1.	Record Nr.	UNISA996465852503316
	Titolo	Fast Software Encryption [[electronic resource]] : Third International Workshop, Cambridge, UK, February 21 - 23, 1996. Proceedings / / edited by Dieter Gollmann
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 1996
	ISBN	3-540-49652-1
	Edizione	[1st ed. 1996.]
	Descrizione fisica	1 online resource (CCXXXVI, 225 p.)
	Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 1039
	Disciplina	005.8/2
	Soggetti	Computers Data encryption (Computer science) Software engineering Algorithms Coding theory Information theory Combinatorics Theory of Computation Cryptology Software Engineering/Programming and Operating Systems Algorithm Analysis and Problem Complexity Coding and Information Theory
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Bibliographic Level Mode of Issuance: Monograph
	Nota di contenuto	Attacks on the HKM / HFX cryptosystem -- Truncated differentials of SAFER -- On the weak keys of blowfish -- High-bandwidth encryption with low-bandwidth smartcards -- ISAAC -- A note on the hash function of Tillich and zémor -- Cryptanalysis of MD4 -- RIPEMD-160: A strengthened version of RIPEMD -- Fast accumulated hashing -- Tiger: A fast new hash function -- The cipher SHARK -- Two practical and provably secure block ciphers: BEAR and LION -- Unbalanced Feistel networks and block cipher design -- A comparison of fast correlation attacks -- Correlation attacks on stream ciphers:

Computing low-weight parity checks based on error-correcting codes -- On the security of nonlinear filter generators -- Faster Luby-Rackoff ciphers -- New structure of block ciphers with provable security against differential and linear cryptanalysis.

Sommario/riassunto

This book constitutes the refereed proceedings of the Third International Workshop on Fast Software Encryption; this workshop was held in conjunction with the program on computer security, cryptology, and coding theory at the Isaac Newton Institute in Cambridge, UK in February 1996. The 18 revised papers presented were carefully selected for inclusion in the volume by the program committee. They report the state of the art in the field of fast encryption algorithms and are organized in sections on block cipher analysis, applications, hash functions, block cipher proposals, correlation analysis, and design criteria for block ciphers.