Proposal: Investigating the Impact of Higher-Degree NLFSR Feedback Functions on Cryptographic Strength and Periodicity

Abdulmumin Sa'ad
Mohammed Mansour
Supervised by: Prof. S. Almuhammadi
King Fahd University of Petroleum and Minerals (KFUPM)

May 1, 2025

Abstract

Nonlinear Feedback Shift Registers (NLFSRs) are widely used in cryptographic systems for generating pseudorandom sequences. While prior work, including Ibraheem and Almuhammadi (2019), has focused on feedback functions of degree 3, there exists a gap in exploring the effects of feedback functions of higher degrees (e.g., degree 4 or above). This proposal aims to construct, analyze, and compare NLFSR feedback functions of higher algebraic degrees with their lower-degree counterparts, in terms of period optimality, cryptographic strength, and resistance to known attacks.

1 Introduction

NLFSRs offer better security properties than LFSRs due to their nonlinear structure. Prior constructions have largely focused on degrees 2 and 3. Higher degrees could increase resistance against algebraic and low-order approximation attacks, but their practical properties and behavior remain underexplored.

This project proposes a systematic construction and evaluation of NLFSR feedback functions of degree 4 and above, leveraging or extending existing enumeration and period-testing methods.

2 Objectives

- Construct NLFSR feedback functions of degree 4 and above.
- Evaluate their periods and determine which achieve optimal periods (i.e., $2^n - 1$).
- Test the higher-degree functions against potential cryptanalytic attacks (e.g., algebraic attacks, fast correlation attacks, and low-order approximation).
- Explore the trade-offs between increased nonlinearity and computational complexity.

3 Motivation and Research Gap

In the study by Al-Hejri and Almuhammadi [**?**], 140 feedback functions of degree 3 with optimal periods were constructed and added to the 127 previously known functions. However, feedback functions of degree 4 remain largely uncharted. Increasing the algebraic degree can improve resistance to cryptanalytic techniques such as:

- Algebraic attacks
- Fast correlation attacks
- Low-order approximation

Yet, the balance between security and computational feasibility needs to be addressed through careful empirical evaluation.

4 Methodology

1. **Function Generation:** Extend the construction framework introduced in [**?**] to systematically enumerate feedback functions of the form:

$$f(x_0, \ldots, x_{n-1}) = x_0 \oplus x_a \oplus x_b \oplus x_c x_d x_e x_f$$

2. **Period Testing:** Implement or adapt the period-testing algorithm to validate the period of each function.
3. **Security Metrics:** Evaluate Boolean function properties (nonlinearity, algebraic degree, correlation immunity) using available cryptographic analysis tools.
4. **Comparison:** Perform a comparative study between degree-3 and degree-4 feedback functions across NLFSR sizes $n = 5$ to 25.

5 Expected Contributions

- A complete or partial list of NLFSR feedback functions of degree 4 with optimal periods.
- Empirical insights into how increasing the algebraic degree affects security and period optimality.
- Recommendations for future constructions of NLFSRs in cryptographic applications.

6 Future Work

The outcomes of this project can pave the way for:

- AI-assisted discovery of higher-degree functions with desirable cryptographic properties.
- Integration with FPGA/ASIC design for high-performance sequence generation.
- Exploration of functions with hybrid degrees (mixed terms of degree 2–4).

References

[1] I. Al-Hejri and S. Almuhammadi, *New NLFSR Functions of Degree 3 with Optimal Periods*, 2019.

[2] S. Almuhammadi, I. Al-Hejri, G. Talib, and A. Gaamel, *NLFSR Functions with Optimal Periods*, Proc. International Conference on Computational Science and Its Applications, Springer, 2018.