1. Record Nr. UNISA996466120803316

Titolo	Security and Cryptography for Networks [[electronic resource]] : 5th International Conference, SCN 2006, Maiori, Italy, September 6-8, 2006, Proceedings / / edited by Roberto De Prisco, Moti Yung
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2006
ISBN	3-540-38081-7
Edizione	[1st ed. 2006.]
Descrizione fisica	1 online resource (XII, 368 p.)
Collana	Security and Cryptology ; ; 4116
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Computer networks Operating systems (Computers) Electronic data processing—Management Algorithms Computers and civilization Cryptology Computer Communication Networks Operating Systems IT Operations Computers and Society
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	Distributed Systems Security: Foundations -- Edge Eavesdropping Games -- Universally Composable Simultaneous Broadcast -- Signature Schemes Variants -- Relations Among Security Notions for Undeniable Signature Schemes -- Concurrent Blind Signatures Without Random Oracles -- Universal Designated Verifier Signatures Without Random Oracles or Non-black Box Assumptions -- Block Ciphers Analysis -- Understanding Two-Round Differentials in AES -- Related-Key Attacks on the Full-Round Cobra-F64a and Cobra-F64b -- Anonymity and E-Commerce -- Constant-Size Dynamic k-TAA -- On Secure Orders in

the Presence of Faults -- Balancing Accountability and Privacy Using E-Cash (Extended Abstract) -- Public Key Encryption and Key Exchange -- About the Security of MTI/C0 and MQV -- Chosen-Ciphertext Secure Threshold Identity-Based Key Encapsulation Without Random Oracles -- A New Key Exchange Protocol Based on MQV Assuming Public Computations -- Secret Sharing -- Ideal Secret Sharing Schemes Whose Minimal Qualified Subsets Have at Most Three Participants -- Cheating Immune (2,n)-Threshold Visual Secret Sharing -- Rational Secret Sharing, Revisited -- Symmetric Key Cryptanalysis and Randomness -- On the Security of HMAC and NMAC Based on HAVAL, MD4, MD5, SHA-0 and SHA-1 (Extended Abstract) -- Distinguishing Stream Ciphers with Convolutional Filters -- On Statistical Testing of Random Numbers Generators -- Applied Authentication -- Lightweight Email Signatures (Extended Abstract) -- Shoehorning Security into the EPC Tag Standard -- Proof-Carrying Proxy Certificates -- Public Key Related Cryptanalysis -- Cryptanalysis of Rainbow -- An Improved LPN Algorithm -- Invited Talk -- Theory and Practice of Multiparty Computation.

Sommario/riassunto

The Conference on Security and Cryptography for Networks 2006 (SCN 2006) was held in Maiori, Italy, on September 6-8, 2006. The conference was the ?fth in the SCN series, and this year marked a change in its name (the former name was Security in Communication Networks). The name change meant to better describe the scope of the conference while preserving the SCN acronym. This year for the ?rst time we had the proceedings volume ready at the conference. We feel thatthe SCN conferencehas maturedandthat it has becomea tradition to hold it regularly in the beautiful setting of the Amal?tan coast as a biennial event. Theconferencebroughttogetherresearchersinthe? eldsofcryptographyand security in order to foster the extension of cooperation and exchange of ideas among them, aiming at assuring safety and trustworthiness of communication networks. The topics covered by the conference this year included: foundations of distributed systems security, signatures schemes, block ciphers, anonymity, e-commerce, public key encryption and key exchange, secret sharing, symmetric and public key cryptanalysis, randomness, authentication. The international Program Committee consisted of 24 members who are top experts in the conference ?elds. We received 81 submissions amongst which 24 papers were selected for presentation at the conference. These proceedings - clude the extended abstract versions of the 24 accepted papers and the short abstract of the invited talk by Ivan Damg? ard.