1. Record Nr. UNISA996466113903316

Titolo	Smart Card Research and Advanced Applications [[electronic resource]] : 7th IFIP WG 8.8/11.2 International Conference, CARDIS 2006, Tarragona, Spain, April 19-21, 2006, Proceedings / / edited by Josep Domingo-Ferrer, Joachim Posegga, Daniel Schreckling
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2006
ISBN	3-540-33312-6
Edizione	[1st ed. 2006.]
Descrizione fisica	1 online resource (XII, 360 p.)
Collana	Security and Cryptology ; ; 3928
Disciplina	005.82
Soggetti	Data encryption (Computer science) Management information systems Computer science Computers and civilization Computer communication systems Operating systems (Computers) Cryptology Management of Computing and Information Systems Computers and Society Computer Communication Networks Operating 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	Smart Card Applications -- Design, Installation and Execution of a Security Agent for Mobile Stations -- Towards a Secure and Practical Multifunctional Smart Card -- Implementing Cryptography on TFT Technology for Secure Display Applications -- A Smart Card-Based Mental Poker System -- A Smart Card Solution for Access Control and Trust Management for Nomadic Users -- Smart Cards and Residential Gateways: Improving OSGi Services with Java Cards -- Zero Footprint Secure Internet Authentication Using Network Smart Card -- An Optimistic NBAC-Based Fair Exchange Method for Arbitrary Items -- Side Channel Attacks -- Generic Cryptanalysis of Combined

Countermeasures with Randomized BSD Representations -- Amplifying Side-Channel Attacks with Techniques from Block Cipher Cryptanalysis -- Power Analysis to ECC Using Differential Power Between Multiplication and Squaring -- Smart Card Networking -- Designing Smartcards for Emerging Wireless Networks -- Smartcard Firewalls Revisited -- Multi-stage Packet Filtering in Network Smart Cards -- Cryptographic Protocols -- Anonymous Authentication with Optional Shared Anonymity Revocation and Linkability -- SEA: A Scalable Encryption Algorithm for Small Embedded Applications -- Low-Cost Cryptography for Privacy in RFID Systems -- Optimal Use of Montgomery Multiplication on Smart Cards -- Off-Line Group Signatures with Smart Cards -- RFID Security -- Analysis of Power Constraints for Cryptographic Algorithms in Mid-Cost RFID Tags -- Noisy Tags: A Pretty Good Key Exchange Protocol for RFID Tags -- MARP: Mobile Agent for RFID Privacy Protection -- Formal Methods -- Certifying Native Java Card API by Formal Refinement -- A Low-Footprint Java-to-Native Compilation Scheme Using Formal Methods -- Automatic Test Generation on a (U)SIM Smart Card.

Sommario/riassunto

Smart cards are an established security research area with a very unique pr- erty: it integrates numerous sub?elds of IT Security, which often appear sc- tered and only loosely connected. Smart card research unites them by providing a common goal: advancing the state of the art of designing and deploying small tokens to increase the security in Information Technology. CARDIS has a tradition of more than one decade, and has established itself asthepremier conferencefor researchresultsinsmartcardtechnology.As smart card research is unique, so is CARDIS; the conference successfully attracts a- demic and industrial researchers without compromising in either way. CARDIS accommodates applied research results as well as theoretical contributions that might or might not become practically relevant. The key to making such a m- ture attractive to both academia and industry is simple: quality of contributions and relevance to the overall subject. This year’s CARDIS made it easy to continue this tradition: we received 76 papers, nearly all of them relevant to the focus of CARDIS and presenting high-quality researchresults. The ProgramCommittee workedhard on selecting the best 25 papers to be presented at the conference. We are very grateful to the members of the Program Committee and the additional referees for generously spending their time on the di?cult task of assessing the value of submitted papers. Daniel Schreckling provided invaluable assistance in handling submissions, managing review reports and editing the proceedings. The assistance of Jordi Castell` a in handling practical aspects of the conference preparation is also greatly appreciated.