1.	Record Nr.	UNISA996465656903316
	Titolo	Information Security Theory and Practice: Security and Privacy of Mobile Devices in Wireless Communication [[electronic resource]] : 5th IFIP WG 11.2 International Workshop, WISTP 2011, Heraklion, Crete, Greece, June 1-3, 2011, Proceedings / / edited by Claudio Agostino Ardagna, Jianying Zhou
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2011
	ISBN	3-642-21040-6
	Edizione	[1st ed. 2011.]
	Descrizione fisica	1 online resource (XIII, 392 p.)
	Collana	Security and Cryptology ; ; 6633
	Disciplina	621
	Soggetti	Computer communication systems Management information systems Computer science Data encryption (Computer science) Algorithms Computer security Computers and civilization Computer Communication Networks Management of Computing and Information Systems Cryptology Algorithm Analysis and Problem Complexity Systems and Data Security 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 -- Title Page -- Preface -- Organization -- Table of Contents -- Keynote Speech -- Can Code Polymorphism Limit Information Leakage? -- Introduction -- Algorithmic Description -- Bucket Types -- Rewriting Algorithms -- Concrete Implementation -- Experimental Evaluation -- Performance -- Attacking a Standard aes Implementation -- Attacking an Unrolled aes Implementation -- Attacking a

Polymorphic aes Implementation -- Can Lisp-Like Languages Help? -- Structure -- Step by Step Explanations -- Rewriter -- Results -- Possible Extensions -- Avoiding Code Growth -- Separating H From F_i -- Randomizing Compilers: A Practical Approach -- References -- Mobile Authentication and Access Control -- Mobile Electronic Identity: Securing Payment on Mobile Phones -- Introduction -- Present-Day Payment Solutions -- NFC -- Bluetooth -- SMS -- Other Solutions -- Using a HISP: Mixing Context, Human Trust and Security -- Choosing a HISP -- Tailoring a HISP -- The Human Contribution -- Demonstrating a HISP -- Reverse Authentication -- Implementation -- Implementation of Approach A -- Implementation of Approach B -- Security Analysis -- Phishing/Credential Harvesting -- Malware -- Man in the Middle -- Conclusion -- References -- Role-Based Secure Inter-operation and Resource Usage Management in Mobile Grid Systems -- Introduction -- Relevant Work and Motivation -- The Proposed domRBAC Model for Modern Collaborative Systems -- domRBAC Elements -- domRBAC Definitions -- Use Cases -- Use Case 1: Resource Usage Management -- Use Case 2: Security Violation -- Conclusion -- References -- Lightweight Authentication -- SSL/TLS Session-Aware User Authentication Using a GAA Bootstrapped Key -- Introduction -- Background -- Man in the Middle Attacks -- Generic Authentication Architecture -- Related Work -- TLS-SA Using a GAA Bootstrapped Key -- The Basic Scheme.
Variants -- Analysis -- Informal Security Analysis -- Security-Efficiency Trade-Offs -- Conclusions -- References -- An Almost-Optimal Forward-Private RFID Mutual Authentication Protocol with Tag Control -- Introduction -- Security Model -- Tools -- Protocol Description -- Properties -- Security Reductions -- Conclusions -- References -- Affiliation-Hiding Authentication with Minimal Bandwidth Consumption -- Introduction -- Linkable vs. Unlinkable AHA -- The Challenge of Group Discovery -- Related Work -- Contributions and Organization -- Non-Interactive Key Distribution -- Definition and Security Model of NIKDS -- A Construction of NIKDS Based on Bilinear Maps (Pairings) -- Our Affiliation-Hiding Authentication Protocol -- Syntax of AHA -- Protocol Definition -- Correctness, Efficiency, and Parameter Selection -- Security Model for AHA -- Adversary Model -- Linkable Affiliation-Hiding Security -- Security Analysis of Our Protocol -- Conclusion -- References -- Algorithms -- Formal Framework for the Evaluation of Waveform Resynchronization Algorithms -- Introduction -- Resynchronization Algorithms -- Problem Statement -- AOC: Amplitude-Only Correlation -- POC: Phase-Only Correlation -- POC Flaw and Threshold-POC -- Complexity of AOC, POC and T-POC -- Evaluation of Resynchronization Algorithms -- Formal Framework -- Benchmarking of Representative Waveforms -- Conclusions and Perspectives -- References -- Solving DLP with Auxiliary Input over an Elliptic Curve Used in TinyTate Library -- Introduction -- Preliminaries -- Discrete Logarithm Problem with Auxiliary Input (DLPwAI) -- Cheon's Algorithm -- DLPwAI in Cryptographic Schemes -- Implementation -- BSGS Algorithm -- KKM Improvement -- Experimental Results -- Parameters -- Results -- Estimations -- Concluding Remarks -- References.
Information Leakage Discovery Techniques to Enhance Secure Chip Design -- Introduction -- EMA Analysis as a Design Phase -- Electromagnetic Emission Analysis -- Information Finding Algorithm -- Complexity Analysis -- Experimental Validation -- Workbench -- Experimental Results -- Conclusion -- References -- Hardware Implementation -- A Cryptographic Processor for Low-Resource Devices: Canning ECDSA and AES Like Sardines -- Introduction --

