# Guest Editorial Special Issue on Intrinsic Hardware Security for Internet of Things Infrastructure

INTERNET of Things (IoT) is an emerging technology in the modern era of big data. It concerns a variety of applications ranging from smart homes, connected vehicles to smart factories, and more. IoT infrastructure typically comprises millions of connected objects and devices that store and exchange sensitive and confidential information. Theft and fraud scenarios, such as hacking and identity forgery, are serious threats to such IoT devices. Embedded hardware security techniques could be a potential solution to preserve the highest level of security within this infrastructure. Physically unclonable functions (PUFs) are among the potential solution to data security and counterfeiting problems. Many more intrinsic hardware security techniques are underway for a highly secure IoT infrastructure as strongly demanded by the IoT community. The focus of this Special Issue is to provide readers with the latest advances in securing IoT infrastructure from the physical layer point-of-view.

The response to our Calls for Papers (CFP) for this Special Issue was great. There were 30 papers submitted from many recognized research groups all over the world. During the review process, each paper was assigned to and reviewed by multiple experts in the field, with a rigorous two-round (and sometimes three!) review process. Thanks to the courtesy of the Editor-in-Chief of this JOURNAL, Prof. Sherman Shen, we were able to accept 12 excellent papers covering various aspects of security challenges in IoT infrastructure. In the following, we will introduce these papers and highlight their main contributions.

In the paper "Multigated Carbon Nanotube Field Effect Transistors-Based Physically Unclonable Functions as Security Keys," the authors proposed the design of multigate CNT-FET-based PUF. A CNT network was selected with specific channel density and dimensions for the devices enabled to generate random bit arrays. They also introduced multigate devices, which can have multiple challenges and generate multiple types of outputs. In conclusion of this proposed work, multigate CNT-FETs with networks of density close to percolation threshold density can be promising in producing low-cost and high-quality cryptographic primitives.

In the paper "Two-Factor Fuzzy Commitment for Unmanned IoT Devices Security," the authors proposed a novel concept of the two factor fuzzy commitment scheme that uses both an intrinsic factor of an IoT device and an environmental factor outside of the IoT device. In order to demonstrate the feasibility of the two-factor fuzzy commitment, they also presented the prototype IoT surveillance camera. There they utilized the image data as an external noisy source and PUF data as an internal noisy source. Finally, they conducted experiments by considering various situations and evaluated the key recovery rate for each experiment case.

In the paper "Design of a Hybrid RF Fingerprint Extraction and Device Classification Scheme," the authors introduced and utilized the principle of RF fingerprinting for wireless devices within the IoT network. They proposed a hybrid classification method by integrating novel RF fingerprint features in a smart manner and carried out extensive experiments to evaluate the performance. Their contribution and novelty are threefold. First, four novel modulation-based features, namely, DCTF, frequency offset, modulation offset, and I/Q offset feature from CTF, were adopted and found effective in classifying ZigBee nodes. Second, a smart hybrid classifier was designed to adaptively integrating features with the weights tuned to the channel conditions. Finally, they constructed a testbed consisting of a low cost USRP SDR as the receiver platform and 54 ZigBee target devices.

Moreover, the paper "An Efficient OFDM-Based Encryption Scheme Using a Dynamic Key Approach" introduced two different encryption schemes. Either Pre-IFFT or Post-IFFT, and employed either a key-less approach or a secret key statically derived from the physical channel parameters. Pre-IFFT schemes have been shown to mitigate the effects of channel fading and to improve bit-error-rate performance, while Post-IFFT encryption was shown to be more secure. Furthermore, a dynamic key generation scheme that improves the performance of existing OFDM encryption techniques was proposed.

In the paper "Analytical Model for Sybil Attack Phases in Internet of Things," the authors presented a comprehensive analysis of Sybil attack in depth. The proposed model may be used to devise an effective countermeasure against Sybil attack. A trained attacker is considered for every phase of launching Sybil attack to analyze the worst case impact of its action on the network. An algorithm using $K$-means clustering is proposed to visualize the deployment location selection procedure of an attacker.

The paper "RF-PUF: Enhancing IoT Security Through Authentication of Wireless Nodes Using *In-Situ* Machine Learning" discussed a conceptual development of RF-PUF and is presented along with a feasibility study showing that the

Digital Object Identifier 10.1109/JIOT.2019.2896751

inherent RF properties arising from the manufacturing process in a wireless node can be exploited as a strong PUF for device authentication in asymmetric IoT networks without any additional hardware at the transmitters. Using an *in-situ* machine learning-based framework, up to 10 000 transmitters can be detected with about 99% accuracy. The proposed method also eliminates the need for preamble-based or key-based identification of modern IoT nodes and enables low-cost secure authentication using the intrinsic properties embedded in the RF signal that does not have any extra hardware cost at the transmitter.

