1.	Record Nr.	UNINA9910298961303321
	Titolo	Applications and Techniques in Information Security : 6th International Conference, ATIS 2015, Beijing, China, November 4-6, 2015, Proceedings / / edited by Wenjia Niu, Gang Li, Jiqiang Liu, Jianlong Tan, Li Guo, Zhen Han, Lynn Batten
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2015
	ISBN	3-662-48683-0
	Edizione	[1st ed. 2015.]
	Descrizione fisica	1 online resource (XVII, 398 p. 147 illus. in color.)
	Collana	Communications in Computer and Information Science, , 1865-0929 ; ; 557
	Disciplina	005.8
	Soggetti	Computer security Data encryption (Computer science) Algorithms Systems and Data Security Cryptology Algorithm Analysis and Problem Complexity
	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 -- Invited Speeches -- Memory Scrapper Attacks - Threats and Mitigations -- A Simple and Provable Secure (Authenticated) Key Exchange Based on LWE -- Contents -- Cryptograph -- An Image Encryption Algorithm Based on Zigzag Transformation and 3-Dimension Chaotic Logistic Map -- Abstract -- 1 Introduction -- 2 Basic Theory of the Proposed Algorithm -- 2.1 Zigzag Transformation -- 2.2 3-Dimension Logistic Chaotic Map -- 3 Algorithm Described -- 4 Simulation Result -- 5 The Security Analysis -- 5.1 Resistance to Exhaustive Attack -- 5.1.1 Analysis of Key Space -- 5.1.2 Keys' Sensitivity Analysis -- 5.2 Resistance to Statistical Attack -- 5.2.1 The Grey Histogram Analysis -- 5.2.2 Correlation Coefficient Analysis -- 5.3 Information Entropy Analysis -- 5.4 Compare the Efficiency of Encryption and Decryption -- 6 Conclusion -- Acknowledgements -- References -- An Improved Cloud-Based Revocable Identity-Based Proxy Re-encryption Scheme -- 1

Flow -- 3.2 Protocol Specification -- 4 Experimental Results and Discussion -- 5 Defense Mechanisms -- 6 Conclusion -- References -- A Lightweight Code-Based Authentication Protocol for RFID Systems -- 1 Introduction -- 2 Related Work -- 3 Error Correction Code (ECC) -- 4 Our Proposed Protocol -- 4.1 QC-MDPC McEliece Encryption -- 4.2 Initialization -- 4.3 Authentication -- 5 Security Analysis -- 6 Performance Analysis -- 7 Conclusion -- References -- An Overview of Ad Hoc Network Security -- Abstract -- 1 Introduction -- 2 Existing Typical Schemes -- 2.1 Threshold Mechanism Schemes -- 2.2 Self-organized Mechanism Schemes -- 2.3 Id-Based Mechanism Schemes -- 2.4 Cluster-Based Mechanism Schemes -- 3 The Comparisons of Those Schemes -- 4 Further Study -- 4.1 A Bi-directional Trust Model -- 4.2 A Trust Model with Parameter -- 5 Conclusions -- References.

Trust Computing and Privacy Protection -- Structural Analysis of IWA Social Network -- Abstract -- 1 Introduction -- 2 Related Work -- 3 Our Approach -- 3.1 Basic Concept of IWA Social Network -- 3.2 IWA Social Network Construction -- 3.3 Community Detection Algorithm -- 4 Experiment -- 4.1 Data Setting -- 4.2 Experimental Results and Analysis -- 5 Conclusion -- References -- A Differentially Private Method for Reward-Based Spatial Crowdsourcing -- 1 Introduction -- 2 Related Work and Background -- 2.1 Related Work -- 2.2 Differential Privacy -- 3 Differentially Private Method -- 3.1 Problem Definition -- 3.2 Building Contour Plot with DP -- 3.3 Task Assignment -- 4 Experiments -- 4.1 Settings -- 4.2 Experiment Results and Comparisons -- 5 Conclusions -- References -- Do Applications Perform Its Original Design? A Preliminary Analysis from Internet Big Data -- Abstract -- 1 Introduction and Motivations -- 2 Measurement Methodology -- 2.1 Overview of Data Sets -- 2.2 Measurement Metrics -- 2.3 Measurement Framework -- 3 Measurement Result -- 3.1 HTTP and HTTPS Performance -- 3.2 FTP Performance -- 3.3 SSH Performance -- 3.4 SMTP Performance -- 4 Conclusion and Future Works -- References -- Trust Prediction with Trust Antecedent Framework Regularization -- Abstract -- 1 Introduction -- 2 Related Work -- 3 Matrix Factorization Model for Trust Prediction -- 4 Modeling Trust Antecedent Framework for Trust Prediction -- 4.1 Factors of Perceived Trustworthiness -- 4.2 The Proposed Framework: tafTrust -- 5 Experiments -- 5.1 Dataset -- 5.2 Evaluation Metrics -- 5.3 Comparison Methods and Details -- 5.4 Impact of Parameter gamma -- 6 Conclusion and Future Work -- Acknowledgments -- References -- Trust Prediction Based on Interactive Relations Strength -- Abstract -- 1 Introduction -- 2 Related Work -- 3 Trust Prediction Framework.

3.1 Modeling Relational Strength in Fields -- 3.2 Trust Prediction Model -- 4 Experiments and Evaluation -- 4.1 Dataset and Evaluation Method -- 4.2 Comparison of Different Trust Predictors -- 5 Conclusions -- Acknowledgments -- References -- Cloud Security and Applications -- You Can't Hide: A Novel Methodology to Defend DDoS Attack Based on Botcloud -- Abstract -- 1 Introduction -- 2 Related Works -- 3 A Novel Methodology of Defending DDoS Attack Based on Botcloud -- 3.1 Identifying Attack Flows -- 3.2 Tracebacking Malicious Processes -- 4 Experiments and Analysis -- 4.1 Experimental Setting -- 4.2 Experimental Results and Analysis -- 5 Conclusion and Future Works -- References -- Quantitative Evaluation Method of Cloud Security -- Abstract -- 1 Introduction -- 2 Related Work -- 3 Cloud Security Indicator System -- 3.1 Principles of Building of Indicator System -- 3.2 Architecture of the Indicator System -- 4 Quantitative Assessment of Cloud Security -- 4.1 Multi-attribute Decision Making Indicator System -- 4.2 Normalization of Decision-Making Index -- 4.3 Multi-attribute

Sommario/riassunto

This book constitutes the refereed proceedings of the International Conference on Applications and Techniques in Information Security, ATIS 2015, held in Beijing, China, in November 2015. The 25 revised full papers and 10 short papers presented were carefully reviewed and selected from 103 submissions. The papers are organized in topical sections on invited speeches; cryptograph; evaluation, standards and protocols; trust computing and privacy protection; cloud security and applications; tools and methodologies; system design and implementations.