Observability attack on stream generators

Ramachandran Anantharaman and Virendra Sule
Department of Electrical Engineering
Indian Institute of Technology - Bombay, India.
e-mail: ramachandran@ee.iitb.ac.in, vrs@ee.iitb.ac.in

Abstract

This paper proposes an internal state recovery attack on special class of stream generators called non-linear combiners and filter generators over finite fields consisting of linear feedback shift registers (LFSRs) and nonlinear functions combining internal states to form output stream. This attack utilizes the concept of an *observer* well known in the theory of Linear Dynamical Systems. An observer is a special linear dynamical system which when fed with the output sequence of the stream generator as an input with arbitrary initial state, reconstructs the internal state of the generator in finite time. This attack is termed as observability attack and it is shown that the computations are of complexity $O(D^4)$ in pre-computation and of $O(D)$ for online computation, where $D = \sum_{i=0}^{d} \binom{n}{i}$ for stream generators with n states and d the degree of the output function, when the stream generator is defined over $\mathbb{F}_2$. The attack is technically applicable over general finite fields and appropriate bounds on computation are estimated. This attack gives an important estimates of time and memory resources required for cryptanalysis of realistic stream ciphers.

Index Terms

Cryptanalysis of Stream ciphers, Observer theory, Stream generators

NOTATIONS AND PRELIMINARIES

$\mathbb{F}_q^n$ is the n-dimensional vector space over the finite field $\mathbb{F}_q$. The space V^o is dual space of $\mathbb{F}_q^n$ which is also a vector space containing functions from $\mathbb{F}_q^n \to \mathbb{F}_q$. The function $\chi_i(x) \in V^o$ is the i^{th}-coordinate function defined as $\chi_i(x) = x_i$. A monomial $\phi \in V^o$ is a function of the form $\prod_i x_i^{d_i}$, where each $0 \leq d_i < q$.

I. NON-LINEAR STREAM GENERATORS

Non-linear stream generators and non-linear combiners are generic constructions used in stream ciphers and pseudo-random generators in Cryptography. Such a generator is a dynamical system over a finite field with state variables and outputs defined over a finite field $\mathbb{F}_q$ and having one or more of its Linear Feedback Shift Registers (LFSRs) driving the update of internal states. In this paper we call such generators which depend on internal state of feedback shift registers (FSRs) as stream generators[1]. When the number of state variables is n, the state $x(k)$ of the system at any time k belongs to $\mathbb{F}_q^n$ and the non-linear output map $g : \mathbb{F}_q^n \to \mathbb{F}_q$ defines the output $z(k) = g(x(k))$. Typical constructions of such stream generators are shown in the figures (1) and (2), with a single LFSR and multiple LFSRs respectively. The internal state of the stream generator, denoted $x(k)$ is the collection of states of all registers of the LFSRs. The output $z(k)$ is in general a non-linear combination of the states of these LFSRs. Given an initial loading of the internal states of the registers specifies an initial state $x(0) \in \mathbb{F}_q^n$ of the system. The system generates a unique output sequence $z(k)$ over $\mathbb{F}_q$ for each initial state $x(0)$. Such systems can be used to generate pseudorandom sequences which can be used for cryptographic applications such as enciphering a stream or as source of randomness which needs to be reconstructed.

A. Cryptanalysis of stream generators

An important problem associated with such non-linear stream generators is that of computing the initial condition of the generator $x(0)$ when an output stream $z(k)$ is made available over a limited length of time k such as over an interval $[k_0, k_0 + m]$, $k_0 > 0$. This problem is also known as the Cryptanalysis problem (or key recovery problem) of the generator when used as a stream cipher or a pseudorandom generator, since the values of state variables at initial loading $x(0)$ consists of the symmetric key K (which is secret) and randomly chosen initializing values

[1]The well known RC4 stream generators is an example which does not use FSR states for stream generation and hence is not included in this class

of states called IV. Such a problem is of NP class for non-linear generators and known to be computationally challenging as the number of states increase. Search for efficient algorithms for solving the Cryptanalysis problem of the generator has continued ever since these have been found suitable for use in Cryptography. In this paper we develop a new approach to the Cryptanalysis of non-linear stream generators called *Observability attack*. This approach is based on observability of linear dynamical systems and construction of an observer defined in Systems Theory and is briefly described as follows.

B. Observability and Observers of dynamical systems

In Mathematical Systems Theory, existence of a unique internal state $x(k_0)$ corresponding to an output sequence $z(k)$ of a dynamical system, for $k \geq k_0$ is called as the property of *Observability* of the system. In Linear Dynamical Systems the unique internal state $x(k)$ of the system can be obtained as a state of another linear dynamical system called an *Observer*. The Observer takes the output sequence $z(k)$, $k \geq k_0$, of the generator as an external input and an arbitrary initial state of its own at k_0. Then there is a minimum m such that the observer state at $k_0 + m$ coincides with the unique internal state of the generator $x(k_0+m)$. Such an Observer construction and the algorithm to compute internal state has however never developed in the past literature for non-linear dynamical systems. It is shown recently in [1] that such an observer can be constructed for dynamical systems with for the state space, a vector space over finite fields. An important advantage of this methodology is that it uses only linear algebraic computations. It is thus important to apply this theory to understand the computational challenges involved in this approach to Cryptanalysis of non-linear combiners and determine conditions under which the attack is likely to be practically feasible. Observability of evolution of permutation maps on a finite set X through a function f on X was discussed in the paper [2]. The approach of this paper however could not be utilized for Cryptanalysis of stream ciphers because it was based on the complex field as the base field for values of the function f. The state space of the dynamics of the permutation under complex field turns out to be an inner product space and the permutation map action on functions on X is a normal operator. No such nice conditions hold when the field is finite. Hence the observability based approach to cryptanalysis of stream generators needed a fresh investigation after the paper [2] which is carried out in this paper. Another recent work on observability of dynamical system and its relevance to Cryptanalysis of stream ciphers is reported in [3]. This work is specially meant for binary field valued variables and utilizes what is known as the semi tensor product representation of Boolean functions and maps. While this paper is relevant to the problem posed here it is important to point out central differences of our approach with this paper. First, the dimension of the linear dynamic model in this approach is always exponential in n and secondly the approach is specifically only applicable to Boolean functions. In fact the proposed approach in this paper is useful for realistic Cryptanalysis mainly because the dimension of the linear system obtained is not too large for the class of stream generators and is never exponential. Moreover our approach is applicable over any finite field and computationally feasible for fields with small characteristics.

