1. Record Nr. UNINA9910874679303321

Titolo	Information Security and Privacy : 29th Australasian Conference, ACISP 2024, Sydney, NSW, Australia, July 15–17, 2024, Proceedings, Part I / / edited by Tianqing Zhu, Yannan Li
Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2024
ISBN	9789819750252 9789819750245
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (507 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14895
Disciplina	005.8
Soggetti	Data protection Data and Information Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Symmetric Key Cryptography -- The Offline Quantum Attack Against Modular Addition Variant of Even-Mansour Cipher -- Known Key Attack on GIFT 64 and GIFT 64 Based on Correlation Matrices -- On the Security Bounds for Block Ciphers without Whitening Key Addition against Integral Distinguishers -- On the Security Bounds for Block Ciphers without Whitening Key Addition against Integral Distinguishers -- Tight Multi user Security of Ascon and Its Large Key Extension -- Differential Distinguishing Attacks on SNOWV, SNOWVi and KCipher2 -- Efficient Search for Optimal Permutations of Refined TypeII Generalized Feistel Structures -- Homomorphic Encryption -- FFHEW High Precision Approximate Homomorphic Encryption with Batch Bootstrapping -- NTRU based FHE for Larger Key and Message Space -- An Efficient Integer-wise ReLU on TFHE -- HERatio Homomorphic Encryption of Rationals using Laurent polynomials -- TFHE Bootstrapping Faster Smaller and Time Space TradeOffs -- Approximate Methods for the Computation of Step Functions in Homomorphic Encryption -- Encryption and its Applications -- Key Cooperative Attribute-Based Encryption -- On the Feasibility of Identity based Encryption with Equality Test against Insider Attacks -- Non interactive Publicly Verifiable Searchable Encryption with Forward and Backward Privacy -- On the Implication from Updatable Encryption to Public Key

Cryptographic Primitives -- Continuous Version of Non malleable Codes from Authenticated Encryption -- Digital Signatures -- Pairing Free ID Based Signatures as Secure as Discrete Logarithm in AGM -- Threshold Ring Signatures with Accountability -- Threshold Signatures with Private Accountability via Secretly Designated Witnesses -- Cryptographic Primitives -- A Novel Window NAF on Koblitz Curves -- Parallel Algorithms on Hyperelliptic Pairings using Hyperelliptic Nets -- AlgSAT a SAT Method for Verification of Differential Trails from an Algebraic Perspective -- Hadamard product argument from Lagrange-based univariate polynomials.

Sommario/riassunto

This volume constitutes the refereed proceedings of the 29th Australasian Conference, ACISP 2024, held in Sydney, NSW, Australia, during July 15–17, 2024. The 70 full papers were carefully reviewed and selected from 232 submission. They are categorized in the following sections: Symmetric Key Cryptography, Homomorphic Encryption, Encryption and its Applications, Digital Signatures.