Lecture Notes in Computer Science 12910

More information about this subseries at http://www.springer.com/series/7410

Shivam Bhasin · Fabrizio De Santis (Eds.)

Constructive Side-Channel Analysis and Secure Design

12th International Workshop, COSADE 2021 Lugano, Switzerland, October 25–27, 2021 Proceedings

Springer

Editors
Shivam Bhasin
Nanyang Technological University
Singapore, Singapore

Fabrizio De Santis
Siemens AG
Munich, Germany

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-89914-1 ISBN 978-3-030-89915-8 (eBook)
https://doi.org/10.1007/978-3-030-89915-8

LNCS Sublibrary: SL4 – Security and Cryptology

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The Twelfth International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE 2021) was held as a hybrid event at the Università della Svizzera italiana, Lugano, Switzerland, during October 25–27, 2021.

The COSADE series of conferences began in 2010 and provides a well-established international platform for researchers, academics, and industry participants to present their work and their current research in implementation attacks, secure implementation, secure design and evaluation, and practical attacks, test platforms and open benchmarks.

This year, we received 31 papers, each of which was assigned to three reviewers. All the submissions went through a rigorous double-blind peer review process. The Program Committee included 40 members from 16 countries, selected among experts from academia and industry in the areas of secure design, side channel attacks and countermeasures, and architectures and protocols. Overall, the Program Committee returned 93 reviews. During the decision process, 14 papers were selected for publication in the COSADE 2021 proceedings. We would like to express our gratitude to the Program Committee members and the 22 subreviewers for their reviews and for their active participation in the paper discussion phase.

The highlights of the COSADE 2021 program include two keynotes and an industrial session. The first keynote entitled "Securing the Next Trillion of Chips via In-Memory and Immersed-in-Logic Design – Beyond Traditional Design Boundaries" was given by Massimo Alioto from the National University of Singapore. The talk explored the road towards truly ubiquitous hardware security from a primitive design perspective, designing PUFs and TRNGs that are inherently immersed in existing memory arrays and logic fabrics. The second keynote entitled "Defending CyberPhysical Systems and Infrastructures from Cyber Attacks" was given by Alberto Sangiovanni Vincentelli from the University of California, Berkeley. The talk explored attacks against critical infrastructure such as gas pipelines, power generation, and water treatment plants, as well as against cars and airplanes.

The industrial session included the following talks: "Introduction to OpenTitan – An Open-source Silicon Root of Trust Project" from G+D Mobile Security GmbH, "Is Revolutionary Hardware for Fully Homomorphic Encryption Important? What Else is Needed?" from Intel Corporation, "Post-Quantum Cryptography with Contemporary Co-Processors" from NXP Semiconductors, and "Analyzing the Harmfulness of Glitches in the Context of Side-Channel Analysis" from Secure-IC S.A.S.

We would like to thank the steering committee, Jean-Luc Danger and Werner Schindler, the general chairs, Alberto Ferrante, Francesco Regazzoni, and Subhadeep Banik, and the local organizers, Liliana Sampietro and Nadia Ruggiero-Ciresa, from Università della Svizzera italiana, for taking care of various aspects of organization. We would also like to thank the Web administrators, Helmut Häfner and Lothar Hellmeier of the University of Stuttgart, for maintaining the COSADE website for 2021. We are very grateful for the financial support received from our generous sponsors Hasler Stiftung, FortifyIQ, NewAE Technology Inc., Riscure, Secure-IC, PQShield, and Rambus Cryptography Research.

Finally, we would like to acknowledge Springer for their active cooperation and timely production of the proceedings.

October 2021

Shivam Bhasin
Fabrizio De Santis

Organization

General Chairs

Alberto Ferrante	Università della Svizzera italiana, Switzerland
Francesco Regazzoni	University of Amsterdam, The Netherlands, and Università della Svizzera italiana, Switzerland
Subhadeep Banik	École Polytechnique Fédérale de Lausanne, Switzerland

Program Committee Chairs

Shivam Bhasin	Nanyang Technological University, Singapore
Fabrizio De Santis	Siemens AG, Germany

Steering Committee

Jean-Luc Danger	Télécom Paris, France
Werner Schindler	Bundesamt für Sicherheit in der Informationstechnik (BSI), Germany