In the paper "Ultrasound Proximity Networking on Smart Mobile Devices for IoT Applications," the authors presented a software modem called "Hush." It utilizes very high frequency sound to transmit data between commodity smart mobile devices. Such software modulates ultrasound in a way, that is, fast, low error, and practically unnoticeable by users. It incorporates a fingerprinting scheme that makes it more difficult for attackers to masquerade by allowing the receiver to learn and recognize packets sent from the intended transmitter. It could achieve a relatively high transmission rate up to 4.99 kb/s.

Another interesting paper "Secured Data Collection With Hardware-Based Ciphers for IoT-Based Healthcare" studied the potential data security threats regarding IoT within the healthcare scenarios. They proposed a new data collection scheme called "SecureData" to provide data security and preserve the privacy of the patients' personal data. A secret cipher algorithm was implemented on the field-programmable gate array (FPGA) hardware platform for such purpose. They also applied secret cipher sharing and share repairing. The performance analysis shows that the SecureData scheme can be efficient in terms of frequency, cost of energy, and overall computation cost of when to apply against attacks.

Furthermore, the paper "Energy Efficient and Side-Channel Secure Cryptographic Hardware for IoT-Edge Nodes" demonstrated an optimized unrolled datapath architecture for "SIMON128" cipher to secure an image-sensor node for IoT-edge devices. This ensured minimal latency, throughput, energy, and area overheads. Different hardware architectures of SIMON128 targeted for low area compact design to high-performance application are explored. While applied to an image sensor node, the authors demonstrated that unrolled datapath with a sufficiently high degree of unrolling can provide at least 83× higher power side channel analysis attack resistance at equivalent performance and energy efficiency with respect to a traditional 128b AES engine.

The paper "Secret Key Generation Over Biased Physical Unclonable Functions With Polar Codes" investigated the problem of secret key generation over noisy and biased PUFs. It also investigated secrecy and reliability issues, which are often the major challenge in designing optimal secret-key generation schemes. The proposed scheme offered many advantages, such as less required PUF bits, lower error rate, and flexible construction. The PUF size for a PUF-based key generator was decreased by approximately 60% compared to previous work. In addition, the required PUF size can be predicted based on the error rate and bias level according to the approximation of achievable secret-key rate.

In the paper "FPGA-Based Symmetric Re-Encryption Scheme to Secure Data Processing for Cloud-Integrated Internet of Things," the authors introduced a new FPGA-based scheme for securing IoT data in public clouds. This typically includes a protocol for establishing a secure session between a client and an on-the-cloud FPGA to process IoT data. Utilizing a symmetric proxy re-encryption, data owners can give temporary access to IoT data in the cloud without divulging the keys used by the IoT devices to encrypt the data. This technique can provide a strong protection against various attacks in the IoT cloud.

Finally, the paper "HCIC: Hardware-Assisted Control-Flow Integrity Checking" proposed a hardware-assisted control-flow integrity (CFI) checking technique to resolve the vulnerabilities that current software-based CFI incurs high performance overhead and hardware-based may require extending the existing processors' instruction-set architectures or suffer some security vulnerabilities. The key technique involves two control flow verification mechanisms.

The experimental results show that the proposed new technique incurs extremely low performance overhead (average 0.95%) and binary size overhead (average 0.78%), which are much lower than traditional CFI approaches.

In conclusion, we wish to express our appreciation to all the authors who responded very positively to our CFP. Thanks to those who got their work accepted to this Special Issue and also to those who did not have the chance this time. We were restricted by a tight time frame so that it was not possible to accept more submissions. Thanks to the voluntary reviewers and experts who have done their best during all the rounds of the review process, which resulted in improving the overall quality of the submissions.

Finally, we appreciate the support of the Editor-in-Chief of this JOURNAL, Prof. Sherman Shen throughout the entire publication process and, of course, the editorial staff.

MOHAMED KHEIR, *Guest Editor*
IMS Connector Systems Group
Baden-Württemberg, Germany

MANOS M. TENTZERIS, *Guest Editor*
School of Electrical and Computer Engineering
Georgia Institute of Technology
Atlanta, GA 30332 USA

AHMED ABDELGAWAD, *Guest Editor*
School of Engineering and Technology
Central Michigan University
Mount Pleasant, MI 48859 USA

ILSUN YOU, *Guest Editor*
Department of Information Security Engineering
Soonchunhyang University
Asan, South Korea

**Mohamed Kheir** (M'17–SM'17) was born in Cairo, Egypt, in 1977. He received the M.Sc. degree in communications technology from the University of Ulm, Ulm, Germany, in 2005, and the Ph.D. degree (Hons.) in information engineering and technology from the German University in Cairo, New Cairo, Egypt, in cooperation with Magdeburg University, Magdeburg, Germany, in 2011.

