1. Record Nr. UNISA996200026503316

Titolo	Codes, Cryptology, and Information Security [[electronic resource]] : First International Conference, C2SI 2015, Rabat, Morocco, May 26-28, 2015, Proceedings - In Honor of Thierry Berger / / edited by Said El Hajji, Abderrahmane Nitaj, Claude Carlet, El Mamoun Souidi
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2015
ISBN	3-319-18681-7
Edizione	[1st ed. 2015.]
Descrizione fisica	1 online resource (XXVI, 375 p. 58 illus.)
Collana	Security and Cryptology ; ; 9084
Disciplina	005.8
Soggetti	Computer security Data encryption (Computer science) Coding theory Information theory Algorithms Computer science—Mathematics Systems and Data Security Cryptology Coding and Information Theory Algorithm Analysis and Problem Complexity Discrete Mathematics in Computer Science
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 -- Invited Papers -- Multidimensional Bell Inequalities and Quantum Cryptography -- 1 Local Realism and CHSH Inequalities -- 1.1 Local Realism -- 1.2 CHSH Inequalities -- 1.3 Quantum World -- 1.4 Complete Set of Inequalities -- 1.5 Generalization to -- 2 Multidimensional Inequalities -- 2.1 Discrete Fourier Transform -- 2.2 Homogeneous Inequalities -- 3 Violation by Quantum Systems -- 3.1 Measurements with Tritters -- 4 Quantum Keys Exchange -- 4.1 Ekert'91 Protocol -- 4.2 The Inequality CHSH-3 -- 4.3 The 3DEB Protocol -- 4.4 The Homogeneous Qutrits Protocol -- 5 Conclusion -- References -- Securing the Web of Things

with Role-Based Access Control -- 1 Introduction -- 2 Overview of WoT -- 2.1 Representation of Things on WoT -- 2.2 Ambient Space Stakeholders -- 2.3 WoT Framework -- 2.4 WoT Security Challenges -- 3 Overview of Role Based Access Control (RBAC) Model -- 4 Security Architecture for WoT -- 4.1 Integrating RBAC in WoT -- 4.2 Policy Enforcement Facitilies -- 4.3 Areas of Control Architecture -- 5 WOT Resources Protection -- 5.1 Documents and Views -- 5.2 Key Generation and Encryption -- 6 Conclusion and Future Work -- References -- On the Security of Long-Lived Archiving Systems Based on the Evidence Record Syntax -- 1 Introduction -- 2 ERS Archiving System -- 2.1 Setup -- 2.2 ERS Specification -- 3 Security Framework -- 3.1 Task-PIOAs -- 3.2 Longterm Implementation Relation -- 3.3 CIS System Model -- 4 ERS System Model -- 4.1 Construction Overview -- 4.2 Signature Service -- 4.3 Timestamp Service -- 4.4 Hash Service -- 4.5 Service Times -- 4.6 Dispatcher -- 4.7 ERS Service -- 5 ERSSecurityProof -- 6 Conclusions -- References -- Differential Attacks Against SPN: A Thorough Analysis -- 1 Introduction -- 2 Differential Attacks Against Substitution-Permutation Networks.
2.1 Substitution-Permutation Networks -- 2.2 Differential Cryptanalysis -- 2.3 Expected Probability of a Differential Characteristic -- 3 From Characteristics to Differentials -- 3.1 Expected Probability of a 2-round Differential -- 3.2 Influence of the Weight of the Differential -- 3.3 Number of Characteristics Within a Given 2-round Differential -- 4 SPNwithanAPNSbox -- 4.1 APN Sboxes over F8 -- 4.2 APN Sboxes over F32 -- 5 MEDP2 can be Tight for a Differential of Non-minimal Weight -- 5.1 Examples where MEDP2 is Tight for a Differential of Weight (-- 5.2 Example where MEDP2 is Tight for a Differential of Weight (-- 6 Conclusions -- References -- On the Properties of Vectorial Functions with Plateaued Components and Their Consequences on APN Functions -- 1 Introduction -- 2 Preliminaries -- 3 Characterizations of Plateaued Boolean and Vectorial Functions -- 3.1 Characterization by Means of the Derivatives -- 3.2 Characterization by Means of Power Moments of the Walsh Transform -- 4 Characterizations of the APN-ness of Componentwise Plateaued Vectorial Functions -- 4.1 Characterization by the Derivatives -- 4.2 Characterization by the Walsh Transform -- 4.3 The Case of Unbalanced Component Functions -- References -- Beyond Cryptanalysis Is Software Security the Next Threat for Smart Cards -- 1 Introduction -- 2 Smart Card Security -- 3 Some Software Attacks Again Java Card -- 3.1 Ambiguity in the Specification: The Type Confusion -- 3.2 Weakness in the Linker Process -- 3.3 Dumping the EEPROM -- 3.4 Dumping the ROM -- 3.5 A Complete Methodology to Attack Smart Card -- 4 Conclusion and Future Works -- References -- Extended Abstract: Codes as Modules over Skew Polynomial Rings -- References -- Regular Papers -- CUBE Cipher: A Family of Quasi-Involutive Block Ciphers Easy to Mask -- Introduction -- 1 Specifications -- 1.1 Key Schedule.
1.2 Instantiations -- 2 Design Rationale -- 3 Security Analysis -- 4 Implementation Aspects -- 4.1 Theoretical Implementation Results -- 4.2 Implementation Results and Comparisons -- 5 Conclusion -- References -- A Dynamic Attribute-Based Authentication Scheme -- 1 Introduction -- 2 ABA Scheme Introduction -- 2.1 Scheme Structure and Workflow -- 2.2 Security Requirements -- 3 Construction of the Dynamic ABA Scheme -- 3.1 Down-to-Top Attribute Tree Construction -- 3.2 Construction Algorithms -- 4 Analysis of the Dynamic ABA Scheme -- 4.1 Correctness Analysis -- 4.2 Security Requirements Analysis -- 4.3 Efficiency Analysis -- 5 Conclusions -- References -- Repeated-Root Isodual Cyclic Codes over Finite Fields -- 1 Introduction -- 2 Preliminaries -- 3 Cyclic Codes of Length 2amps over -- 4

