Enstitüsü : Fen Bilimleri
Dalı : Matematik - Bilgisayar
Programı : Matematik
Tez Danışmanı : Prof. Dr. Erol BALKANAY
Tez Türü ve Tarihi : Doktora – Temmuz 2010

ÖZET

SİMETRİK DİZAYNLAR, KODLAR VE SIR PAYLAŞIM ŞEMALARI ÜZERİNE BİR ÇALIŞMA

Selda ÇALKAVUR

Bu tez çalışmasının konusu, simetrik dizaynın kodu ile ilgili sır paylaşım şemaları arasındaki ilişkiyi araştırmaktır.

Tezin ilk bölümünde; $(v, b, r, k, \lambda)-$ dizayn, $(v, k, \lambda)-$ simetrik dizayn ve $t-(v, k, \lambda)-$dizayn kavramları incelenmiştir.

İkinci bölümde lineer kodlar anlatılmıştır. Bu kapsamda; Hamming uzaklığı, minimum uzaklık, Hamming ağırlığı, dual kod ve eşlik-denetim matrisi kavramları açıklanmıştır. Ayrıca bir dizaynın kodu, bir simetrik dizaynın kodu ve bir simetrik dizaynın genişletilmiş kodu verilmiştir.

Üçüncü bölüm, sır paylaşım problemine ayrılmıştır. "Sır paylaşımı" kavramı açıklanmış ve Massey'in sır paylaşım şeması anlatılmıştır. Ayrıca minimal erişim kümesi kavramı verilmiş ve dual kodlar üzerine kurulan sır paylaşım şemalarının erişim yapıları incelenmiştir. Minimal kodsözcükleri incelenmiş ve sır paylaşımının demokratiklik derecesi açıklanmıştır.

Dördüncü bölümde, simetrik dizaynın kodundan, sır paylaşım şemalarına geçiş araştırılmıştır. Simetrik dizaynın kodu üzerinde kurulan sır paylaşım şemasındaki minimal erişim küme sayısı hesaplanmıştır. Ayrıca $(v, k, \lambda)-$simetrik dizaynın ikili C kodunun dualindeki kodsözcükleri için $w_{maks} < \frac{2(k+\lambda)}{\lambda}$ ise $C^{\perp}$ dual kodundaki sıfırdan farklı tüm kodsözcüklerinin minimal olduğu gösterilmiştir.

Anahtar Sözcükler: Dizayn, simetrik dizayn, $t-$dizayn, lineer kod, genişletilmiş kod, sır paylaşımı, sır paylaşım şeması, sır paylaşımının demokratiklik derecesi, minimal erişim kümesi, minimal kodsözcüğü.

Bilim Dalı Sayısal Kodu: 0924

University : İstanbul Kültür University
Institute : Institute of Science
Science Programme : Mathematics and Computer
Programme : Mathematics
Supervisor : Prof. Dr. Erol BALKANAY
Degree Awarded and Date : Ph. D. July 2010

ABSTRACT

SYMMETRIC DESIGNS, CODES AND A STUDY ON SECRET SHARING SCHEMES

Selda ÇALKAVUR

The subject of this thesis is to investigate the relationship between the associated secret sharing scheme and the code of a symmetric design.

In the first chapter of the thesis, $(v, b, r, k, \lambda)-$ design, $(v, k, \lambda)-$ symmetric design and $t-(v, k, \lambda)-$design concepts are examined.

In the second chapter, linear codes are explained. Within this context the concepts of Hamming distance, minimum distance, Hamming weight, dual code and parity-check matrix are given. Furthermore, the code of a design, the code of a symmetric design and the extended code of a symmetric design are explained.

Third chapter is allocated to the secret sharing problem. The secret sharing concept is explained and Massey's secret sharing scheme is described. Furthermore, minimal access set concept is given, the access structures of secret sharing schemes that are based on dual codes are explained. Minimal codewords are discussed and the degree of democratic of the secret sharing is explained.

In the fourth chapter, the transition from the code of symmetric design to secret sharing schemes are investigated. We have presented the number of minimal access sets in the secret sharing scheme that constructed over the code of symmetric designs. We also show that if $w_{maks} < \frac{2(k+\lambda)}{\lambda}$ for the dual code $C^{\perp}$ of the code C of $(v, k, \lambda)-$symmetric design then all of the codewords of $C^{\perp}$ are minimal.

Key Words: Design, symmetric design, $t-$design, linear code, extended code, secret sharing, secret sharing scheme, democratic of degree of secret sharing, minimal access set, minimal codeword.

Science Code: 0924