Power Analysis Attacks Revealing The Secrets Of Smart Cards Author Stefan Mangard Published On October 2010

The three-volume set constitutes the proceedings of the 16th International Conference on Wireless Algorithms, Systems, and Applications, WASA 2021, which was held during June 25-27, 2021. The conference took place in Nanjing, China.The 103 full and 57 short papers presented in these proceedings were carefully reviewed and selected from 315 submissions. The contributions in Part II of the set are subdivided into the following topical sections: Scheduling & Optimization II; Security; Data Center Networks and Cloud Computing; Privacy-Aware Computing; Internet of Vehicles; Visual Computing for IoT; Mobile Ad-Hoc Networks.

This book provides the foundations for understanding hardware security and trust, which have become major concerns for national security over the past decade. Coverage includes security and trust issues in all types of electronic devices and systems such as ASICs, COTS, FPGAs, microprocessors/DSPs, and embedded systems. This serves as an invaluable reference to the state-of-the-art research that is of critical significance to the security of, and trust in, modern society's microelectronic-supported infrastructures.

This book constitutes the proceedings of the Second International Conference on Network Computing and Information Security, NCIS 2012, held in Shanghai, China, in December 2012. The 104 revised papers presented in this volume were carefully reviewed and selected from 517 submissions. They are organized in topical sections named: applications of cryptography; authentication and non-repudiation; cloud computing; communication and information systems; design and analysis of cryptographic algorithms; information hiding and watermarking; intelligent networked systems; multimedia computing and intelligence; network and wireless network security; network communication; parallel and distributed systems; security modeling and architectures; sensor network; signal and information processing; virtualization techniques and applications; and wireless network.

The two-volume proceedings LNCS 9665 + LNCS 9666 constitutes the thoroughly refereed proceedings of the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2016, held in Vienna, Austria, in May 2016. The 62 full papers included in these volumes were carefully reviewed and selected from 274 submissions. The papers are organized in topical sections named: (pseudo)randomness; LPN/LWE; cryptanalysis; masking; fully homomorphic encryption; number theory; hash

functions; multilinear maps; message authentification codes; attacks on SSL/TLS; real-world protocols; robust designs; lattice reduction; latticed-based schemes; zero-knowledge; pseudorandom functions; multi-party computation; separations; protocols; round complexity; commitments; lattices; leakage; in differentiability; obfuscation; and automated analysis, functional encryption, and non-malleable codes.

Provides the authoritative and up-to-date information required for securing IoT architecture and applications The vast amount of data generated by the Internet of Things (IoT) has made information security vital for not only personal privacy, but also for the sustainability of the IoT itself. Security and Privacy in the Internet of Things brings together high-quality research on IoT information security models, architectures, techniques, and application domains. This concise yet comprehensive volume explores state-of-the-art mitigations in IoT security while addressing important privacy challenges across different IoT layers. Divided into three parts, the book provides timely coverage of IoT architecture, security technologies and mechanisms, and applications. The authors outline emerging trends in IoT security and privacy with a focus on areas such as smart homes and cities, e-health, critical infrastructure, and industrial applications. Topics include authentication and access control, the use of blockchains for IoT

transactions, attack detection and prevention, energy-efficient management of IoT objects, and secure integration of IoT and Cloud computing. Presenting the current body of knowledge in a single volume, Security and Privacy in the Internet of Things: Discusses a broad range of IoT architectures and applications Covers both the logical and physical security of IoT devices Examines IoT security and privacy standards, protocols, and approaches Addresses the secure integration of IoT and social networks Describes privacy preserving techniques, intrusion detection systems, and threat and vulnerability analyses Security and Privacy in the Internet of Things: Architectures, Techniques, and Applications is essential reading for researchers, industry practitioners, and students involved in IoT development and deployment.

This book constitutes the thoroughly refereed post-conference proceedings of the 6th International Workshop, COSADE 2015, held in Berlin, Germany, in April 2015. The 17 revised full papers presented were carefully selected from 48 submissions. the focus of this workshop was on following topics: side-channel attacks, FPGA countermeasures, timing attacks and countermeasures, fault attacks, countermeasures, and Hands-on Side-channel analysis.