From 2012 to 2015, he was a Lecturer with the Chair of Microwave Engineering, University of Kiel, Kiel, Germany, where he was involved in several research projects and lecturing duties. Since 2015, he has been an RF-Development Engineer with IMS Connector Systems GmbH, Löffingen, Germany, where he is responsible for the design and development of high-speed and multichannel data connectors for mobile base stations and automotive applications. His current research interests include microwave measurement techniques, microwave/mm-wave integrated circuits, and RF identification and security.

Dr. Kheir was a recipient of the Early Career Award of the 27th Conference in Precision Electromagnetic Measurements in 2010. He serves as a Reviewer for multiple IEEE/IET journals and letters. He has been an Associate Editor of IEEE ACCESS since 2017.

**Manos M. Tentzeris** (S'89–M'98–SM'03–F'10) received the Diploma degree (*magna cum laude*) in electrical and computer engineering from the National Technical University of Athens, Athens, Greece, and the M.S. and Ph.D. degrees in electrical engineering and computer science from the University of Michigan at Ann Arbor, Ann Arbor, MI, USA.

He is currently a Ken Byers Professor of flexible electronics with the School of Electrical and Computer Engineering (ECE), Georgia Institute of Technology, Atlanta, GA, USA. He has served as the Head of the ECE Electromagnetics Technical Interest Group, Georgia Institute of Technology, as the Georgia Electronic Design Center Associate Director for RFID/Sensors research, and as the Georgia Institute of Technology NSF-Packaging Research Center Associate Director for RF Research and the RF Alliance Leader. He was a Visiting Professor with the Technical University of Munich, Munich, Germany, in 2002, GTRI-Ireland, Athlone, Ireland, in 2009, and LAAS-CNRS, Toulouse, France, in 2010. He heads the ATHENA Research Group (20 Researchers), Riverside, CA, USA. He has given over 100 invited talks to various universities and companies all over the world. He has authored over 650 papers in refereed journals and conference proceedings, 5 books, and 25 book chapters. He has helped to develop academic programs in 3-D/inkjet-printed RF electronics and modules, flexible electronics, origami and morphing electromagnetics, highly integrated/multilayer packaging for RF and wireless applications using ceramic and organic flexible materials, paper-based RFID's and sensors, wireless sensors and biosensors, wearable electronics, "Green" electronics, energy harvesting and wireless power transfer, nanotechnology applications in RF, microwave MEMS, SOP-integrated (UWB, multiband, millimeter wave, and conformal) antennas.

Dr. Tentzeris was a recipient or co-recipient of the 2017 Georgia Institute of Technology Outstanding Achievement in Research Program Development Award, the 2016 Bell Labs Award Competition Third Prize, the 2015 IET Microwaves, Antennas and Propagation Premium Award, the 2014 Georgia Institute of Technology ECE Distinguished Faculty Achievement Award, the 2014 IEEE RFID-TA Best Student Paper Award, the 2013 IET Microwaves, Antennas and Propagation Premium Award, the 2012 FiDiPro Award in Finland, the iCMG Architecture Award of Excellence, the 2010 IEEE Antennas and Propagation Society Piergiorgio L. E. Uslenghi Letters Prize Paper Award, the 2011 International Workshop on Structural Health Monitoring Best Student Paper Award, the 2010 Georgia Institute of Technology Senior Faculty Outstanding Undergraduate Research Mentor Award, the 2009 IEEE TRANSACTIONS ON COMPONENTS AND PACKAGING TECHNOLOGIES Best Paper Award, the 2009 E. T. S. Walton Award from the Irish Science Foundation, the 2007 IEEE APS Symposium Best Student Paper Award, the 2007 IEEE MTT-S IMS Third Best Student Paper Award, the 2007 ISAP 2007 Poster Presentation Award, the 2006 IEEE MTT-S Outstanding Young Engineer Award, the 2006 Asia–Pacific Microwave Conference Award, the 2004 IEEE TRANSACTIONS ON ADVANCED PACKAGING Commendable Paper Award, the 2003 NASA Godfrey "Art" Anzic Collaborative Distinguished Publication Award, the 2003 IBC International Educator of the Year Award, the 2003 IEEE CPMT Outstanding Young Engineer Award, the 2002 International Conference on Microwave and Millimeter-Wave Technology Best Paper Award (Beijing, China), the 2002 Georgia Institute of Technology–ECE Outstanding Junior Faculty Award, the 2001 ACES Conference Best Paper Award, the 2000 NSF CAREER Award, and the 1997 Best Paper Award of the International Hybrid Microelectronics and Packaging Society. He was the TPC Chair of IEEE IMS 2008 Symposium and the Chair of the 2005 IEEE CEM-TD Workshop. He is the Vice Chair of the RF Technical Committee (TC16) of the IEEE CPMT Society. He is the founder and the Chair of the RFID Technical Committee (TC24) of the IEEE MTT-S and the Secretary/Treasurer of the IEEE C-RFID. He is an Associate Editor of the IEEE TRANSACTIONS ON MICROWAVE THEORY AND TECHNIQUES, the IEEE TRANSACTIONS ON ADVANCED PACKAGING, and the *International Journal on Antennas and Propagation*. He is a member of URSI-Commission D, the MTT-15 Committee, and the Technical Chamber of Greece. He served as one of the IEEE MTT-S Distinguished Microwave Lecturers from 2010 to 2012 and is one of the IEEE CRFID Distinguished Lecturers. He is an Associate Member of EuMA and a Fellow of the Electromagnetic Academy.

