

# Chapter 17

## Error Linear Complexity Measures of Binary Multisequences

**Sindhu M.**

*Amrita Vishwa Vidyapeetham, India*

**Sajan Kumar S.**

*Amrita Vishwa Vidyapeetham, India*

**M. Sethumadhavan**

*Amrita Vishwa Vidyapeetham, India*

### ABSTRACT

*The joint linear complexity and  $k$ -error joint linear complexity of an  $m$ -fold  $2^n$  periodic multisequence can be efficiently computed using Modified Games Chan algorithm and Extended Stamp Martin Algorithm respectively. In this chapter the authors derive an algorithm which, given a constant  $c$  and an  $m$ -fold  $2^n$  periodic binary multisequence  $S$ , computes the minimum number  $k$  of errors and the associated error multisequence needed over a period of  $S$  for bringing the joint linear complexity of  $S$  below  $c$ . They derived another algorithm for finding the joint linear complexity of  $3 \cdot 2^n$  periodic binary multisequence.*

### INTRODUCTION

In complexity measures for sequences over finite fields, such as the linear complexity and the  $k$ -error linear complexity is of great relevance to cryptology, in particular, to the area of stream ciphers. There are basically two types of requirements for suitability of a keystream generated by a stream cipher. One of the requirements is the keystream sequence must pass various statistical

tests for randomness. This is to make it difficult to capture any information about the plaintext by an attacker from any possible statistical deficiencies in the keystream. The second is that it should be very hard to predict the entire keystream from the knowledge of a part of it. For this purpose, one is interested to know how hard a sequence might be to predict. This requirement leads to the study of several complexity measures for sequences. The most significant complexity measure is the linear complexity: length of the shortest linear recurrence relation satisfied by the sequence and

DOI: 10.4018/978-1-60960-123-2.ch017

related concept of  $k$ -error linear complexity (see Kaida, T. (1999)).

The major problem in stream cipher cryptography is generating a pseudorandom sequence of elements from a short random key. We mainly use LFSRs for the construction of stream ciphers. On the other hand, LFSRs can also be used to mount attacks on stream cipher systems. This attack is based on the Berlekamp-Massey algorithm: given a sequence  $S$  with terms in a finite field  $F_q$  of length  $n$ , the Berlekamp-Massey algorithm computes the feedback polynomial of the shortest LFSR that can generate the sequence  $S$  in  $O(n^2)$  time. In fact, if the shortest LFSR is of length  $\ell$ , then the algorithm needs just  $2\ell$  consecutive terms of the output sequence to determine its feedback polynomial. So this algorithm forms a universal attack on keystream generators since it carries the potential of substituting any keystream generator by its shortest linear equivalent. This leads to the concept of linear complexity of sequences. For a stream cipher system to be secure against the Berlekamp-Massey attack, it must not be possible to approximate the keystream sequence closely with a sequence of significantly smaller linear complexity. This means that changing a few terms in the keystream sequence must not cause a significant decrease of the linear complexity. This requirement leads to the concept of  $k$ -error linear complexity.

To take advantage of the general purpose processing units employed in the present day computers over public/private networks, we need the keystream to be a sequence of a few bytes, instead of bits. Such keystream generators are better suited for software implementation, and provide high throughput. Such ciphers are called word based (or vectorized) ciphers since they produce more than one bit per clock cycle. The theory of such stream ciphers requires the study of the complexity measures for multisequences, i.e., for parallel streams of finitely many sequences. In this direction, the joint linear complexity and the joint linear complexity profile of multisequences

have been investigated. The theory of  $k$ -error joint linear complexity of multisequences has been investigated recently.

An  $m$  fold  $N$  periodic multisequence  $S$  can be interpreted as an  $m \times N$  matrix over  $F_q$ . For defining the  $k$ -error joint linear complexity of multisequences, we need the following definitions of term distance and column distance.

