

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, Doocho 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

Evaluation Using RO PUF for Enhancing SCA-Resistant Dual-Rail Implementation -- 1 Introduction -- 2 Technical Background -- 2.1 Silicon Process Variation and Dual-Rail Impacts -- 2.2 Silicon Process Variation Alleviation -- 2.3 RO PUF Architecture -- 3 Dual-Rail PV Evaluation Using RO PUF -- 3.1 Thermal Effect to RO Pair -- 3.2 FPGA Evaluation -- 4 Dual-Rail Implementation -- 4.1 Dual Core Placement -- 4.2 Symmetric Dual-Rail Precharge Logic (DPL) -- 5 Experimental Analysis -- 5.1 Selection of Distinguisher -- 5.2 EM Surface Scan Acquisition -- 6 Security Evaluation -- 6.1 CPA Analysis -- 6.2 MIA Analysis -- 6.3 Experimental Summary -- 7 Conclusions -- References

-- Compact Implementations of LEA Block Cipher for Low-End Microprocessors -- 1 Introduction -- 2 Related Works -- 2.1 LEA Block Cipher -- 2.2 8-Bit Embedded Platform AVR -- 3 Proposed Method -- 3.1 On the Fly Versus Separate Computation Modes -- 3.2 Speed Optimization -- 3.3 Size Optimization -- 3.4 Implementations for 16-Bit MSP Embedded Processors.

4 Results -- 4.1 Speed Optimization -- 4.2 Size Optimization -- 5 Conclusion -- References

-- Compact Implementations of LSH -- 1 Introduction -- 2 Related Works -- 2.1 Hash Structure -- 2.2 8-Bit Embedded Platform: AVR -- 2.3 16-Bit Embedded Platform: MSP -- 2.4 32-Bit Embedded Platforms: ARM -- 3 Proposed Method -- 3.1 8-Bit AVR Platform -- 3.2 16-Bit MSP Platform -- 3.3 32-Bit ARM Platform -- 4 Results -- 4.1 8-Bit AVR Platform -- 4.2 16-Bit MSP Platform -- 4.3 32-Bit ARM Platform -- 5 Conclusion -- References

-- Detection of Rogue Devices in WLAN by Analyzing RF Features and Indoor Location of the Device -- Abstract -- 1 Introduction -- 2 Related Study -- 3 Rogue (MAC Spoofing) Device Detection Mechanism -- 3.1 Training Phase -- 3.2 Detection Phase -- 3.3 Experiments -- 4 Conclusions -- Acknowledgement -- References

-- Cryptography -- Security Analysis on RFID Mutual Authentication Protocol -- 1 Introduction -- 2 Review of Handle Manipulation Attack -- 3 Analysis of Attack Effects -- 3.1 Attack Effects -- 3.2 Link Timing Analysis -- 4 Conclusion -- References

-- How Much Randomness Can Be Extracted from Memoryless Shannon Entropy Sources? -- 1 Introduction -- 1.1 Entropy -- 1.2 Entropy Estimating -- 1.3 Problem Statement -- 1.4 Our Results and Applications -- 1.5 Organization -- 2 Preliminaries -- 2.1 Basic Definitions -- 2.2 Extractors -- 2.3 Technical Facts -- 3 Proof of Theorem3 -- 3.1 Characterizing Extractable Entropy -- 3.2 Determining the Threshold  $t$  -- 3.3 Putting This All Together -- 4 Conclusion -- References

-- Two Types of Special Bases for Integral Lattices -- 1 Introduction -- 2 Preliminaries -- 2.1 Lattice -- 2.2 Hermite Normal Form -- 3 Two Types of Bases for Any Integral Lattice -- 3.1 First Type -- 3.2 Second Type -- 4 Conclusion and Open Problems -- References

-- Keyword Updatable PEKS -- 1 Introduction -- 2 Preliminaries.

2.1 Identity-Based Proxy Re-encryption -- 3 Keyword-Updatable PEKS -- 4 Construction of KU-PEKS -- 5 Applications -- References

-- On Partitioning Secret Data Based on Concept of Functional Safety -- 1 Introduction -- 2 Preliminaries -- 3 Security Analysis -- 3.1 Attack Model -- 3.2 Metrics and Security Notions -- 3.3 How to Enhance Security -- 4 Proposed Method -- 4.1 Problem Settings -- 4.2 Partitioning Algorithm -- 5 Experimental Evaluation -- 5.1 Results for Quadratic Renyi Entropy -- 5.2 Discussions on Min-entropy and Guessing Entropy -- 6 Conclusion -- References

-- Unbounded Hierarchical Identity-Based Encryption with Efficient Revocation -- 1 Introduction -- 1.1 Our Contributions -- 1.2 Related Work -- 2 Preliminaries -- 2.1 Bilinear Groups -- 2.2 Complexity Assumption -- 2.3 Hierarchical IBE -- 2.4 Revocable HIBE -- 3 Hierarchical Identity-

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.

---