

1. Record Nr.	UNINA9910726293303321
Titolo	Innovative Security Solutions for Information Technology and Communications : 15th International Conference, SecITC 2022, Virtual Event, December 8–9, 2022, Revised Selected Papers / / edited by Giampaolo Bella, Mihai Doinea, Helge Janicke
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2023
ISBN	9783031326363 3031326369
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (351 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 13809
Disciplina	005.8
Soggetti	Data protection Data and Information Security Seguretat informàtica Sistemes de telecomunicació Tecnologia de la informació Congressos Llibres electrònics
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Interactional Freedom and Cybersecurity -- Lightweight Permutation-Based Cryptography for the Ultra-Low-Power Internet of Things -- Bridges connecting Encryption Schemes -- Superpoly Recovery of Grain-128AEAD Using Division Property -- On Single-Server Delegation of RSA -- Constructing Pairing Free Unbounded Inner Product -- Functional Encryption Schemes with Unbounded Inner Product Policy -- Efficient Distributed Keys Generation of Threshold Paillier Cryptosystem -- Statistical tests for symmetric primitives An application to NIST Lightweight finalists -- MILP-aided Cryptanalysis of the FUTURE Block Cipher -- Easy-ABE: An Easy Ciphertext-Policy Attribute-Based Encryption -- MOTUS: How Quantized Parameters Improve Protection of Model and Its Inference Input -- Lightweight Authentication using Noisy Key Derived from Physically Unclonable Function -- Card-Based Zero-Knowledge Proof Protocol for Pancake Sorting -- Activity

Detection from Encrypted Remote Desktop Protocol Traffic -- Application-Oriented Anonymization Framework for Social Network Datasets and IoT Environments -- AI-Powered Vulnerability Detection for Secure Source Code Development -- Towards Verifying Physical Assumption in Card-Based Cryptography -- The Security of Quasigroups Based Substitution Permutation Networks -- Unbounded Revocable Decentralized Multi-Authority Attribute-Based Encryption Supporting Non-Monotone Access Structures.

Sommario/riassunto

This book constitutes the refereed post-conference proceedings of the 15th International Conference on Innovative Security Solutions for Information Technology and Communications, SecITC 2022, held as a virtual event, during December 8–9, 2022. The 19 revised full papers presented together with 1 invited talk were carefully reviewed and selected from 53 submissions. The papers cover topics such as cryptographic algorithms, digital forensics and cyber security and much more.