**1.1 Definition:** Let  $S=(S^{(1)}, S^{(2)}, \dots, S^{(m)})$  and  $T=(T^{(1)}, T^{(2)}, \dots, T^{(m)})$  be two  $m$  fold  $N$  periodic multisequences over  $F_q$ . We define the term distance  $\delta_T(S, T)$  between  $S$  and  $T$  as the number of entries in  $S$  that are different from the corresponding entries in  $T$ , and the column distance  $\delta_C(S, T)$  as the number of columns in  $S$  that are different from the corresponding columns in  $T$ . We define the individual distance vector by  $\delta_r(S, T) = (\delta_1, \delta_2, \dots, \delta_m)$ , where  $\delta_j$  is the Hamming distance between the  $j^{\text{th}}$  rows of  $S$  and  $T$  for  $1 \leq j \leq m$ .

**1.2 Definition:** Let  $S=(S^{(1)}, S^{(2)}, \dots, S^{(m)})$  be an  $m$  fold  $N$  periodic multisequences over  $F_q$ . For an integer  $k$  with  $0 \leq k \leq mN$ , the  $k$ -error joint linear complexity  $L_{N,k}(S)$  of  $S$  is the smallest possible joint linear complexity obtained by changing  $k$  or fewer terms of  $S$  in its first period of length  $N$  and then continuing the changes periodically with period  $N$ . In other words,  $L_{N,k}(S) = \min_T L(T)$  where the minimum is taken over all  $m$  fold  $N$  periodic multisequence  $T$  over  $F_q$  with term distance  $\delta_T(S, T) \leq k$ .

**1.3 Definition:** Let  $S$  be an  $m$  fold  $N$  periodic multisequence over  $F_q$ . For an integer  $k$  with  $0 \leq k \leq N$ , the  $k$ -error  $F_q$  linear complexity  $L_{N,k}^q(S)$  of  $S$  is the smallest possible joint linear complexity obtained by changing  $k$  or fewer columns of  $S$  in its first period of length  $N$  and then continuing the changes periodically with period  $N$ . In other words,  $L_{N,k}^q(S) = \min_T L(T)$  where the minimum is taken over all  $m$  fold  $N$  periodic multisequences  $T$  over  $F_q$  with column distance  $\delta_C(S, T) \leq k$ . Alternatively, if  $S$  is the  $N$  periodic sequence with terms in  $F_{q^m}$  corresponding to the

8 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

[www.igi-global.com/chapter/error-linear-complexity-measures-binary/50726](http://www.igi-global.com/chapter/error-linear-complexity-measures-binary/50726)

## Related Content

---

### Consequences of Corruption on Economy, Politics, and Society: The Case of India

Asim Kumar Karmakar, Priyanthi Bagchiand Somnath Karmakar (2023). *Theory and Practice of Illegitimate Finance* (pp. 54-67).

[www.irma-international.org/chapter/consequences-of-corruption-on-economy-politics-and-society/330623](http://www.irma-international.org/chapter/consequences-of-corruption-on-economy-politics-and-society/330623)

### Current Network Security Technology

Göran Pulkkis, Kaj J. Grahnanand Peik Åström (2012). *Cyber Crime: Concepts, Methodologies, Tools and Applications* (pp. 417-429).

[www.irma-international.org/chapter/current-network-security-technology/60962](http://www.irma-international.org/chapter/current-network-security-technology/60962)

### Detecting Anomalous Ratings in Collaborative Filtering Recommender Systems

Zhihai Yangand Zhongmin Cai (2016). *International Journal of Digital Crime and Forensics* (pp. 16-26).

[www.irma-international.org/article/detecting-anomalous-ratings-in-collaborative-filtering-recommender-systems/150856](http://www.irma-international.org/article/detecting-anomalous-ratings-in-collaborative-filtering-recommender-systems/150856)

### Information Hiding Model Based on Channel Construction of Orthogonal Basis

Bao Kangsheng (2021). *International Journal of Digital Crime and Forensics* (pp. 1-18).

[www.irma-international.org/article/information-hiding-model-based-on-channel-construction-of-orthogonal-basis/277089](http://www.irma-international.org/article/information-hiding-model-based-on-channel-construction-of-orthogonal-basis/277089)

### Spatio-Temporal Just Noticeable Distortion Model Guided Video Watermarking

Yaqing Niu, Sridhar Krishnanand Qin Zhang (2012). *Crime Prevention Technologies and Applications for Advancing Criminal Investigation* (pp. 66-84).

[www.irma-international.org/chapter/spatio-temporal-just-noticeable-distortion/66833](http://www.irma-international.org/chapter/spatio-temporal-just-noticeable-distortion/66833)