This book constitutes revised selected papers from the 9th International Workshop on Constructive Side-Channel Analysis and Secure Design, COSADE

2018, held in Singapore, in April 2018.The 14 papers presented in this volume were carefully reviewed and selected from 31 submissions. They were organized in topical sections named: countermeasures against side-channel attacks; tools for side-channel analysis; fault attacks and hardware trojans; and side-channel analysis attacks.

These proceedings contain the papers selected for presentation at the 23rd International Information Security Conference (SEC 2008), co-located with IFIP World Computer Congress (WCC 2008), September 8–10, 2008 in Milan, Italy. In response to the call for papers, 143 papers were submitted to the conference. All papers were evaluated on the basis of their signi?cance, novelty,and technical quality, and reviewed by at least three members of the program committee. Reviewing was blind meaning that the authors were not told which committee members reviewed which papers. The program committee meeting was held electronically, holding intensive discussion over a period of three weeks. Of the papers submitted, 42 full papers and 11 short papers were selected for presentation at the conference. A conference like this just does not happen; it depends on the volunteer efforts of a host of individuals. There is a long list of people who volunteered their time and energy to put together the conference and who deserve acknowledgment. We thank all members of the program committee

and the external reviewers for their hard work in the paper evaluation. Due to the large number of submissions, p- gram committee members were required to complete their reviews in a short time frame. We are especially thankful to them for the commitment they showed with their active participation in the electronic discussion.

Power analysis attacks allow the extraction of secret information from smart cards. Smart cards are used in many applications including banking, mobile communications, pay TV, and electronic signatures. In all these applications, the security of the smart cards is of crucial importance. Power Analysis Attacks: Revealing the Secrets of Smart Cards is the first comprehensive treatment of power analysis attacks and countermeasures. Based on the principle that the only way to defend against power analysis attacks is to understand them, this book explains how power analysis attacks work. Using many examples, it discusses simple and differential power analysis as well as advanced techniques like template attacks. Furthermore, the authors provide an extensive discussion of countermeasures like shuffling, masking, and DPA-resistant logic styles. By analyzing the pros and cons of the different countermeasures, this volume allows practitioners to decide how to protect smart cards.

This volume of Advances in Intelligent and Soft Computing contains accepted papers presented at SOCO 2013, CISIS 2013 and ICEUTE 2013, all conferences held in the beautiful and historic city of Salamanca (Spain), in September 2013. Soft computing represents a collection or set of computational techniques in machine learning, computer science and some engineering disciplines, which investigate, simulate, and analyze very complex issues and

phenomena. After a through peer-review process, the 8th SOCO 2013 International Program Committee selected 40 papers which are published in these conference proceedings, and represents an acceptance rate of 41%. In this relevant edition a special emphasis was put on the organization of special sessions. Four special sessions were organized related to relevant topics as: Systems, Man, and Cybernetics, Data Mining for Industrial and Environmental Applications, Soft Computing Methods in Bioinformatics, and Soft Computing Methods, Modelling and Simulation in Electrical Engineer. The aim of the 6th CISIS 2013 conference is to offer a meeting opportunity for academic and industry-related researchers belonging to the various, vast communities of Computational Intelligence, Information Security, and Data Mining. The need for intelligent, flexible behaviour by large, complex systems, especially in mission-critical domains, is intended to be the catalyst and the aggregation stimulus for the overall event. After a through peer-review process, the CISIS 2013 International Program Committee selected 23 papers which are published in these conference proceedings achieving an acceptance rate of 39%. In the case of 4th ICEUTE 2013, the International Program Committee selected 11 papers which are published in these conference proceedings. The selection of papers was extremely rigorous in order to maintain the high quality of the conference and we would like to thank the members of the Program Committees for their hard work in the reviewing process. This is a crucial process to the creation of a high standard conference and the SOCO, CISIS and ICEUTE conferences would not exist without their help. This book constitutes revised selected papers from the 20th International Conference on Information Security and Cryptology, ICISC 2017, held in Seoul, South Korea, in November/December 2017. The total of 20 papers presented in this volume were carefully

reviewed and selected from 70 submissions. The papers were organized in topical sections named: symmetric key encryption; homomorphic encryption, side channel analysis and implementation; broadcast encryption; elliptic curve; signature and protocol; and network and system security.

