

| | |
|-------------------------|--|
| 1. Record Nr. | UNINA9910157616803321 |
| Autore | Sliwa Wanda <1931-> |
| Titolo | Cyclodextrins : properties and applications / / Wanda Sliwa and Tomasz Girek |
| Pubbl/distr/stampa | Weinheim, Germany : , : Wiley-VCH, , 2017 ©2017 |
| ISBN | 3-527-69530-3 3-527-69529-X |
| Descrizione fisica | 1 online resource (337 pages) : illustrations |
| Disciplina | 547.7815 |
| Soggetti | Cyclodextrins |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Nota di bibliografia | Includes bibliographical references at the end of each chapters and index. |

| | |
|-------------------------|--|
| 2. Record Nr. | UNINA9910349277103321 |
| Titolo | Provable Security : 13th International Conference, ProvSec 2019, Cairns, QLD, Australia, October 1–4, 2019, Proceedings / / edited by Ron Steinfeld, Tsz Hon Yuen |
| Pubbl/distr/stampa | Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019 |
| ISBN | 3-030-31919-9 |
| Edizione | [1st ed. 2019.] |
| Descrizione fisica | 1 online resource (XI, 382 p. 131 illus., 9 illus. in color.) |
| Collana | Security and Cryptology, , 2946-1863 ; ; 11821 |
| Disciplina | 005.8 |
| Soggetti | Cryptography Data encryption (Computer science) Computers Computer networks Software engineering Cryptology Computing Milieux Computer Communication Networks Software Engineering |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Nota di bibliografia | Includes bibliographical references and index. |
| Nota di contenuto | Lattice-based IBE with equality test in standard model -- A critique of game-based denitions of receipt-freeness for voting -- One-Round Authenticated Group Key Exchange from Isogenies -- History-Free Sequential Aggregate MAC Revisited -- An Ecient Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks Using Online/Offine Certificateless Aggregate Signature -- Secure Online/Offine Attribute-based Encryption for IOT Users in Cloud Computing -- Identity-Concealed Authenticated Encryption from Ring Learning With Errors -- Towards Enhanced Security for Certificateless Public-key Authenticated Encryption with Keyword Search -- TumbleBit++: A Comprehensive Privacy Protocol Providing Anonymity and Amount-invisibility -- A Lattice-Based Anonymous Distributed E-Cash from Bitcoin -- Plaintext-Veriably-Checkable |

Encryption -- Improved Cryptanalysis of the KMOV Elliptic Curve Cryptosystem -- Hierarchical Functional Signcryption: Notion and Construction -- FSPVDSse: A Forward Secure Publicly Verifiable Dynamic SSE scheme -- A Hidden Markov Model-Based Method for Virtual Machine Anomaly Detection -- Password-based Authenticated Key Exchange from Standard Isogeny Assumptions -- A centralized digital currency system with rich functions -- A Practical Lattice-Based Sequential Aggregate Signature -- Provably Secure Proactive Secret Sharing Without the Adjacent Assumption -- Space-Ecient and Secure Substring Searchable Symmetric Encryption Using an Improved DAWG -- A Coin-Free Oracle-Based Augmented Black Box Framework -- Chameleon Hash Time-Lock Contract for Privacy Preserving Payment Channel Networks -- Solving ECDLP via List Decoding -- On-demand Privacy Preservation for Cost-Ecient Edge Intelligence Model Training.

Sommario/riassunto

This book constitutes the refereed proceedings of the 13th International Conference on Provable Security, ProvSec 2019, held in Cairns, QLD, Australia, in October 2019. The 18 full and 6 short papers presented were carefully reviewed and selected from 51 submissions. The papers focus on provable security as an essential tool for analyzing security of modern cryptographic primitives, including a special theme on “Practical Security.”.
