1. Record Nr. UNINA9910484305203321

Titolo	Information Security and Privacy : 14th Australasian Conference, ACISP 2009 Brisbane, Australia, July 1-3, 2009 Proceedings / / edited by Colin Boyd, Juan González Nieto
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2009
ISBN	3-642-02620-6
Edizione	[1st ed. 2009.]
Descrizione fisica	1 online resource (XI, 470 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 5594
Classificazione	DAT 050f DAT 460f SS 4800
Altri autori (Persone)	BoydColin <1959-> Gonzalez NietoJuan M
Disciplina	004.6
Soggetti	Computer networks Data protection Cryptography Data encryption (Computer science) Electronic data processing - Management Coding theory Information theory Algorithms Computer Communication Networks Data and Information Security Cryptology IT Operations Coding and Information Theory
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based on print version record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Invited Lecture -- Is the Information Security King Naked? -- Network Security -- Measurement Study on Malicious Web Servers in the .nz Domain -- A Combinatorial Approach for an Anonymity Metric -- On Improving the Accuracy and Performance of Content-Based File Type Identification -- Symmetric Key Encryption -- Attacking 9 and 10

Rounds of AES-256 -- Cryptographic Properties and Application of a Generalized Unbalanced Feistel Network Structure -- Lightweight Block Ciphers Revisited: Cryptanalysis of Reduced Round PRESENT and HIGHT -- Improved Cryptanalysis of the Common Scrambling Algorithm Stream Cipher -- Testing Stream Ciphers by Finding the Longest Substring of a Given Density -- New Correlations of RC4 PRGA Using Nonzero-Bit Differences -- Hash Functions -- Analysis of Property-Preservation Capabilities of the ROX and ESh Hash Domain Extenders -- Characterizing Padding Rules of MD Hash Functions Preserving Collision Security -- Distinguishing Attack on the Secret-Prefix MAC Based on the 39-Step SHA-256 -- Inside the Hypercube -- Meet-in-the-Middle Preimage Attacks on Double-Branch Hash Functions: Application to RIPEMD and Others -- On the Weak Ideal Compression Functions -- Invited Lecture -- Hardening the Network from the Friend Within -- Public Key Cryptography -- Reducing the Complexity in the Distributed Computation of Private RSA Keys -- Efficiency Bounds for Adversary Constructions in Black-Box Reductions -- Building Key-Private Public-Key Encryption Schemes -- Multi-recipient Public-Key Encryption from Simulators in Security Proofs -- Fair Threshold Decryption with Semi-Trusted Third Parties -- Conditional Proxy Broadcast Re-Encryption -- Security on Hybrid Encryption with the Tag-KEM/DEM Framework -- Protocols -- A Highly Scalable RFID Authentication Protocol -- Strengthening the Securityof Distributed Oblivious Transfer -- Towards Denial-of-Service-Resilient Key Agreement Protocols -- A Commitment-Consistent Proof of a Shuffle -- Implementation -- Finite Field Multiplication Combining AMNS and DFT Approach for Pairing Cryptography -- Random Order m-ary Exponentiation -- Jacobi Quartic Curves Revisited.

Sommario/riassunto

This book constitutes the refereed proceedings of the 14th Australasian Conference on Information Security and Privacy, ACISP 2009, held in Brisbane, Australia, during July 1-3, 2009. The 29 revised full papers presented together with two invited talks were carefully reviewed and selected from 106 submissions. The papers are organized in topical sections on network security, symmetric key encryption, hash functions, public key cryptography, protocols, and implementation.