The chapters in this book present the work of researchers, scientists, engineers, and teachers engaged with developing unified foundations, principles, and technologies for cyber-physical security. They adopt a multidisciplinary approach to solving related problems in next-generation systems, representing views from academia, government bodies, and industrial partners, and their contributions discuss current work on modeling, analyzing, and understanding cyber-physical systems.

It has been more than 20 years since the seminal publications on side-channel attacks. They aim at extracting secrets from embedded systems while they execute cryptographic algorithms, and they consist of two steps, measurement and analysis. This useful textbook/guide tackles the analysis part, especially under situations where the targeted device is protected by random masking. The book advances in the field and provides the reader with mathematical formalizations. Furthermore, it presents all known analyses within the same notation framework, thereby allowing the reader to rapidly understand and learn contrasting approaches. The examples presented are taken from real-world datasets. This unique text/reference will be useful as a higher-level introduction to the topic, as well as for self-study by researchers and professionals needing a concise guidebook. Maamar Ouladj is an expert in embedded systems security, currently working in Algiers, Algeria. Sylvain Guilley is general manager and chief technical officer at Secure-IC S.A.S., currently working in Paris, France.

This book constitutes the thoroughly refereed post-conference proceedings of the 10th International Workshop on Information Security Applications, WISA 2009, held in Busan, Korea, during August 25-27, 2009. The 27 revised full papers presented were carefully reviewed and selected from a total of 79 submissions. The papers are organized in topical sections on mutlimedia security, device security, HW implementation security, applied cryptography, side channel attacks, cryptograptanalysis, anonymity/authentication/access controll, and network security.

This volume contains the workshopproceedings of the accompanying workshops of the 14th Financial Cryptograpy and Data Security International Conference 2010, held on Tenerife, Canary Islands, Spain, January 25-28, 2010. FinancialCryptographyandData Securityis a majorinternationalforumfor research, advanced development, education, exploration, and debate regarding information assurance, with a speci?c focus on commercial contexts. The c-ference covers all aspects of securing transactions and systems and especially encourages original work focusing on both fundamental and applied real-world deployments on all aspects surrounding commerce security. Three workshops were co-located with FC 2010: the Workshop on Real-Life CryptographicProtocolsandStandardization(RLCPS),theWorkshoponEthics in Computer Security Research (WECSR), and the Workshop on Lightweight Cryptography for Resource-Constrained Devices (WLC). Intimate and colorful by tradition, the high-quality program was not the only attraction of FC. In the past, FC conferences have been held in highly research-synergistic locations such as Tobago, Anguilla, Dominica, Key West, Guadelupe, Bermuda, the Grand Cayman, and Cozumel Mexico. 2010 was the ?rst year that the conference was held on

European soil, in the Spanish Canary Islands, in Atlantic waters, a few miles across Morocco. Over 100 researchers from more than 20 countries were in attendance.

Security of Information and Networks includes invited and contributed papers on information assurance, security, and public policy. It covers Ciphers, Mobile Agents, Access Control, Security Assurance, Intrusion Detection, and Security Software.

The 1st volume of 'Advances in Microelectronics: Reviews' Book Series contains 19 chapters written by 72 authors from academia and industry from 16 countries. With unique combination of information in each volume, the 'Advances in Microelectronics: Reviews' Book Series will be of value for scientists and engineers in industry and at universities. In order to offer a fast and easy reading of the state of the art of each topic, every chapter in this book is independent and self-contained. All chapters have the same structure: first an introduction to specific topic under study; second particular field description including sensing applications. Each of chapter is ending by well selected list of references with books, journals, conference proceedings and web sites. This book ensures that readers will stay at the cutting edge of the field and get the right and effective start point and road map for the further researches and developments.