Program Committee

Diego Aranha	Aarhus University, Denmark
Aydin Aysu	North Carolina State University, USA
Alessandro Barenghi	Politecnico di Milano, Italy
Lejla Batina	Radboud University, The Netherlands
Sebastian Berndt	University of Lübeck, Germany
Jakub Breier	Silicon Austria Labs, Austria
Ileana Buhan	Radboud University, The Netherlands
Anupam Chattopadhyay	Nanyang Technological University, Singapore
Chitchanok Chuengsatiansup	University of Adelaide, Australia
Lauren De Meyer	Rambus Cryptography, The Netherlands
Jean-Max Dutertre	Ecole Nationale Superieure des Mines de Saint-Étienne (ENSMSE), France
Wieland Fischer	Infineon Technologies, Germany
Fatemah Ganji	Worcester Polytechnic Institute, USA
Benedikt Gierlichs	Katholieke Universiteit Leuven, Belgium
Dong-Guk Han	Kookmin University, South Korea
Annelie Heuser	Inria and CNRS, France
Johann Heyszl	Fraunhofer AISEC, Germany
Naofumi Homma	Tohuku University, Japan

Dirmanto Jap	Nanyang Technological University, Singapore
Jens-Peter Kaps	George Mason University, USA
Elif Bilge-Kavun	University of Passau, Germany
Juliane Krämer	Technische Universität Darmstadt, Germany
Victor Lomne	NinjaLab, France
Patrick Longa	Microsoft Research, USA
Stefan Mangard	Technische Universität Graz, Austria
Nele Mentens	Leiden University, The Netherlands, and KU Leuven, Belgium
Debdeep Mukhopadhyay	IIT Kharagpur, India
Zakaria Najm	Nanyang Technological University, Singapore
Ralph Nyberg	Infineon Technologies, Germany
Colin O'Flynn	NewAE Technology Inc., Canada
Daniel Page	University of Bristol, UK
Stjepan Picek	Technische Universität Delft, The Netherlands
Chester Rebeiro	Indian Institute of Technology Madras, India
Georg Sigl	Technische Universität München, Germany
François-Xavier Standaert	Université Catholique de Louvain, Belgium
Marc Stöttinger	Hessen3C, Germany
Ruggero Susella	STMicroelectronics, Italy
Wen Wang	Yale University, USA
Vittorio Zaccaria	Politecnico di Milano, Italy
Fan Zhang	Zhejiang University, China

Additional Reviewers

Anubhab Baksi
Debapriya Basu Roy
Anirban Chakraborty
Durba Chatterjee
Christoph Dobraunig
Zheng Gong
Mathieu Gross
Michael Gruber
Loïc Masure
Michael Meyer
Florian Mendel
Marcel Müller
Robert Primas
Martin Rehberg
Thomas Schamberger
Florian Sieck
Nikhilesh Singh
Sujoy Sinha Roy
Lars Tebelmann
Jean-Pierre Thibault
Jo Vliegen
Lennert Wouters

Presentation Abstracts

Introduction to OpenTitan – An Open-Source Silicon Root of Trust Project

Michael Tempelmeier

G+D Mobile Security GmbH, Prinzregentenstraße 159, 81677 München, Germany
michael.tempelmeier@gi-de.com, mtemp@opentitan.org

Abstract. RISC-V architectures are gaining more and more attention in both academia and industry. Security tokens also gain more and more attention. While they make authentication more secure, some concerns about their trustworthiness and their secure implementation remain [1].

OpenTitan is the first open-source project that provides a free, open-source hardware reference implementation and guidelines to create silicon root of trust (RoT) chips. It is stewarded by lowRISC and the main contributing partners are: ETH Zürich, G+D Mobile Security, Google, Nuvoton, Western Digital and Seagate [2]. OpenTitan brings the well-known concepts of open source (cryptographic) software to hardware. It enables security through transparency as the cryptographic primitives can be audited by the public [3]. Thus, the cryptographic (hardware) strength is not based on security-by-obscurity.

OpenTitan can be used for various security applications, like an universal 2nd factor (U2F) authentication key, or a platform integrity module. Its security model ensures the trustworthy state of the chip throughout its complete life cycle. Changes in the state of the chip are configured via one time programmable (OTP) memory. Devices can be personalized with a cryptographic identity. It is ensured that changes in the ownership do not allow to read out the previous owner's credentials.

