

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 3031209176
Edizione	[1st ed. 2022.]
Descrizione fisica	1 online resource (292 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 13600
Disciplina	016.391 005.8
Soggetti	Cryptography Data encryption (Computer science) Computer networks Computer networks - Security measures Application software Cryptology Computer Communication Networks Mobile and Network Security 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

Attacks -- Construction of a New UAV Management System based on UMIA Technology -- FP2-MIA: A Membership Inference Attack Free of Posterior Probability in Machine Unlearning -- Practical Federated Learning for Samples with Different IDs -- Blockchain -- Reinforcement-Mining: Protecting Reward in Selfish Mining -- FolketID: A Decentralized Blockchain-based NemID Alternative against DDosS Attacks -- Secure Collaboration between Consortiums in Permissioned Blockchains -- Foundations -- (Public) Verifiability For Composable Protocols Without Adaptivity Or Zero-Knowledge -- Practical Non-Malleable Codes from Symmetric-key Primitives in 2-Split-State Model -- Cryptographic Role-Based Access Control, Reconsidered.

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.
