1. Record Nr. UNINA9910483202903321

Titolo	Security, Privacy, and Applied Cryptography Engineering : 5th International Conference, SPACE 2015, Jaipur, India, October 3-7, 2015, Proceedings / / edited by Rajat Subhra Chakraborty, Peter Schwabe, Jon Solworth
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2015
ISBN	3-319-24126-5
Edizione	[1st ed. 2015.]
Descrizione fisica	1 online resource (XVIII, 373 p. 88 illus. in color.)
Collana	Security and Cryptology ; ; 9354
Disciplina	005.82
Soggetti	Computer security Computer communication systems Data encryption (Computer science) Management information systems Computer science Algorithms Systems and Data Security Computer Communication Networks Cryptology Management of Computing and Information Systems Algorithm Analysis and Problem Complexity
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Intro -- Preface -- Message from the General Chairs -- SPACE 2015 -- Abstracts of Invited Talks -- Boring Crypto -- Introduction to Security Analysis of Crypto APIs -- The Tor Network: Free Software for a Free Society -- Post-Quantum Cryptography -- Inferring Programmer Expectations to Protect Program Execution -- Side Channel Attacks: Types, Methods and Countermeasures -- Contents -- Efficient Protocol for Authenticated Email Search -- 1 Introduction -- 2 Preliminaries -- 2.1 Cryptographic Primitives and Complexity Assumptions -- 2.2 Authenticated Data Structure -- 2.3 System Overview -- 3 Proposed Protocol -- 3.1 Setup -- 3.2 Update -- 3.3 Intersection -- 3.4 Union --

3.5 Composite Query -- 4 Comparison -- 4.1 Analytical Comparison -- 4.2 Experimental Results -- 5 Conclusion -- Analyzing Traffic Features of Common Standalone DoS Attack Tools -- 1 Introduction -- 2 Related Work -- 3 Experiment -- 3.1 DoS Tools Selection -- 3.2 Environment -- 3.3 Measurement -- 4 DoS Traffic Properties -- 4.1 Traffic Burst Behavior -- 4.2 Flow Count -- 4.3 Flow Parallelity -- 4.4 HTTP Requests Per Flow -- 4.5 HTTP Request URIs -- 4.6 Flow Packet Count -- 5 Discussion -- 5.1 Traffic Features and Aggregation -- 5.2 Repeating Patterns -- 5.3 Evasion Techniques -- 5.4 Future Work -- 6 Conclusions -- Design of Cyber Security for Critical Infrastructures: A Case for a Schizoid Design Approach -- Introduction -- Goals of Designing a Virtual SCADA Lab -- Virtual SCADA Testbed Design Methodology -- Distributed VSCADA Testbed System Architecture Design -- VSCADA Backend Architecture Design -- VSCADA Frontend Architecture Design -- Network Simulation/Emulation Architecture Design -- VSCADA Implementation -- Human Machine Interface (HMI) -- SCADA Master Control Server -- Communication Protocol -- Linux Containers/NS2 Interface -- Software Simulators.
Cyber Security Case Study -- Network Security Scenario -- Data Injection Attack Implementation -- Conclusion -- Designing for Attack Surfaces: Keep Your Friends Close, but Your Enemies Closer -- 1 Introduction -- 2 Background -- 2.1 System Configuration -- 2.2 Trends in System Configuration -- 3 Attack Surfaces -- 4 Proposed Approach -- 5 Deploying the Approach -- 5.1 Hierarchical State Machine Model -- 5.2 Proposing Attack Surfaces -- 5.3 Finding Flow Errors -- 5.4 Mediating Flow Errors -- 5.5 Testing the Resulting System -- 6 Conclusions -- Improving Application Security through TLS-Library Redesign -- Introduction -- Related Work -- API Pitfalls -- Improved APIs and Static Analysis -- Privilege Separation -- Specialized Cryptographic Key Isolation -- Threat Model -- Design of libtlssep -- Libtlssep Architecture -- LibtlssepAPI and Configuration -- Security, Programmability, and Performance -- Security Benefits of libtlssep's API and Architecture -- Programmability -- Performance -- Conclusion -- How Not to Combine RC4 States -- 1 Introduction -- 1.1 Contribution and Organization of the Paper -- 2 Description and Analysis of the RC4B Stream Cipher -- 2.1 Description of RC4B -- 2.2 Analysis of RC4B -- 3 Description and Analysis of Quad-RC4 and m-RC4 Stream Ciphers -- 3.1 Description of Quad-RC4 -- 3.2 Analysis of Quad-RC4 -- 3.3 Description of m-RC4 -- 3.4 Analysis for Even m -- 3.5 Analysis for General m -- 3.6 The Flaws in the Design -- 4 Experimental Results -- 5 Conclusion -- Preimage Analysis of the Maelstrom-0 Hash Function -- 1 Introduction -- 2 Related Work -- 3 Specifications of Maelstrom-0 -- 4 Pseudo Preimage Attack on the 6-Round Reduced Compression Function -- 5 Preimage of the Maelstrom-0 Hash Function -- 6 Conclusion -- Meet-in-the-Middle Attacks on Round-Reduced Khudra -- 1 Introduction -- 2 Specifications of Khudra -- 2.1 Notations.
3 MitM Attacks on Round-Reduced Khudra -- 3.1 A MitM Attack on 13-Round Khudra -- 3.2 A MitM Attack on 14-Round Khudra -- 4 Conclusion and Discussion -- Improved Key Recovery Attack on Round-reduced Hierocrypt-L1 in the Single-Key Setting -- 1 Introduction -- 2 Specification of Hierocrypt-L1 -- 3 A Differential Enumeration MitM Attack on HC-L1 -- 4 Conclusion -- S-boxes, Boolean Functions and Codes for the Resistance of Block Ciphers to Cryptographic Attacks, with or without Side Channels -- Introduction -- Known S-boxes with Good Properties -- The Case m<n -- Protection of S-boxes against Side Channel Attacks -- Masking -- Masking Schemes -- An Open Problem with Multiple Facets -- Boolean Functions, Vectorial Boolean Functions and Error Correcting Codes for