C. Previous work on Cryptanalysis of the stream generator

In past stream generators were cryptanalyzed using the correlation as well as algebraic attacks see [4]. In the former, correlation of the output stream $z(k)$ for $k \geq k_0$ with that of the internal states $x(k)$ is estimated. While correlation attack is statistical, the algebraic attack directly solves the non linear polynomial system of equations with state variables as unknowns related to the output stream. Such a computation is of NP class and increases in complexity with the number of variables. Both of these attacks have not been known to scale up for realistic sizes of stream generators. The work in [5], [6], [7] addressed to the problem of cryptanalysis of stream generators. The basic idea reported in [6], [7] is to construct a linear system model for the output stream in terms of the monomials in the variables. The proposed method in our paper differs from the above by the method of construction of the linear model. The previous work uses a monomial basis for construction of a linear system of equations relating the output stream. This is broadly known as extended linearization (XL) method of solving multivariate algebraic equations. The proposed methodology constructs a restriction of the Koopman operator on a space which is invariant and contains the co-ordinate functions. The dimension of the linear model constructed through this linear method will be equal to the dimension of the linear model constructed in [6] at the worst case and hence has a distinctive advantage since not all monomials be present in the invariant subspace. Further in this paper we propose a new approach to solving the problem of computing the internal state by using the Observer theory well known in Linear dynamical systems. We show that this theory is useful to solve the nonlinear internal state recovery problem by linear algebraic computations and is scalable for practically feasible computation for realistic sizes of number of

states n when the dimension of an invariant subspace associated with the dual of the non-linear state map F is not too large. In fact this is true of the class of stream generators with LFSRs used for state update. This is a fresh new approach to the problem and is believed by the authors to have been unknown in the previous literature.

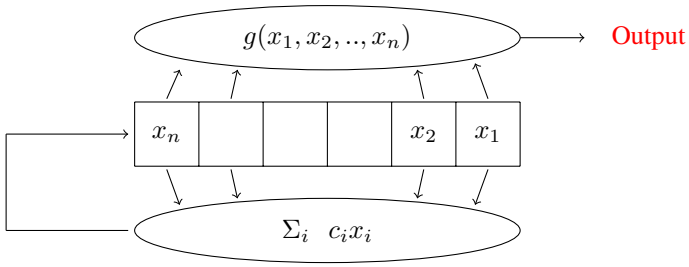

Fig. 1. Stream generator with with 1 LFSR

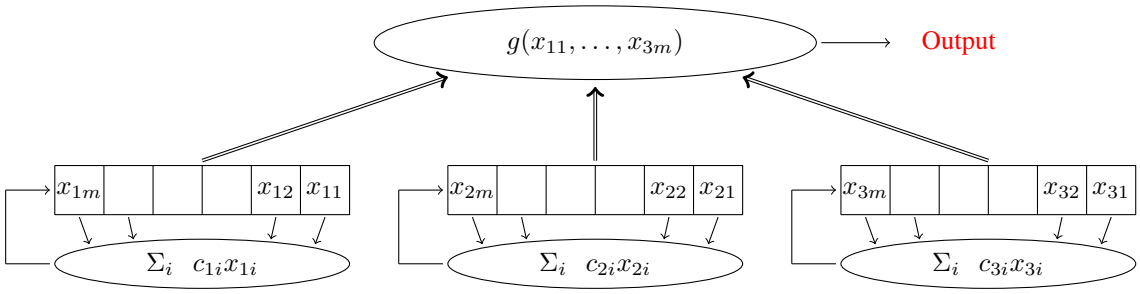

Fig. 2. Stream generator with 3 LFSRs

D. Mathematical model of the stream generator

Mathematically any non-linear stream generator with linear state update and non-linear output map as in figure (1) and (2) can be represented as a dynamical system in the following way

$$\begin{aligned} x(k+1) &= Ax(k) \\ z(k) &= g(x(k)) \end{aligned} \tag{1}$$

where $x \in \mathbb{F}_q^n$, A is a matrix over $\mathbb{F}_q^{n \times n}$, g is a non-linear function from $\mathbb{F}_q^n \to \mathbb{F}_q$. When the stream generator is of the form (1), the A matrix is in companion form and the output is a non-linear function of the internal states. In the form (2), the A matrix is a block diagonal form representing the matrices in companion form of feedback polynomials of individual LFSRs and the output is a non-linear function g of all the states.

II. Koopman Linear System for Dynamical Systems over Finite Fields

Mathematically, any dynamical system over a finite field can be modelled as

$$\begin{aligned} x(k+1) &= F(x(k)) \\ z(k) &= g(x(k)) \end{aligned} \tag{2}$$

where $x(k) \in \mathbb{F}_q^n$, $z(k) \in \mathbb{F}_q^m$ are the internal state and outputs while $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$, $g : \mathbb{F}_q^n \to \mathbb{F}_q^m$ are the state transition map and output map respectively. Let V^o be the vector space of $\mathbb{F}_q$-valued functions over $\mathbb{F}_q^n$. The Koopman operator F^* for the system (2) is a map from $V^o \to V^o$ defined as

$$F^* h(x) = h \circ F(x) = h(F(x))$$

where $h(x) \in V^o$. The Koopman Linear System (KLS) corresponding to (2) is a linear dynamical system over V^o defined as

$$h_{k+1}(x) = F^* h_k(x)$$

Algorithm 1 Construction of W_1 - the smallest F^*-invariant subspaces spanning $\chi_i(x)$ and $g(x)$

procedure F^*-INVARIANT SUBSPACE(W_1)
  Outputs:
  W_1 - the smallest invariant subspace which span the coordinate functions $\chi_i(x)$ and the non-linear function $g(x)$.
  $\mathcal{B}$ - the basis for the invariant subspace W_1
  Compute the cyclic Subspace
    $Z(\chi_1; F^*) = \langle \chi_1, F^*\chi_1, \ldots, (F^*)^{l_1-1}\chi_1 \rangle$
  Set of basis functions $\mathcal{B} = \{\chi_1, F^*\chi_1, \ldots, (F^*)^{l_1-1}\chi_1\}$
  if $\chi_2, \chi_3, \ldots, \chi_n \in$ Span$\{\mathcal{B}\}$ **then**
    $W_1 \leftarrow$ Span$\{\mathcal{B}\}$
    go to 14
  else
    Find the smallest i such that $\chi_i \notin$ span$\{\mathcal{B}\}$
    Compute the smallest l_i such that
      $(F^*)^{l_i}\chi_i \in$ Span$\{\mathcal{B} \cup \langle \chi_i, F^*\chi_i, \ldots, (F^*)^{l_i-1}\chi_i \rangle\}$
    $V_i = \{\chi_i, F^*\chi_i, \ldots, (F^*)^{l_i-1}\chi_i\}$
    Append the set V_i to $\mathcal{B}$
    go to 5
  if $g \in$ Span$\{\mathcal{B}\}$ **then**
    halt
  else
    Compute the smallest j such that
      $(F^*)^j g \in$ Span$\{\mathcal{B} \cup \langle g, F^*g, \ldots, (F^*)^{j-1}g \rangle\}$
    $V_g = \{g, F^*g, \ldots, (F^*)^{j-1}g\}$
    Append the set V_g to $\mathcal{B}$
    halt

