1. Record Nr. UNINA9910465421903321

Titolo	Algebraic geometry modeling in information theory [[electronic resource] /] / edited by Edgar Martinez Moro
Pubbl/distr/stampa	Hackensack, NJ, : World Scientific, 2013
ISBN	1-299-28125-7 981-4335-76-2
Descrizione fisica	1 online resource (334 p.)
Collana	Series on coding theory and cryptology ; ; v. 8
Altri autori (Persone)	Martinez-MoroEdgar
Disciplina	003/.54
Soggetti	Coding theory Geometry, Algebraic Cryptography Electronic books.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	Contents; Preface; Sage: A Basic Overview for Coding Theory and Cryptography D. Joyner; 0.1. Introduction; 0.2. What is Sage?; 0.2.1. Functionality of selected components of Sage; 0.2.2. History; 0.2.3. Why Python?; 0.2.4. The CLI; 0.2.5. The GUI; 0.2.6. Open source philosophy; 0.3. Coding theory functionality in Sage; 0.3.1. General constructions; 0.3.2. Coding theory functions; 0.3.3. Weight enumerator polynomial; 0.3.4. More code constructions; 0.3.5. Automorphism group of a code; 0.3.6. Even more code constructions; 0.3.7. Block designs and codes; 0.3.8. Special constructions 0.3.9. Coding theory bounds0.3.10. Asymptotic bounds; 0.4. Cryptography in Sage; 0.4.1. Classical cryptography; 0.4.2. Algebraic cryptosystems; 0.4.3. RSA; 0.4.4. Discrete logs; 0.4.5. Diffle-Hellman; 0.4.6. Linear feedback shift registers; 0.4.7. BBS streamcipher; 0.4.8. Blum-Goldwasser cryptosystem; 0.5. Miscellaneous topics; 0.5.1. Duursma zeta functions; 0.5.2. Self-dual codes; 0.5.3. Cool example (on self-dual codes); 0.6. Coding theory not implemented in Sage; References; Aspects of Random Network Coding O. Geil and C. Thomsen; 1.1. Introduction; 1.2. The network coding problem 1.2.1. Linear network coding for multicast1.2.2. A polynomial time

algorithm for solving the multicast problem; 1.3. Random network coding; 1.3.1. The algebraic approach; 1.3.2. The combinatorial approach; 1.3.2.1. Flow bounds; 1.3.2.2. The bounds by Balli, Yan, and Zhang; 1.4. Bibliographic notes; References; Steganography from a Coding Theory Point of View C. Munuera; 2.1. Introduction; 2.1.1. What is steganography?; 2.1.2. Digital steganography; 2.1.3. Steganography, cryptography and watermarking; 2.1.4. About this chapter; 2.2. Steganographic systems; 2.2.1. The cover
2.2.2. Steganographic schemes2.2.3. Selection rules; 2.2.4. Parameters; 2.2.5. Proper stegoschemes; 2.3. Error-Correcting codes; 2.3.1. Correcting errors; 2.3.2. Linear codes over fields; 2.3.3. An example: binary Hamming codes; 2.3.4. Generalized Hamming weights for linear codes; 2.4. Linking the problems; 2.4.1. Stegoschemes and error-correcting codes; 2.4.2. Group codes and stegoschemes; 2.4.3. Linear stegoschemes over rings Zq; 2.4.4. Linear stegoschemes over fields; 2.5. Bounds; 2.5.1. The domain of stegoschemes; 2.5.2. Balls and entropy; 2.5.3. A Hamming-like bound
2.5.4. Asymptotic bounds2.5.5. Perfect stegoschemes; 2.5.6. Another new problem for coding theory; 2.6. Nonshared selection rules; 2.6.1. Wet paper codes; 2.6.2. Solvability and the weight hierarchy of codes; 2.6.3. The rank of random matrices; 2.7. The ZZW embedding construction; 2.7.1. Description of the method; 2.7.2. Asymptotic behavior; 2.8. Bibliographical notes and further reading; Acknowledgments; References; An Introduction to LDPC Codes I. Marquez-Corbella and E. Martnez-Moro; 3.1. Introduction; 3.2. Representation for LDPC codes; 3.2.1. Tanner graph; 3.3. Communication channels
3.4. Decoding algorithms

Sommario/riassunto

Algebraic & geometry methods have constituted a basic background and tool for people working on classic block coding theory and cryptography. Nowadays, new paradigms on coding theory and cryptography have arisen such as: Network coding, S-Boxes, APN Functions, Steganography and decoding by linear programming. Again understanding the underlying procedure and symmetry of these topics needs a whole bunch of non trivial knowledge of algebra and geometry that will be used to both, evaluate those methods and search for new codes and cryptographic applications. This book shows those methods in a self