

1. Record Nr.	UNISA996466051703316
Titolo	Cryptographic Hardware and Embedded Systems -- CHES 2013 [[electronic resource]] : 15th International Workshop, Santa Barbara, CA, USA, August 20-23, 2013, Proceedings // edited by Guido Marco Bertoni, Jean-Sébastien Coron
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2013
ISBN	3-642-40349-2
Edizione	[1st ed. 2013.]
Descrizione fisica	1 online resource (XIV, 490 p. 172 illus.)
Collana	Security and Cryptology ; ; 8086
Disciplina	005.82
Soggetti	Data encryption (Computer science) Computer security Algorithms Cryptology Systems and Data Security Algorithm Analysis and Problem Complexity
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Side-channel attacks -- Physical unclonable function -- Lightweight cryptography -- Hardware implementations and fault attacks -- Efficient and secure implementations -- Elliptic curve cryptography -- masking -- Side-channel attacks and countermeasures.
Sommario/riassunto	This book constitutes the proceedings of the 15th International Workshop on Cryptographic Hardware and Embedded Systems, CHES 2013, held in Santa Barbara, CA, USA, in August 2013. The 27 papers presented were carefully reviewed and selected from 132 submissions. The papers are organized in the following topical sections: side-channel attacks; physical unclonable function; lightweight cryptography; hardware implementations and fault attacks; efficient and secure implementations; elliptic curve cryptography; masking; side-channel attacks and countermeasures.