for $h(k) \in V^o$. The paper [1] develops the theory of Koopman operator for dynamical systems over finite fields. It is shown that for each solution trajectory of (2), there exists a solution trajectory of the KLS having the same dynamical evolution. This means that if a point $x(0) \in \mathbb{F}_q^n$ is on a orbit (or chain) of length L under F, then there exists a function $h_{x(0)}(x)$ which is on an orbit (or chain) of length L under F^*. Since the space of functions V^o is of exponential dimension (equal to q^n), a reduced order linear system is developed which retains the information regarding the solution trajectories of the original dynamical system (2).

This system, called as the Reduced Order Koopman Linear System (RO-KLS) is the constructed by the restriction of the operator F^* to the smallest invariant subspace $W_1 \in V^o$ consisting the coordinate functions χ_i and the output functions $g_i(x)$. The following section describes the algorithm to compute the RO-KLS for stream generators.

A. RO-KLS for stream generators

As discussed above, construction of the F^*-invariant subspace W_1 plays an integral part to construct the RO-KLS. The dimension of the linear system is equal to dimension of the smallest F^*-invariant subspace of V^o consisting of the coordinate functions and the output function g. The construction of this subspace is described in the algorithm 1.

Once the invariant subspace W_1 and computed, let its basis be $\mathcal{B} = \{\psi_1(x), \ldots, \psi_N(x)\}$. The RO-KLS (as evaluation map) is the linear system of dimension $dim(W_1)$ and can be expressed in terms of matrices with this specific basis $\mathcal{B}$. Let the dynamical system be

$$\begin{aligned} y(k+1) &= K_1 y(k) \\ x(k) &= C y(k) \\ y_{op}(k) &= \Gamma y(k) \end{aligned} \tag{3}$$

where K_1^T is the restriction of Koopman operator on the invariant subspace W_1, C is the matrix corresponding to the map from the basis functions $\mathcal{B}$ to the vector of coordinate functions $[\chi_1(x), \ldots, \chi_n(x)]^T$, and Γ is the matrix corresponding to representation of the function g in terms of the basis functions $\mathcal{B}$.

Given any initial condition $x(0)$ of the non-linear stream generator, initiating the RO-KLS with

$$y(0) = \begin{bmatrix} \psi_1(x(0)) \\ \vdots \\ \psi_N(x(0)) \end{bmatrix}$$

it has been proven that the sequence $y_{op}(k)$ is same as the output of the stream generator (1) initiated with the same $x(0)$.

B. Dimension of W_1

Given the RO-KLS in (3), the first question which needs to be answered is "*Is there any bound on the dimension of W_1?*". The stream generator as in (1) is one of few systems for which this question can be answered convincingly in the affirmative. Since the internal dynamics of the stream generator is linear, the dimension of the RO-KLS solely depends on the non-linear output function g.

Lemma 1. *Given an dynamical system over finite field with linear internal dynamics as in* (1) *and a monomial ϕ, then*

$$\textit{degree } (F^*\phi) \ \leq \ \textit{degree } (\phi)$$

where F^* is the Koopman operator.

Proof. Assume that the system (1) evolves over $\mathbb{F}_q^n$, where $q = p^m$. Let the monomial be

$$\phi(x_1, \ldots, x_n) = \prod_{j \subset \{1,2,\ldots,n\}} x_j^{d_j}$$

where each $d_j < q - 1$ and the degree of the monomial ϕ is $\sum_j d_j$. The action $F^*\phi(x_1, \ldots, x_n)$ is defined as

$$F^*\phi(x_1, .., x_n) = \phi(f_1(x_1, .., x_n), .., f_n(x_1, .., x_n))$$

where $f_1, \ldots, f_n$ are functions corresponding to the state transition for each x_i. Since the internal dynamics of the stream generator is linear, each function f_i can be written as

$$f_i(x_1, \ldots, x_n) = \sum a_{ij} x_j$$

and these a_{ij} are entries of the matrix A in (1). In particular,

$$F^*\phi = F^*(\prod_j x_j^{d_j}) = \prod_j (\sum_{k=1}^n a_{jk} x_k)^{d_j}$$

This means

$$\text{degree } (F^*\phi) = \text{degree } \left(\prod_j (\sum_{k=1}^n a_{jk} x_k)^{d_j} \right)$$

Also,

$$\text{degree } \left((\sum_{k=1}^n a_{jk} x_k)^{d_j} \right) \leq d_j$$

the less than sign is because there can be a case where all a_{jk} can be zero. So, each term in the product

$$\text{degree } \left(\prod_j (\sum_{k=1}^n a_{jk} x_k)^{d_j} \right)$$

has a degree $\leq d_j$ and hence

$$\text{degree } (F^*\phi) = \text{degree } \left(\prod_j (\sum_{k=1}^{n} a_{jk} x_k)^{d_j} \right)$$
$$\leq \sum_j d_j = \text{degree } (\phi)$$

□

Remark 1. *The main take away point in the above lemma is that given a linear dynamics and a monomial ϕ, the action of Koopman operator on the monomial will not increase the degree of the monomial and this information is used to create upper bounds on the dimension of W_1*

Given any non-linear function g and a linear dynamics, it can be written as a sum of monomials and the function g has a degree d_g which is the largest degree of the constituent monomials. From the above lemma, it can be seen that the action of F^* on g does not increase the degree.

Theorem 1. *Given a non-linear stream generator (1) over $\mathbb{F}_q^n$ with the output g having a degree d, the size of the invariant subspace W_1 is bounded by*

$$\textit{dim } (W_1) = \frac{(1 - n^{d+1})}{1 - n}$$

Proof. Since the degree of g is d, and from lemma (1), the invariant subspace W_1 can have functions only upto degree d. A counting of all the independent monomials oven n-variables from $\mathbb{F}_q^n \to \mathbb{F}_q$ gives an upper bound on the the dimension of the invariant subspace W_1.

For example, with degree r, the total number of independent monomials is upper bounded by n^r since the degree is r and there are n variables to choose from it and the variables can get repeated too (which means that in the specific monomial, that variable has a power > 1). Hence, conservative estimate on the number of independent monomials of degree r over n variables is n^r.