The standard hardware toplevel of OpenTitan features a RISC-V Ibex core, hardened against fault attacks; 512 kB eFlash, 64 kB SRAM, and 16 kB ROM; an AES and Keccak module, protected by first order domain-oriented masking and hardened against fault attacks; the OpenTitan big-number accelerator (OTBN) for asymmetric cryptography; and various other (security) components which enable OpenTitan to be a full self-sustainable security IC. On the software side, OpenTitan features a reference implementation of the secure boot system, software that runs on the OTBN, as well as host software to communicate with the OpenTitan chip.

The cryptographic research community is encouraged to contribute to OpenTitan by analyzing the design early in its design stages. The industry can built their own chips based on OpenTitan, but also contributing hardware IPs to the project. FPGA prototyping can be done on a Xilinx Kintex 7 XC7K410T FPGA like provided by the ChipWhisperer CW310 board, as well as on a Xilinx Artix 7 XC7A200T FPGA like provided by the Nexys Video

board. However the latter requires a reduced flash size. Dedicate build scripts for both target boards are provided. Software debugging can be done in a verilator simulation or on the FPGA using openocd and gdb.

Keywords: OpenTitan · RISC-V · open-source hardware · RoT

References

1. Schink, M., Wagner, A., Unterstein, F., Heyszl, J.: Security and trust in open source security tokens. IACR Trans. Cryptogr. Hardw. Embedd. Syst. (3), 176–201 (2021). https://doi.org/10.46586/tches.v2021.i3.176-201
2. OpenTitan project page. https://opentitan.org/
3. OpenTitan Source Code. https://github.com/lowRISC/opentitan

Is Revolutionary Hardware for Fully Homomorphic Encryption Important? What Else is Needed?

Charlotte Bonte[1], Rosario Cammarota[1], Wei Dai[5], Joshua Fryman[1], Huijing Gong[1], Duhyeong Kim[1], Raghavan Kumar[1], Kim Laine[5], Poornima Lalwaney[1], Sanu Mathew[1], Nojan Sheybani[1,3], Anand Rajan[1], Andrew Reinders[1], Michael Steiner[1], Vikram Suresh[1], Sachin Taneja[1], Marc Trifan[1,2], Alexander Viand[1,4], Wei Wang[5], Wen Wang[1], Chris Wilkerson[1], Jin Yang[1]

[1] Intel Corp, USA
[2] University of California, Irvine, USA
[3] University of California, San Diego, USA
[4] ETH Zurich, Switzerland
[5] Microsoft, USA
rosario.cammarota@intel.com

Abstract. In spite of strong advances in confidential computing technologies, critical information is encrypted only temporarily – while not in use – and remains unencrypted during computation in most present-day computing infrastructures. The inability to keep critical information encrypted during computation can hinder the ability to fully share data and extract its maximum value.

Fully Homomorphic Encryption (FHE) is a cryptographic method to protect information confidentiality by enabling the processing of encrypted data without decrypting. However, the application of FHE carries a severe “performance tax” that is difficult to overcome with existing hardware.

The need for revolutionary hardware to enable FHE applications was identified by DARPA in the context of the DPRIVE program. As part of the DPRIVE program execution, Intel and Microsoft are realizing a platform to make FHE technologies more accessible by developing revolutionary hardware and software stack. Furthermore, the team is committed to the development of international standards and best practices. Overall, the initiative can enable unprecedented, cost-effective FHE performance, and pave the path for industrial deployment.

Keywords: Cryptographic hardware · Fully homomorphic encryption · Standards

Fully Homomorphic Encryption for all

Protecting the confidentiality of critical information—whether personal data or corporate intellectual property—is of strategic importance to businesses. In spite of the strong advances in trusted execution environments and other confidential computing technologies to protect data while at rest and in transit, data is unencrypted during computation. It is during this decrypted state that data can become more vulnerable to misuse, and third-party data leakage can incur severe fines for data handlers.

