1. Record Nr. UNINA9910483812503321

Titolo	Applied Cryptography and Network Security : 15th International Conference, ACNS 2017, Kanazawa, Japan, July 10-12, 2017, Proceedings / / edited by Dieter Gollmann, Atsuko Miyaji, Hiroaki Kikuchi
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2017
ISBN	3-319-61204-2
Edizione	[1st ed. 2017.]
Descrizione fisica	1 online resource (XVI, 710 p. 167 illus.)
Collana	Security and Cryptology ; ; 10355
Disciplina	005.82
Soggetti	Computer security Data encryption (Computer science) Data protection Computer communication systems Software engineering Application software Systems and Data Security Cryptology Security Computer Communication Networks Software Engineering Information Systems Applications (incl. Internet)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Sampling From Arbitrary Centered Discrete Gaussians For Lattice-Based Cryptography -- Simple Security Definitions for and Constructions of 0-RTT Key Exchange -- TOPPSS: Cost-minimal Password-Protected Secret Sharing based on Threshold OPRF -- Secure and Efficient Pairing at 256-bit Security Level -- Data Protection and Mobile Security No Free Charge Theorem: a Covert Channel via USB Charging Cable on Mobile Devices -- Are You Lying: Validating the Time-Location of Outdoor Images -- Lights, Camera, Action! Exploring Effects of Visual

Distractions on Completion of Security Tasks -- A Pilot Study of Multiple Password Interference between Text and Map-based Passwords -- Hierarchical Key Assignment with Dynamic Read-Write Privilege Enforcement and Extended KI-Security -- A Novel GPU-Based Implementation of the Cube Attack – Preliminary Results Against Trivium -- Related-Key Impossible-Differential Attack on Reduced-Round SKINNY -- Faster Secure Multi-Party Computation of AES and DES Using Lookup Tables -- An experimental study of the BDD approach for the search LWE problem -- Efficiently Obfuscating Re-Encryption Program under DDH Assumption -- Lattice-Based Group Signatures: Achieving Full Dynamicity with Ease -- A Practical Chosen Message Power Analysis Approach against Ciphers with the Key Whitening Layers -- Side-Channel Attacks meet Secure Network Protocols -- Lattice-based DAPS and Generalizations: Self-Enforcement in Signature Schemes -- Forward-Secure Searchable Encryption on Labeled Bipartite Graphs -- Bounds in Various Generalized Settings of the Discrete Logarithm Problem -- An Enhanced Binary Characteristic Set Algorithm And Its Applications to Algebraic Cryptanalysis -- Accountable Storage -- Maliciously Secure Multi-Client ORAM -- Legacy-Compliant Data Authentication for Industrial Control System Traffic -- Multi-Client Oblivious RAM Secure Against Malicious Servers -- Breaking and Fixing Mobile App Authentication with OAuth2.0-based Protocols -- Adaptive Proofs have Straightline Extractors (in the Random Oracle Model) -- How to Achieve Bounded Key Dependent Message Security -- Signature Schemes with Randomized Verification -- SCRAPE: Scalable Randomness Attested by Public Entities -- cMix : Mixing with Minimal Real-Time Asymmetric Cryptographic Operation -- Almost Optimal Oblivious Transfer from QA-NIZK -- OnionPIR: Effective Protection of Sensitive Metadata in Online Communication Networks.

Sommario/riassunto

This book constitutes the proceedings of the 15th International Conference on Applied Cryptology and Network Security, ACNS 2017, held in Kanazawa, Japan, in July 2017. The 34 papers presented in this volume were carefully reviewed and selected from 149 submissions. The topics focus on innovative research and current developments that advance the areas of applied cryptography, security analysis, cyber security and privacy, data and server security.