1. Record Nr. UNISA996465920403316

Titolo	Information Theoretic Security [[electronic resource]] : 4th International Conference, ICITS 2009, Shizuoka, Japan, December 3-6, 2009. Revised Selected Papers / / edited by Kaoru Kurosawa
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2010
ISBN	1-280-38803-X 9786613565952 3-642-14496-9
Edizione	[1st ed. 2010.]
Descrizione fisica	1 online resource (X, 249 p. 23 illus.)
Collana	Security and Cryptology ; ; 5973
Disciplina	005.8/2
Soggetti	Data encryption (Computer science) Coding theory Information theory Computer security Algorithms Computer communication systems Management information systems Computer science Cryptology Coding and Information Theory Systems and Data Security Algorithm Analysis and Problem Complexity Computer Communication Networks Management of Computing and Information Systems
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	Leakage Resilient Cryptography -- Survey: Leakage Resilience and the Bounded Retrieval Model -- A Lower Bound on the Key Length of Information-Theoretic Forward-Secure Storage Schemes -- Quantum Cryptography and Indistinguishability -- Security of Key Distribution and Complementarity in Quantum Mechanics -- Free-Start

Distinguishing: Combining Two Types of Indistinguishability Amplification -- Connection to Computational Security -- Code-Based Public-Key Cryptosystems and Their Applications -- On the Security of Pseudorandomized Information-Theoretically Secure Schemes -- Secret Sharing -- Efficient Statistical Asynchronous Verifiable Secret Sharing with Optimal Resilience -- On the Optimization of Bipartite Secret Sharing Schemes -- Linear Threshold Multisecret Sharing Schemes -- Key Agreement from Common Randomness -- Multiterminal Secrecy Generation and Tree Packing -- Information Theoretic Security Based on Bounded Observability -- Random Graph and Group Testing -- Group Testing and Batch Verification -- Reliable Data Transmision and Computation -- What Can Cryptography Do for Coding Theory? -- Cryptanalysis of Secure Message Transmission Protocols with Feedback -- The Optimum Leakage Principle for Analyzing Multi-threaded Programs -- Fingerprint and Watermarking -- A General Conversion Method of Fingerprint Codes to (More) Robust Fingerprint Codes against Bit Erasure -- An Improvement of Pseudorandomization against Unbounded Attack Algorithms – The Case of Fingerprint Codes -- Statistical-Mechanical Approach for Multiple Watermarks Using Spectrum Spreading.

Sommario/riassunto

ICITS2009washeldattheShizuokaConventionandArtsCenter“GRANSHIP” in Japan during December 3–6,2009.This was the 4th International Conference on Information Theoretic Security. Over the last few decades, we have seen several research topics studied - quiringinformationtheoreticalsecurity,alsocalledunconditionalsecurity, where there is no unproven computational assumption on the adversary. (This is the framework proposed by Claude Shannon in his seminal paper.) Also, coding as well as other aspects of information theory have been used in the design of cryptographic schemes. Examples are authentication, secure communication, key exchange, multi-party computation and information hiding to name a few. A related area is quantum cryptography that predominantly uses information theory for modeling and evaluation of security. Needless to say, information t- oretically secure cryptosystems are secure even if the factoring assumption or the discrete log assumption is broken. Seeing the multitude of topics in m- ern cryptographyrequiring informationtheoreticalsecurity or using information theory, it is time to have a regular conference on this topic. This was the fourth conference of this series, aiming to bring together the leading researchers in the area of information and/or quantum theoretic security.