Fully Homomorphic Encryption (FHE) enables users to delegate computation to the cloud by enabling the cloud to process users' inputs while they remain encrypted and return encrypted output to the intended recipients. However, the adoption of FHE by industry has been slow. First, in spite of the tremendous advances in FHE, processing encrypted data still incurs a significant "performance tax" even for simple operations (ciphertext operations can be several orders of magnitude slower than clear text operations on existing hardware). Second, there is lack of automation tools for translating data and applications to enable FHE [1]. Third, the absence of international standards and best practices (including risk management tools) for secure and correct FHE deployment complicates the endorsement of FHE-based solutions [2].

The DARPA DPRIVE program [3] is the first publicly visible program that aims to build a hardware platform to enable continuous data protection with FHE, and to forge a path to commercialization intercepting segments such as healthcare, finance, communication (5G to XG), and cloud computing. Under the DPRIVE program, Intel is designing an application-specific integrated circuit (ASIC) accelerator to reduce the "performance tax" currently associated with FHE. Intel is collaborating with Microsoft to deliver a complete solution [4]. The design includes flexible arithmetic circuits for algebraic lattices with unprecedented vector parallelism capacity, to dramatically improve ciphertext computation speed, coupled with near-memory computation, to reduce data movement. The software stack will leverage the Microsoft SEAL library augmented with bootstrapping [5], and automatic translation tools to explore trade-offs in algorithmic optimization and data encoding to fit the performance requirements [6].

When fully realized, the accelerator can deliver a massive improvement in executing FHE workloads over existing CPU-driven systems, potentially reducing ciphertext processing time by five orders of magnitude. But the development of technology alone is not nearly enough to enable FHE for all. The team works with international standards bodies to develop standards and best practices for FHE usage. It continues to engage in academic research world-wide [7], including FHE cryptography, automation and risk management tools, next generation computer architecture such as in-memory compute.

References

1. Agrawal, et al.: Exploring Design and Governance Challenges in the Development of Privacy-Preserving Computation. arXiv:2101.08048
2. Cammarota, et al.: Trustworthy AI Inference Systems: An Industry Research View. arXiv:2008.04449

3. Building Hardware to Enable Continuous Data Protection. https://www.darpa.mil/news-events/2020-03-02)
4. Intel to Collaborate with Microsoft on DARPA program. https://www.intel.com/content/www/us/en/newsroom/news/intel-collaborate-microsoft-darpa-program.html
5. Microsoft SEAL. https://github.com/microsoft/SEAL
6. Viand, et al.: Fully Homomorphic Encryption Compilers. arXiv:2101.07078
7. Private AI Collaborative Research Institute. https://www.private-ai.org/

Post-quantum Cryptography with Contemporary Co-processors

Kronecker, Schönhage-Strassen, Nussbaumer and Beyond

Joppe W. Bos, Joost Renes and Christine van Vredendaal
NXP Semiconductors
{joppe.bos,joost.renes,christine.cloostermans}@nxp.com

Abstract. There are currently over 30 billion IoT (Internet of Things) devices installed worldwide. To secure these devices from various threats one usually relies on public-key cryptographic primitives whose operations can be costly to compute on resource-constrained IoT devices. To support such operations these devices often include a dedicated co-processor for cryptographic procedures, typically in the form of a big integer arithmetic unit. Such existing arithmetic co-processors do not offer the functionality that is expected by upcoming post-quantum cryptographic primitives. Regardless, contemporary systems may exist in the field for many years to come. We discuss how to re-use existing hardware for post-quantum cryptography, and in particular how this applies to the various finalists in the post-quantum standardization effort led by NIST.

Analyzing the Harmfulness of Glitches in the Context of Side-Channel Analysis

Sylvain Guilley and Sofiane Takarabt

[1] Secure-IC S.A.S., 104 Boulevard du Montparnasse (7th floor), 75014 Paris, France
{sylvain.guilley,sofiane.takarabt}@secure-ic.com

1 Introduction

Hiding and masking are two countermeasure strategies to protect hardware circuits against power and electromagnetic analyses. However, those protections are complex to implement correctly. Hiding requires perfect balancing, and masking shall take into consideration glitches.

In this presentation, we present a tool which allows to detect harmful glitches in a combinational netlist.