Construction of Cyclic Isodual Codes of Length 2amps over -- 5 Cyclic Isodual Codes of Length 2amps over -- References -- Formal Enforcement of Security Policies on Parallel Systems with Risk Integration -- 1 Introduction -- 2 State of the Art -- 3 The Specification Logic of Security Policy -- 3.1 Syntax of a Logic -- 3.2 Semantics of -- 4 The Specification Language of Program -- 4.1 Syntax -- 4.2 Semantic -- 5 Formal Enforcement of Security Policies with Risk Integration -- 6 Example -- 7 Conclusion and Future Work -- References -- Countermeasures Mitigation for Designing Rich Shell Code in Java Card -- 1 Introduction -- 2 JavaCardSecurity -- 3 Embedded Countermeasures -- 3.1 State of the Art of Attacks Against Java Cards -- 3.2 Mitigating the Attacks with Affordable Countermeasures -- 3.3 Checking the Jump Boundaries -- 4 Mitigating the Control Flow Countermeasures -- 4.1 Principle of the Control Flow Extraction -- 4.2 Parameters Exchange between the Controller and the Shell Code -- 5 Experiments: The Java Self Modifying Code Revisited. 5.1 Type Confusion Exploitation -- 5.2 Completeness of the Countermeasure -- 6 Conclusion and Future Works -- References -- Weaknesses in Two RFID Authentication Protocols -- 1 Introduction -- 2 Preliminaries -- 2.1 Code-Based Cryptography -- 2.2 Randomized McEliece Cryptosystem -- 2.3 McEliece Cryptography Based on QC-MDPC Codes -- 2.4 Notations -- 3 Malek and Miri's Protocol -- 3.1 Review of the Malek and Miri's Protocol -- 3.2 Desynchronization Attack -- 4 Li et al.'s Protocol -- 4.1 Review of the Li et al.'s Protocol -- 4.2 Traceability Attack -- 5 Improved Protocol -- 5.1 Algorithm of Compute -- 5.2 Description of Improved Protocol -- 6 Conclusion -- References -- Square Code Attack on a Modified Sidelnikov Cryptosystem -- 1 Introduction -- 2 Preliminary Facts -- 3 Code-Based Public-Key Encryption Schemes -- 3.1 McEliece Encryption Scheme -- 3.2 Niederreiter Encryption Scheme -- 4 Wieschebrink's Masking Technique -- 4.1 Modified McEliece Scheme -- 4.2 Modified Niederreiter Scheme -- 5 Recovering the Random Columns in Polynomial Time -- 5.1 Reed-Muller Based Encryption Scheme -- 5.2 Description of the Attack -- 5.3 Complexity of the Attack -- 6 Conclusion -- References -- A Family of Six-Weight Reducible Cyclic Codes and their Weight Distribution -- 1 Introduction -- 2 Definitions, Notation and Main Assumption -- 3 Some Preliminary Results -- 4 AFormalProofofTheorem1 -- 5 Conclusion -- References -- Codes over L(GF(2)m,GF(2)m), MDS Diffusion Matrices and Cryptographic Applications -- 1 Additive Block Codes over -- 1 Additive Block Codes over GF(2)m and MDS Diffusion Matrices -- 1.1 Codes over a Finite Alphabet -- 1.2 Block Codes over -- 1.3 Systematic Block Codes -- 1.4 generator Matrix of a Systematic Block Code -- 1.5 Equivalence of Systematic Block Codes -- 1.6 MDS Systematic Block Codes and MDS Matrices.
1.7 MDS Diffusion Matrices for Cryptographic Applications -- 1.8 Ring Structures over -- 2 L-codes -- 2.1 Definition of -- 2.2 Duality of -- 3 Linear Codes over Subrings of -- 3.1 Notations and Remarks -- 3.2 Diagonal Endomorphisms -- 3.3 Subrings with a Single Generator -- 3.4 Block-Diagonal Subrings -- 4 Examples of Constructions -- 4.1 MDS Diffusion Matrices Derived from MDS Linear Codes over -- 4.2 An Example of Symmetric Automorphisms -- 4.3 Iterative Constructions on -- 5 Conclusion -- References -- A Higher Order Key Partitioning Attack with Application to LBlock -- 1 Introduction -- 2 Biclique Cryptanalysis -- 3 Description of LBlock -- 3.1 Notation -- 4 Higher Order Key Partitioning MitM Attack -- 4.1 A Low Data Complexity Attack on LBlock -- 5 Conclusion -- References -- A Note on the Existence of Self-Dual Skew Codes over Finite Fields -- 1 Introduction