So, a function g having degree d can have other terms of degree d or less too. So, counting all the independent monomials of degree d or less gives an upper bound on the dimension of W_1. This gives

$$\text{dim } (W_1) = 1 + n + n^2 + \cdots + n^d$$

where 1 is for the constant function, n is for linear functions and so on. The expression is the partial sum of the geometric series and simplifies to $\frac{1-n^{d+1}}{1-n}$ □

Remark 2. *Note that the estimate in (1) does not take the field equation into account. For $d \geq q$, the powers x_i^r, $(r > q)$ in the monomial gets reduced to a power $x_i^{r_d}$ where $r_d = r \bmod q$ and one can have better estimates to the dimension of W_1 for specific fields. Also, the estimate in theorem (1) is the best upper bound on the dimension of W_1 whenever $d < q$.*

For a vector space over the finite field $\mathbb{F}_2$, any variable x_i satisfies the equation $x_i^2 = x_i$ (as functions) which drastically reduces the dimension of W_1.

Corollary 1. *Given a stream generator (1) over $\mathbb{F}_2^n$, with the non-linear function having degree d, the dimension of W_1 is upper bounded by*

$$\textit{dim } (W_1) \leq \sum_{i=0}^{d} \binom{n}{i}$$

The corollary (1) can be proved by a simple counting argument of number of distinct monomials of degree less than or equal to d over n variables. It is pertinent to see that when the degree d is less, the dimension of the subspace W_1 is much smaller when compared with the dimension of the dual space V^o (which is of exponential size 2^n, for a n-state stream generator).

The table I compares the upper bounds for any 80-bit stream generator over $\mathbb{F}_2$ for small degrees (d) of the non-linear function g. The maximum dimension of the subspace W_1 are computed for each d using corollary (1). Also, by theorem (1), the upper bound of the subspace W_1 is of order n^d, which is also computed for comparison.

$degree\ (d)$	$maximum\ dim\ of\ W_1$	n^d	$n^d/max\ dim\ W_1$	$max\ dim(W_1)/dim(Vo)$
1	81	80	1	6.7×10^{-23}
2	3241	6400	1.97	2.7×10^{-21}
3	8.54×10^4	5.12×10^5	6	7×10^{-20}
4	1.67×10^6	4.1×10^7	24.57	1.4×10^{-18}
5	2.57×10^7	3.28×10^9	127.47	2.1×10^{-17}
6	3.26×10^8	2.62×10^{11}	803.6	2.7×10^{-16}

TABLE I

UPPER BOUNDS ON DIMENSION OF W_1 FOR DIFFERENT DEGREES OF OUTPUT FUNCTION FOR A 80 VARIABLE STREAM GENERATOR OVER $\mathbb{F}_2$

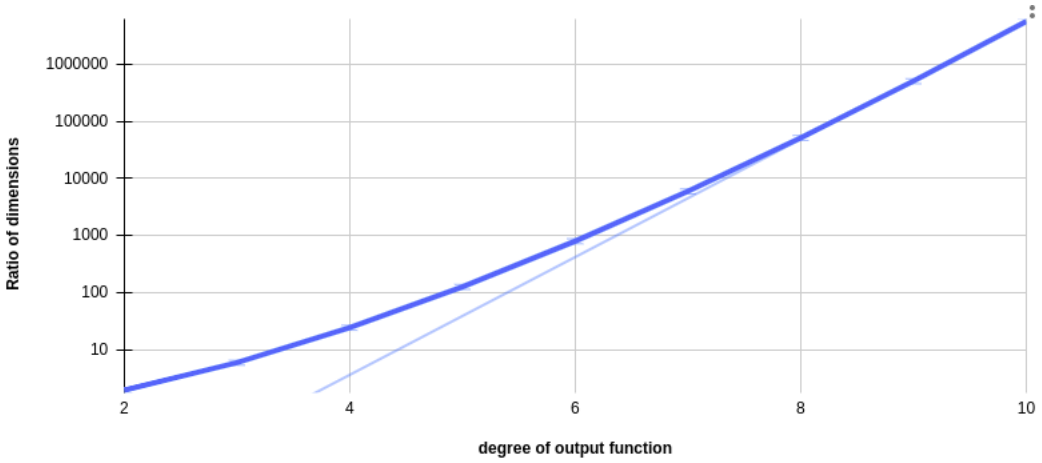

Fig. 3. Ratio of $n^d/dim(W_1)$ vs the degree d for a 80-bit stream generator

Further, since the stream generator is over $\mathbb{F}_2$, the dimension of the dual space V^o is 2^n (which is 2^{80} in this case), the upper bound on dimension of W_1 is shown as a fraction of the dimension of the dual space V^o.

Remark 3. *It can be seen that the dimension of W_1 is even lesser than n^d which was a upper bound on the dimension of W_1 for a stream generator over a general $\mathbb{F}_q$. The figure 3 shows the ratio of n^d to $dim(W_1)$ for different degrees d of the output function for a 80-bit stream generator over $\mathbb{F}_2$. It can be seen that the graph is linear in the log-scale and hence it can be concluded that the dimension of W_1 for the stream generator over $\mathbb{F}_2$ is much smaller than 80^d. The light blue line in the figure shows the best exponential approximation of the data points.*

Next an approach to compute the internal state $x(k_0)$ of the stream generator, given the sequence of outputs $z(k_0), z(k_0+1), \ldots$ is explored.

III. COMPUTATION OF INTERNAL STATE FOR A STREAM GENERATOR OVER $\mathbb{F}_2^n$

Given the linear system (3) starting from an internal state $y(k_0)$, the output $y_{op}(k)$ at each $k \geq k_0$ is given by

$$y_{op}(k_0+k) = \Gamma y(k_0+k) = \Gamma\ K_1^k y(k_0)$$

Given the output $z(k), \quad k = k_0, k_0+1, \ldots$ generated by the non-linear stream generator (1) starting from an initial condition $x(k_0)$, it is proved in [1] that when the RO-KLS (3) is initiated with $y(k_0)$ as

$$y(k_0) = \begin{bmatrix} \psi_1(x(k_0)) \\ \psi_2(x(k_0)) \\ \vdots \\ \psi_N(x(k_0)) \end{bmatrix}$$

then the sequence $y_{op}(k),\ \ k = k_0, k_0+1, \dots$ generated by (3) is same as $z(k)$ generated by the non-linear stream generator (1). Since the RO-KLS is a linear system, the vector of output sequence can be written as linear map on $y(k_0)$ as follows

