1. Record Nr. UNINA9910855389703321

Autore	Oswald Elisabeth
Titolo	Topics in Cryptology – CT-RSA 2024 : Cryptographers' Track at the RSA Conference 2024, San Francisco, CA, USA, May 6–9, 2024, Proceedings / / edited by Elisabeth Oswald
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
ISBN	9783031588686 3031588681
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (490 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14643
Disciplina	5,824
Soggetti	Cryptography Data encryption (Computer science) Computer networks Computer engineering Coding theory Information theory Cryptology Computer Communication Networks Computer Engineering and Networks Coding and Information Theory
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	A Public Key Identity-Based Revocation Scheme: Fully Attribute-Hiding and Function Private -- The Security of the Full EDHOC Protocol in the Multi-user Setting -- The Multi-User Security of MACs via Universal Hashing in the Ideal Cipher Model -- Automated-based Rebound Attacks on ACE Permutation -- Batch Signatures, Revisited -- History-Free Sequential Aggregation of Hash-and-Sign Signatures -- TFHE Public-Key Encryption Revisited -- Differential Privacy for Free? Harnessing the Noise in Approximate Homomorphic Encryption -- The Exact Multi-User Security of 2-Key Triple DES -- Improved Meet-in-the-Middle Attacks on 9-Round AES-192 -- Identity-Based Encryption from LWE with More Compact Master Public Key -- Towards Compact

	Identity-based Encryption on Ideal Lattices -- Attribute-Based Signatures with Advanced Delegation, and Tracing -- Lattice-based Threshold, Accountable, and Private Signature -- Ascon MAC, PRF, and Short-Input PRF -- Interactive Oracle Arguments in the QROM and Applications to Succinct Verification of Quantum Computation -- Parameterization of Fault Adversary Models - Connecting Theory and Practice -- Cutting the GRASS: Threshold GRoup Action Signature Schemes.
Sommario/riassunto	This book constitutes the refereed proceedings of the Cryptographer's Track at the RSA Conference 2024, CT-RSA 2024, held in San Francisco, CA, USA, during May 6–9, 2024. The 18 full papers presented in this volume were carefully reviewed and selected from 46 submissions. The conference presents papers on subjects such as public key cryptography; symmetric cryptography; signatures; homomorphic encryption; identity-based encryption; constructions; and threshold signatures and fault attacks.