1. Record Nr. UNINA9910317805003321

Titolo	Calorimetry : design, theory and applications in porous solids / / Juan Carlos Moreno Pirajan, editor
Pubbl/distr/stampa	[Place of publication not identified] : , : IntechOpen, , [2018] ©2018
ISBN	1-83881-294-6 1-78923-439-5
Descrizione fisica	1 online resource (124 pages) : illustrations
Disciplina	536.6
Soggetti	Calorimetry
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references.

2. Record Nr. UNISA996200361403316

Titolo	Information Security [[electronic resource]] : 18th International Conference, ISC 2015, Trondheim, Norway, September 9-11, 2015, Proceedings / / edited by Javier Lopez, Chris J. Mitchell
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2015
ISBN	3-319-23318-1
Edizione	[1st ed. 2015.]
Descrizione fisica	1 online resource (XIII, 570 p. 110 illus.)
Collana	Security and Cryptology ; ; 9290
Disciplina	005.82
Soggetti	Computer security Data encryption (Computer science) Algorithms Computer science—Mathematics Special purpose computers Computers and civilization Systems and Data Security Cryptology Algorithm Analysis and Problem Complexity Math Applications in Computer Science Special Purpose and Application-Based Systems Computers and Society
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- Cryptography I: Signatures -- Black-Box Separations on Fiat-Shamir-Type Signatures in the Non-Programmable Random Oracle Model -- 1 Introduction -- 1.1 Our Results -- 2 Preliminaries -- 2.1 Digital Signature Scheme -- 2.2 Canonical Identification Scheme -- 2.3 Fiat-Shamir Transformation -- 3 Impossibility of Proving the Security of FS-Type Signatures in the NPROM -- 4 Security Incompatibility Between the DL Assumption and the EUF-CMA Security of the Schnorr Signature in the NPROM -- References -- The Generic Transformation from Standard Signatures to

Identity-Based Aggregate Signatures -- 1 Introduction -- 2 Preliminaries -- 2.1 Indistinguishability Obfuscation -- 2.2 Puncturable PRFs -- 2.3 Universal Parameters -- 3 Identity-Based Aggregate Signatures -- 4 Generic Construction of Identity-Based Aggregate Signatures -- 5 Conclusions -- A Appendix -- 1 Public Key Encryption -- 2 Signature Schemes -- 3 Additively Homomorphic Encryption -- References -- Leveled Strongly-Unforgeable Identity-Based Fully Homomorphic Signatures -- 1 Introduction -- 1.1 Motivation -- 1.2 Contribution -- 1.3 Paper Organization -- 2 Preliminaries -- 2.1 Entropy and Statistical Distance -- 2.2 Background on Lattices and Hard Problems -- 2.3 Permutation Branching Program. -- 3 Identity-Based Homomorphic Trapdoor Functions -- 3.1 Definition -- 3.2 Construction: Basic Algorithms and Security -- 4 Homomorphic Evaluation and Noise Analysis -- 4.1 Basic Homomorphic Evaluation -- 4.2 The Homomorphic Output and Input Evaluation -- 4.3 Correctness of Homomorphic Evaluation and Noise Analysis -- 5 Strongly-Unforgeable Identity-Based Fully Homomorphic Signatures -- 5.1 Definition -- 5.2 Construction -- 6 Conclusions -- References -- Graded Signatures -- 1 Introduction -- 2 Definitions and Security Modeling.
3 Graded Signatures with Linear Signature Size and Verification Time -- A Preliminaries -- References -- System and Software Security -- Dynamically Provisioning Isolation in Hierarchical Architectures -- 1 Introduction -- 2 Background and Related Work -- 3 Isolation and Co-Location -- 3.1 Locality -- 3.2 Confinements -- 4 SafeHaven -- 4.1 Overview -- 4.2 Migrating Confinements -- 4.3 Allocation -- 5 Case Studies -- 5.1 Case 1: System-Wide Covert Channel -- 5.2 Case 2: Moving Target Defence -- 5.3 Other Policies -- 6 Conclusion -- A Appendix: Migration Frequency and Performance -- References -- Factors Impacting the Effort Required to Fix Security Vulnerabilities -- 1 Introduction -- 2 Related Work -- 3 Secure Software Development at SAP -- 4 Research Approach -- 5 Study Results -- 5.1 Vulnerability-Fixing Process -- 5.2 Factors that Impact the Vulnerability-Fix Time -- 5.3 Discussion -- 6 Impacts and Limitations of the Study -- 6.1 Impacts of the Study -- 6.2 Limitations of the Study -- 7 Lessons Learned -- 8 Conclusions -- References -- Software Security Maturity in Public Organisations -- 1 Introduction -- 2 Background -- 2.1 OpenSAMM -- 2.2 BSIMM -- 3 Method -- 4 Results -- 4.1 Practices with a High Degree of Maturity -- 4.2 Practices with a Low Degree of Maturity -- 4.3 Result Summary -- 5 Discussion -- 6 Conclusion and Further Work -- A Questionnaire -- A.1 Governance -- A.2 Construction/Intelligence -- A.3 Verification/Touchpoints -- A.4 Deployment -- References -- Cryptanalysis I: Block Ciphers -- Extending the Applicability of the Mixed-Integer Programming Technique in Automatic Differential Cryptanalysis -- 1 Introduction -- 2 MIP-based Automatic Differential Analysis -- 3 Automatic Search for Related-Key Differential Characteristics of PRIDE -- 3.1 Description of PRIDE.
3.2 Modelling the Differential Behavior of gi(j)() with Linear Inequalities -- 4 Constructing MIP Models Whose Feasible Regions are Exactly the Sets of All Differential Characteristics of SIMON -- 5 Automatic Analysis of the Propagation of Differences -- 6 Conclusion and Discussion -- A 2-round Iterative Related-key Differential Characteristics with Probability 2-4 for PRIDE -- References -- Automatic Search for Linear Trails of the SPECK Family -- 1 Introduction -- 2 Preliminaries -- 2.1 Notions -- 2.2 Description of SPECK -- 2.3 Automatic Search Framework -- 2.4 Linear Approximation of Modulo Addition -- 3 Linear Results on SPECK -- 3.1 Details of the Search -- 3.2 Search Results --

