1. Record Nr. UNINA9910768182403321

Titolo	Information Security : 6th International Conference, ISC 2003, Bristol, UK, October 1-3, 2003, Proceedings / / edited by Colin Boyd, Wenbo Mao
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2003
ISBN	3-540-39981-X
Edizione	[1st ed. 2003.]
Descrizione fisica	1 online resource (XII, 448 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 2851
Disciplina	005.8
Soggetti	Data encryption (Computer science) Computer networks Computers, Special purpose Operating systems (Computers) Algorithms Management information systems Computer science Cryptology Computer Communication Networks Special Purpose and Application-Based Systems Operating Systems Algorithm Analysis and Problem Complexity Management of Computing and Information Systems
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 -- Revisiting Software Protection -- Network Security -- Enabling Shared Audit Data -- Cryptographically Generated Addresses (CGA) -- Validating and Securing Spontaneous Associations between Wireless Devices -- Single Sign-On Using Trusted Platforms -- Public-Key Algorithms -- Easy Verifiable Primitives and Practical Public Key Cryptosystems -- Reactively Secure Signature Schemes -- Validating Digital Signatures without TTP’s Time-Stamping and Certificate Revocation -- A Fast Signature Scheme Based on New On-line

Computation -- Cryptographic Protocols -- Distributed RSA Signature Schemes for General Access Structures -- Divisible Voting Scheme -- Unconditionally Secure Homomorphic Pre-distributed Bit Commitment and Secure Two-Party Computations -- The Design and Implementation of Protocol-Based Hidden Key Recovery -- Invited Talk -- Intrinsic Limitations of Digital Signatures and How to Cope with Them -- Protocol Attacks -- On the Security of Fair Non-repudiation Protocols -- Security Analysis of a Password Authenticated Key Exchange Protocol -- Attacks on Public Key Algorithms -- Zero-Value Point Attacks on Elliptic Curve Cryptosystem -- Cryptanalysis of an Algebraic Privacy Homomorphism -- Analysis of the Insecurity of ECMQV with Partially Known Nonces -- Block Ciphers -- Hardware-Focused Performance Comparison for the Standard Block Ciphers AES, Camellia, and Triple-DES -- A Note on Weak Keys of PES, IDEA, and Some Extended Variants -- Foundations of Differential Cryptanalysis in Abelian Groups -- Authorization -- Trust and Authorization in Pervasive B2E Scenarios -- A Logic Model for Temporal Authorization Delegation with Negation -- Watermarking -- Zero-Distortion Authentication Watermarking -- Designated Verification of Non-invertible Watermark -- Software Security -- Proactive Software Tampering Detection -- Run-Time Support for Detection of Memory Access Violations to Prevent Buffer Overflow Exploits -- Towards a Business Process-Driven Framework for Security Engineering with the UML -- Codes and Related Issues -- Error Correcting and Complexity Aspects of Linear Secret Sharing Schemes -- Systematic Treatment of Collusion Secure Codes: Security Definitions and Their Relations -- Short c-Secure Fingerprinting Codes -- The Role of Arbiters in Asymmetric Authentication Schemes.

Sommario/riassunto

The 2003 Information Security Conference was the sixth in a series that started with the InformationSecurity Workshopin 1997.A distinct feature of this series is the wide coverage of topics with the aim of encouraging interaction between researchers in di?erent aspects of information security. This trend continued in the program of this year’s conference. There were 133 paper submissions to ISC 2003. From these submissions the 31papersintheseproceedingswereselectedbytheprogramcommittee, covering a wide range of technical areas. These papers are supplemented by two invited papers; athirdinvitedtalkwaspresentedattheconferencebutisnotrepresented by a written paper. We would like to extend our sincere thanks to all the authors that submitted papers to ISC 2003, and we hope that those whose papers were declined will be able to ?nd an alternative forum for their work. We are also very grateful to the three eminent invited speakers at the conference: Paul van Oorschot (Carleton University, Canada), Ueli Maurer (ETH Zur ¨ ich, Switzerland), and Andy Clark (Inforenz Limited, UK). We were fortunate to have an energetic team of experts who took onthe task of the program committee. Their names may be found overleaf, and we thank them warmly for their considerable e?orts. This team was helped by an even larger number of individuals who reviewed papers in their particular areas of expertise. A list of these names is also provided, which we hope is complete.