2 Analyzing Glitches

Glitches are transient transitions occurring in netlists owing to the property of combinational netlist to evaluate the output as soon as any input arrives. It is known that glitches can occur upon non-linear conditions on the inputs hence can demask otherwise perfectly masked netlists. Therefore, glitches can induce a first-order leakage despite all nets are (statically) perfectly masked, as it has already been demonstrated several times (e.g., on Canright masked S-Box [1] or on ISW scheme [3]).

Managing glitches has been the topic of many researches. For instance, "threshold implementation" and "domain-oriented masking" aim at making glitches harmless by design. Combinational logic "pipelining" or implementation in "look-up-tables" allows to remove glitches.

But to the best of our knowledge, no tool to diagnose glitches has been demonstrated. Still, it is possible to classify glitches as either harmless or harmful, typically using leakage spectral decomposition [2].

The theoretical tool is the mutation of the netlist, which consists in inserting an artificial edge (modeling a delay in a wire/gate). This modified netlist is analyzed in terms of sensitivity with respect to the unmasked variable. The detection of glitches yielding a leakage can be speeded-up with adequate Walsh-transform spectral computations [5].

3 Automated Analysis with Catalyzr Tool

In this talk, we recall such analyses, and show how it is implemented in a tool, namely Catalyzr [1]. We also validate this static analysis with real simulations, which attest of the concordance in the detection.

Let us recall that the methodology leveraged in the tool does not require timing assumptions (like the exact gate or interconnect delays), since it performs an exhaustive search amongst all possible glitching situations. In this respect, this approach allows for a constructive repair of netlists to remove harmful glitches (through iterative detection-repair cycles).

References

1. Canright, D.: A very compact S-box for AES. In: Rao, J.R., Sunar, B., (eds.) CHES 2005. LNCS, vol. 3659, pp. 441–455. Springer, Heidelberg (2005). https://doi.org/10.1007/11545262_32
2. Guilley, S., Heuser, A., Ming, T., Rioul, O.: Stochastic side-channel leakage analysis via orthonormal decomposition. In: Farshim, P., Simion, E., (eds.) SecITC 2017. LNCS, vol. 10543, pp. 12–27. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-69284-5_2
3. Roy, D.B., Bhasin, S., Guilley, S., Danger, J.-L., Mukhopadhyay, D.: From theory to practice of private circuit: A cautionary note. In: 33rd IEEE International Conference on Computer Design, ICCD 2015, New York City, NY, USA, October 18-21, 2015, pp. 296–303. IEEE Computer Society (2015)
4. Secure-IC. Catalyzr tool, 2021. https://cadforassurance.org/tools/software-assurance/catalyzr/, https://www.secure-ic.com/solutions/catalyzr/. Accessed 2 July 2021
5. Takarabt, S., Guilley, S., Souissi, Y., Sauvage, L., Mathieu, Y., Karray, K.: Formal evaluation and construction of glitch-resistant masked functions. In: 2021 IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2021, Washington DC, USA, 12–15 December 2021. IEEE (2021)

Keynotes

Securing the Next Trillion of Chips via In-Memory and Immersed-in-Logic Design – Beyond Traditional Design Boundaries

Massimo Alioto

ECE - National University of Singapore
massimo.alioto@nus.edu.sg, malioto@ieee.org

Abstract. Divide-and-conquer design methodologies facilitate building block design, but conflict with basic security requirements, while also precluding opportunities for efficient system integration and inexpensive embedment of security features. Indeed, conventional design partitioning vastly facilitates the identification of attack targets, and reduces the related effort by focusing on specific areas of the overall attack surface. At the same time, the insertion of security primitives as standalone blocks is inherently additive in terms of area, power, design effort and integration effort, limiting their embeddability in low-cost devices (i.e., the vast majority of the upcoming trillion chips for the Internet of Things).

In this keynote, the road towards ubiquitous hardware security is pursued from a primitive design perspective, designing PUFs and TRNGs that are inherently immersed in existing memory arrays and logic fabrics, and breaking the boundaries of traditional system partitioning. From a non-recurring engineering cost viewpoint, design and system integration entail lower effort and very low silicon area thanks to extensive circuit reuse, while also facilitating technology and design portability. At the same time, their immersed and distributed nature offers inherent physical-level obfuscation against several physical attacks targeting specific primitive instances with well-defined boundaries and ports, while also allowing full reuse of conventional techniques to protect memories and logic. Stricter data locality also facilitates architecture-level security, confining secure keys within the same logic module that they are used in (e.g., within the same cryptographic engine, or within the same memory encrypting its own data). Several silicon demonstrations are illustrated to quantify the benefits and the limits of existing techniques, and identify opportunities and challenges for the decade ahead. At the end of the keynote, fundamental directions on how to make hardware security more pervasive and unceasing are discussed.

