1. Record Nr. UNISA996466454303316

Titolo	Progress in Cryptology – AFRICACRYPT 2019 [[electronic resource]] : 11th International Conference on Cryptology in Africa, Rabat, Morocco, July 9–11, 2019, Proceedings / / edited by Johannes Buchmann, Abderrahmane Nitaj, Tajjeeddine Rachidi
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019
ISBN	3-030-23696-X
Edizione	[1st ed. 2019.]
Descrizione fisica	1 online resource (XVI, 449 p. 705 illus., 52 illus. in color.)
Collana	Security and Cryptology ; ; 11627
Disciplina	005.8
Soggetti	Computer security Computer communication systems Computers Coding theory Information theory Software engineering Systems and Data Security Computer Communication Networks Computing Milieux Coding and Information Theory Software Engineering
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Protocols -- Tiny WireGuard Tweak -- Extended 3-Party ACCE and Application to LoRaWAN 1.1 -- Post-Quantum Cryptography -- The Mersenne Low Hamming Combination Search Problem can be reduced to an ILP Problem -- Simple Oblivious Transfer Protocols Compatible with Supersingular Isogenies -- An IND-CCA-Secure Code-Based Encryption Scheme Using Rank Metric -- Zero-Knowledge -- UC-Secure CRS Generation for SNARKs -- On the Efficiency of Privacy-Preserving Smart Contract Systems -- Lattice Based Cryptography -- Ring Signatures based on Middle-Product Learning with Errors Problems -- Sampling the Integers with Low Relative Error -- A Refined

Analysis of the Cost for Solving LWE via uSVP -- New Schemes and Analysis -- Memory-Efficient High-Speed Implementation of Kyber on Cortex-M4 -- Reducing the Cost of Authenticity with Leakages: a CIML2-Secure AE Scheme with One Call to a Strongly Protected Tweakable Block Cipher -- An Improvement of Correlation Analysis for Vectorial Boolean Functions -- Block Ciphers -- On MILP-Based Automatic Search for Differential Trails Through Modular Additions with Application to Bel-T -- Practical Attacks on Reduced-Round AES -- Six Shades of AES -- Side-Channel Attacks and Countermeasures -- Revisiting Location Privacy from a Side-Channel Analysis Viewpoint -- Side Channel Analysis of SPARX-64/128: Cryptanalysis and Countermeasures -- Analysis of Two Countermeasures against the Signal Leakage Attack -- Signatures -- Handling Vinegar Variables to Shorten Rainbow Key Pairs -- Further Lower Bounds for Structure-Preserving Signatures in Asymmetric Bilinear Groups -- A New Approach to Modelling Centralised Reputation Systems.

Sommario/riassunto

This book constitutes the refereed proceedings of the 11th International Conference on the Theory and Application of Cryptographic Techniques in Africa, AFRICACRYPT 2019, held in Rabat, Morocco, in July 2019. The 22 papers presented in this book were carefully reviewed and selected from 53 submissions. The papers are organized in topical sections on protocols; post-quantum cryptography; zero-knowledge; lattice based cryptography; new schemes and analysis; block ciphers; side-channel attacks and countermeasures; signatures. AFRICACRYPT is a major scientific event that seeks to advance and promote the field of cryptology on the African continent. The conference has systematically drawn some excellent contributions to the field. The conference has always been organized in cooperation with the International Association for Cryptologic Research (IACR).