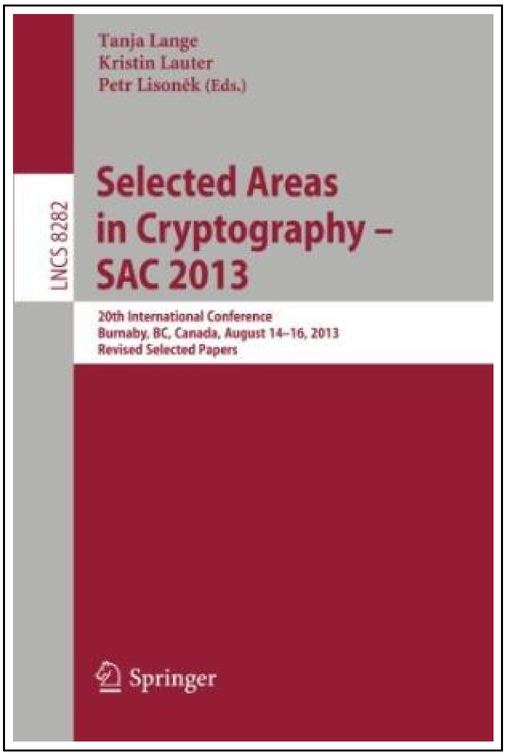
Selected Areas in Cryptography -- SAC 2013



Tanja Lange
Kristin Lauter
Petr Lisoněk (Eds.)

Selected Areas in Cryptography – SAC 2013

LNCS 8282

20th International Conference
Burnaby, BC, Canada, August 14–16, 2013
Revised Selected Papers

Springer

Filesize: 1.18 MB

Reviews

An incredibly great book with perfect and lucid reasons. It really is writter in straightforward words instead of confusing. I am just very easily could get a delight of reading through a written pdf.
(Curt Bogan)

SELECTED AREAS IN CRYPTOGRAPHY -- SAC 2013

DOWNLOAD PDF

Condition: New. Publisher/Verlag: Springer, Berlin | 20th International Conference, Burnaby, BC, Canada, August 14-16, 2013, Revised Selected Papers | This book constitutes the proceedings of the 20th International Conference on Selected Areas in Cryptography, SAC 2013, held in Burnaby, Canada, in August 2013. The 26 papers presented in this volume were carefully reviewed and selected from 98 submissions. They are organized in topical sections named: lattices; discrete logarithms; stream ciphers and authenticated encryption; post-quantum (hash-based and system solving); white box crypto; block ciphers; elliptic curves, pairings and RSA; hash functions and MACs; and side-channel attacks. The book also contains 3 full-length invited talks. | The Realm of the Pairings.- A Three-Level Sieve Algorithm for the Shortest Vector Problem.- Improvement and Efficient Implementation of a Lattice-based Signature Scheme.- Towards Practical Lattice-Based Public-Key Encryption on Reconfigurable Hardware.- Practical approaches to varying network size in combinatorial key pre distribution schemes.- Similarities between encryption and decryption: how far can we go.- A Group Action on Z p and the Generalized DLP with Auxiliary Inputs.- Solving a 6120-bit DLP on a Desktop Computer.- Stream ciphers and authenticated encryption How to Recover Any Byte of Plaintext on RC4.- The LOCAL attack: Cryptanalysis of the authenticated encryption scheme ALE.- AEGIS: A Fast Authenticated Encryption Algorithm.- Fast Exhaustive Search for Quadratic Systems in F2 on FPGAs.- Faster Hash-based Signatures with Bounded Leakage.- White-Box Security Notions for Symmetric Encryption Schemes.- Two Attacks on a White-Box AES Implementation.- Extended Generalized Feistel Networks using Matrix Representation.- Zero-Correlation Linear Cryptanalysis with FFT and Improved Attacks on ISO Standards Camellia and CLEFIA.- Implementing Lightweight Block Ciphers on x86 Architectures.- A new index calculus algorithm with complexity L(1=4 + o(1)) in small characteristic.- High Precision Discrete Gaussian Sampling on FPGAs.- Discrete Ziggurat: A Time-Memory Trade-off for Sampling from a Gaussian Distribution over the Integers.-...

Read Selected Areas in Cryptography -- SAC 2013 Online

Download PDF Selected Areas in Cryptography -- SAC 2013