1.

Record Nr.	UNISA996200345703316
Titolo	Lightweight Cryptography for Security and Privacy [[electronic resource]] : Third International Workshop, LightSec 2014, Istanbul, Turkey, September 1-2, 2014, Revised Selected Papers / / edited by Thomas Eisenbarth, Erdinç Öztürk
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2015
ISBN	3-319-16363-9
Edizione	[1st ed. 2015.]
Descrizione fisica	1 online resource (XIII, 169 p. 33 illus.)
Collana	Security and Cryptology ; ; 8898
Disciplina	005.8
Soggetti	Data encryption (Computer science) Computer security Computer communication systems Algorithms Cryptology Systems and Data Security Computer Communication Networks 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	The SIMON and SPECK Block Ciphers on AVR 8-Bit Microcontrollers -- The Multiplicative Complexity of Boolean Functions on Four and Five Variables -- A Flexible and Compact Hardware Architecture for the SIMON Block Cipher -- AES Smaller Than S-Box: Minimalism in Software Design on Low End Microcontrollers -- Differential Factors: Improved Attacks on SERPENT -- Ciphertext-Only Fault Attacks on PRESENT -- Relating Undisturbed Bits to Other Properties of Substitution Boxes -- Differential Sieving for 2-Step Matching Meet-in-the-Middle Attack with Application to LBlock -- Match Box Meet-in-the-Middle Attacks on the SIMON Family of Block Ciphers -- A Provably Secure Offline RFID Yoking-Proof Protocol with Anonymity.
Sommario/riassunto	This book constitutes the refereed post-conference proceedings of the Third International Workshop on Lightweight Cryptography for Security

and Privacy, LightSec 2014, held in Istanbul, Turkey, in September 2014. The 10 full papers presented were carefully reviewed and selected from 24 submissions. The papers are organized in the following topical sections: efficient implementations and designs; attacks; and protocols.