1. Record Nr. UNISA996465681303316

Titolo	Cryptology and Network Security [[electronic resource]] : 9th International Conference, CANS 2010, Kuala Lumpur, Malaysia, December 12-14, 2010, Proceedings / / edited by Swee-Huay Heng, Rebecca N. Wright, Bok-Min Goi
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2010
ISBN	1-280-39072-7 9786613568649 3-642-17619-4
Edizione	[1st ed. 2010.]
Descrizione fisica	1 online resource (XIII, 355 p. 66 illus.)
Collana	Security and Cryptology ; ; 6467
Disciplina	005.8
Soggetti	Data encryption (Computer science) Computer communication systems Computer programming Computer science—Mathematics Coding theory Information theory Data structures (Computer science) Cryptology Computer Communication Networks Programming Techniques Discrete Mathematics in Computer Science Coding and Information Theory Data Structures and Information Theory
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	Block Ciphers -- Cryptanalysis of Reduced-Round MIBS Block Cipher -- Impossible Differential Cryptanalysis of ARIA Reduced to 7 Rounds -- An Algorithm Based Concurrent Error Detection Scheme for AES -- Invited Talk I -- Cryptography for Unconditionally Secure Message Transmission in Networks (Invited Talk) -- Wireless Network Security --

Performance and Security Aspects of Client-Side SSL/TLS Processing on Mobile Devices -- A Practical Cryptographic Denial of Service Attack against 802.11i TKIP and CCMP -- User Tracking Based on Behavioral Fingerprints -- Hash Functions -- On the Collision and Preimage Resistance of Certain Two-Call Hash Functions -- Integral Distinguishers of Some SHA-3 Candidates -- Near-Collisions on the Reduced-Round Compression Functions of Skein and BLAKE -- Public Key Cryptography -- Practical Algebraic Cryptanalysis for Dragon-Based Cryptosystems -- Generating Parameters for Algebraic Torus-Based Cryptosystems -- Analysis of the MQQ Public Key Cryptosystem -- Efficient Scalar Multiplications for Elliptic Curve Cryptosystems Using Mixed Coordinates Strategy and Direct Computations -- Invited Talk II -- Cryptography Meets Hardware: Selected Topics of Hardware-Based Cryptography (Invited Talk) -- Secure Mechanisms -- Towards a Cryptographic Treatment of Publish/Subscribe Systems -- STE3D-CAP: Stereoscopic 3D CAPTCHA -- TRIOB: A Trusted Virtual Computing Environment Based on Remote I/O Binding Mechanism -- Cryptographic Protocols -- Dynamic Group Key Exchange Revisited -- Towards Practical and Secure Coercion-Resistant Electronic Elections -- Anonymous Credentials -- Predicate Encryption with Partial Public Keys -- Anonymous Credential Schemes with Encrypted Attributes -- One Time Anonymous Certificate: X.509 Supporting Anonymity.

Sommario/riassunto

The 9th International Conference on Cryptology and Network Security (CANS 2010) was held in Kuala Lumpur, Malaysia during December 12–14, 2010. The conference was co-organized by the Multimedia University (MMU), Malaysia, and Universiti Tunku Abdul Rahman (UTAR), Malaysia. The conference received 64 submissions from 22 countries, out of which 21 were accepted after a careful and thorough review process. These proceedings also contain abstracts for two invited talks. All submissions were reviewed by at least three members of the Program Committee; those authored or co-authored by Program Committee members were reviewed by at least ?ve reviewers. P- gram Committee members were allowed to use external reviewers to assist with their reviews, but remained responsible for the contents of the review and r- resenting papers during the discussion and decision making. The review phase was followed by a 10-day discussion phase in which each paper with at least one supporting review was discussed, additional experts were consulted where needed, and ?nal decisions were made. We thank the Program Committee for their hard work in selecting the p- gram. We also thank the external reviewers who assisted with reviewing and the CANS Steering Committee for their help. We thank Shai Halevi for use of his Web-Submission-and-Review software that was used for the electronic s- mission and review of the submitted papers, and we thank the International Association for Cryptologic Research (IACR) for Web hosting of the software.