Related Work -- System Overview -- Hardware Architecture -- Arithmetic-Level Implementation -- Algorithm-Level Implementation -- The SHA-1 Algorithm -- The AES Algorithm -- ECC Scalar Multiplication -- ECDSA Implementation -- Results -- Conclusions -- References -- An Evaluation of Hash Functions on a Power Analysis Resistant Processor Architecture -- Introduction -- Background -- Side-Channel Attacks on Hash Functions -- The Power-Trust Platform -- Our Variant of the Power-Trust Platform -- Implementation of Hash Functions on the Power-Trust Platform -- Results -- Instruction Set Agility -- Performance -- Conclusions -- References -- A Comparison of Post-Processing Techniques for Biased Random Number Generators -- Introduction -- Known Techniques for De-Biasing -- Compression with Cryptographic Hash -- Compression Using the Von Neumann Corrector -- Compression Based on Good Linear Codes -- Comparison of Random Bias of Different Post-Processing Functions -- Comparison of Adversary Bias of Different Post-Processing Functions -- Adversary Bias after Linear Compression -- Adversary Bias after Von Neumann Compression -- Linear Compression Outperforming the Von-Neumann Compression -- The Use of Linear Codes with Large d -- Implementation -- Construction of Linear Corrector Functions Based on Cyclic Codes -- Resource Utilization -- Conclusion -- References -- Security and Cryptography.
AES Variants Secure against Related-Key Differential and Boomerang Attacks -- Introduction -- Our Contribution -- Framework for Protection against Related Key Differential and Boomerang Attacks -- Some Definitions and Notation -- Protection against Related-Key Differential Attack of [4] -- Protection against Related-Key Boomerang Attack of [3] -- Security of Improved May et al.'s AES Key Schedule against Related-key Attack -- Equivalent Keys in May et al.'s Key Schedule -- An Improved May et al.'s Key Schedule -- Improved May et al.'s Key Schedule is Secure against Related-Key Differential Attack -- Improved May et al.'s Key Schedule is Secure against Related-Key Boomerang Attack -- A New On-the-fly Key Schedule for AES Secure against Related-Key Differential and Boomerang Attacks -- Hardware Implementation -- References -- Leakage Squeezing Countermeasure against High-Order Attacks -- Introduction -- State of the Art -- First Order Masking Overview -- Vulnerability of the Masking against 1O-Attacks -- Vulnerability of the Masking against 2O-Attacks -- Proposed Masking Method for ``Leakage Squeezing'' -- Masking Principle -- Formal Security Assessment and Motivation for Some Bijections -- Experiments on Masked DES Implementations -- ROM Implementation -- USM Implementation -- Complexity and Throughput Results -- Information-Theoretic Evaluation of the Proposed Solutions -- Evaluation of the Implementations against 2O-Attacks -- Conclusion and Perspectives -- References -- Security Attacks and Measures (Short Papers) -- Differential Fault Analysis of the Advanced Encryption Standard Using a Single Fault -- Introduction -- Background -- The Advanced Encryption Standard -- The Fault Model -- The Fault Analysis -- The First Step of the Fault Attack -- Analysis of the First Step of the Fault Attack -- The Second Step of the Fault Attack.
Analysis of the Second Step of the Fault Attack -- Attacking other Bytes -- Comparison with Previous Work -- Conclusion -- References -- Entropy of Selectively Encrypted Strings -- Introduction -- Terminology and Definitions -- Languages -- Entropy -- Selective Encryption -- Confidentiality of Selective Encryption -- Zero- and First-Order Languages -- Second-Order Languages -- Third-Order Languages -- n-Order Languages -- Concluding Remarks -- References -- Practical Attacks on HB and HB+ Protocols -- Introduction -- Description of the

HB and HB+ Protocols -- Passive Attacks on HB Protocol -- Simple Walker Algorithm -- k-Basis Walker Algorithm -- Algorithm Analysis -- Experimental Results -- Conclusions -- References -- Attacks on a Lightweight Mutual Authentication Protocol under EPC C-1 G-2 Standard -- Introduction -- Review SRP -- Initialization Phase -- The (i+1)th Authentication Round -- Vulnerabilities of SRP -- Reveal EPC_s -- Privacy Analysis -- Revised Protocol -- Security Analysis -- Conclusion -- References -- Security Attacks -- A SMS-Based Mobile Botnet Using Flooding Algorithm -- Introduction -- Background and Motivation -- Related Works -- Challenging Issues -- Our Works and Contributions -- The Overview of the Proposed SMS-Based Botnet -- Stealthiness Study -- Topology Study Based on Simulation -- Simulation Setup -- Simulation Results -- Botnet Construction -- Botnet Maintaining -- Defense Strategies -- Conclusion -- References -- FIRE: Fault Injection for Reverse Engineering -- Introduction -- State of the Art -- Physical Attacks on Cryptographic Systems -- Solving Linear Boolean Systems -- The Case of DES -- The Case of AES -- Fault Injection -- Translation of the FI into Equations -- Random and unknown Faults -- SCARE Conclusion of a FIRE Attack -- Results with Various Fault Models and Contexts -- Conclusion -- References. Hardware Trojan Side-Channels Based on Physical Unclonable Functions.

Sommario/riassunto

This volume constitutes the refereed proceedings of the 5th IFIP WG 11.2 International Workshop on Information Security Theory and Practices: Security and Privacy of Mobile Devices in Wireless Communication, WISTP 2011, held in Heraklion, Crete, Greece, in June 2011. The 19 revised full papers and 8 short papers presented together with a keynote speech were carefully reviewed and selected from 80 submissions. They are organized in topical sections on mobile authentication and access control, lightweight authentication, algorithms, hardware implementation, security and cryptography, security attacks and measures, security attacks, security and trust, and mobile application security and privacy.