1. Record Nr. UNINA9910484198103321

Titolo	Information Security and Privacy : 11th Australasian Conference, ACISP 2006, Melbourne, Australia, July 3-5, 2006, Proceedings / / edited by Lynn Batten, Reihaneh Safavi-Naini
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2006
ISBN	3-540-35459-X
Edizione	[1st ed. 2006.]
Descrizione fisica	1 online resource (XII, 446 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 4058
Altri autori (Persone)	BattenLynn Margaret Safavi-NainiReihanah
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Electronic data processing - Management Operating systems (Computers) Computer networks Coding theory Information theory Algorithms Cryptology IT Operations Operating Systems Computer Communication Networks Coding and Information Theory
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	Stream Ciphers -- Algebraic Attacks on Clock-Controlled Stream Ciphers -- Cache Based Power Analysis Attacks on AES -- Distinguishing Attack on SOBER-128 with Linear Masking -- Evaluating the Resistance of Stream Ciphers with Linear Feedback Against Fast Algebraic Attacks -- Symmetric Key Ciphers -- Ensuring Fast Implementations of Symmetric Ciphers on the Intel Pentium 4 and Beyond -- Improved Cryptanalysis of MAG -- On Exact Algebraic [Non-

]Immunity of S-Boxes Based on Power Functions -- Network Security -- Augmented Certificate Revocation Lists -- Online/Offline Signatures and Multisignatures for AODV and DSR Routing Security -- Towards an Invisible Honeypot Monitoring System -- Cryptographic Applications -- Adaptively Secure Traitor Tracing Against Key Exposure and Its Application to Anywhere TV Service -- Fingercasting—Joint Fingerprinting and Decryption of Broadcast Messages -- More on Stand-Alone and Setup-Free Verifiably Committed Signatures -- Secure Implementation -- API Monitoring System for Defeating Worms and Exploits in MS-Windows System -- Hiding Circuit Topology from Unbounded Reverse Engineers -- The Role of the Self-Defending Object Concept in Developing Distributed Security-Aware Applications -- Signatures -- Efficient and Provably Secure Multi-receiver Identity-Based Signcryption -- Efficient Identity-Based Signatures Secure in the Standard Model -- Event-Oriented k-Times Revocable-iff-Linked Group Signatures -- Key Replacement Attack Against a Generic Construction of Certificateless Signature -- Theory -- A Novel Range Test -- Efficient Primitives from Exponentiation in ? p -- PA in the Two-Key Setting and a Generic Conversion for Encryption with Anonymity -- Statistical Decoding Revisited -- Invited Talk -- Towards Provable Security for Ubiquitous Applications -- SecurityApplications -- Oblivious Scalar-Product Protocols -- On Optimizing the k-Ward Micro-aggregation Technique for Secure Statistical Databases -- Provable Security -- Direct Chosen-Ciphertext Secure Identity-Based Key Encapsulation Without Random Oracles -- Generic Transforms to Acquire CCA-Security for Identity Based Encryption: The Cases of FOpkc and REACT -- Tag-KEM from Set Partial Domain One-Way Permutations -- Protocols -- An Extension to Bellare and Rogaway (1993) Model: Resetting Compromised Long-Term Keys -- Graphical Representation of Authorization Policies for Weighted Credentials -- Secure Cross-Realm C2C-PAKE Protocol -- Hashing and Message Authentication -- Constructing Secure Hash Functions by Enhancing Merkle-Damgård Construction -- Forgery and Key Recovery Attacks on PMAC and Mitchell’s TMAC Variant -- Side Channel Attacks Against HMACs Based on Block-Cipher Based Hash Functions.

Sommario/riassunto

The 11th Australasian Conference on Information Security and Privacy (ACISP 2006) was held in Melbourne, 3–5 July, 2006. The conference was sponsored by Deakin University, the Research Network for a Secure Australia, and was organized in cooperation with the University of Wollongong. The conference brought together researchers,practitioners and a wide range of other users from academia, industries and government organizations. The program included 35 papers covering important aspects of information security technologies. The papers were selected from 133 submissions through a two-stage anonymous review process. Each paper received at least three reviews by members of the Program Committee, and was then scrutinized by the whole committee during a two-week discussion. There were 19 papers eligible for the “best student paper” award. The award was given to Yang Cui from the U- versity of Tokyo for the paper “Tag-KEM from Set Partial Domain One-Way Permutations. ” In addition to the regular papers the program also included three invited talks. Bart Preneel gave an invited talk entitled “Electronic Identity Cards: Threats and Opportunities. ” Mike Burmester’s talk was “Towards Provable - curity for Ubiquitous Applications. ” The details of the third talk had not been ?nalized at the time of publication of these proceedings. We wish to thank all the authors of submitted papers for providing the c- tent for the conference;their high-quality submissions madethe task of selecting a program very di?cult.