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.

This book constitutes revised selected papers from the 7th International Workshop on Constructive Side-Channel Analysis and Secure Design, COSADE 2016, held in Graz, Austria, in April 2016. The 12 papers presented in this volume were carefully reviewed and selected from 32 submissions. They were organized in topical sections named: security and physical attacks; side-channel analysis (case studies); fault analysis; and side-channel analysis (tools).

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.

This book constitutes the thoroughly refereed post-conference proceedings of the 11th International Conference on Smart Card Research and Advanced Applications, CARDIS 2012, held in Graz, Austria, in November 2012. The 18 revised full papers presented together with an invited talk were carefully reviewed and selected from 48 submissions. The papers are organized in topical sections on Java card security, protocols, side-channel attacks, implementations, and implementations for resource-constrained devices.

This volume contains revised and extended research articles written by prominent researchers participating in ICFWI 2011 conference. The 2011 International Conference on Future Wireless Networks and Information Systems (ICFWI 2011) has been held on November 30 ~ December 1, 2011, Macao, China. Topics covered include Wireless Information Networks, Wireless Networking Technologies, Mobile Software and Services, intelligent computing, network management, power engineering, control engineering, Signal and Image Processing, Machine Learning, Control Systems and Applications, The book will offer the states of arts of tremendous advances in Wireless Networks and Information Systems and also serve as an excellent reference work for

researchers and graduate students working on Wireless Networks and Information Systems.

This book constitutes the thoroughly refereed post-conference proceedings of the 17th International Conference on Financial Cryptography and Data Security (FC 2013), held at Bankoku Shinryokan Busena Terrace Beach Resort, Okinawa, Japan, April 1-5, 2013. The 14 revised full papers and 17 short papers were carefully selected and reviewed from 125 submissions. The papers are grouped in the following topical sections: electronic payment (Bitcoin), usability aspects, secure computation, passwords, privacy primitives and non-repudiation, anonymity, hardware security, secure computation and secret sharing, authentication attacks and countermeasures, privacy of data and communication, and private data retrieval.

The second international conference on INformation Systems Design and Intelligent Applications (INDIA – 2015) held in Kalyani, India during January 8-9, 2015. The book covers all aspects of information system design, computer science and technology, general sciences, and educational research. Upon a double blind review process, a number of high quality papers are selected and collected in the book, which is composed of two different volumes, and covers a variety of topics, including natural language processing, artificial intelligence,

security and privacy, communications, wireless and sensor networks, microelectronics, circuit and systems, machine learning, soft computing, mobile computing and applications, cloud computing, software engineering, graphics and image processing, rural engineering, e-commerce, e-governance, business computing, molecular computing, nano computing, chemical computing, intelligent computing for GIS and remote sensing, bio-informatics and bio-computing. These fields are not only limited to computer researchers but also include mathematics, chemistry, biology, bio-chemistry, engineering, statistics, and all others in which computer techniques may assist.

This book constitutes the thoroughly refereed post-proceedings of the 17th Annual International Workshop on Selected Areas in Cryptography, SAC 2010, held in Waterloo, Ontario, Canada in August 2010. The 24 revised full papers presented together with 2 invited papers were carefully reviewed and selected from 90 submissions. The papers are organized in topical sections on hash functions, stream ciphers, efficient implementations, coding and combinatorics, block ciphers, side channel attacks, and mathematical aspects.

This book constitutes the refereed proceedings of the Third International Workshop on Constructive Side-Channel Analysis and Secure Design, COSADE 2012, held in Darmstadt, Germany, May 2012. The 16 revised full papers presented together with two invited talks were carefully reviewed and selected from 49 submissions. The papers are organized in topical sections on practical side-channel analysis; secure design; side-channel attacks on RSA; fault

attacks; side-channel attacks on ECC; different methods in side-channel analysis.

