Power Analysis Attacks Revealing The Secrets Of Smart Cards

Advances In Information Security By Stefan Mangard

2007 03 12

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.

The Hardware Hacking Handbook takes you deep inside embedded devices to show how different kinds of attacks work, then guides you

through each hack on real hardware. Embedded devices are chip-size microcomputers small enough to be included in the structure of the object they control, and they're everywhere—in phones, cars, credit cards, laptops, medical equipment, even critical infrastructure. This

means understanding their security is critical. The Hardware Hacking Handbook takes you deep inside different types of embedded systems, revealing the designs, components, security limits, and reverse-engineering challenges you need to know for executing effective

hardware attacks. Written with wit and infused with hands-on lab experiments, this handbook puts you in the role of an attacker interested in breaking security to do good. Starting with a crash course on the architecture of embedded devices, threat modeling, and attack trees,

you'll go on to explore hardware interfaces, ports and communication protocols, electrical signaling, tips for analyzing firmware images, and more. Along the way, you'll use a home testing lab to perform fault-injection, side-channel (SCA), and simple and differential power

analysis (SPA/DPA) attacks on a variety of real devices, such as a crypto wallet. The authors also share insights into real-life attacks on embedded systems, including Sony's PlayStation 3, the Xbox 360, and Philips Hue lights, and provide an appendix of the equipment needed

for your hardware hacking lab – like a multimeter and an oscilloscope – with options for every type of budget. You'll learn: • How to model security threats, using attacker profiles, assets, objectives, and countermeasures • Electrical basics that will help you understand

communication interfaces, signaling, and measurement • How to identify injection points for executing clock, voltage, electromagnetic, laser, and body-biasing fault attacks, as well as practical injection tips • How to use timing and power analysis attacks to extract passwords and cryptographic

keys • Techniques for leveling up both simple and differential power analysis, from practical measurement tips to filtering, processing, and visualization Whether you're an industry engineer tasked with understanding these attacks, a student starting out in the field, or

an electronics hobbyist curious about replicating existing work, The Hardware Hacking Handbook is an indispensable resource – one you'll always want to have onhand.

This book constitutes the refereed proceedings of the 28th Annual International Cryptology Conference,

CRYPTO 2008, held in Santa Barbara, CA, USA in August 2008. The 32 revised full papers presented were carefully reviewed and selected from 184 submissions. Addressing all current foundational, theoretical and research aspects of cryptology, cryptography, and cryptanalysis as

well as advanced applications, the papers are organized in topical sections on random oracles, applications, public-key crypto, hash functions, cryptanalysis, multiparty computation, privacy, zero knowledge, and oblivious transfer. 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.

Security, Privacy, and Applied

Cryptography Engineering
7th International Workshop, COSADE 2016, Graz, Austria, April 14-15, 2016, Revised Selected Papers
Cryptographic Hardware and Embedded Systems - CHES 2009 11th International Conference,

CARDIS 2012, Graz, Austria, November 28-30, 2012, Revised Selected Papers

Constructive Side-Channel Analysis and Secure Design

Revealing the Secrets of Smart Cards

10th International Workshop, WISA 2009, Busan, Korea, August 25-27,

2009, Revised Selected Papers

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.

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.

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 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.

Progress in Cryptology - INDOCRYPT 2011

Power Analysis Attacks

Wireless Algorithms, Systems, and

Applications

Field-Coupled Nanocomputing

Cryptographic Hardware and Embedded Systems -- CHES 2012

Applied Cryptography and Network Security

28th Annual International

Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008, Proceedings

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.

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 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.

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.

ICCWS 2022 17th International Conference on Cyber Warfare and Security

Cryptographic Hardware and Embedded Systems -- CHES 2010 IFIP 20th World Computer Congress, IFIP SEC'08, September

7-10, 2008, Milano, Italy

Financial Cryptography and Data Security

Second International Conference, NCIS 2012, Shanghai, China, December 7-9, 2012, Proceedings

Secure Integrated Circuits and

Systems

Paradigms, Progress, and Perspectives

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 refereed proceedings of the 5th International Workshop on Cryptographic Hardware and Embedded Systems, CHES 2003, held in Cologne, Germany in September 2003. The 32 revised full

papers presented were carefully reviewed and selected from 111 submissions. The papers are organized in topical sections on side channel attack methodology, hardware factorization, symmetric cypher attacks and countermeasures, secure hardware

logic, random number generators, efficient multiplication, efficient arithmetics, attacks on asymmetric cryptosystems, implementation of symmetric cyphers, hyperelliptic curve cryptography, countermeasures to side channel leakage, and security of

standards.

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.

These proceedings contain the papers selected for presentation at the 23rd Inter- tional Information Security Conference (SEC 2008), co-located with IFIP World Computer Congress

(WCC 2008), September 8–10, 2008 in Milan, Italy. In - sponse to the call for papers, 143 papers were submitted to the conference. All - pers 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 - tensive 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.

An Efficient Algorithmic Approach
14th International Workshop, Leuven, Belgium, September 9-12, 2012, Proceedings
Selected Areas in Cryptography
Cryptanalytic Attacks on RSA
20th International Conference, TACAS

2014, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2014, Grenoble, France, April 5-13, 2014, Proceedings

20th International Conference, Seoul, South Korea, November 29 - December

1, 2017, Revised Selected Papers
9th International Conference, Inscrypt 2013, Guangzhou, China, November 27-30, 2013, Revised Selected Papers

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.

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 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.

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.

