

1. Record Nr.	UNINA9910485151703321
Titolo	Applied Cryptography and Network Security : 19th International Conference, ACNS 2021, Kamakura, Japan, June 21–24, 2021, Proceedings, Part I // edited by Kazue Sako, Nils Ole Tippenhauer
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2021
ISBN	3-030-78372-3
Edizione	[1st ed. 2021.]
Descrizione fisica	1 online resource (XIV, 482 p. 72 illus., 21 illus. in color.)
Collana	Security and Cryptology, , 2946-1863 ; ; 12726
Disciplina	005.82
Soggetti	Data protection Computer engineering Computer networks Coding theory Information theory Application software Operating systems (Computers) Data and Information Security Computer Engineering and Networks Coding and Information Theory Computer and Information Systems Applications Operating Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Cryptographic Protocols -- Adaptive-ID Secure Hierarchical ID-Based Authenticated Key Exchange under Standard Assumptions without Random Oracles -- Analysis of Client-side Security for Long-term Time-stamping Services -- Towards Efficient and Strong Backward Private Searchable Encryption with Secure Enclaves -- Secure and Fair Protocols -- CECMLP: New Cipher-Based Evaluating Collaborative Multi-Layer Perceptron Scheme in Federated Learning -- Blind Polynomial Evaluation and Data Trading -- Coin-Based Multi-Party Fair Exchange -- Cryptocurrency and Smart Contracts -- P2DEX: Privacy-

Preserving Decentralized Cryptocurrency Exchange -- WOTS+ up my Sleeve! A Hidden Secure Fallback for Cryptocurrency Wallets -- Terrorist Attacks for Fake Exposure Notifications in Contact Tracing Systems -- Digital Signatures -- Unlinkable and Invisible -Sanitizable Signatures -- Partially Structure-Preserving Signatures: Lower Bounds, Constructions and More -- An Efficient Certificate-Based Signature Scheme in the Standard Model -- Embedded System Security -- SnakeGX: a sneaky attack against SGX Enclaves -- Telepathic Headache: Mitigating Cache Side-Channel Attacks on Convolutional Neural Networks -- Efficient FPGA Design of Exception-Free Generic Elliptic Curve Cryptosystems -- Lattice Cryptography -- Access Control Encryption from Group Encryption -- Password Protected Secret Sharing from Lattices -- Efficient Homomorphic Conversion Between (Ring) LWE Ciphertexts.

---

#### 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.

---