Huber, Michael

Combinatorial designs for authentication and secrecy codes. (English) Zbl 1209.94041


This monograph provides a tutorial on combinatorial designs, which gives an overview of the theory. Furthermore, the application of combinatorial designs to authentication and secrecy codes is described in depth. The author gives an introduction to the theory of combinatorial designs (t-designs, finite geometries, Latin squares, orthogonal arrays, perpendicular and authentication perpendicular arrays, splitting t-designs, etc.). Foundational and current results concerning the construction and characterization of authentication and secrecy codes are exposed later (general authentication codes, authentication codes with secrecy and with secrecy in the verification oracle model, authentication codes with splitting and also with arbitration).

This close relationship of designs with cryptography and information security was first revealed in Shannon’s seminal paper on secrecy systems. This monograph brings together in one source foundational and current contributions concerning design-theoretic constructions and characterizations of authentication and secrecy codes.

Reviewer: Vladimír Lacko (Košice)

MSC:

94A60 Cryptography
94A62 Authentication, digital signatures and secret sharing

Keywords:
combinatorial designs; authentication; secrecy; cryptography

Software:
OEIS; DISCRETA; DESIGN

Full Text: DOI