Information Systems Design and Intelligent Applications

The Hardware Hacking Handbook

5th International Conference,

SPACE 2015, Jaipur, India, October 3-7, 2015, Proceedings
Advances in Cryptology - CRYPTO 2008
Security of Information and Networks
Cryptographic Hardware and

Embedded Systems -- CHES 2003 Information Security Theory and Practice: Security and Privacy of Mobile Devices in Wireless Communication

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.

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 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.

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.

Volume 1

The 48 Laws Of Power

5th IFIP WG 11.2 International Workshop, WISTP 2011, Heraklion, Crete, Greece, June 1-3, 2011, Proceedings

Smart Card Research and Advanced

Applications
17th International Workshop, SAC 2010, Waterloo, Ontario, Canada, August 12-13, 2010, Revised Selected Papers
Cyber-Physical Systems Security
THE MILLION COPY

INTERNATIONAL BESTSELLER Drawn from 3,000 years of the history of power, this is the definitive guide to help readers achieve for themselves what Queen Elizabeth I, Henry Kissinger,

Louis XIV and Machiavelli learnt the hard way. Law 1: Never outshine the master Law 2: Never put too much trust in friends; learn how to use enemies Law 3: Conceal your intentions Law 4: Always

say less than necessary. The text is bold and elegant, laid out in black and red throughout and replete with fables and unique word sculptures. The 48 laws are illustrated through the tactics,

triumphs and failures of great figures from the past who have wielded - or been victimised by - power. _____ _____ __ (From the Playboy interview with Jay-Z, April 2003)

PLAYBOY: Rap careers are usually over fast: one or two hits, then styles change and a new guy comes along. Why have you endured while other rappers haven't? JAY-Z: I would say that it's from still

being able to relate to people. It's natural to lose yourself when you have success, to start surrounding yourself with fake people. In The 48 Laws of Power, it says the worst thing you can do is build a fortress

around yourself. I still got the people who grew up with me, my cousin and my childhood friends. This guy right here (gestures to the studio manager), he's my friend, and he told me that one of my

records, Volume Three, was wack. People set higher standards for me, and I love it. 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 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. 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.

16th International Conference, WASA 2021, Nanjing, China, June 25–27, 2021,

Proceedings, Part II
Side-Channel Analysis of Embedded Systems
Network Computing and Information Security
12th International Conference on Cryptology in India,

Chennai, India, December 11-14, 2011, Proceedings
17th International Conference, FC 2013, Okinawa, Japan, April 1-5, 2013, Revised Selected Papers
Why Cryptography Should Not

Rely on Physical Attack Complexity

Future Wireless Networks and Information Systems

Power Analysis AttacksRevealing the Secrets of Smart CardsSpringer Science & Business Media

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 book tackles the

analysis part, especially under situations where the targeted device is protected by random masking. The authors explain advances in the field and provide the reader with mathematical formalizations. They present all known analyses within the same notation framework, which

allows the reader to rapidly understand and learn contrasting approaches. It will be useful as a graduate level introduction, also for self-study by researchers and professionals, and the examples are taken from real-world datasets.

This book constitutes the proceedings

of the 8th International Conference on Applied Cryptography and Network Security, ACNS 2010, held in Beijing, China, in June 2010. The 32 papers presented in this volume were carefully reviewed and selected from 178 submissions. The papers are divided in topical sections on public

key encryption, digital signature, block ciphers and hash functions, side-channel attacks, zero knowledge and multi-party protocols, key management, authentication and identification, privacy and anonymity, RFID security and privacy, and internet security.

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. 5th International Workshop, Cologne, Germany, September 8-10, 2003,

Proceedings
Tools and Algorithms for the Construction and Analysis of Systems
Information Security and Cryptology – ICISC 2017
Proceedings of Second International Conference INDIA 2015, Volume 2
Theory and Practice of Cryptography

Solutions for Secure Information Systems

Breaking Embedded Security with Hardware Attacks

11th International Workshop Lausanne, Switzerland, September 6-9, 2009 Proceedings

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.

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 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 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.

12th International Workshop, Santa Barbara, USA, August 17-20,2010, Proceedings

8th International Conference, ACNS

2010, Beijing, China, June 22-25, 2010, Proceedings

Proceedings of the First International Conference on Security of Information and Networks (Sin 2007), 7-10 ZMay 2007, Gazimagusa (TRNC), North Cyprus

Proceedings of the IFIP TC 11 23rd International Information Security Conference

Information Security Applications

Information Security and Cryptology

6th International Workshop, COSADE 2015, Berlin, Germany,

April 13-14, 2015. Revised Selected Papers

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.

The LNCS series reports state-of-the-art results in computer science

research, development, and education, at a high level and in both printed and electronic form. Enjoying tight cooperation with the R & D community, with numerous individuals, as well as with prestigious organizations and

societies, LNCS has grown into the most comprehensive computer science research forum available. The scope of LNCS, including its subseries LNAI and LNBI, spans the whole range of computer science and information technology

including interdisciplinary topics in a variety of application fields. The type of material published traditionally includes proceedings (published in time for the respective conference) post-proceedings (consisting of throughly revised final

full papers) research monographs (which may be based on outstanding PhD work, research projects, technical reports, etc.) More recently, several color-cover sublines have been added featuring, beyond a collection of

papers, various added-value components; these sublines include tutorials (textbook-like monographs or collections of lectures given at advanced courses) state-of-the-art surveys (offering complete and mediated coverage of a topic) hot

topics (introducing emergent topics to the broader community) In parallel to the printed book, each new volume is published electronically in LNCS Online. Book jacket.

9th International Workshop,

COSADE 2018, Singapore, April 23–24, 2018, Proceedings
Third International Workshop, COSADE 2012, Darmstadt, Germany, May 3-4, 2012. Proceedings
Side Channel Attacks