1. Record Nr. NYU004389908

Autore	[SAC (Conference) (19th : 2012 : Windsor, Ont.)]
Titolo	Selected areas in cryptography : 19th International Conference, SAC 2012, Windsor, ON, Canada, August 15-16, 2012, Revised selected papers / Lars R. Knudsen, Huapeng Wu (eds.).
Pubbl/distr/stampa	Berlin ; New York : Springer, ©2013
ISBN	9783642359996 364235999X 3642359981 9783642359989
Descrizione fisica	1 online resource.
Collana	Lecture notes in computer science, 0302-9743 ; 7707 LNCS sublibrary. SL 4, Security and cryptology
Classificazione	54.62
Altri autori (Persone)	Knudsen, Lars, 1962- Wu, Huapeng, 1965-
Disciplina	005.8/2
Collocazione	Electronic access
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes author index.
Nota di contenuto	Cryptanalysis -- An All-In-One Approach to Differential Cryptanalysis for Small Block Ciphers / Martin R. Albrecht, Gregor Leander -- A New Method for Solving Polynomial Systems with Noise over F2 and Its Applications in Cold Boot Key Recovery / Zhenyu Huang, Dongdai Lin -- Cryptanalysis of the Xiao -- Lai White-Box AES Implementation / Yoni De Mulder, Peter Roelse, Bart Preneel -- Digital Signatures -- A Practical Leakage-Resilient Signature Scheme in the Generic Group Model / David Galindo, Srinivas Vivek -- Forward Secure Signatures on Smart Cards / Andreas Hülsing, Christoph Busold, Johannes Buchmann -- The Stafford Tavares Lecture -- Extracts from the SHA-3 Competition / Vincent Rijmen -- Stream Ciphers -- Cryptanalysis of the "Kindle" Cipher / Alex Biryukov, Gaëtan Leurent, Arnab Roy -- Cryptographically Strong de Bruijn Sequences with Large Periods / Kalikinkar Mandal, Guang Gong -- Cryptanalysis of the Loiss Stream Cipher / Alex Biryukov, Aleksandar Kircanski, Amr M. Youssef. Implementations -- Efficient Arithmetic on Elliptic Curves over Fields of Characteristic Three / Reza R. Farashahi, Hongfeng Wu, Chang-An Zhao

-- Efficient Implementation of Bilinear Pairings on ARM Processors / Gurleen Grewal, Reza Azarderakhsh, Patrick Longa, Shi Hu, David Jao -- Towards Faster and Greener Cryptoprocessor for Eta Pairing on Supersingular Elliptic Curve over F21223 / Jithra Adikari, M. Anwar Hasan, Christophe Negre -- Feasibility and Practicability of Standardized Cryptography on 4-bit Micro Controllers / Nisha Jacob, Sirote Saetang, Chien-Ning Chen, Sebastian Kutzner, San Ling -- Block Cipher Cryptanalysis -- All Subkeys Recovery Attack on Block Ciphers: Extending Meet-in-the-Middle Approach / Takanori Isobe, Kyoji Shibutani -- Improved Cryptanalysis of the Block Cipher KASUMI / Keting Jia, Leibo Li, Christian Rechberger, Jiazhe Chen, Xiaoyun Wang -- Meet-in-the-Middle Technique for Integral Attacks against Feistel Ciphers / Yu Sasaki, Lei Wang -- Lattices -- Attacking (EC)DSA Given Only an Implicit Hint / Jean-Charles Faugère, Christopher Goyet, Guénaël Renault.
Lattice Reduction for Modular Knapsack / Thomas Plantard, Willy Susilo, Zhenfei Zhang -- Hash Functions -- The Boomerang Attacks on the Round-Reduced Skein-512 / Hongbo Yu, Jiazhe Chen, Xiaoyun Wang -- Boomerang and Slide-Rotational Analysis of the SM3 Hash Function / Aleksandar Kircanski, Yanzhao Shen, Gaoli Wang, Amr M. Youssef -- Hash Functions -- Provable Security of BLAKE with Non-ideal Compression Function / Elena Andreeva, Atul Luykx, Bart Mennink -- Block Cipher Constructions -- \textnormal\textscTWINE : A Lightweight Block Cipher for Multiple Platforms / Tomoyasu Suzaki, Kazuhiko Minematsu, Sumio Morioka, Eita Kobayashi -- Recursive Diffusion Layers for (Lightweight) Block Ciphers and Hash Functions / Shengbao Wu, Mingsheng Wang, Wenling Wu -- Miscellaneous -- Private Stream Search at Almost the Same Communication Cost as a Regular Search / Matthieu Finiasz, Kannan Ramchandran -- An Optimal Key Enumeration Algorithm and Its Application to Side-Channel Attacks / Nicolas Veyrat-Charvillon, Benoît Gérard, Mathieu Renauld, François-Xavier Standaert.

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.