3.3 Linear Distinguishers -- 3.4 Key Recovery Attacks -- 4 Another Implementation of Wallen's Algorithm -- 5 Conclusions -- A Straightforward Implementations of Wallen's Algorithm -- A.1 The Top-Down Method -- A.2 The Bottom-Up Method -- B The Gray_Visit Procedure -- References -- From Distinguishers to Key Recovery: Improved Related-Key Attacks on Even-Mansour -- 1 Introduction -- 2 Notation -- 3 Generic Related-Key Key-Recovery Attacks on Even-Mansour Ciphers -- 3.1 Key-Recovery Attacks on r-round `39`42`" 613A``45`47`"603AIEM with Independent Keys -- 3.2 Extension to 2-Round Even-Mansour with a Linear Key Schedule -- 4 Application to Prøst-OTR -- 5 Conclusion -- A Proof-of-concept Implementation for a 64-Bit Permutation -- References -- Cryptography II: Protocols -- Oblivious PAKE: Efficient Handling of Password Trials -- 1 Introduction -- 1.1 Oblivious PAKE and Our Contributions -- 2 Oblivious PAKE Model -- 3 Transforming PAKE Protocols into -- 3.1 Requirements on PAKE -- 3.2 The Compiler -- 3.3 Relation to LAKE -- 3.4 Security Analysis -- 3.5 Oblivious PAKE Instantiation -- 3.6 Processing Multi-Component Messages -- 4 Concrete Instantiation Examples.
4.1 Oblivious SPAKE -- 5 Conclusion -- References -- Secure and Efficient Private Set Intersection Cardinality Using Bloom Filter -- 1 Introduction -- 2 Preliminaries -- 2.1 Security Model for Semi-honest Adversary [7] -- 2.2 Security Model for Malicious Adversary [7] -- 2.3 Goldwasser-Micali (GM) Encryption [8] -- 2.4 Bloom Filter [2] -- 3 Protocol -- 3.1 The PSI-CA -- 3.2 The APSI-CA -- 3.3 The PSI -- 3.4 The APSI -- 4 Security -- 5 Efficiency -- 6 Conclusion -- References -- On the Efficiency of Multi-party Contract Signing Protocols -- 1 Introduction -- 2 MPCS Requirements -- 3 Efficiency -- 4 Topologies -- 4.1 Ring -- 4.2 Sequential -- 4.3 Star -- 4.4 Mesh -- 5 Related Work -- 6 MPCS Protocols Overview -- 6.1 The TTP -- 7 Asynchronous Optimistic MPCS Protocols -- 7.1 An Asynchronous Optimistic MPCS Protocol Using Ring Topology -- 7.2 An Asynchronous Optimistic MPCS Protocol with Sequential, Star and Mesh Topology -- 8 Protocol Comparison -- 9 Conclusions -- References -- On the Provable Security of the Dragonfly Protocol -- 1 Introduction -- 2 Security Model -- 2.1 Model -- 2.2 Security Assumptions -- 3 The Dragonfly Protocol -- 4 Security Proof of Dragonfly Protocol -- 5 Conclusion -- References -- Network and Cloud Security -- Multipath TCP IDS Evasion and Mitigation -- 1 Introduction -- 1.1 Motivation and Research Questions -- 1.2 Contribution -- 1.3 Paper Structure -- 2 Related Work -- 3 Background -- 3.1 Multipath Networking -- 3.2 Network Security Reflections -- 3.3 Snort -- 4 Experimental Methodology -- 4.1 Client Side -- 4.2 Server Side -- 5 Statistical Analysis of Snort Rules -- 5.1 Results -- 5.2 Trends -- 6 Evaluation of Snort -- 6.1 Operation -- 6.2 Results -- 6.3 Discussion -- 7 Proposed Solution -- 7.1 Implementation -- 7.2 Validation -- 8 Outlook -- 9 Concluding Remarks -- References.
Provenance Based Classification Access Policy System Based on Encrypted Search for Cloud Data Storage -- 1 Introduction -- 2 Related Work -- 3 Provenance -- 4 PBCAP System Design -- 4.1 System Architecture -- 4.2 Provenance Based Classification Policy -- 5 Provenance Based Classification Scheme -- 5.1 Preliminaries -- 5.2 Policy Based Classification Scheme -- 5.3 Security Proof -- 6 Concluding Remarks -- References -- Multi-user Searchable Encryption in the Cloud -- 1 Introduction -- 2 Multi-user Searchable Encryption (MUSE) -- 3 Our Solution -- 3.1 Idea -- 3.2 Preliminaries -- 3.3 Protocol Description -- 3.4 Correctness -- 4 Security Model -- 4.1 Security with the CSP as Adversary -- 4.2 Security with the Proxy as Adversary -- 5 Security Analysis -- 5.1 Index Privacy with the CSP as

