1. Record Nr. UNISA996466007103316

| | |
|---|---|
| Titolo | Transactions on Computational Science X [[electronic resource] ] : Special Issue on Security in Computing, Part I / / edited by Marina L. Gavrilova, C. J. Kenneth Tan |
| Pubbl/distr/stampa | Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2010 |
| ISBN | 1-283-47736-X<br>9786613477361<br>3-642-17499-X |
| Edizione | [1st ed. 2010.] |
| Descrizione fisica | 1 online resource (XVIII, 366 p. 111 illus., 68 illus. in color.) |
| Collana | Transactions on Computational Science, , 1866-4733 ; ; 6340 |
| Disciplina | 004.6 |
| Soggetti | Computer communication systems<br>Software engineering<br>Application software<br>Management information systems<br>Computer science<br>Algorithms<br>Data encryption (Computer science)<br>Computer Communication Networks<br>Software Engineering<br>Information Systems Applications (incl. Internet)<br>Management of Computing and Information Systems<br>Algorithm Analysis and Problem Complexity<br>Cryptology |
| 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 author index. |
| Nota di contenuto | A Dynamic Security Framework for Ambient Intelligent Systems: A Smart-Home Based eHealth Application -- NTRU-Like Public Key Cryptosystems beyond Dedekind Domain up to Alternative Algebra -- Identity-Based Key Exchange Protocols without Pairings -- Building a Side Channel Based Disassembler -- A Versatile Framework for Implementation Attacks on Cryptographic RFIDs and Embedded Devices |

-- An Adaptive Robust Watermarking Algorithm for Audio Signals Using SVD -- Trust-Based Security Level Evaluation Using Bayesian Belief Networks -- Implementation of QoSS (Quality-of-Security Service) for NoC-Based SoC Protection -- Signcryption with Non-interactive Non-repudiation without Random Oracles -- Block-Level Added Redundancy Explicit Authentication for Parallelized Encryption and Integrity Checking of Processor-Memory Transactions -- A Weakest Precondition Approach to Robustness -- PET SNAKE: A Special Purpose Architecture to Implement an Algebraic Attack in Hardware -- Green Secure Processors: Towards Power-Efficient Secure Processor Design -- A New Peer-to-Peer Micropayment Protocol Based on Transferable Debt Token.

Sommario/riassunto

The LNCS journal Transactions on Computational Science reflects recent developments in the field of Computational Science, conceiving the field not as a mere ancillary science but rather as an innovative approach supporting many other scientific disciplines. The journal focuses on original high-quality research in the realm of computational science in parallel and distributed environments, encompassing the facilitating theoretical foundations and the applications of large-scale computations and massive data processing. It addresses researchers and practitioners in areas ranging from aerospace to biochemistry, from electronics to geosciences, from mathematics to software architecture, presenting verifiable computational methods, findings, and solutions and enabling industrial users to apply techniques of leading-edge, large-scale, high performance computational methods. The 10th issue of the Transactions on Computational Science, edited by Edward David Moreno, is the first of two publications focusing on security in computing. The 14 papers included in the volume address a wide range of applications and designs, such as new architectures, novel hardware implementations, cryptographic algorithms, and security protocols.