1. Record Nr. UNINA9910483316003321

Titolo	Security in Communication Networks [[electronic resource]] : 4th International Conference, SCN 2004, Amalfi, Italy, September 8-10, 2004, Revised Selected Papers / / edited by Carlo Blundo, Stelvio Cimato
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2005
ISBN	3-540-30598-X
Edizione	[1st ed. 2005.]
Descrizione fisica	1 online resource (XII, 388 p.)
Collana	Security and Cryptology ; ; 3352
Disciplina	005.8
Soggetti	Data encryption (Computer science) Computer communication systems Operating systems (Computers) Computers and civilization Management information systems Computer science Algorithms Cryptology Computer Communication Networks Operating Systems Computers and Society Management of Computing and Information Systems Algorithm Analysis and Problem Complexity
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 Talk -- ECRYPT: The Cryptographic Research Challenges for the Next Decade -- Reduction of Security/Primitives -- Relationships Between Diffie-Hellman and “Index Oracles” -- On the Security Notions for Public-Key Encryption Schemes -- Efficient Unconditional Oblivious Transfer from Almost Any Noisy Channel -- Signature Schemes -- A Provably Secure Short Transitive Signature Scheme from Bilinear Group Pairs -- Group Signatures with Separate and Distributed Authorities --

Threshold Cryptography in Mobile Ad Hoc Networks -- Anonymity and Privacy -- Designated Verifier Signatures: Anonymity and Efficient Construction from Any Bilinear Map -- Group Signatures: Better Efficiency and New Theoretical Aspects -- Efficient Blind Signatures Without Random Oracles -- Authentication and Identification -- Minimalist Cryptography for Low-Cost RFID Tags (Extended Abstract) -- On the Key Exposure Problem in Chameleon Hashes -- Zero Knowledge -- Identity-Based Zero-Knowledge -- Public Key Cryptosystems -- A Robust Multisignature Scheme with Applications to Acknowledgement Aggregation -- Efficient Key Encapsulation to Multiple Parties -- Improved Signcryption from q-Diffie-Hellman Problems -- Distributed Cryptography -- Colored Visual Cryptography Without Color Darkening -- On the Size of Monotone Span Programs -- Universally Composable DKG with Linear Number of Exponentiations -- Cryptanalysis of Public Key Cryptosystems -- An Algebraic Approach to NTRU (q = 2 n) via Witt Vectors and Overdetermined Systems of Nonlinear Equations -- Efficient Cryptanalysis of RSE(2)PKC and RSSE(2) PKC -- Cryptanalysis -- The Decimated Sample Based Improved Algebraic Attacks on the Nonlinear Filters -- Non-randomness of the Full 4 and 5-Pass HAVAL -- Email Security -- Controlling Spam by Secure Internet Content Selection -- Key Distribution and Feedback Shift Registers -- On Session Identifiers in Provably Secure Protocols -- How to Embed Short Cycles into Large Nonlinear Feedback-Shift Registers.

Sommario/riassunto

The 4th International Conference on Security in Communication Networks 2004 (SCN2004)was held at the “Diocese Hall” of the Archdiocese of Amal?-Cavade’ Tirreni and the “Armorial Bearings Hall” of the Archbishop Palace in Amal?, Italy, on September 8–10, 2004. Previous conferences also took place in Amal? in 1996, 1999 and 2002. The conference aimed at bringing together researchers in the fields of cryptography and security in communication networks to foster cooperation and the exchange of ideas. The main topics included all technical aspects of data security, including: anonymity, authentication, block ciphers, complexity-based cryptography, cry- analysis, digital signatures, distributed cryptography, hash functions, identification, implementations, key distribution, privacy, public key encryption, threshold cryptography, and zero knowledge. The Program Committee, consisting of 21 members, considered 79 papers and selected 26 for presentation; one of them was withdrawn by the authors. These papers were selected on the basis of originality, quality and relevance to cryptography and security in communication networks. Due to the high number of submissions, paper selection was a difficult and challenging task, and many good submissions had to be rejected. Each submission was refereed by at least three reviewers and some had four reports or more. We are very grateful to all the program committee members, who devoted much effort and valuable time to read and select the papers. In addition, we gratefully acknowledge the help of colleagues who reviewed submissions in their areas of expertise. They are all listed on page VII and we apologize for any inadvertent omissions. These proceedings include the revised versions of the 26 accepted papers and the abstract of the invited talk by Bart Preneel (ECRYPT: the Cryptographic Research Challenges for the Next Decade).