$$\begin{bmatrix} y_{op}(k_0) \\ y_{op}(k_0+1) \\ \vdots \\ y_{op}(k_0+N) \end{bmatrix} = \begin{bmatrix} \Gamma \\ K_1\Gamma \\ \vdots \\ K_1^{N-1}\Gamma \end{bmatrix} y(k_0) =: \mathcal{O}\ y(k_0) \tag{4}$$

where $\mathcal{O}$ is called the *observability matrix* corresponding to the linear system (3). Given any sequence of outputs $z(k),\ k \geq k_0$, the linear system of equations (4) needs to be solved for $y(k_0)$ with $y_{op}(k) = z(k)$. An unique solution for (4) exists if the observability matrix $\mathcal{O}$ is of full rank. Once $y(k_0)$ is computed, the internal state $x(k_0)$ of the original non-linear stream generator can be computed through the map C defined in (3). The condition that the matrix $\mathcal{O}$ is of full rank is what in linear systems theory parlance is defined as the system (3) being *Observable* [8]. When the matrix $\mathcal{O}$ is not of full rank, then multiple $y(k_0)$ exists for the given stream of outputs. This leads to multiple $x(k_0)$ through the map C.

Remark 4. *Given a stream generator (1) and its RO-KLS being of dimension N, at the most N outputs are needed to compute the initial state as anything more would not increase the rank of $\mathcal{O}$ (due to Cayley-Hamilton theorem).*

A. Dynamic Observer

In the previous part, the RO-KLS is constructed and the internal state $x(k_0)$ can be computed from the sequence of outputs starting from $z(k),\ k \geq k_0$. Furthermore, in this section, we construct an new linear dynamical system called as a *dynamic observer* [8], [9], which takes the output of the non-linear stream generator $z(k)$ and computes the current internal state $x(k)$ of the non-linear stream generator. Whenever the RO-KLS is observerable, such a dynamical system can always be constructed.

Mathematically the dynamic observer is a dynamical system defined as

$$\begin{aligned} \hat{y}(k+1) &= K_1\hat{y}(k) + L(z(k) - y_{op}(k)) \\ \hat{x}(k) &= C\hat{y}(k) \end{aligned} \tag{5}$$

where, $\hat{y}(k) \in \mathbb{F}_q^n$ is the observer state, $z(k)$ is the output of the stream generator, $\hat{x}(k)$ is the computed internal state of the stream generator, K_1 and C are as defined as in (3). The matrix L, known as *observer gain* is chosen such that $K_1 - L\Gamma$ is nilpotent. From the linear systems theory, it can proved that whenever the system (3) is observable, such a L exists. Also, whenever such a L exists such that $(K_1 - L\Gamma)$ is nilpotent, the system (3) is defined to be *detectable*. The set of observable linear systems is a subset in the set of detectable linear systems.

Given the stream generator (1) and its RO-KLS as constructed in (3), the dynamic observer construction is graphically illustrated in figure (4)

For an available output sequence starting from time k_0, the observer states can be initialized to any arbitrary initial condition $\hat{y}(k_0)$ and whenever the RO-KLS is detectable, the computed internal state of the stream generator $\hat{x}(k)$ converges to the true internal state of the stream generator in maximum N_0 time instants, where N_0 is the index of nilpotence of $(K_1 - L\Gamma)$.

To summarize, given a stream generator and its corresponding RO-KLS, whenever the RO-KLS is observable, the internal state $x(k_0)$ can be uniquely computed from the sequence of outputs starting from k_0 by solving the linear equations (4). If the RO-KLS system is detectable, then the internal state is uniquely computed at $x(k_0+N_0)$ from a sequence of outputs starting from k_0 using the dynamic observer (5) and N_0 is the index of nilpotence of $K_1 - L\Gamma$ matrix used in observer construction.

Remark 5. *Though it is possible to uniquely determine the initial condition $x(k_0)$ from a sequence of outputs $z(k)$ starting from $k = k_0$ whenever the system is observable, the construction of dynamic observer is potentially a better option. This is because the observer based approach inherently uses matrix-vector multiplication to do forward computation of the observer dynamics while solution to (4) involves solving linear system of equations. Also, the dynamic observer reconstructs the internal state uniquely for a larger class of stream generators (whenever the RO-KLS is detectable).*

When the RO-KLS is neither observable nor detectable, then unique computation of the internal state of the stream generator is not possible from the output stream $z(k_0), z(k_0+1), \dots$, for any $k \geq k_0$. But equation (4) can

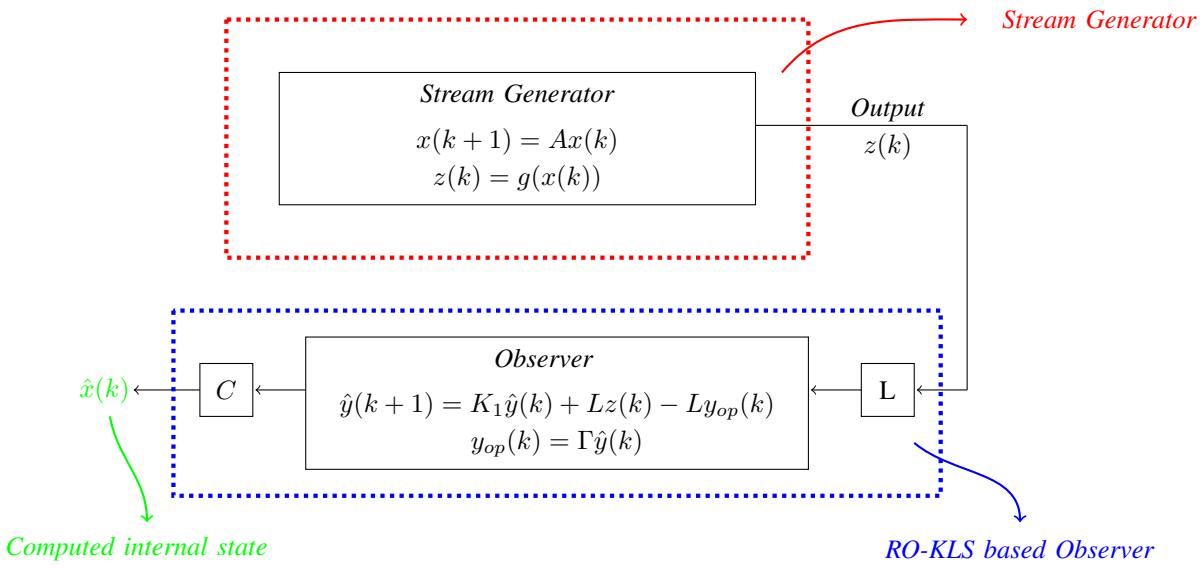

Fig. 4. Dynamic Observer for Stream generator using RO-KLS

be used to compute all possible values of $y(k_0)$ for the given output stream and use these $y(k_0)$ to compute all possible $x(k_0)$ with the map C defined in (3).

