| | | |
|---|---|---|
| 1. | Record Nr. | UNISA996465754303316 |
| | Titolo | Provable Security [[electronic resource] ] : 7th International Conference, ProvSec 2013, Melaka, Malaysia, October 23-25, 2013, Proceedings / / edited by Willy Susilo, Reza Reyhanitabar |
| | Pubbl/distr/stampa | Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2013 |
| | ISBN | 3-642-41227-0 |
| | Edizione | [1st ed. 2013.] |
| | Descrizione fisica | 1 online resource (X, 347 p. 36 illus.) |
| | Collana | Security and Cryptology ; ; 8209 |
| | Disciplina | 005.8 |
| | Soggetti | Data encryption (Computer science)<br>Computer security<br>Computers and civilization<br>E-commerce<br>Application software<br>Computer science<br>Cryptology<br>Systems and Data Security<br>Computers and Society<br>e-Commerce/e-business<br>Computer Appl. in Administrative Data Processing<br>Computer Science, general |
| | Lingua di pubblicazione | Inglese |
| | Formato | Materiale a stampa |
| | Livello bibliografico | Monografia |
| | Note generali | Bibliographic Level Mode of Issuance: Monograph |
| | Nota di contenuto | On Modeling Terrorist Frauds: Addressing Collusion in Distance Bounding Protocols -- Authenticated Key Exchange Protocols Based on Factoring Assumption -- Efficient, Pairing-Free, Authenticated Identity Based Key Agreement in a Single Round -- CIL Security Proof for a Password-Based Key Exchange -- Non Observability in the Random Oracle Model -- Indistinguishability against Chosen Ciphertext Verification Attack Revisited: The Complete Picture -- Input-Aware Equivocable Commitments and UC-secure Commitments with Atomic Exchanges -- Towards Anonymous Ciphertext Indistinguishability with |

Identity Leakage -- k-Time Proxy Signature: Formal Definition and Efficient Construction -- Anonymous Signcryption against Linear Related-Key Attacks -- Improved Authenticity Bound of EAX, and Refinements -- The Security of the OCB Mode of Operation without the SPRP Assumption -- A Short Universal Hash Function from Bit Rotation, and Applications to Blockcipher Modes -- How to Remove the Exponent GCD in HK09 -- Translation-Randomizable Distributions via Random Walks -- RKA Secure PKE Based on the DDH and HR Assumptions -- Computationally Efficient Dual-Policy Attribute Based Encryption with Short Ciphertext -- Factoring-Based Proxy Re-Encryption Schemes -- Towards a Secure Certificateless Proxy Re-Encryption Scheme.

Sommario/riassunto

This book constitutes the refereed proceedings of the 7th International Conference on Provable Security, ProvSec 2013, held in Melaka, Malaysia, in October 2013. The 18 full papers presented together with 1 invited talk were carefully reviewed and selected from 44 submissions. The papers cover the following topics: key exchange protocols, security models, signature and signcryption schemes, authenticated encryption, theory, and public key encryption.

2. Record Nr. UNISA996465750503316

Titolo: Case-Based Reasoning Research and Development [[electronic resource] ] : Second International Conference on Case-Based Reasoning, ICCBR-97 Providence, RI, USA, July 25-27, 1997 Proceedings / / edited by David B. Leake, Enric Plaza

Pubbl/distr/stampa: Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 1997

ISBN: 3-540-69238-X

Edizione: [1st ed. 1997.]

Descrizione fisica: 1 online resource (XIV, 654 p.)

Collana: Lecture Notes in Artificial Intelligence ; ; 1266

Disciplina: 006.3/33

Soggetti:
Artificial intelligence
Information technology
Business—Data processing
Artificial Intelligence
IT in Business

