1.

Record Nr.	UNINA9911049090603321
Autore	Patarin Jacques
Titolo	Guide to Feistel Ciphers : Security Proofs and Cryptanalysis / / by Jacques Patarin, Emmanuel Volte, Benoît Cogliati
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2026
ISBN	3-031-99850-2
Edizione	[2nd ed. 2026.]
Descrizione fisica	1 online resource (616 pages)
Collana	Information Security and Cryptography, , 2197-845X
Disciplina	005.824
Soggetti	Cryptography Data encryption (Computer science) Data protection Computer science - Mathematics Mathematical statistics Cryptology Data and Information Security Probability and Statistics in Computer Science Mathematical Applications in Computer Science
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
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 --

Sommario/riassunto

Feistel networks are one of the easiest ways to build pseudorandom permutations. Thanks to this property, many secret key algorithms (symmetric ciphers) have been designed as Feistel networks, and it is possible to design many others. The most famous of them is probably the Data Encryption Standard algorithm, a former U.S. National Institute of Standards and Technology standard block cipher, originally released in 1977. This book provides a comprehensive survey of different kinds of Feistel ciphers, including their definitions and mathematical/computational properties. Topics and features: Description of the best-known attacks against the Data Encryption Standard algorithm, including linear cryptanalysis, differential cryptanalysis, and Davies’ attack Generic attacks against balanced, unbalanced, and generalized Feistel networks Up-to-date security analysis of balanced Feistel networks Quantum cryptanalysis of Feistel networks 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.