1) Illustrative Example: Consider a 4-bit stream generator over $\mathbb{F}_2$ as follows. The internal state update is through a LFSR with feedback polynomial

$$x^4 + x + 1$$

The state transition matrix A is

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

Let x_0, x_1, x_2, x_3 be the register contents. The output stream $z(k)$ is generated as $g(x_0, x_1, x_2, x_3) = x_0x_1$.

The subspace W_1 is computed to be of dimension 10. A basis of this subspace is chosen as in (6)

$$\left\{ \begin{array}{c} x_0, x_1, x_2, x_3, x_1x_2, x_2x_3, x_0x_3 + x_1x_3, \\ x_0x_1 + x_0x_2 + x_1x_2 + x_1, \\ x_1x_2 + x_1x_3 + x_2x_3 + x_2, \\ x_0x_2 + x_1x_2 + x_0x_3 + x_1x_3 + x_2x_3 + x_3 \end{array} \right\} \tag{6}$$

The matrix K_1, C and Γ are computed to be

$$K_1 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\Gamma = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

The RO-KLS is constructed as in equation (3). It can be seen that the observability matrix $\mathcal{O}$ defined in (4) is of full rank and hence the RO-KLS is observable and L can be computed such that $K_1 - L\Gamma$ is a nilpotent matrix. The L is computed as

$$L = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}^T$$

This concludes the design of the observer. The index of nilpotence of $K_1 - L\Gamma$ is 10 and hence the reconstructed state $\hat{x}(k)$ is equal to the original internal state of the stream generator from the 10^{th} time instant starting from the observation of the output. The observer dynamics (5) is now initiated with arbitrary initial condition $\hat{y}(k_0)$ and by using the output stream from $z(k_0)$, the internal state of the stream generator can be uniquely computed from $k_0 + 10$. The following table gives the comparison between the internal state of the stream generator and the reconstructed state through the observer

k	$x(k_0+k)^T$	z(k)	$\hat{x}(k_0+k)^T$
0	[1 1 1 0]	1	[1 0 1 0]
1	[1 1 0 0]	1	[0 1 0 1]
2	[1 0 0 0]	0	[1 0 1 0]
3	[0 0 0 1]	0	[0 1 0 0]
4	[0 0 1 0]	0	[1 0 0 1]
5	[0 1 0 0]	0	[0 0 1 1]
6	[1 0 0 1]	0	[0 1 1 1]
7	[0 0 1 1]	0	[1 1 1 1]
8	[0 1 1 0]	0	[1 1 1 0]
9	[1 1 0 1]	1	[1 1 0 1]
10	[1 0 1 0]	0	[1 0 1 0]
11	[0 1 0 1]	0	[0 1 0 1]

TABLE II

THE INTERNAL STATES OF THE STREAM GENERATOR $x(k)$ AND THE RECONSTRUCTED STATES $\hat{x}(k)$ THROUGH OBSERVER

It can be seen that the observer reconstructs the original internal state in $k_0 + 10$ time instances. The initial condition $x(k_0)$ can be recomputed from $\hat{x}(k_0 + 10)$ by inverting the dynamics of the LFSR. The computation gives $x(k_0) = [1\ 1\ 1\ 0]^T$.

B. Computation of $x(0)$ from an arbitrary internal state $x(k)$

Given the stream generator as in (1), computation of the initial condition $x(0)$ from the sequence of outputs $(z(k_0), z(k_0 + 1), \dots)$ starting from a time instant k_0 is an important problem in cryptography as it can break the encryption scheme modeled using this stream generator. From (4), whenever the corresponding RO-KLS of the stream generator is observable (the $\mathcal{O}$ being full rank), the internal state $x(k_0)$ can be computed uniquely. Under the assumption that the system is detectable, the internal state of the stream generator can be uniquely computed at a time instant $k_0 + N_0$, where N_0 is the index of nilpotence of $K_1 - L\Gamma$.

Algorithm 2 Retrieval of initial condition $x(0)$ using observerability attack

procedure OBSERVABILITY ATTACK
  Outputs:
    Reconstruction of internal states $x(k)$ from the output sequence $z(k)$ starting from k_0
    Retrieval of initial condition $x(0)$ of the stream generator.
  Compute the invariant subspace W_1 using the algorithm (1) and the construct the RO-KLS of the stream generator.
  if RO-KLS detectable **then**
    Construct the dynamic observer as in figure (4) and reconstruct the internal state uniquely at $x(k_0 + L)$, L is the index of nilpotence of $K_1 + L\Gamma$
    if Internal Dynamics of stream generator reversible **then**
      Compute the initial condition $x(0)$ uniquely from the unique $x(k_0 + L)$
    else
      Compute the all possible initial condition $x(0)$ satisfying $A^{(k_0+L)}x(0) = x(k_0 + L)$
  else
    Solve for all the solutions $y(k_0)$ of the linear equation (4) for the given output sequence.
    The internal states $x(k_0) = Cy(k_0)$ are the set of possible states which could generate the output sequence.
  halt

Once this internal state is uniquely computed at some $x(k)$, the initial condition $x(0)$ is computed by reversing the dynamics of the stream generator. But to uniquely reverse the dynamics, the internal dynamics of the stream generator should be reversible or equivalently the matrix A needs to be invertible. Whenever the system dynamics is a $1-1$ map (or a permutation) over $\mathbb{F}_q^n$, the dynamical system is said to be *non-singular*. And whenever the system is non-singular and RO-KLS being detectable, unique retrieval of $x(0)$ is possible from the output sequences starting from any time instant k_0.

If the internal dynamics of the stream is not a permutation over $\mathbb{F}_q^n$ but detectable, then instead of a unique $x(0)$, there would be a family of initial conditions corresponding to the unique $x(k_0 + N_1)$ reconstructed from the dynamic observer.

When the RO-KLS is neither detectable nor observable, then there are multiple initial conditions $y(k_0)$ for the output sequence $z(k)$ which can be computed through equation (4). These $y(k_0)$ lie on a linear subspace. Corresponding to these $y(k_0)$ solutions, there exists multiple points $x(k_0)$ in the state space of the stream generator. These correspond to possibly multiple symmetric keys in the initial state $x(0)$. In practise however, superfluous multiple keys corresponding to same output stream rarely exists as these denote redundant keys. Hence stream generators are rarely likely to be unobservable.

The algorithm 2 summarizes the discussion about the retrieval of initial condition $x(0)$ from the sequence of outputs $z(k_0), z(k_0 + 1), \ldots,$ using the RO-KLS.

