1. Record Nr.   UNISA996466445603316

   Titolo   Constructive Side-Channel Analysis and Secure Design [[electronic
                        resource]] : 10th International Workshop, COSADE 2019, Darmstadt,
                        Germany, April 3–5, 2019, Proceedings / / edited by Ilia Polian, Marc
                        Stöttinger

   Pubbl/distr/stampa   Cham : , : Springer International Publishing : , : Imprint : Springer, ,
                        2019

   ISBN   3-030-16350-4

   Edizione   [1st ed. 2019.]

   Descrizione fisica   1 online resource (X, 303 p. 230 illus., 64 illus. in color.)

   Collana   Security and Cryptology ; ; 11421

   Disciplina   005.8

   Soggetti   Computer security
                        Computer organization
                        Microprogramming
                        Coding theory
                        Information theory
                        Operating systems (Computers)
                        Systems and Data Security
                        Computer Systems Organization and Communication Networks
                        Control Structures and Microprogramming
                        Coding and Information Theory
                        Operating Systems

   Lingua di pubblicazione   Inglese

   Formato   Materiale a stampa

   Livello bibliografico   Monografia

   Nota di contenuto   Side-Channel Attacks -- Fault-Injection Attacks -- White-Box Attacks
                        -- Side-Channel Analysis Methodologies -- Security Aspects of Post-
                        Quantum Schemes -- Countermeasures Against Implementation
                        Attacks.

   Sommario/riassunto   This book constitutes revised selected papers from the 10th
                        International Workshop on Constructive Side-Channel Analysis and
                        Secure Design, COSADE 2019, held in Darmstadt, Germany, in April
                        2019. The 14 papers presented together with one keynote and one
                        invited talk in this volume were carefully reviewed and selected from 34

submissions. They were organized in topical sections named: Side-Channel Attacks; Fault-Injection Attacks; White-Box Attacks; Side-Channel Analysis Methodologies; Security Aspects of Post-Quantum Schemes; and Countermeasures Against Implementation Attacks.