**Ahmed Abdelgawad** (GS'07–M'11–SM'17) received the M.S. and Ph.D. degrees in computer engineering from the University of Louisiana at Lafayette, Lafayette, LA, USA, in 2007 and 2011, respectively.

In 2011, he joined IBM, as a design aids and automation engineering professional with the Semiconductor Research and Development Center. In 2012, he joined Central Michigan University, Mount Pleasant, MI, USA, as a Computer Engineering Assistant Professor, where he became a Computer Engineering Associate Professor in 2017. He served as a PI and a Co-PI for several funded grants from the NSF. He has authored or co-authored 2 books and over 78 papers in related journals and conferences. His current research interests include distributed computing for wireless sensor network (WSN), Internet of Things (IoT), structural health monitoring, data fusion techniques for WSN, low power embedded systems, video processing, digital signal processing, robotics, RFID, localization, very large scale integration, and field-programmable gate array design.

Dr. Abdelgawad served as a Reviewer for several conferences and journals, including IEEE WF-IoT, IEEE ISCAS, IEEE SAS, the IEEE INTERNET OF THINGS JOURNAL, *IEEE Communications Magazine*, the IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, the IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT, and Springer and Elsevier journals. He served on the Technical Committees of IEEE ISCAS 2007, IEEE ISCAS 2008, and IEEE ICIP 2009 conferences. He served on the Administration Committee of IEEE SiPS 2011. He also served on the Organizing Committee of ICECS in 2013 and 2015. He was the Publicity Chair in North America of the IEEE WF-IoT in 2016, 2018, and 2019 conferences. He was the Finance Chair of IEEE ICASSP 2017. He was the TPC Co-Chair of I3C'17 and GIoTS 2017, and the Technical Program Chair of IEEE MWSCAS 2018. He has been the keynote speaker for many international conferences and has conducted many webinars. He is currently the IEEE Northeast Michigan Section Chair and an IEEE SPS IoT SIG member.

**Ilsun You** (M'12–SM'13) received the M.S. and Ph.D. degrees in computer science from Dankook University, Seoul, South Korea, in 1997 and 2002, respectively, and the Ph.D. degree from Kyushu University, Fukuoka, Japan, in 2012.

From 1997 to 2004, he was with Thin Multimedia, Inc., Santa Clara, CA, USA, Internet Security Company Ltd., and Hanjo Engineering Company Ltd., Anyang, South Korea, as a Research Engineer. He is currently an Associate Professor with the Department of Information Security Engineering, Soonchunhyang University, Asan, South Korea. He has authored or co-authored over 180 papers. His current research interests include 4/5G security, security for wireless networks and mobile Internet, and IoT security.

Dr. You has served or is currently serving as a main organizer for international conferences and workshops such as MIST, MobiWorld, and MobiSec. He is the Editor-in-Chief of the *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*. He is on the Editorial Board of *Information Sciences*, the *Journal of Network and Computer Applications*, IEEE ACCESS, *Intelligent Automation & Soft Computing*, the *International Journal of Ad Hoc and Ubiquitous Computing*, *Computing and Informatics*, and the *Journal of High Speed Networks*. He is a Fellow of the IET.