1.	Record Nr.	UNISA996465327503316
	Autore	Ding Cunsheng
	Titolo	The Stability Theory of Stream Ciphers [[electronic resource] /] / by Cunsheng Ding, Guozhen Xiao, Weijuan Shan
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 1991
	ISBN	3-540-46626-6
	Edizione	[1st ed. 1991.]
	Descrizione fisica	1 online resource (X, 194 p.)
	Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 561
	Disciplina	652/.8
	Soggetti	Data encryption (Computer science) Computer security Operating systems (Computers) Numerical analysis Cryptology Systems and Data Security Operating Systems Numerical Analysis
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Bibliographic Level Mode of Issuance: Monograph
	Nota di contenuto	Stream ciphers -- The BAA attacks on several classes of stream ciphers -- Measure indexes on the security of stream ciphers -- The stability of linear complexity of sequences -- The period stability of sequences -- Summary and open problems.

Sommario/riassunto

Secure message transmission is of extreme importance in today's information-based society. Stream encryption is a practically important means to this end. This monograph is devoted to a new aspect of stream ciphers, namely the stability theory of stream ciphers, with the purpose of developing bounds on complexity which can form part of the basis for a general theory of data security and of stabilizing stream-cipher systems. The approach adopted in this monograph is new. The topic is treated by introducing measure indexes on the security of stream ciphers, developing lower bounds on these indexes, and establishing connections among them. The treatment involves the stability of boolean functions, the stability of linear complexity of key

streams, the period stability of key streams, and the stability of source codes. Misleading ideas about stream ciphers are exposed and new viewpoints presented. The numerous measure indexes and bounds on them that are introduced here, the approach based on spectrum techniques, andthe ten open problems presented will all be useful to the reader concerned with analyzing and designing stream ciphers for securing data.