1. Record Nr. UNINA9910143884303321

Titolo	Security in Communication Networks : Third International Conference, SCN 2002, Amalfi, Italy, September 11-13, 2002, Revised Papers / / edited by Stelvio Cimato, Clemente Galdi, Giuseppe Persiano
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2003
ISBN	3-540-36413-7
Edizione	[1st ed. 2003.]
Descrizione fisica	1 online resource (IX, 263 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 2576
Disciplina	005.8
Soggetti	Computer communication systems Data encryption (Computer science) Operating systems (Computers) Algorithms Computers and civilization Computers Law and legislation Computer Communication Networks Cryptology Operating Systems Algorithm Analysis and Problem Complexity Computers and Society Legal Aspects of Computing
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	Invited Talks -- Some Applications of Polynomials for the Design of Cryptographic Protocols -- Secure Multi-party Computation Made Simple -- Forward Security -- Forward Secrecy in Password-Only Key Exchange Protocols -- Weak Forward Security in Mediated RSA -- Foundations of Cryptography -- On the Power of Claw-Free Permutations -- Equivocable and Extractable Commitment Schemes -- An Improved Pseudorandom Generator Based on Hardness of Factoring -- Intrusion-Resilient Signatures: Generic Constructions, or Defeating

Strong Adversary with Minimal Assumptions -- Key Management -- Efficient Re-keying Protocols for Multicast Encryption -- On a Class of Key Agreement Protocols Which Cannot Be Unconditionally Secure -- A Group Key Distribution Scheme with Decentralised User Join -- Cryptanalysis -- On a Resynchronization Weakness in a Class of Combiners with Memory -- On Probability of Success in Linear and Differential Cryptanalysis -- Differential Cryptanalysis of a Reduced-Round SEED -- System Security -- Medical Information Privacy Assurance: Cryptographic and System Aspects -- A Format-Independent Architecture for Run-Time Integrity Checking of Executable Code -- Signature Schemes -- How to Repair ESIGN -- Forward-Secure Signatures with Fast Key Update -- Constructing Elliptic Curves with Prescribed Embedding Degrees -- A Signature Scheme with Efficient Protocols -- Zero Knowledge -- Efficient Zero-Knowledge Proofs for Some Practical Graph Problems -- Reduction Zero-Knowledge -- A New Notion of Soundness in Bare Public-Key Model -- Information Theory and Secret Sharing -- Robust Information-Theoretic Private Information Retrieval -- Trading Players for Efficiency in Unconditional Multiparty Computation -- Secret Sharing Schemes on Access Structures with Intersection Number Equal to One.