1.	Record Nr.	UNINA9910767529903321
	Titolo	Fast software encryption : 5th international workshop, FSE '98, Paris, France, March 23-25, 1998 : proceedings / / Serge Vaudenay (editor)
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer, , [1998] Â©1998
	ISBN	3-540-69710-1
	Edizione	[1st ed. 1998.]
	Descrizione fisica	1 online resource (VIII, 297 p.)
	Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 1372
	Disciplina	004
	Soggetti	Computer science
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Bibliographic Level Mode of Issuance: Monograph
	Nota di bibliografia	Includes bibliographical references at the end of each chapters and index.
	Nota di contenuto	Cryptanalysis I -- New Results in Linear Cryptanalysis of RC5 -- Higher Order Differential Attack of a CAST Cipher -- Cryptanalysis of TWOPRIME -- New Stream Ciphers -- JEROBOAM -- Fast Hashing and Stream Encryption with Panama -- Joint Hardware / Software Design of a Fast Stream Cipher -- Design Construction Analysis -- On the Security of the Hashing Scheme Based on SL 2 -- About Feistel Schemes with Six (or More) Rounds -- Monkey: Black-Box Symmetric Ciphers Designed for MONopolizing KEYs -- Hash Functions -- MRD Hashing -- New Constructions for Secure Hash Functions -- Pseudo-Random Generators -- Cryptanalytic Attacks on Pseudorandom Number Generators -- New Block Ciphers -- CS-Cipher -- On the Design and Security of RC2 -- Serpent: A New Block Cipher Proposal -- Modes of Operations -- Attacking Triple Encryption -- Cryptanalysis of Some Recently-Proposed Multiple Modes of Operation -- Cryptanalysis II -- Differential Cryptanalysis of the ICE Encryption Algorithm -- The First Two Rounds of MD4 are Not One-Way -- Differential Cryptanalysis of KHF.