БЪЛГАРСКА АКАДЕМИЯ НА НАУКИТЕ
ИНСТИТУТ ПО МАТЕМАТИКА И ИНФОРМАТИКА

Утвърдил:
(проф. дмн П. Бойваленков, Директор на ИМИ-БАН)

КОНСПЕКТ
за кандидат-докторантски изпит
по докторска програма Методи за обработка и защита на данни
по допълнителен конкурс за учебната 2023/24 година
и по основен конкурс за учебната 2024/25 година

1. Кодове, поправящи грешки. Разстояние по Хеминг. Декодиране. Двоичен симетричен канал. Минимално кодово разстояние. Откриващи и декодиращи способности на кодовете.
2. Основна задача на теорията на кодирането. Граница на Хеминг и следствия. Съвършени кодове – дефиниция и примери.
3. Крайни полета, векторни пространства над крайни полета. Линейни кодове. Кодиране и декодиране с линейни кодове. Граница на Варшамов-Джилберт.
4. Ортогоналност в линейни пространства над крайни полета. Дуален код. Проверочна матрица. Синдроми и синдромно декодиране. Кодове на Хеминг.
5. Циклични кодове. Пораждащ полином, пораждаща и проверочна матрица.
6. Граница на Сингълтън. МДР кодове. Кодове на Рийд-Соломон.
7. Дизайни –определения и свойства. Симетрични дизайни.
8. Крайни геометрии и дизайни. Теореми на Брук-Райзер и Брук-Човла-Райзер.
9. Групи от пермутации. Действие на група върху множество. Групи от пермутации и дизайни.
10. Разширяване на дизайни.
11. Адамарови матрици и дизайни.
12. Булеви функции. Векторни булеви функции.
13. Графи – основни понятия, представяне, видове графи.
14. Канонична форма. Изоморфизъм на графи.
15. Криптографска система, място и роля на криптографските методи и средства. Класически и съвременен криптоанализ.
16. Симетрична и асиметрична криптография. Блокови шифри (DES, AES).
17. Системи с публичен ключ (RSA). Електронен подпис (ЕлГамал).
18. Кодове, поправящи изтривания.
19. Смесени двоични и троични кодове.
20. Сферични кодове и дизайни – примери, дефиниции и свойства.
21. Общи свойства на дървета на Щайнер.

Примерна литература

1. Fundamentals of Error-Correcting codes, W. C. Huffman, V. Pless, Cambridge University Press, 2003
2. The Theory of Error-Correcting codes, J. MacWilliams, N. J. A. Sloane, North-Holland, 1977
3. Cryptography and data security, D. E. Denning, Addison-Wesley Publishing Company, 1982
4. Coding theory and Cryptography, the essentials, D.C. Hankerson, CRC Press, 2000
5. Lovász L., Pelikán J., Vesztergombi K., Discrete Mathematics Elementary and Beyond, Springer Undergraduate Texts in Mathematics 2003
6. Analysis of Boolean Functions, O'Donnell R., May 2021 arXiv edition, https://www.cs.cmu.edu/~odonnell/papers/Analysis-of-Boolean-Functions-by-Ryan-ODonnell.pdf
7. A new table of binary/ternary mixed covering codes, Ostergard P.R.J., Hamalainen H.O., Des. Codes Cryptogr., 1 (1997), 151-178.
8. The Steiner Tree Problem, Hwang F.K., Richards D.S., Winter P., Annals of Discrete Mathematics, Volume 53. Elsevier, 1992
9. В. Тончев, Комбинаторни структури и кодове, Университетско издание "Климент Охридски", София, 1988

дата: 22.02.2024 г. Съставили: …… (доц. д-р Христо Костадинов) …… (гл. ас. д-р Константин Делчев)

Конспектът е обсъден и одобрен на заседания на секция **„Математически основи на информатиката"** на 26.02.2024 г.

Ръководител секция: ……
(Христо Костадинов)

Разгледан от Директорския съвет на ИМИ-БАН на 21.03.2024 г. (протокол № 13).

Приет от Научния съвет на ИМИ-БАН на 22.03.2024 г. (протокол № 3).