CHES 2009, the 11th workshop on Cryptographic Hardware and Embedded Systems, was held in Lausanne, Switzerland, September 6–9, 2009. The wo- shop was sponsored by the International Association for Cryptologic Research (IACR). The workshop attracted a record number of 148 submissions from 29 co- tries, of which the Program Committee selected 29 for publication in the wo- shop proceedings, resulting in an acceptance rate of 19.6%, the lowest in the history of CHES. The review process followed strict standards: each paper - ceived at least four reviews, and some asmanyaseightreviews.Membersofthe Program Committee were restricted to co-authoring at most two submissions, and their papers were evaluated by an extended number of reviewers. The ProgramCommittee included 53 members representing 20 countries and ?ve continents. These members were carefully selected to represent academia, industry, and government, as well as to include world-class experts in various research ?elds of interest to CHES. The Program Committee was supported by 148 external reviewers. The total number of people contributing to the - view process, including Program Committee members, external reviewers, and Program Co-chairs, exceeded 200. The papers collected in this volume represent cutting-edge worldwide - search in the rapidly growing and evolving area of cryptographic engineering.

This book constitutes the proceedings of the 14th International Workshop on Cryptographic Hardware and Embedded Systems, CHES 2012, held in Leuven, Belgium, in September 2012. The 32 papers presented together with 1 invited talk were carefully reviewed and selected from 120 submissions. The papers are organized in the following topical sections: intrusive attacks and countermeasures; masking; improved fault attacks and side channel analysis; leakage

resiliency and security analysis; physically unclonable functions; efficient implementations; lightweight cryptography; we still love RSA; and hardware implementations.

This book constitutes the proceedings of the 20th International Conference on Tools and Algorithms for the Construction and Analysis of Systems, TACAS 2014, which took place in Grenoble, France, in April 2014, as part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2014. The total of 42 papers included in this volume, consisting of 26 research papers, 3 case study papers, 6 regular tool papers and 7 tool demonstrations papers, were carefully reviewed and selected from 161 submissions. In addition the book contains one invited contribution. The papers are organized in topical sections named: decision procedures and their application in analysis; complexity and termination analysis; modeling and model checking discrete systems; timed and hybrid systems; monitoring, fault detection and identification; competition on software verification; specifying and checking linear time properties; synthesis and learning; quantum and probabilistic systems; as well as tool demonstrations and case studies.

Information Systems (IS) are a nearly omnipresent aspect of the modern world, playing crucial roles in the fields of science and engineering, business and law, art and culture, politics and government, and many others. As such, identity theft and unauthorized access to these systems are serious concerns. Theory and Practice of Cryptography Solutions for Secure Information Systems explores current trends in IS security technologies, techniques, and concerns, primarily through the use of cryptographic tools to safeguard valuable information resources. This reference book serves the needs of professionals, academics, and students requiring dedicated information systems free from outside interference, as well as developers

of secure IS applications. This book is part of the Advances in Information Security, Privacy, and Ethics series collection.

Field-coupled nanocomputing (FCN) paradigms offer fundamentally new approaches to digital information processing that do not utilize transistors or require charge transport. Information transfer and computation are achieved in FCN via local field interactions between nanoscale building blocks that are organized in patterned arrays. Several FCN paradigms are currently under active investigation, including quantum-dot cellular automata (QCA), molecular quantum cellular automata (MQCA), nanomagnetic logic (NML), and atomic quantum cellular automata (AQCA). Each of these paradigms has a number of unique features that make it attractive as a candidate for post-CMOS nanocomputing, and each faces critical challenges to realization. This State-of-the-Art-Survey provides a snapshot of the current developments and novel research directions in the area of FCN. The book is divided into five sections. The first part, Field-Coupled Nanocomputing Paradigms, provides valuable background information and perspectives on the QDCA, MQCA, NML, and AQCA paradigms and their evolution. The second section, Circuits and Architectures, addresses a wide variety of current research on FCN clocking strategies, logic synthesis, circuit design and test, logic-in-memory, hardware security, and architecture. The third section, Modeling and Simulation, considers the theoretical modeling and computer simulation of large FCN circuits, as well as the use of simulations for gleaning physical insight into elementary FCN building blocks. The fourth section, Irreversibility and Dissipation, considers the dissipative consequences of irreversible information loss in FCN circuits, their quantification, and their connection to circuit structure. The fifth section, The Road Ahead: Opportunities and Challenges, includes an edited transcript of the panel

discussion that concluded the FCN 13 workshop.