C. Numerical Example

Consider the 80-bit stream generator made up of a single LFSR of 80 bit with the characteristic polynomial $p(x)$ as

$$p(x) = x^{80} + x^{53} + x^{47} + x^{35} + x^{33} + x^{10} + 1$$

The characteristic polynomial determines the feedback coefficients of the LFSR. The non-linear output function is

$$\begin{aligned} g(x_1, \ldots, x_{80}) &= \text{Majority}(x_1, x_{26}, x_{52}) \\ &= x_1x_{26} + x_1x_{52} + x_{26}x_{52} \end{aligned}$$

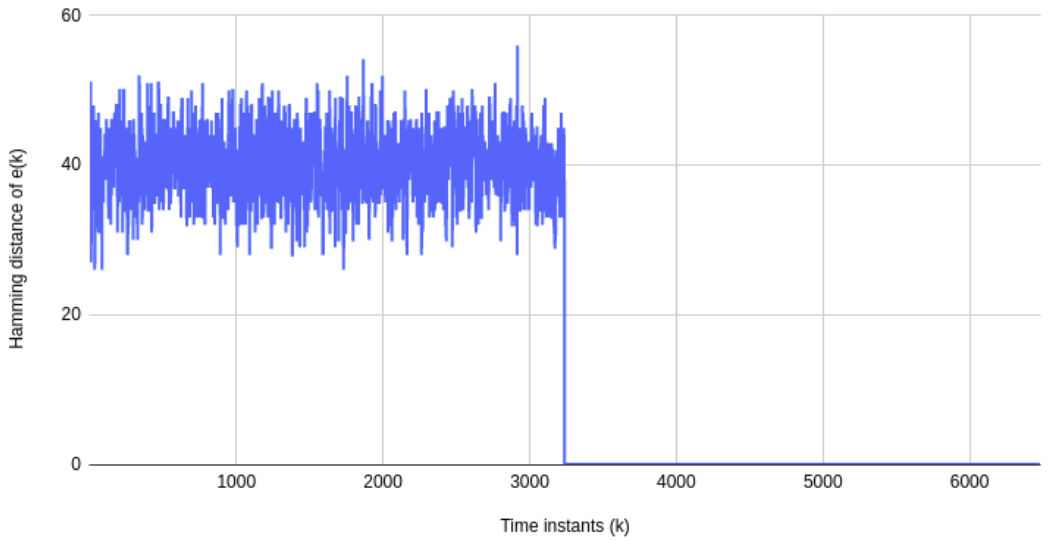

Fig. 5. Hamming distance of the error between the internal state of the stream generator and the reproduced state through dynamic observer

The dimension of the subspace W_1 is computed to be 3240. The RO-KLS is a linear system of dimension 3240 with the matrices $K_1 \in \mathbb{F}_2^{3240\times3240}$, $\Gamma \in \mathbb{F}_2^{1\times3240}$ and $C \in \mathbb{F}_2^{80\times3240}$ and

$$\begin{aligned} y(k+1) &= K_1 y(k) \\ y_{op}(k) &= \Gamma y(k) \\ x(k) &= C y(k) \end{aligned}$$

The RO-KLS is verified as observable and hence there exists a matrix $L \in \mathbb{F}_2^{3240\times1}$ such that $K_1 - L\Gamma$ is a nilpotent matrix. Once L is computed, the observer is designed as in figure (4). The internal states of the observer is $\hat{y}(k)$. The dynamics of the observer is

$$\hat{y}(k+1) = K_1\hat{y}(k) + Lz(k)$$

and the computed internal state of the stream generator is $\hat{x}(k)$ which is

$$\hat{x}(k) = C\hat{y}(k)$$

The observer is initiated with random $\hat{y}(0)$ and it can be seen that the computed state $\hat{x}(k)$ converges to the internal state $x(k)$ of the stream generator within a 3240 time instances, which is the dimension of the RO-KLS.

As a verification, let the difference in estimation at each time instant be $e(k) = x(k) - \hat{x}(k)$. For convenience, the Hamming distance of $e(k)$ is chosen as a matric. The Hamming distance for a vector over $\mathbb{F}_2$ is the number of non-zero entries in that vector. It is seen from the figure that the Hamming distance of the error is continuously zero after 3240 time instances.

IV. Computational complexity of computing internal states

The complexity of computing the internal states of the filter generator is primarily dependent on the size of the RO-KLS. Once the RO-KLS is computed, further complexities are polynomial in the size of the RO-KLS. The overall computations for recovery of internal state of a stream generator can be divided into two parts. The first part dealing with the construction of the RO-KLS which is offline (and need to be done once for a given stream generator) and the second (the online part) being recovery of the internal state of the filter generator from the given output stream $z(k)$ using the RO-KLS.

A. Preliminary offline computations

The offline computation concerns with the construction of the RO-KLS from a given non-linear filter generator. Since the internal dynamics is linear and by theorem 1, the dimension of the RO-KLS depends on the degree of the output function. Let D be the maximum possible dimension of this subspace (which is equal to the number of independent functions in n-variables with degree less than or equal to d and D is given as in theorem (1) or corollary (1) depending on the field.). Let $\mathcal{S}$ be a space of functions over $\mathbb{F}_q^n$ of degree less than or equal to d. So any function of degree less than or equal to d can be written as a linear combination of a chosen basis of $\mathcal{S}$ and hence a vector of dimension D. For example a 4 bit filter generator over $\mathbb{F}_2$ with the output restricted to degree 2, one ordered-basis for $\mathcal{S}$ is given below

$$\mathcal{B}_{\mathcal{S}} = \{1, x_1, x_2, x_3, x_4, x_1x_2, x_1x_3, x_1x_4, x_2x_3, x_2x_4, x_3x_4\}$$

Such a basis is referred to as the monomial basis. For example, given a function $h(x_1, x_2, x_3, x_4) = x_1 + x_1x_3 + x_2x_4$, it is written as the vector $[0, 1, 0, 0, 0, 0, 1, 0, 0, 1, 0]^T$ with the basis $\mathcal{B}_{\mathcal{S}}$. Computation of a basis for W_1, the invariant subspace spanning the coordinate and output functions is the main part of RO-KLS construction. Let the output function g be represented as vector $v_g \in \mathbb{F}_q^D$ with a chosen basis of $\mathcal{S}$. Let $g_i = (F^*)^i g$ denote the action of Koopman operator F^* i-times on the function g. From theorem 1, it is known that deg $F^*g \leq d$, (d = degree of g) and hence every iterate $(F^*)^i$ on g is of degree $\leq d$ and hence in the span of $\mathcal{S}$. Each of these iterates $(F^*)^i$ g can be represented as a vector v_{g_i} over $\mathbb{F}_q^F$. Similarly, all the coordinate functions χ_i are in the span of $\mathcal{S}$ and hence have an unique representation as a vector v_{x_i}. Starting with v_g, one needs to find the smallest l such that the vector v_{g_l} is linearly dependent on

$$v_{x_1}, \ldots, v_{x_n}, v_g, v_{g_1}, \ldots, v_{g_{l-1}} \tag{7}$$

This is a linear algebraic computation over the vectors $\mathbb{F}_q^D$ which is of order D^3. In the worst case the dimension of W_1 is going to be D. Hence the offline computations are going to be at the most of order D^4

