1. Record Nr. UNINA9910767571803321

Titolo	Information and communication security : second International Conference, ICICS '99, Sydney, Australia, November 9-11, 1999 : proceedingsity / / Vijay Varadharajan, Yi Mu (editors)
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer, , [1999] Â©1999
ISBN	3-540-47942-2
Edizione	[1st ed. 1999.]
Descrizione fisica	1 online resource (XII, 328 p.)
Collana	Lecture Notes in Computer Science ; ; 1726
Disciplina	005.8
Soggetti	Computer security Telecommunication systems - Security measures
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	Keynote Speech -- International Cryptography -- Cryptanalysis -- Reaction Attacks against Several Public-Key Cryptosystem -- Cryptanalysis of Some AES Candidate Algorithms -- Language Based Approach to Security -- Issues in the Design of a Language for Role Based Access Control -- Extending Erlang for Safe Mobile Code Execution -- Electronic Commerce and Secret Sharing -- Detachable Electronic Coins -- Linear Secret Sharing with Divisible Shares -- Efficient Publicly Verifiable Secret Sharing Schemes with Fast or Delayed Recovery -- Digital Signatures -- Zero-Knowledge Proofs of Possession of Digital Signatures and Its Applications -- Signature Scheme for Controlled Environments -- On the Cryptographic Value of the q th Root Problem -- Keynote Speech -- Protecting Critical Information Systems -- Security Protocols -- Delegation Chains Secure Up to Constant Length -- Optimal Construction of Unconditionally Secure ID-Based Key Sharing Scheme for Large-Scale Networks -- Enhancing the Resistance of a Provably Secure Key Agreement Protocol to a Denial-of-Service Attack -- An Extended Logic for Analyzing Timed-Release Public-Key Protocols -- Applications -- Bringing Together X.509 and EDIFACT Public Key Infrastructures: The DEDICA Project -- User Identification System Based on Biometrics for Keystroke -- Boundary Conditions that Influence Decisions about Log File Formats in Multi-

application Smart Cards -- Send Message into a Definite Future -- Cryptography -- Efficient Accumulators without Trapdoor Extended Abstract -- Evolutionary Heuristics for Finding Cryptographically Strong S-Boxes -- Incremental Authentication of Tree-Structured Documents -- Complexity and Security Functions -- Plateaued Functions -- On the Linear Complexity of the Naor-Reingold Pseudo-Random Function -- On the Channel Capacity of Narrow-Band Subliminal Channels.

Sommario/riassunto

ICICS’99, the Second International Conference on Information and Communication Security, was held in Sydney, Australia, 9-11 November 1999. The conference was sponsored by the Distributed System and Network Security - search Unit, University of Western Sydney, Nepean, the Australian Computer Society, IEEE Computer Chapter (NSW), and Harvey World Travel. I am grateful to all these organizations for their support of the conference. The conference brought together researchers, designers, implementors and users of information security systems and technologies. A range of aspects was addressed from security theory and modeling to system and protocol designs and implementations to applications and management. The conference consisted of a series of refereed technical papers and invited technical presentations. The program committee invited two distinguished key note speakers. The ?rst keynote speech by Doug McGowan, a Senior Manager from Hewlett-Packard, USA, discussed cryptography in an international setting. Doug described the current status of international cryptography and explored possible future trends and new technologies. The second keynote speech was delivered by Sushil Ja-dia of George Mason University, USA. Sushil’s talk addressed the protection of critical information systems. He discussed issues and methods for survivability of systems under malicious attacks and proposed a fault-tolerance based approach. The conference also hosted a panel on the currently much debated topic of Internet censorship. The panel addressed the issue of censorship from various viewpoints namely legal, industrial, governmental and technical.