1. Record Nr. UNINA9910438051503321

Autore	Peeters Eric
Titolo	Advanced DPA theory and practice : towards the security limits of secure embedded circuits / / Eric Peeters
Pubbl/distr/stampa	New York, NY, : Springer, c2013
ISBN	1-4614-6783-7
Edizione	[1st ed. 2013.]
Descrizione fisica	1 online resource (xvi, 139 pages) : illustrations (some color)
Collana	Gale eBooks
Disciplina	005.8
Soggetti	Embedded computer systems - Security measures Data encryption (Computer science) Cryptography
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 index.
Nota di contenuto	General Introduction -- Side-Channel Cryptanalysis: a brief survey -- CMOS devices: sources and models of emanation -- Measurement of the power consumption -- Electromagnetic Leakage -- Statistical Tools -- Higher Order Attacks -- Towards the Evaluation of an Implementation against Side-Channel Attacks -- General Conclusion and Possible Further Directions.
Sommario/riassunto	Advanced DPA Theory and Practice provides a thorough survey of new physical leakages of embedded systems, namely the power and the electromagnetic emanations. The book presents a thorough analysis about leakage origin of embedded system. This book examines the systematic approach of the different aspects and advanced details about experimental setup for electromagnetic attack. The author discusses advanced statistical methods to successfully attack embedded devices such as high-order attack, template attack in principal subspaces, machine learning methods. The book includes theoretical framework to define side-channel based on two metrics: mutual information and success rate.