| | |
|---|---|
| 1. Record Nr. | UNINA9910624307603321 |
| Titolo | Provable and Practical Security : 16th International Conference, ProvSec 2022, Nanjing, China, November 11–12, 2022, Proceedings / / edited by Chunpeng Ge, Fuchun Guo |
| Pubbl/distr/stampa | Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2022 |
| ISBN | 9783031209178<br>3031209176 |
| Edizione | [1st ed. 2022.] |
| Descrizione fisica | 1 online resource (292 pages) |
| Collana | Lecture Notes in Computer Science, , 1611-3349 ; ; 13600 |
| Disciplina | 016.391<br>005.8 |
| Soggetti | Cryptography<br>Data encryption (Computer science)<br>Computer networks<br>Computer networks - Security measures<br>Application software<br>Cryptology<br>Computer Communication Networks<br>Mobile and Network Security<br>Computer and Information Systems Applications |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Note generali | Includes index. |
| Nota di contenuto | Encryption -- A Generic Construction of CCA-secure Attribute-based Encryption with Equality Test -- Secure-Channel Free Certificateless Searchable Public key Authenticated Encryption with Keyword Search -- More Efficient Verifiable Functional Encryption -- Subverting Deniability -- Epoch Confidentiality in Updatable Encryption -- Lattice Based Cryptography -- Simplified Server-Aided Revocable Identity-Based Encryption from Lattices -- Lattice-based Public Key Cryptosystems invoking Linear Mapping Mask -- Batched Fully Dynamic Multi-key FHE from FHEW-like Cryptosystems -- Zero-knowledge Range Arguments for Signed Fractional Numbers from Lattices -- Information Security -- Fast Out-of-band Data Integrity Monitor to Mitigate Memory Corruption |

Sommario/riassunto

This book constitutes the refereed proceedings of the 16th International Conference on Provable Security, ProvSec 2022, held in Nanjing, China, in November 11–12,2022. The 15 full papers and 4 short papers were presented carefully reviewed and selected from 52 submissions. The papers focus on provable security as an essential tool for analyzing security of modern cryptographic primitives. They are divided in the following topical sections: Encryption; Lattice Based Cryptography; Information Security; Blockchain; and Foundations.