the Adversary -- 6 Performance Analysis -- 7 Related Work -- 8 Conclusion -- References -- Cryptography III: Encryption and Fundamentals -- CCA Secure PKE with Auxiliary Input Security and Leakage Resiliency -- 1 Introduction -- 2 Preliminaries -- 2.1 Strengthened Subgroup Indistinguishability Assumption -- 2.2 All-but-One Lossy Functions -- 2.3 Chameleon Hash Function -- 2.4 Goldreich-Levin Theorem for Large Fields -- 2.5 DDH Assumption -- 2.6 Min-entropy -- 3 Auxiliary Input and Leakage Resilient Public Key Encryption -- 3.1 Auxiliary Input CCA Security of PKE -- 3.2 Leakage Resilient CCA Security of PKE -- 4 The Generic Construction -- 5 Instantiation over a Group of Known Order -- 6 Conclusions -- References -- General Circuit Realizing Compact Revocable Attribute-Based Encryption from Multilinear Maps -- 1 Introduction -- 2 Preliminaries -- 2.1 The Notion of RABE for General Circuits -- 2.2 Multilinear Maps and Complexity Assumptions -- 3 RABE-I -- 4 RABE-II -- 5 Efficiency -- 6 Conclusion -- References -- Hashing into Jacobi Quartic Curves -- 1 Introduction.
2 Jacobi Quartic Curves.

Sommario/riassunto

This book constitutes the refereed proceedings of the 18th International Conference on Information Security, ISC 2015, held in Trondheim, Norway, in September 2015. The 30 revised full papers presented were carefully reviewed and selected from 103 submissions. The papers cover a wide range of topics in the area of cryptography and cryptanalysis and are organized in the following topical sections: signatures; system and software security; block ciphers; protocols; network and cloud security; encryption and fundamentals; PUFs and implementation security; and key generation, biometrics and image security. .