1. Record Nr. UNINA9910349410703321

Titolo	Information Security : 21st International Conference, ISC 2018, Guildford, UK, September 9–12, 2018, Proceedings / / edited by Liqun Chen, Mark Manulis, Steve Schneider
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2018
ISBN	9783319991368 3319991361
Edizione	[1st ed. 2018.]
Descrizione fisica	1 online resource (XI, 522 p. 85 illus.)
Collana	Security and Cryptology, , 2946-1863 ; ; 11060
Disciplina	005.8
Soggetti	Data protection Data structures (Computer science) Information theory Computer engineering Computer networks Computers Computer science Data and Information Security Data Structures and Information Theory Computer Engineering and Networks Computing Milieux Computer Communication Networks Computer Science Logic and Foundations of Programming
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Invited Paper -- Relaxed Lattice-Based Signatures with Short Zero-Knowledge Proofs -- Software Security -- Secure Code Execution: A Generic PUF-driven System Architecture -- Lumus: Dynamically Uncovering Evasive Android Applications -- ICUFuzzer: Fuzzing ICU Library for Exploitable Bugs in Multiple Software -- How Safe is Safety Number? A User Study on SIGNAL's Fingerprint and Safety Number Methods for Public Key Verification -- Symmetric Ciphers and

Cryptanalysis -- Speeding up MILP Aided Differential Characteristic Search with Mastui's Strategy -- Automatic Search for Related-key Differential Trails in SIMON-like Block Ciphers Based on MILP -- Linear Cryptanalysis of Reduced-Round Speck with a Heuristic Approach: Automatic Search for Linear Trails -- Conditional Cube Searching and Applications on Trivium-Variant Ciphers -- Data Privacy and Anonymization -- Practical Attacks on Relational Databases Protected via Searchable Encryption -- A Simple Algorithm for Estimating Distribution Parameters from n-Dimensional Randomized Binary Responses -- Outsourcing and Assisted Computing -- Enforcing Access Control for the Cryptographic Cloud Service Invocation based on Virtual Machine Introspection -- Multi-Authority Fast Data Cloud-Outsourcing for Mobile Devices -- Hide The Modulus: A Secure Non-Interactive Fully Verifiable Delegation Scheme for Modular Exponentiations via CRT -- Offline Assisted Group Key Exchange -- Advanced Encryption -- Function-Dependent Commitments for Verifiable Multi-Party Computation -- On Constructing Pairing-free Identity-Based Encryptions -- Multi-Key Homomorphic Proxy Re-Encryption -- Verifiable Decryption for Fully Homomorphic Encryption -- Privacy-Preserving Applications -- Platform-independent Secure Blockchain-Based Voting System -- Privacy in Crowdsourcing: A Systematic Review -- Advanced Signatures -- Anonymous yet Traceable Strong Designated Verifier Signature -- Strongly Unforgeable Signature Resilient to Polynomially Hard-to-Invert Leakage under Standard Assumptions -- A Revocable Group Signature Scheme with Scalability from Simple Assumptions and Its Implementation -- Network Security -- Fast Flux Service Network Detection via Data Mining on Passive DNS Traffic -- Beyond Cookie Monster Amnesia: Real World Persistent Online Tracking -- Cyber-risks in the Industrial Internet of Things: towards a method for continuous assessment.

Sommario/riassunto

This book constitutes the proceedings of the 21st International Conference on Information Security, ISC 2018, held in Guildford, UK, in September 2018. The 26 full papers presented in this volume were carefully reviewed and selected from 59 submissions. The book also includes one invited talk in full-paper length. The papers were organized in topical sections named: software security; symmetric ciphers and cryptanalysis; data privacy and anonymization; outsourcing and assisted computing; advanced encryption; privacy-preserving applications; advanced signatures; and network security. .