1. Record Nr. UNISA996464436003316

Titolo	. Part II : 19th international conference, ACNS 2021, Kamakura, Japan, June 21-24, 2021 : proceedings Applied cryptography and network security. / / Kazue Sako, Nils Ole Tippenhauer (editors)
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2021] ©2021
ISBN	3-030-78375-8
Edizione	[1st ed. 2021.]
Descrizione fisica	1 online resource (XIV, 512 p. 125 illus., 77 illus. in color.)
Collana	Security and Cryptology ; ; 12727
Disciplina	005.82
Soggetti	Data encryption (Computer science)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Analysis of Applied Systems -- Breaking and Fixing Third-Party Payment Service for Mobile Apps -- DSS: Discrepancy-Aware Seed Selection Method for ICS Protocol Fuzzing -- Threat for the Secure Remote Password Protocol and a Leak in Apple's Cryptographic Library -- Secure Computations -- Privacy-Preserving Data Aggregation with Probabilistic Range Validation -- LLVM-based Circuit Compilation for Practical Secure Computation -- An Efficient Passive-to-Active Compiler for Honest-Majority MPC over Rings -- Cryptanalysis -- Experimental Review of the IKK Query Recovery Attack: Assumptions, Recovery Rate and Improvements -- Efficient Methods to Search for Best Differential Characteristics on SKINNY -- Towards Efficient LPN-Based Symmetric Encryption -- System Security -- A Differentially Private Hybrid Approach to Traffic Monitoring -- Proactive Detection of Phishing Kit Traffic -- Vestige: Identifying Binary Code Provenance for Vulnerability Detection -- SoK: Auditability and Accountability in Distributed Payment Systems -- Defending Web Servers Against Flash Crowd Attacks -- Cryptography and its Applications -- TurboIKOS: Improved Non-interactive Zero-Knowledge and Post-Quantum Signatures -- Cryptanalysis of the Binary Permuted Kernel Problem -- Security Comparisons and Performance Analyses of Post-Quantum Signature Algorithms -- Tighter Proofs for the SIGMA and TLS 1.3 Key Exchange Protocols -- Improved Structured Encryption for SQL

Databases via Hybrid Indexing. .

Sommario/riassunto

The two-volume set LNCS 12726 + 12727 constitutes the proceedings of the 19th International Conference on Applied Cryptography and Network Security, ACNS 2021, which took place virtually during June 21-24, 2021. The 37 full papers presented in the proceedings were carefully reviewed and selected from a total of 186 submissions. They were organized in topical sections as follows: Part I: Cryptographic protocols; secure and fair protocols; cryptocurrency and smart contracts; digital signatures; embedded system security; lattice cryptography; Part II: Analysis of applied systems; secure computations; cryptanalysis; system security; and cryptography and its applications.