1. Record Nr. UNINA9910483965003321

Titolo	Information Security and Cryptology - ICISC 2014 : 17th International Conference, Seoul, South Korea, December 3-5, 2014, Revised Selected Papers / / edited by Jooyoung Lee, Jongsung Kim
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2015
ISBN	3-319-15943-7
Edizione	[1st ed. 2015.]
Descrizione fisica	1 online resource (XIII, 448 p. 83 illus.)
Collana	Security and Cryptology ; ; 8949
Disciplina	005.8
Soggetti	Computer security Data encryption (Computer science) Management information systems Computer science Systems and Data Security Cryptology 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 contenuto	General Bounds for Small Inverse Problems and Its Applications to Multi-Prime RSA -- On the Security of Distributed Multiprime RSA -- Formal Modeling of Random Oracle Programmability and Verification of Signature Unforgeability Using Task-PIOAs -- Algebraic Cryptanalysis of Yasuda, Takagi and Sakurai’s Signature Scheme -- Discrete Logarithms for Torsion Points on Elliptic Curve of Embedding Degree 1 -- Efficient Key Dependent Message Security Amplification Against Chosen Ciphertext Attacks -- A Fast Phase-Based Enumeration Algorithm for SVP Challenge Through y-Sparse Representations of Short Lattice Vectors -- How Much Can Complexity of Linear Cryptanalysis Be Reduced? -- Format-Preserving Encryption Algorithms Using Families of Tweakable Blockciphers -- Bicliques with Minimal Data and Time Complexity for AES -- Fault Analysis on SIMON Family of Lightweight Block Ciphers -- A Clustering Approach for Privacy-Preserving in Social Networks -- Securely Solving Classical Network

Flow Problems -- Remote IP Protection Using Timing Channels -- Detecting Camouflaged Applications on Mobile Application Markets -- WrapDroid: Flexible and Fine-Grained Scheme Towards Regulating Behaviors of Android Apps -- A Collision Attack on a Double-Block-Length Compression Function Instantiated with Round-Reduced AES-256 -- LSH: A New Fast Secure Hash Function Family -- Lossless Data Hiding for Binary Document Images Using n-Pairs Pattern -- Montgomery Modular Multiplication on ARM-NEON Revisited -- A Fair and Efficient Mutual Private Set Intersection Protocol from a Two-Way Oblivious Pseudorandom Function -- Security Analysis of Polynomial Interpolation-Based Distributed Oblivious Transfer Protocols -- Compact and Efficient UC Commitments Under Atomic-Exchanges -- Issuer-Free Adaptive Oblivious Transfer with Access Policy -- Memory Address Side-Channel Analysis on Exponentiation -- Mutant Differential Fault Analysis of Trivium MDFA.

Sommario/riassunto

This book constitutes the thoroughly refereed post-conference proceedings of the 17th International Conference on Information Security and Cryptology, ICISC 2014, held in Seoul, South Korea in December 2014. The 27 revised full papers presented were carefully selected from 91 submissions during two rounds of reviewing. The papers provide the latest results in research, development and applications in the field of information security and cryptology. They are organized in topical sections on RSA security, digital signature, public key cryptography, block ciphers, network security, mobile security, hash functions, information hiding and efficiency, cryptographic protocol, and side-channel attacks.