-- 2 Generalities on Self-dual Skew Codes -- 3 Self-dual Skew Codes Generated by Skew Binomials -- 4 Self-dual Skew Codes Generated by Least Common Left Multiples of Skew Polynomials -- 5 Existence of Self-dual Skew Codes over Finite Fields with Odd Characteristic -- References -- The Weight Distribution of a Family of Lagrangian-Grassmannian Codes -- 1 Introduction -- 2 Projective Isotropic Lines in a Symplectic Space of Dimension 4 over any Finite Field -- 3 is a Class of Three-Weight Linear Codes -- 4 Conclusion -- References -- Algorithms of Constructing Linear and Robust Codes Based on Wavelet Decomposition and its Application -- 1 Introduction -- 2 The Basic Tenets of the Wavelet Transform -- 3 The Construction of Linear Code Based on Wavelet Transform -- 4 The Construction of Robust Code Based on Wavelet Linear Code -- 5 Implementation of Wavelet Robust Codes in ADV612 Chip -- 6 Conclusion -- References.
Failure of the Point Blinding Countermeasure Against Fault Attack in Pairing-Based Cryptography.

Sommario/riassunto

This book constitutes the proceedings of the First International Conference on Codes, Cryptology and Information Security, C2SI 2015, held in Rabat, Morocco, in May 2015. The 22 regular papers presented together with 8 invited talks were carefully reviewed and selected from 59 submissions. The first aim of this conference is to pay homage to Thierry Berger for his valuable contribution in teaching and disseminating knowledge in coding theory and cryptography in Morocco since 2003. The second aim of the conference is to provide an international forum for researchers from academia and practitioners from industry from all over the world for discussion of all forms of cryptology, coding theory and information security.