1. Record Nr. UNINA9910791961103321

Titolo	Advanced linear cryptanalysis of block and stream ciphers [[electronic resource] /] / edited by Pascal Junod and Anne Canteaut
Pubbl/distr/stampa	Amsterdam ; ; Washington, D.C., : IOS Press, c2011
ISBN	6613433039 1-283-43303-6 9786613433039 1-60750-844-3
Descrizione fisica	1 online resource (144 p.)
Collana	Cryptology and information security series, , 1871-6431 ; ; v. 7
Altri autori (Persone)	JunodPascal CanteautAnne
Disciplina	005.8/2 005.82
Soggetti	Cryptography Ciphers
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and indexes.
Nota di contenuto	Title page; Preface; Contents; Experimenting Linear Cryptanalysis; Linear Cryptanalysis Using Multiple Linear Approximations; Linear Attacks on Stream Ciphers; Using Tools from Error Correcting Theory in Linear Cryptanalysis; Correlation Analysis in GF(2n); Subject Index; Author Index
Sommario/riassunto	The origins of linear cryptanalysis can be traced back to a number of seminal works of the early 1990's. Since its invention, several theoretical and practical aspects of the technique have been studied, understood and generalized, resulting in more elaborated attacks against certain ciphers, but also in some negative results regarding the potential of various attempts at generalization. This book gives an overview of the current state of the discipline and it takes a look at potential future developments, and is divided into five parts. The first part deals with basic assumptions in linear cry