1.	Record Nr.	UNINA9910483515103321
	Titolo	Information Security Applications : 16th International Workshop, WISA 2015, Jeju Island, Korea, August 20-22, 2015, Revised Selected Papers / / edited by Ho-won Kim, Dooho Choi
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2016
	ISBN	3-319-31875-6
	Edizione	[1st ed. 2016.]
	Descrizione fisica	1 online resource (XVI, 438 p. 127 illus.)
	Collana	Security and Cryptology ; ; 9503
	Disciplina	005.8
	Soggetti	Computer security Data encryption (Computer science) Computer communication systems Management information systems Computer science Systems and Data Security Cryptology Computer Communication Networks 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 bibliografia	Includes bibliographical references and index.
	Nota di contenuto	Intro -- Preface -- Organization -- Keynote Speech -- Cyber Security Using Adversarial Learning and Conformal Prediction -- Contents -- Hardware Security -- M-ORAM: A Matrix ORAM with Log N Bandwidth Cost -- 1 Introduction -- 1.1 Related Work -- 1.2 Contribution and Paper Organization -- 2 M-ORAM Structure and Key Management -- 2.1 Server Storage Structure -- 2.2 Client Storage Structure -- 2.3 Recursive M-ORAM Construction -- 2.4 Encryption/Decryption Key Management -- 3 M-ORAM Operation -- 3.1 Read/Write Operation -- 3.2 Add/Delete Operation -- 4 Performance Analysis -- 4.1 M-ORAM Communication Overhead -- 4.2 Comparison of Bandwidth Cost with Binary Tree Based ORAM -- 5 Security Analysis -- 5.1 Security Requirements -- 5.2 Random Re-encryption -- 5.3 Indistinguishable Access Pattern -- 6 Conclusion -- References -- Process Variation

Based Encryption -- 3.1 Construction -- 3.2 Security Analysis -- 4 Revocable Hierarchical Identity-Based Encryption -- 4.1 KUNode Algorithm -- 4.2 Construction -- 4.3 Security Analysis -- 5 Conclusion -- References -- Publishing Graph Data with Subgraph Differential Privacy -- 1 Introduction -- 2 Related Work -- 3 Background -- 4 Subgraph-Differential Privacy -- 4.1 Problem -- 4.2 Definition -- 4.3 Mechanism -- 5 Evaluation -- 5.1 Preserving Average Node Degree -- 5.2 Preserving Triangle Counting -- 6 Conclusions and Future Work -- References -- An Improved Analysis of Broadcast Attacks on the GGH Cryptosystem -- 1 Introduction -- 2 Preliminaries -- 2.1 The Basic Concepts of Lattices and Lattice Hard Problems -- 2.2 GGH Cryptosystem -- 2.3 Plantard et al.'s Broadcast Attack on the GGH Cryptosystem -- 3 A Correction to Plantard et al.'s SVP Broadcast Attack -- 4 Efficiency Analysis of the Attack Using the SVP Algorithm -- 5 The New Attack Using the CVP Algorithm -- 6 Conclusion -- References.