Improving Counter-Measures to SCA -- Correlation Immune Boolean Functions, Vectorial Functions with Correlation Immune Graphs, Complementary Information Set Codes -- Linear Complementary Dual Codes -- Simulations of Optical Emissions for Attacking AES and Masked AES -- Introduction -- Background on Photonic Emission -- Photonic Emissions in CMOS -- Photons Emission by the SRAM during the Reading Operation -- Background on AES -- The Masked AES Algorithm -- Photonic Side Channel Attacks on AES -- Monitoring the SRAM -- Key Recovery in the Simple Model -- Chosen Plaintext Attack in the Simple Model -- Key Recovery in the Generic Model -- Photonic Side Channel Attacks on Masked AES -- Key Recovery -- Two Different Bytes of the Masked Message (with the Same Masks) -- One Byte of the Masked Message and of the Associated Mask -- Numerical Model and Comparison -- Conclusion -- Fault Tolerant Infective Countermeasure for AES -- Introduction -- Preliminaries: The Infective Countermeasure -- Information Theoretic Evaluation of the Infective Countermeasure -- The Evaluation Methodology.
Evaluating the Security of the Infective Countermeasure against DFA -- Security against Single Fault Injections -- Security against Multiple Fault Injection -- Instruction Skip Threats to the Infective Countermeasure -- Possible Attacks on the Infective Countermeasure: Affecting Flow Sequence -- The Instruction Skip Fault Model -- Instruction Skip Attack on the Infective Countermeasure -- The Information Leakage : A Formal Quantification -- The Loopholes in the Infective Countermeasure : A Closer Look -- A Modified Infective Countermeasure -- Instruction Skip Attack on the Modified Algorithm -- Simulation and Experimental Results -- Simulation Results -- Experimental Results -- Conclusions -- Security of the Bit String cstr in the Modified Countermeasure -- Modified Transparency Order Property: Solution or Just Another Attempt -- Introduction -- Related Work -- Our Contributions -- Preliminaries -- Optimal S-boxes -- Cryptographic Properties of S-boxes -- Affine Equivalence -- Generating S-boxes -- Random Search -- Genetic Algorithm -- Evolved S-boxes -- Affine Transformations -- Success Rate Evaluation of DPA Attacks on the Synthesized S-boxes -- Conclusion -- Investigating SRAM PUFsin large CPUs and GPUs -- 1 Introduction -- 2 Experimental Setup for the CPU -- 3 CPU Registers -- 3.1 Boot Process -- 3.2 Kernel -- 3.3 GRUB -- 3.4 Coreboot -- 4 CPU Cache -- 4.1 Cache Operation -- 4.2 Coreboot -- 5 GPU Experimental Setup -- 6 GPU Multiprocessor Shared Memory -- 7 Discussion -- 7.1 Future Work -- Reconfigurable LUT: A Double Edged Sword for Security-Critical Applications -- Introduction -- Rationale of the RLUT -- Comparison with Dynamic Configuration -- RLUT and Security -- Destructive Applications of RLUT -- Adversary Model -- Trigger Design the Hardware Trojans -- Trojan Description -- Constructive Applications for RLUT -- Customizable Sboxes.
Sbox Scrambling for DPA Resistance -- Conclusions -- Trigger Generation for Hardware Trojans -- Architecture Considerations for Massively Parallel Hardware Security Platform -- Introduction -- Cryptography as a Service (CaaS) -- Levels of Trust and Security -- Usage Scenarios -- Typical Operations Needed for CaaS -- Preferred Properties of Cloud-Based High-Performance CaaS -- Building Hardware for CaaS Back-End -- Designing CaaS -- The Proposed Design -- Why Smart Cards? -- The Case Study: HMAC-Based One-Time Password -- Why Would HOTP Will Benefit from CaaS? -- Moving HOTP into CaaS -- HOTP Implementation -- Performance Results - A Single Card -- Improving Expected Performance -- Performance Results - Network of Processors -- Future Directions -- Conclusions --

