S. O. Shestakov, “On insecurity of cryptosystems based on generalized reed-solomon codes,” *Discrete Mathematics and Applications*, vol. 2, no. 4, pp. 439–444, 1992.

[17] J. van Tilburg, “On the McEliece public-key cryptosystem,” in *Advances in Cryptology – CRYPTO’88*, ser. Lecture Notes in Computer Science, S. Goldwasser, Ed. Berlin: Springer-Verlag, 1988, vol. 403, pp. 119–131.

[18] E. V. York, “Algebraic description and construction of error correcting codes: A linear systems point of view,” Ph.D. dissertation, Department of Mathematics, University of Notre Dame, Indiana, USA, May 1997.

[19] I. Zaballa. “On a partial realization problem”. Preprint.