1. Record Nr. UNISA996465991403316

Titolo	Information security theory and practices : smart cards, mobile and ubiquitous computing systems : First IFIP TC6/W G 8.8/ WG 11.2 International Workshop, WISTP 2007, Heraklion, Crete, Greece, May 9-11, 2007, proceedings / / Damien Sauveron [three others] (editors)
Pubbl/distr/stampa	Berlin ; ; Heidelberg ; ; New York : , : Springer-Verlag, , [2007] ©2007
ISBN	3-540-72354-4
Edizione	[1st ed. 2007.]
Descrizione fisica	1 online resource (260 p.)
Collana	Lecture notes in computer science ; ; 4462
Disciplina	005.8
Soggetti	Data protection Computer systems - Access control Smart cards Mobile computing - Security measures Ubiquitous computing - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Mobility -- A Smart Card Based Distributed Identity Management Infrastructure for Mobile Ad Hoc Networks -- A New Resilient Key Management Protocol for Wireless Sensor Networks -- Hardware and Cryptography I -- Efficient Use of Random Delays in Embedded Software -- Enhanced Doubling Attacks on Signed-All-Bits Set Recoding -- Privacy -- Securing the Distribution and Storage of Secrets with Trusted Platform Modules -- Distributed Certified Information Access for Mobile Devices -- Cryptography Scheme -- Linkability of Some Blind Signature Schemes -- Optimistic Non-repudiation Protocol Analysis -- Secure Remote User Authentication Scheme Using Bilinear Pairings -- Cryptanalysis of Some Proxy Signature Schemes Without Certificates -- Smart Card -- Performance Evaluation of Java Card Bytecodes -- Reverse Engineering Java Card Applets Using Power Analysis -- An Embedded System for Practical Security Analysis of Contactless Smartcards -- A Comparative Analysis of Common Threats, Vulnerabilities, Attacks and Countermeasures Within Smart Card and

Wireless Sensor Network Node Technologies -- Small Devices -- Mobile Phones as Secure Gateways for Message-Based Ubiquitous Communication -- An Information Flow Verifier for Small Embedded Systems -- Survey and Benchmark of Stream Ciphers for Wireless Sensor Networks -- Hardware and Cryptography II -- Fault Attacks for CRT Based RSA: New Attacks, New Results, and New Countermeasures -- CRT RSA Algorithm Protected Against Fault Attacks -- Combinatorial Logic Circuitry as Means to Protect Low Cost Devices Against Side Channel Attacks.

Sommario/riassunto

With the rapid technological development of information technology, computer systems and especially embedded systems are becoming more mobile and ub- uitous. Ensuring the security of these complex and yet resource-constraineds- temshasemergedasoneofthemostpressingchallengesforresearchers. Although there are a number of information security conferences that look at particular aspects of the challenge, we decided to create the Workshop in Information - curity Theory and Practices (WISTP) to consider the problem as a whole. In additiontheworkshopaimsto bringtogetherresearchersandpractitionersin- lated disciplines and encourage interchange and practical co-operation between academia and industry. Although this is the ?rst ever WISTP event, the response from researchers wassuperbwithover68paperssubmittedforpotentialinclusionintheworksh op and proceedings. The submissions were reviewed by at least three reviewers, in most cases by four, and for program committee (PC) papers at least ?ve reviewers. This long and rigorous process was only possible thanks to the hard work of the PC members and additional reviewers, listed in the following pages. We would like to express our gratitude to the PC members, who were very supportive from the very beginning of this project. Thanks are also due to the additional expert reviewers who helped the PC to select the ?nal 20 workshop papers for publication in the proceedings. Of course we highly appreciate the e? orts of all the authors who submitted papers to WISTP 2007. We hope they will contribute again to a future edition and encourage others to do so.