Efficient and Secure Elliptic Curve Cryptography for 8-bit AVR Microcontrollers -- Introduction 2 pg -- Side-Channel Analysis on the AVR 1 pg -- Timing Analysis -- Simple Power Analysis -- Prime Field Arithmetic -- Arithmetic Modulo Ed25519 Group Order -- Scalar Multiplication -- Extended Twisted Edwards Coordinates -- Variable-Base Scalar Multiplication -- Flash Memory Address Leakage Through Power -- Fixed-Base ECSM for Ed25519 Key Generation and Signing -- Projective Coordinate Randomization -- Hashing and PRNG -- Elliptic Curve Protocols -- Benchmarking Results 1 pg -- Timing and Simple Power Analysis Leakage Evaluation -- Application of CRI's Methodology to ECC -- Measurement Setup and Capture of Power Traces -- SPA Leakage Analysis -- Side-Channel Analysis Results 1 pg -- Conclusion -- ATmega328P Microcontroller and Chipwhisperer -- Algorithms -- Towards Practical Attribute-Based Signatures -- 1 Introduction -- 2 About IRMA -- 3 IRMA's Selective Disclosure Proofs as Digital Signatures -- 3.1 IRMA Signature Scheme.
3.2 Diversification between SD Proofs Used for Authentication and Signatures.

Sommario/riassunto

This book constitutes the refereed proceedings of the 5th International Conference on Security, Privacy, and Applied Cryptography Engineering, SPACE 2015, held in Jaipur, India, in October 2015. The 17 full papers presented in this volume were carefully reviewed and selected from 57 submissions. The book also contains 4 invited talks in full-paper length. The papers are devoted to various aspects of security, privacy, applied cryptography, and cryptographic engineering.