Lingua di pubblicazione: Inglese

Formato: Materiale a stampa

Livello bibliografico: Monografia

| | |
|---|---|
| Note generali | Bibliographic Level Mode of Issuance: Monograph |
| Nota di contenuto | Case-based reasoning in color matching -- Estimating software development effort with case-based reasoning -- Applying case-based reasoning to automated deduction -- A Case-based approach for elaboration of design requirements -- Case-Based reasoning in an ultrasonic rail-inspection system -- CBR in a changing environment -- Case-based reasoning for information system design -- Applying memory-based learning to indexing of reference ships for case-based conceptual ship design -- CBR for document retrieval: The FAllQ project -- Combining medical records with case-based reasoning in a mixed paradigm design — TROPIX architecture & implementation -- Ocram-CBR: A Shell for Case-Based Educational Systems -- From troubleshooting to process design: Closing the manufacturing loop -- ForMAT and Parka: A technology integration experiment and beyond -- Encouraging self-explanation through case-based tutoring: A case study -- Lessons learned from deployed CBR systems and design decisions made in building a commercial CBR tool -- Using case-based reasoning for reusing software knowledge -- New technology bliss and pain in a large customer service center -- An engineering approach for troubleshooting case bases -- A large case-based reasoner for legal cases -- A scalable approach for question based indexing of encyclopedic texts -- An explicit representation of reasoning failures -- On the admissibility of concrete domains for CBR based on description logics -- Similarity metrics: A formal unification of cardinal and non-cardinal similarity measures -- The case for graph-structured representations -- The evaluation of a hierarchical case representation using context guided retrieval -- Refining conversational case libraries -- Perspectives: A declarative bias mechanism for case retrieval -- Using introspective learning to improve retrieval in CBR: A case study in air traffic control -- Using machine learning for assigning indices to textual cases -- How case-based reasoning and cooperative query answering techniques support RICAD -- What you saw is what you want: Using cases to seed information retrieval -- On the relation between the context of a feature and the domain theory in case-based planning -- Theoretical analysis of case retrieval method based on neighborhood of a new problem -- The adaptation knowledge bottleneck: How to ease it by learning from cases -- A case study of case-based CBR -- Solution-relevant abstractions constrain retrieval and adaptation -- Selecting most adaptable diagnostic solutions through Pivoting-Based Retrieval -- Towards improving case adaptability with a genetic algorithm -- Merge strategies for multiple case plan replay -- Loose coupling of failure explanation and repair: Using learning goals to sequence learning methods -- Using a case base of surfaces to speed-up reinforcement learning -- PAC analyses of a ‘similarity learning’ IBL algorithm -- Examining locally varying weights for nearest neighbor algorithms -- Case-based planning to learn -- A utility-based approach to learning in a mixed case-based and model-based reasoning architecture -- Qualitative knowledge to support reasoning about cases -- Integrating rule induction and case-based reasoning to enhance problem solving -- Using software process modeling for building a case-based reasoning methodology: Basic approach and case study -- Stratified case-based reasoning in non-refinable abstraction hierarchies -- Supporting combined human and machine planning: An interface for planning by analogical reasoning -- Using case-based reasoning for argumentation with multiple viewpoints -- Maintaining unstructured case bases -- An analogical |

| | |
|---|---|
| | theory of creativity in design -- Experimental study of a similarity metric for retrieving pieces from structured plan cases: Its role in the originality of plan case solutions -- Creative design: Reasoning and understanding -- Fuzzy modelling of case-based reasoning and decision -- Probabilistic indexing for case-based prediction -- A probabilistic model for case-based reasoning -- Case based reasoning, fuzzy systems modeling and solution composition. |
| Sommario/riassunto | This book constitutes the refereed proceedings of the Second International Conference on Case-Based Reasoning, ICCBR-97, held in Providence, RI, USA, in July 1997. The volume presents 39 revised full scientific papers selected from a total of 102 submissions; also included are 20 revised application papers. Among the topics covered are representation and formalization, indexing and retrieval, adaptation, learning, integrated approaches, creative reasoning, CBR and uncertainty. This collection of papers is a comprehensive documentation of the state of the art in CBR research and development. |

3.

| | |
|---|---|
| Record Nr. | UNINA9910697574203321 |
| Titolo | Making IT happen [[electronic resource] ] : transforming military information technology / / edited by Joseph N. Mait |
| Pubbl/distr/stampa | Washington, DC : , : Center for Technology and National Security Policy, National Defense University, , [2005] |
| Descrizione fisica | 1 online resource (iv, 73 pages) : color illustrations, color map |
| Collana | Defense & technology papers |
| Altri autori (Persone) | MaitJoseph N. <1958-> |
| Soggetti | Netcentric computing<br>Internetworking (Telecommunication)<br>United States Armed Forces Information technology |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Note generali | Title from title screen (viewed on April 8, 2011).<br>"September 2005." |
| Nota di bibliografia | Includes bibliographical references. |