1. Record Nr. UNINA9910484185803321

Titolo	Information and Communications Security : 10th International Conference, ICICS 2008 Birmingham, UK, October 20 - 22, 2008. Proceedings / / edited by Liqun Chen, Mark Ryan, Guilin Wang
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2008
ISBN	3-540-88625-7
Edizione	[1st ed. 2008.]
Descrizione fisica	1 online resource (XIII, 436 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 5308
Classificazione	54.62
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Coding theory Information theory Computer programming Data structures (Computer science) Data protection Algorithms Cryptology Coding and Information Theory Programming Techniques Data Structures and Information Theory Data and Information Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Invited Talk -- Attestation: Evidence and Trust -- Authentication -- A Novel Solution for End-to-End Integrity Protection in Signed PGP Mail -- Unclonable Lightweight Authentication Scheme -- Threat Modelling in User Performed Authentication -- Access with Fast Batch Verifiable Anonymous Credentials -- Side Channel Analysis -- Quantifying Timing Leaks and Cost Optimisation -- Method for Detecting Vulnerability to Doubling Attacks -- Side Channel Analysis of Some Hash Based MACs: A Response to SHA-3 Requirements -- Cryptanalysis

-- Key Recovery Attack on Stream Cipher Mir-1 Using a Key-Dependent S-Box -- Analysis of Two Attacks on Reduced-Round Versions of the SMS4 -- Applying Time-Memory-Data Trade-Off to Meet-in-the-Middle Attack -- Access Control -- Beyond User-to-User Access Control for Online Social Networks -- Revocation Schemes for Delegation Licences -- Reusability of Functionality-Based Application Confinement Policy Abstractions -- Towards Role Based Trust Management without Distributed Searching of Credentials -- Software Security -- BinHunt: Automatically Finding Semantic Differences in Binary Programs -- Enhancing Java ME Security Support with Resource Usage Monitoring -- Pseudo-randomness Inside Web Browsers -- System Security -- Verifiable and Revocable Expression of Consent to Processing of Aggregated Personal Data -- Embedding Renewable Cryptographic Keys into Continuous Noisy Data -- Automated Device Pairing for Asymmetric Pairing Scenarios -- Applied Cryptography -- Algebraic Description and Simultaneous Linear Approximations of Addition in Snow 2.0. -- Towards an Information Theoretic Analysis of Searchable Encryption -- A Bootstrap Attack on Digital Watermarks in the Frequency Domain -- Improved Data Hiding Technique for Shares in Extended Visual Secret Sharing Schemes -- Security Protocols -- Efficient Multi-authorizer Accredited Symmetrically Private Information Retrieval -- Specification of Electronic Voting Protocol Properties Using ADM Logic: FOO Case Study -- Publicly Verifiable Remote Data Integrity.

Sommario/riassunto

This book constitutes the refereed proceedings of the 10th International Conference on Information and Communications Security, ICICS 2008, held in Birmingham, UK, in October 2008. The 27 revised full papers presented together with one invited paper were carefully reviewed and selected from 125 submissions. The papers are organized in topical sections on authentication, side channel analysis, cryptanalysis, access control, software security, system security, applied cryptography, and security protocols.