1.	Record Nr.	UNINA9910143605903321
	Titolo	Fast Software Encryption : 7th International Workshop, FSE 2000, New York, NY, USA, April 10-12, 2000. Proceedings / / edited by Bruce Schneier
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2001
	ISBN	3-540-44706-7
	Edizione	[1st ed. 2001.]
	Descrizione fisica	1 online resource (VIII, 324 p.)
	Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 1978
	Disciplina	005.8/2
	Soggetti	Data encryption (Computer science) Algorithms Coding theory Information theory Computer science—Mathematics Cryptology Algorithm Analysis and Problem Complexity Coding and Information Theory Discrete Mathematics in 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	Specific Stream-Cipher Cryptanalysis -- Real Time Cryptanalysis of A5/1 on a PC -- Statistical Analysis of the Alleged RC4 Keystream Generator -- New Ciphers -- The Software-Oriented Stream Cipher SSC2 -- Mercy: A Fast Large Block Cipher for Disk Sector Encryption -- AES Cryptanalysis 1 -- A Statistical Attack on RC6 -- Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent -- Correlations in RC6 with a Reduced Number of Rounds -- Block-Cipher Cryptanalysis 1 -- On the Interpolation Attacks on Block Ciphers -- Stochastic Cryptanalysis of Crypton -- Power Analysis -- Bitslice Ciphers and Power Analysis Attacks -- Securing the AES Finalists Against Power Analysis Attacks -- General Stream-Cipher Cryptanalysis -- Ciphertext only Reconstruction of Stream Ciphers Based on

Sommario/riassunto

Since 1993, cryptographic algorithm research has centered around the Fast So- ware Encryption (FSE) workshop. First held at Cambridge University with 30 attendees, it has grown over the years and has achieved worldwide recognition as a premiere conference. It has been held in Belgium, Israel, France, Italy, and, most recently, New York. FSE 2000 was the 7th international workshop, held in the United States for the rst time. Two hundred attendees gathered at the Hilton New York on Sixth Avenue, to hear 21 papers presented over the course of three days: 10{12 April 2000. These proceedings constitute a collection of the papers presented during those days. FSE concerns itself with research on classical encryption algorithms and - lated primitives, such as hash functions. This branch of cryptography has never been more in the public eye. Since 1997, NIST has been shepherding the Adv- ced Encryption Standard (AES) process, trying to select a replacement algorithm for DES. The rst AES conference, held in California the week before Crypto 98, had over 250 attendees. The second conference, held in Rome two days before FSE 99, had just under 200 attendees. The third AES conference was held in conjunction with FSE 2000, during the two days following it, at the same hotel.