1.

Record Nr.	UNINA9910298971103321
Autore	Budaghyan Lilya
Titolo	Construction and analysis of cryptographic functions / / by Lilya Budaghyan
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2014
ISBN	3-319-12991-0
Edizione	[1st ed. 2014.]
Descrizione fisica	1 online resource (172 p.)
Disciplina	003.54 004 005.82 511.6
Soggetti	Coding theory Information theory Data encryption (Computer science) Difference equations Functional equations Combinatorial analysis Coding and Information Theory Cryptology Difference and Functional Equations Combinatorics
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.
Nota di contenuto	Introduction -- Generalities -- Equivalence relations of functions -- Bent functions -- New classes of APN and AB polynomials -- Construction of planar functions.
Sommario/riassunto	This book covers novel research on construction and analysis of optimal cryptographic functions such as almost perfect nonlinear (APN), almost bent (AB), planar and bent functions. These functions have optimal resistance to linear and/or differential attacks, which are the two most powerful attacks on symmetric cryptosystems. Besides cryptographic applications, these functions are significant in many

branches of mathematics and information theory including coding theory, combinatorics, commutative algebra, finite geometry, sequence design and quantum information theory. The author analyzes equivalence relations for these functions and develops several new methods for construction of their infinite families. In addition, the book offers solutions to two longstanding open problems, including the problem on characterization of APN and AB functions via Boolean, and the problem on the relation between two classes of bent functions.