INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI
SHORT ABSTRACT OF THESIS

Name of the Student	:	Deepak Agrawal
Roll Number	:	166102008
Programme of Study	:	Ph.D.

Thesis Title: Construction and Analysis of Nonlinear Secret Sharing Schemes

Name of Thesis Supervisor(s)	:	Dr. Smarajit Das and Dr. Srinivasan Krishnaswamy
Thesis Submitted to the Department/ Center	:	EEE
Date of completion of Thesis Viva-Voce Exam	:	25-6-2025
Key words for description of Thesis Work	:	Secret sharing scheme, Linear SSS, Nonlinear SSS, Tompa Woll attack, Nordstrom Robinson code

SHORT ABSTRACT

A secret sharing scheme is a method by which a set of shares are generated from secret data. These shares are then distributed among a set of participants. The secret can then be recovered from the shares of legitimate subsets of participants. The set of these subsets is called the access structure of the scheme. If the functions that recover the secret from the shares are all linear, then the scheme is called a linear secret sharing scheme. The inherent linearity of these secret recovery functions enable participants to cheat by wrongly declaring their shares during secret recovery. An example of such an attack is the `Tompa-Woll' attack. In these attacks, the wrongly declared share leads to a wrongly recovered secret. However, the cheating participants can use the linearity of the recovery function to calculate the correct secret from the wrongly recovered one. Various verification techniques have been devised to detect this kind of cheating. An alternate method of resisting such attacks is by designing schemes with nonlinear secret recovery functions. These functions must be such that the cheating participants gain no information about the actual secret from the wrongly recovered one. This motivates the study of nonlinear secret sharing schemes.

We constructed access structures of nonlinear secret sharing schemes based on the Nordstrom-Robinson code and other codes derived from the Nordstrom-Robinson code. Further, access structures for schemes based on a few Hadamard codes have also been derived.

We then look at nonlinear boolean functions from a secret sharing point of view. In particular, boolean expressions derived from linear equations over the ring Z4 have been explored. Closed-form formulae for such expressions have been derived. We have then derived a few information-theoretic results that enable us to analyse these equations from a secret sharing point of view. A couple of secret sharing schemes are then designed and analysed based on these results.