1. Record Nr. UNINA9910254838303321

| | |
|---|---|
| Autore | Nachef Valerie |
| Titolo | Feistel Ciphers : Security Proofs and Cryptanalysis / / by Valerie Nachef, Jacques Patarin, Emmanuel Volte |
| Pubbl/distr/stampa | Cham : , : Springer International Publishing : , : Imprint : Springer, , 2017 |
| Edizione | [1st ed. 2017.] |
| Descrizione fisica | 1 online resource (XV, 309 p. 39 illus., 6 illus. in color.) |
| Disciplina | 005.82 |
| Soggetti | Data encryption (Computer science)<br>Mathematical statistics<br>Computer science—Mathematics<br>Computer science - Mathematics<br>Cryptology<br>Probability and Statistics in Computer Science<br>Mathematical Applications in Computer Science |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Nota di bibliografia | Includes bibliographical references at the end of each chapters. |
| Nota di contenuto | Part 1 Definitions and first security results -- Chapter 1 Classical Feistel ciphers, first properties -- Chapter 2 Generalized Feistel ciphers, first properties -- Chapter 3 Luby-Rackoff Theorems -- Chapter 4 The coefficient H method -- Part 2 Generic Attacks -- Chapter 5 Introduction to cryptanalysis -- Chapter 6 Classical Feistel ciphers -- Chapter 7 Contracting Feistel ciphers -- Chapter 8 Expanding Feistel ciphers -- Chapter 9 Generalized Feistel ciphers -- Chapter 10 Classical Feistel ciphers with internal permutations -- Part 3: DES and other specific Feistel ciphers -- Chapter 11 DES (Definition, differential and linear cryptanalysis of DES) -- Chapter 12 3DES with 2 keys -- Chapter 13: XDES, 3DES with 3 keys -- Chapter 14 Bear-Lion, Cast, RC6, MARS, Coconut, Simon, Lucifer -- Part 4 Improved security results -- Chapter 15 Proofs beyond the birthday bound with the coupling method -- Chapter 16 Proofs beyond the birthday bound with the coefficient H method -- Chapter 17 Proofs based on games -- Chapter 18 Indifferentiability. |

Sommario/riassunto

This book provides a comprehensive survey of different kinds of Feistel ciphers, including their definition and mathematical/computational properties. Feistel Networks form the base design of the Data Encryption Standard algorithm, a former US NIST standard block cipher, originally released in 1977, and the framework used by several other symmetric ciphers ever since. The results consolidated in this volume provide an overview of this important cipher design to researchers and practitioners willing to understand the design and security analysis of Feistel ciphers.