This book constitutes the proceedings of the 16th International Symposium on Research in Attacks, Intrusions and Defenses, former Recent Advances in Intrusion Detection, RAID 2013, held in Rodney Bay, St. Lucia in October 2013. The volume contains 22 full papers that were carefully reviewed and selected from 95 submissions, as well as 10 poster papers selected from the 23 submissions. The papers address all current topics in computer security ranged from hardware-level security, server, web, mobile, and cloud-based security, malware analysis, and web and network privacy.

This Special Issue provides an opportunity for researchers in the area of side-channel attacks (SCAs) to highlight the most recent exciting technologies. The research papers published in this Special Issue represent recent progress in the field, including research on power analysis attacks, cache-based timing attacks, system-level countermeasures, and so on.

This book constitutes the thoroughly refereed post-conference proceedings of the 9th International Conference on Information Security and Cryptology, Inscrypt 2013, held in Guangzhou, China, in November 2013. The 21 revised full papers presented together with 4 short papers were carefully reviewed and selected from 93 submissions. The papers cover the topics of Boolean function and block cipher, sequence and stream cipher, applications: systems and theory, computational number theory, public key cryptography, has function, side-channel and leakage, and application and system security.

RSA is a public-key cryptographic system, and is the most famous and widely-used cryptographic system in today's digital world. Cryptanalytic Attacks on RSA, a professional book, covers almost all known cryptanalytic attacks and defenses of the RSA cryptographic

system and its variants. Since RSA depends heavily on computational complexity theory and number theory, background information on complexity theory and number theory is presented first, followed by an account of the RSA cryptographic system and its variants. This book is also suitable as a secondary text for advanced-level students in computer science and mathematics.

This book constitutes the refereed proceedings of the 12th International Conference on Cryptology in India, INDOCRYPT 2011, held in Chennai, India, in December 2011. The 22 revised full papers presented together with the abstracts of 3 invited talks and 3 tutorials were carefully reviewed and selected from 127 submissions. The papers are organized in topical sections on side-channel attacks, secret-key cryptography, hash functions, pairings, and protocols.

On any advanced integrated circuit or "system-on-chip" there is a need for security. In many applications the actual implementation has become the weakest link in security rather than the algorithms or protocols. The purpose of the book is to give the integrated circuits and systems designer an insight into the basics of security and cryptography from the implementation point of view. As a designer of integrated circuits and systems it is important to know both the state-of-the-art attacks as well as the countermeasures. Optimizing for security is different from optimizations for speed, area, or power consumption. It is therefore difficult to attain the delicate balance between the extra cost of security measures and the added benefits.

This book presents two practical physical attacks. It shows how attackers can reveal the secret key of symmetric as well as asymmetric cryptographic algorithms based on these attacks, and presents countermeasures on the software and the hardware level that can help to prevent

them in the future. Though their theory has been known for several years now, since neither attack has yet been successfully implemented in practice, they have generally not been considered a serious threat. In short, their physical attack complexity has been overestimated and the implied security threat has been underestimated. First, the book introduces the photonic side channel, which offers not only temporal resolution, but also the highest possible spatial resolution. Due to the high cost of its initial implementation, it has not been taken seriously. The work shows both simple and differential photonic side channel analyses. Then, it presents a fault attack against pairing-based cryptography. Due to the need for at least two independent precise faults in a single pairing computation, it has not been taken seriously either. Based on these two attacks, the book demonstrates that the assessment of physical attack complexity is error-prone, and as such cryptography should not rely on it. Cryptographic technologies have to be protected against all physical attacks, whether they have already been successfully implemented or not. The development of countermeasures does not require the successful execution of an attack but can already be carried out as soon as the principle of a side channel or a fault attack is sufficiently understood.