Side Channel Attacks and Countermeasures -- Secure Binary Field Multiplication -- 1 Introduction -- 2 Binary Field Multiplications -- 3 Side Channel Attacks on Binary Field Multiplications -- 4 Secure Binary Field Multiplication -- 5 Conclusion -- References -- An Improved Second-Order Power Analysis Attack Based on a New Refined Expecter -- 1 Introduction -- 2 Preliminaries -- 2.1 Notation -- 2.2 Masked and Randomized Countermeasure for AES -- 2.3 Description of the SOCPA -- 2.4 The Reasonable Hamming Weight Estimator Functions -- 3 The Proposed Attack -- 3.1 The Refined Expecter -- 3.2 Workflow -- 4 Experimentation -- 4.1 Attack Environment -- 4.2 Experimental Results -- 5 Conclusion -- A Performance Evaluation of Reasonable Hamming Weight Estimator Functions -- References -- Various Threat Models to Circumvent Air-Gapped Systems for Preventing Network Attack -- 1 Introduction -- 2 Related Work -- 3 Threat Model -- 4 Technical Background -- 4.1 Collecting Sound Signal with Redefining Terminal Pin Number -- 4.2 OFDM Communication at Acoustic Band -- 4.3 FHSS Communication at Acoustic Band -- 4.4 Verification of Transmitting Error and Recovery Code -- 5 Experiment Design -- 5.1 Environment and System Configuration -- 6 Experiment and Results -- 6.1 The Maximum Communication Distance of Each Frequency in only Speaker Environment and with Microphone Environment -- 6.2 Comparison of the Transmission Success Rate of Each Frequency in the Environment with only Speaker and with Microphone -- 6.3 Comparison of Data Transmission of Each Frequency in only Speaker Environment and with Microphone Environment -- 7 Discussion and Conclusion -- 7.1 Discussion -- 7.2 Conclusion -- References -- An Improved Masking Scheme for S-Box Software Implementations -- 1 Introduction -- 2 Previous Software Masking Schemes -- 3 An Improved Addition Masking in Software.

3.1 Pre-computation -- 3.2 An Improved Addition Masking -- 3.3 Comparison Analysis of the Improved Masking Scheme -- 4 Implementations and Security Analysis -- 5 Conclusion -- A Appendix: Security Analysis -- References -- Security and Threat Analysis -- Open Sesame! Hacking the Password -- 1 Introduction -- 2 Related Works -- 2.1 Previous Works -- 2.2 Target Devices -- 3 Proposed Method -- 3.1 Modeling Movements and Keystroke Events -- 3.2 Countermeasures -- 4 Evaluation -- 5 Conclusion -- References -- BurnFit: Analyzing and Exploiting Wearable Devices -- 1 Introduction -- 2 Related Works -- 3 Background -- 3.1 Wearable Device Overview -- 3.2 Bluetooth Low Energy (BLE) -- 3.3 Threat Model -- 4 Vulnerability Analysis of Wearable Devices -- 4.1 Methodology -- 4.2 Update Channel Analysis -- 4.3 Data Channel Analysis -- 4.4 BLE

Channel Analysis -- 4.5 Device Analysis -- 5 Exploiting Wearable Devices -- 6 Discussion -- 6.1 Failure to Debug Hardware -- 6.2 Improving the Security of Wearable Devices -- 7 Conclusion -- References -- Security Analysis of FHSS-type Drone Controller -- 1 Introduction -- 2 Background and Attack Model -- 2.1 Frequency Hopping Spread Spectrum -- 2.2 Radio Control System for RC Aircraft -- 2.3 Attack Model -- 3 Methodology -- 3.1 Extracting the Hopping Sequence -- 3.2 Overcoming Limited SDR Bandwidth -- 3.3 Possible Attack Vectors -- 4 Implementation and Results -- 4.1 Equipment -- 4.2 Test Target Selection and Basic Analysis -- 4.3 FHSS Sequence Extraction -- 4.4 Baseband Extractor -- 5 Related Work -- 5.1 Drone Security -- 5.2 FHSS Security -- 5.3 Bluetooth Security -- 6 Discussion and Future Works -- 7 Conclusion -- References -- Encryption is Not Enough: Inferring User Activities on KakaoTalk with Traffic Analysis -- 1 Introduction -- 2 Inferring User Activities on KakaoTalk -- 2.1 Threat Model.

2.2 User Activities on KakaoTalk.

Sommario/riassunto

This book constitutes the thoroughly refereed post-workshop proceedings of the 16th International Workshop on Information Security Applications, WISA 2015, held on Jeju Island, Korea, in August 2015. The 35 revised full papers presented in this volume were carefully reviewed and selected from 78 submissions. The papers are organized in topical sections such as hardware security; cryptography, side channel attacks and countermeasures; security and threat analysis; IoT security; network security; cryptography; application security.