INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI
SHORT ABSTRACT OF THESIS

Name of the Student	:	SUMAN ROY
Roll Number	:	126102024
Programme of Study	:	Ph.D.

Thesis Title: On the Generation and Analysis of Pseudorandom Sequences over Arbitrary Finite Fields

Name of Thesis Supervisor(s)	:	Dr. Srinivasan Krishnaswamy
Thesis Submitted to the Department/ Center	:	Electronics and Electrical Engineering
Date of completion of Thesis Viva-Voce Exam	:	6th May 2021
Key words for description of Thesis Work	:	Pseudorandom sequences, Linear Feedback Shift Registers, Nonlinear Feedforward Generators, Balance Property, Linear Complexity, de Bruijn Sequences.

SHORT ABSTRACT

A sequence generated by a deterministic algorithm is called a pseudorandom sequence if it satisfies statistical properties similar to a truly random sequence. Such sequences arise in many applications starting from key generation in cryptography to spread-spectrum communication, and so on. This thesis deals with the topics related to the generation and analysis of pseudorandom sequences.

Many pseudorandom sequence generators are based on Linear Feedback Shift Registers (LFSRs). LFSR is a shift register whose input bit is a linear function of some bits of the shift register value. Nonlinear feed-forward logic can be used along with a primitive-LFSR to increase the linear complexity of the generated sequences. Such an arrangement is called a Non-Linear Feed-forward Generator (NLFG). In this work, the statistical distribution of sequences generated by NLFGs over arbitrary finite fields has been analysed. Then two novel methods of extending nonlinear feed-forward logic to word-based LFSRs have been described. A special kind of word-based LFSRs, known as σ-LFSRs, has been considered here. The first NLFG configuration uses permutation matrices while the second one sees a σ-LFSR over an extension field. For the first scheme, using simulation it has been shown that the statistical distribution of each component sequence is better than that of an existing scheme. And, for the second scheme, we have mathematically analysed the statistical distribution of the output vector sequence and have shown that it is more balanced compared to the sequences generated by schemes available in literature.

The last part of this thesis deals with the generation of de Bruijn sequences. An n-th order binary de Bruijn sequence is a periodic sequence of length 2^n in which every n-length subsequence occurs exactly once in each period. These sequences have good statistical properties associated with randomness such as long period, balance, ideal n-tuple distribution, and high linear complexity. Due to these reasons, de Bruijn sequence generators are used in many pseudorandom number generators and are also used as building blocks for stream ciphers. Here, we describe a method of traversing a set of n-th order binary de Bruijn sequences using a series of graph-theoretic transformations.