B. Online computations

Once the linear model of the filter generator computed, the dynamic observer does only forward computations. Let N be the dimension of W_1. At each stage, the observer updates the internal state as

$$\hat{y}(k+1) = K_1\hat{y}(k) + L(z(k) - y_{op}(k))$$

The second part of the update $L(z(k) - y_{op}(k))$ is a vector-scalar multiplication as both $z(k)$ and $y_{op}(k)$ are scalars and L is a vector of length N and is of complexity $O(N)$. The first part $K_1\hat{y}(k)$ is matrix-vector multiplication. In general it is of order $O(N^2)$ but we look to exploit the structure of K_1. Choosing the basis of W_1 as in equation (7), it can be seen that the matrix representation of K_1 is a block triangular matrix.

$$K_1 = \begin{bmatrix} K_{11} & 0 \\ K_{21} & K_{22} \end{bmatrix}$$

where K_{11} is the system matrix A as in equation (1). K_{21} is defined as

$$K_{21} = \begin{bmatrix} 0 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & 0 \\ \alpha_1 & \ldots & \alpha_n \end{bmatrix}$$

and K_{22} as

$$K_{22} = \begin{bmatrix} 0 & 1 & \ldots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \ldots & 1 \\ \beta_0 & \beta_1 & \ldots & \beta_{l-1} \end{bmatrix}$$

where α_i and β_i are from the linear dependency relation

$$(f^*)^l(x) = \sum_{i=1}^{n} \alpha_i \chi_i(x) + \sum_{i=1}^{l-1} \beta_i (f^*)^i(x)$$

The operation $K_1\hat{y}(k)$ is a matrix-vector multiplication and in general of order $O(N^2)$. But by construction of the matrix K_1, it can be made simpler. Let $\hat{y}(k) = [\hat{y}_1(k) \;\; \hat{y}_2(k)]^T$ where the dimension of $\hat{y}_1$ is n and $\hat{y}_2$ is l where, $l = N - n$. So the computation of $K_1\hat{y}(k)$ is equal to computing $K_{11}\hat{y}_1(k)$ and $K_{21}\hat{y}_1(k)$ and $K_{22}\hat{y}_2(k)$. The individual operations are

- $K_{11}\hat{y}_1(k)$ is a matrix-vector multiplication of dimension n. Assuming no structure of A, the total number of operations is n^2.
- $K_{21}\hat{y}_1(k)$ is a matrix-vector multiplication. The dimension of K_{21} is $l \times n$. But the first $l-1$ rows of K_{21} are 0 and hence it is only a vector-vector product with total n operations.
- K_{22} is in companion form. The first $l-1$ rows need one computation of $K_{22}[i, i+1]\hat{y}_2[i+1]$ and each is of $O(1)$ and a cumulative $l-1$ operations. The l^{th}-row is a vector-vector product of dimension l and a total of l operations. Hence the total number of operations is $2l-1$.

Cumulatively, there is a total of $n^2 + n + 2l - 1$ operations. We know that $l = D - n$ and $l >> n$. Hence the total complexity of online computations is $O(N)$.

Also, the computation $\hat{x}(k) = C\hat{y}(k)$ is needed to compute the internal state of the filter generator. There are totally $n^2 l$ operations. And with $l >> n$, the computations are of order $O(N)$. Hence the effective online computations are of order $O(N)$.

Also, the reconstructed internal state through the observer converges to the internal state of the filter in M time instants where M is the index of nilpotence of $K_1 - L\Gamma$. The total online computations to reconstruct the internal state is of order $O(NM)$.

Remark 6. *It is to be noted that the dimension N of the subspace W_1 has an upper bound D. So, in essence, the online computations are of order $O(D)$.*

V. Conclusion

The idea of observability based attack on stream ciphers uses the dynamic observer construction well known in linear system. However it is extended to nonlinear stream generators by considering the reduced Koopman linear system. This approach allows construction of the observer to nonlinear systems and computation of the internal state by linear algebraic computation. The online computational complexity to recover the internal state is $O(D)$ with an offline precomputation of complexity $O(D^4)$ where D is the $\sum_d \binom{n}{i}$. This type of attack can be extended to any pseudorandom generators over finite fields and the reconstructed state of the observer equals to the internal state of the random number generator whenever the RO-KLS is detectable. Such an attack for stream generators is also theoretically applicable to stream generators with non-linear internal dynamics. However the bounds on dimensions of RO-KLS in case of nonlinear state dynamics cannot be obtained as easily as in the present case.

References

[1] R. Anantharaman and V. Sule, "Koopman operator approach for computing structure of solutions and observability of non-linear finite state system," *arXiv.org identifier: 2010.10752*, 2020.

[2] R. E. Byerly, L. D. Drager, and J. M. Lee, "Observability of permutations, and stream ciphers," *IEEE Transactions on Information Theory*, vol. 49, pp. 3326–3330, 2003.

[3] J. Zhong and D. Lin, "Linearization of nonlinear filter generators and application to cryptanalysis of stream ciphers," *Journal of Complexity*, vol. 35, pp. 29–45, 2016.

[4] A. Klein, *Stream Ciphers*. Springer-Verlag, 2013.

[5] S. R∅njom and T. Helleseth, "A new attack on filter generator," *IEEE Transactions on Information Theory*, vol. 53, pp. 1752–1757, 2007.

[6] S. R∅njom, G. Gong, and T. Helleseth, "On attacks on filtering generators using linear subspace structures," *Proceedings of International Workshop - Sequences, Subsequences and Consequences*, pp. 204–217, 2007.

[7] S. R∅njom and T. Helleseth, "The linear vector space spanned by the nonlinear filter generator," *Proceedings of International Workshop - Sequences, Subsequences and Consequences*, pp. 169–183, 2007.

[8] T. Kailath, *Linear systems*. Pearson; United States, 1979.

[9] W. M. Wonham, *Linear Multivariable Control: a Geometric approach*. Springer-Verlag New York Inc., 1979.