1. Record Nr. UNICASRML0298321

Titolo	La Gran Bretagna : e la resistenza partigiana in Italia 1943-1945 / Massimo de Leonardis
Pubbl/distr/stampa	Napoli, : ESI, 1988
Descrizione fisica	430 p. ; 22 cm.
Lingua di pubblicazione	Italiano
Formato	Materiale a stampa
Livello bibliografico	Monografia

2. Record Nr. UNINA9910624322003321

Titolo	Cryptology and Network Security : 21st International Conference, CANS 2022, Abu Dhabi, United Arab Emirates, November 13–16, 2022, Proceedings / / edited by Alastair R. Beresford, Arpita Patra, Emanuele Bellini
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2022
ISBN	9783031209741 3031209745
Edizione	[1st ed. 2022.]
Descrizione fisica	1 online resource (393 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 13641
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Computer engineering Computer networks Computer networks - Security measures Data protection Cryptology Computer Engineering and Networks Mobile and Network Security 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	Zero-knowledge and MPC -- Efficient NIZK Arguments with Straight-Line Simulation and Extraction -- Updatable NIZKs from Non-Interactive Zaps -- Through the Looking-Glass: Benchmarking Secure Multi-Party Computation Comparisons for ReLU's -- Public-key Infrastructure -- Oh SSH-it, what's my fingerprint? A Large-Scale Analysis of SSH Host Key Fingerprint Verification Records in the DNS -- Attribute-based Anonymous Credential: Optimization for Single-Use and Multi-Use -- Auditable Asymmetric Password Authenticated Public Key Establishment -- (Augmented) Broadcast Encryption from Identity Based Encryption with Wildcard -- Attacks and Countermeasures -- Passive Triangulation Attack on ORide -- HyperDetector: Detecting, Isolating, and Mitigating Timing Attacks in Virtualized Environments -- Cryptanalysis and Provable Security -- The Construction and Application of (Related-Key) Conditional Differential Neural Distinguishers on KATAN -- How to Design Authenticated Key Exchange for Wearable Devices: Cryptanalysis of AKE for Health Monitoring and Countermeasures via Distinct SMs with Key Split and Refresh -- Cryptanalysis of the Multi-Power RSA Cryptosystem Variant -- Provable Security of HADES Structure -- Cryptographic Protocols -- Practical Single-pass Oblivious Aggregation and Billing Computation Protocols for Smart Meters -- Anonymous Random Allocation and Its Applications -- ACDC: Anonymous Crowdsourcing using Digital Cash -- Blockchain and Payment Systems -- Analyzing Price Deviations in DeFi Oracles -- Redacting Blockchain without Exposing Chameleon Hash Collisions -- Codes and Post-Quantum Cryptography -- Efficient Proofs of Retrievability using Expander Codes -- Post-Quantum Electronic Identity: Adapting OpenID Connect and OAuth 2.0 to the Post-Quantum Era.
Sommario/riassunto	This book constitutes the refereed proceedings of the 21st International Conference on Cryptology and Network Security, CANS 2022, which was held during November 13-16, 2022. The conference was took place in Abu Dhabi, United Arab Emirates. The 18 full and 2 short papers presented in these proceedings were carefully reviewed and selected from 54 submissions. They were organized in topical sections as follows: zero-knowledge and MPC; public-key infrastructure; attacks and countermeasures; cryptanalysis and provable security; cryptographic protocols; blockchain and payment systems; and codes and post-quantum cryptography.