Biography: Massimo Alioto (M'01–SM'07-F'16) received the MSc degree in Electronics Engineering and the Ph.D. degree in Electrical Engineering from the University of Catania (Italy) in 1997 and 2001. He is currently a Professor at the Department of Electrical and Computer Engineering, National University of Singapore, where he leads the Green IC group, and is the Director of the Integrated Circuits and Embedded Systems area, and the FD-FAbrICS research center at NUS. Previously, he held positions at the University of Siena, Intel Labs – CRL (2013), University of Michigan Ann Arbor (2011–2012), BWRC – University of California, Berkeley (2009–2011), and EPFL (Switzerland, 2007).

He has authored or co-authored more than 300 publications on journals and conference proceedings. He is author of four books, including Enabling the Internet of Things - from Circuits to Systems (Springer, 2017), and the latest on Adaptive Digital Circuits for Power-Performance Range beyond Wide Voltage Scaling (Springer, 2020). His primary research interests include self-powered wireless integrated systems, near-threshold circuits for green computing, widely energy-scalable integrated systems, data-driven integrated systems, hardware security, and emerging technologies, among the others.

He is the Editor in Chief of the IEEE Transactions on VLSI Systems (2019–2020), and was the Deputy Editor in Chief of the IEEE Journal on Emerging and Selected Topics in Circuits and Systems (2018). In 2020–2022 he is Distinguished Lecturer of the IEEE Solid-State Circuits Society. In 2009–2010 he was Distinguished Lecturer of the IEEE Circuits and Systems Society, for which he is/was also member of the Board of Governors (2015–2020), and Chair of the "VLSI Systems and Applications" Technical Committee (2010–2012). He served as Guest Editor of several IEEE journal special issues, and Associate Editor of a number of IEEE and ACM journals. He is/was Technical Program Chair and Track Chair in a number of IEEE conferences (e.g., ISCAS 2023, SOCC, ICECS), and is currently in the IEEE "Digital architectures and systems" ISSCC subcommittee, and the ASSCC TPC. Prof. Alioto is an IEEE Fellow.

Defending CyberPhysical Systems and Infrastructures from Cyber Attacks

Alberto Sangiovanni-Vincentelli

University of California Berkeley
alberto@berkeley.edu

Abstract. Attacks against critical infrastructure such gas pipelines, power generation and water treatment plants, as well as against cars and airplanes are very possible and may create disruptions that we can only start imagining. The talk frames the problem and describes the industrial landscape in this domain.

Short Bio

Alberto Sangiovanni Vincentelli is the Edgar L. and Harold H. Buttner Chair of Electrical Engineering and Computer Sciences at the University of California, Berkeley. In 2001, he received the Kaufman Award for his pioneering contributions to EDA from the Electronic Design Automation Consortium. In 2011, he was awarded the IEEE/RSE Maxwell Medal "for groundbreaking contributions that have had an exceptional impact on the development of electronics and electrical engineering or related fields". He co-founded Cadence and Synopsys, listed in NASDAQ with market cap of over 90 Billion USD. He presently serves on the Board of Directors of Cadence Design Systems Inc., KPIT Technologies, Expert.ai, Cy4Gate (Public companies), and is the Chair of the Board of Quantum Motion, Phoelex, Innatera, and Phononic Vibes. He consulted for Intel, HP, TI, ST Microelectronics, Mercedes, BMW, Magneti Marelli, Telecom Italia, United Technologies, Camozzi Group, Pirelli, General Motors, UniCredit, and UnipolSAI. He is also serving as member of the Advisory Board of the Politecnico di Milano, and as Chairman of the International Advisory Council and of the Strategy Board of MIND (Milano Innovation District). He is a member of the United States National Academy of Engineering, an IEEE and ACM Fellow. He received an honorary Doctorate from Aalborg University (Denmark) and one from KTH (Sweden). He has published more than 1000 papers and 19 books.

Contents