1. Record Nr. UNINA9910484830403321

Autore	Mukherjee Chandra Sekhar
Titolo	Design and Cryptanalysis of ZUC : A Stream Cipher in Mobile Telephony / / by Chandra Sekhar Mukherjee, Dibyendu Roy, Subhamoy Maitra
Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2021
ISBN	981-334-882-8
Edizione	[1st ed. 2021.]
Descrizione fisica	1 online resource (XVIII, 98 p. 17 illus., 2 illus. in color.)
Collana	SpringerBriefs on Cyber Security Systems and Networks, , 2522-557X
Disciplina	621.384560286
Soggetti	Computer science Cryptography Data encryption (Computer science) Computer Science Cryptology
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	1. Introduction and Preliminaries -- 2. Introduction and Preliminaries -- 3. Introduction and Preliminaries -- 4. Introduction and Preliminaries -- 5. Introduction and Preliminaries -- 6. Test Vectors for ZUC.
Sommario/riassunto	This book is a timely document of state-of-the art analytical techniques in the domain of stream cipher design and analysis with a specific cipher, named ZUC. It links new research to brief contextual literature review in the domain of complex LFSR-based stream ciphers. A snapshot of how stream ciphers are deployed in the mobile telephony architecture, one of the most well-known topics for more than five decades in the domain of computer and communication sciences, is presented in this book. The book provides an in-depth study on design and cryptanalysis of ZUC as well as relevant research results in this field with directions towards future analysis of this cipher.