1.

Record Nr.	UNINA9910739451003321
Titolo	Selected Areas in Cryptography : 19th International Conference, SAC 2012, Windsor, Canada, August 15-16, 2012, Revised Selected Papers / / edited by Lars R. Knudsen, Huapeng Wu
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2013
ISBN	3-642-35999-X
Edizione	[1st ed. 2013.]
Descrizione fisica	1 online resource (XIV, 407 p. 61 illus.)
Collana	Security and Cryptology, , 2946-1863 ; ; 7707
Disciplina	005.82
Soggetti	Cryptography Data encryption (Computer science) Data protection Algorithms Computer networks Application software Cryptology Data and Information Security Computer Communication Networks Computer and Information Systems Applications
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Cryptanalysis -- An All-In-One Approach to Differential Cryptanalysis for Small Block Ciphers -- A New Method for Solving Polynomial Systems with Noise over F2 and Its Applications in Cold Boot Key Recovery -- Cryptanalysis of the Xiao – Lai White-Box AES Implementation -- Digital Signatures A Practical Leakage-Resilient Signature Scheme in the Generic Group Model -- Forward Secure Signatures on Smart Cards -- The Stafford Tavares Lecture Extracts from the SHA-3 Competition -- Stream Ciphers Cryptanalysis of the “Kindle” Cipher -- Cryptographically Strong de Bruijn Sequences with Large Periods -- Cryptanalysis of the Loiss Stream Cipher -- Implementations -- Efficient Arithmetic on Elliptic Curves over Fields of Characteristic Three -- Efficient Implementation of Bilinear Pairings on

ARM Processors -- Towards Faster and Greener Cryptoprocessor for Eta Pairing on Supersingular Elliptic Curve over F21223 -- Feasibility and Practicability of Standardized Cryptography on 4-bit Micro Controllers -- Block Cipher Cryptanalysis -- All Subkeys Recovery Attack on Block Ciphers: Extending Meet-in-the-Middle Approach -- Improved Cryptanalysis of the Block Cipher KASUMI -- Meet-in-the-Middle Technique for Integral Attacks against Feistel Ciphers -- Attacking (EC) DSA Given Only an Implicit Hint -- Lattice Reduction for Modular Knapsack -- Hash Functions -- The Boomerang Attacks on the Round-Reduced Skein-512 -- Boomerang and Slide-Rotational Analysis of the SM3 Hash Function -- Provable Security of BLAKE with Non-ideal Compression Function -- Block Cipher Constructions TWINE: A Lightweight Block Cipher for Multiple Platforms -- Recursive Diffusion Layers for (Lightweight) Block Ciphers and Hash Functions -- Miscellaneous -- Private Stream Search at Almost the Same Communication Cost as a Regular Search -- An Optimal Key Enumeration Algorithm and Its Application to Side-Channel Attacks.

Sommario/riassunto

This book constitutes the thoroughly refereed post-conference proceedings of the 19th International Conference on Selected Areas in Cryptography, SAC 2012, held in Windsor, Ontario, Canada, in August 2012. The 24 papers presented were carefully reviewed and selected from 87 submissions. They are organized in topical sections named: cryptanalysis, digital signatures, stream ciphers, implementations, block cipher cryptanalysis, lattices, hashfunctions, blockcipher constructions, and miscellaneous.