Guest Editorial
Securing IoT Hardware: Threat Models and Reliable, Low-Power Design Solutions

IT IS well understood that for Internet of Things (IoT), security of underlying hardware is the key to safe and reliable operation. IoT service stack relies on security of network, software, and firmware, all of which, in turn, depend on functionality provided by the underlying hardware. The hardware may be compromised or attacked by multiple threat actors. The designer may create a backdoor that leaks vital information such as encryption key used in secure channel; the manufacturer may tamper the design by inserting hardware Trojans or introducing artifacts with known reliability vulnerabilities. Either of these actors may enable writing into protected memory areas that may store secure hash of trusted code base, allowing malware to boot directly on the hardware. Today's designs integrate IP blocks from multiple vendors; manufactured, tested, and repaired by different companies spanning across the globe. Consequently, there are many entry points for the hardware to be compromised. For a trusted hardware design, protection and security of intellectual property cores are of paramount importance. This special section aims to publish novel solutions for security problems related to hardware used in IoT.

- *Secured IoT Hardware*: Induction of any form of third-party intervention in the hardware design methodology may raise grave security concern for IoT hardware. Securing IoT hardware can be in the form of protecting intellectual property cores against false claim of ownership/piracy/counterfeit. The first form of security measure requires anti-piracy methodologies such as digital watermarking, hardware metering, computational forensic engineering, and obfuscation that can nullify the false claim of ownership or detect unauthorized pirated designs. The second form of threat, which is formally called "hardware Trojan," is an act of deliberate insertion into a design (such as intellectual property core, hardware) by a rogue designer or vendor, and also requires detection/correction strategies as a security measure. Both hardware threats discussed above may occur in any of the design abstraction levels (behavioral, register transfer, layout, etc.). Handling the threats higher in the abstraction level provides more assurance against possible attacks, however, it requires a more sophisticated approach. Further more, the level at which protective measure is applied often dictates the preprocessing or postprocessing style of the approach. These calls for novel technique that embeds hardware security measure a higher abstraction level for protection of IoT devices.
- *Reliable IoT Hardware*: Due to multiple factors affecting reliability of hardware used in IoT devices, these devices are always at a risk of malfunctioning. For example, a manufacturer may deliberately change the width of a metal line for causing premature electromigration defect, possibly triggering a timed Trojan. Multiple trigger mechanisms may be used to attack hardware such as: 1) reducing device dimensions; 2) scaling supply voltage; and 3) modulating frequency of operation. Methodologies should incorporate techniques that provide resiliency/tolerance against such faults at higher abstraction levels to assure greater reliability from the beginning of design flow.
- *Low-Cost IoT Hardware:* Another design aspect of hardware for IoT devices is performance and power. Consumer demand drives integration of multiple functionalities, often achieved by integrating dedicated IP cores and general purpose processors working in tandem. This creates a unique challenge in maintaining security and integrity of data passing through various IP blocks. Standard solutions involving redundancy, diversity, and check run up against power, performance, and latency constraints.

This special section features 13 papers (with one paper published already in the May 2017 issue), covering diverse topics in the context of the challenges outlined above.

The problem of IP theft for IoT frameworks is addressed in "Using Scan Side Channel to Detect IP Theft." Azriel *et al.* present a methodology for detection of IP theft in VLSI devices that exploits the internal test scan chains, designed for production test automation. The paper demonstrates the power of the presented approach with a test case of an open source Bitcoin SHA-256 accelerator, containing more than 80 000 registers.

In "AES Datapath Optimization Strategies for Low-Power Low-Energy Multisecurity-Level Internet-of-Things Applications," Bui *et al.* present hardware optimization strategies for Advanced Encryption Standard for high-peed, ultralow-power, ultralow-energy IoT applications with multilevel of security. The design introduced in the paper supports multiple security levels through multiple key sizes, power, and energy optimization for both datapath and key expansion. The authors reach greater security and lower energy per bit in terms of security.

Digital Object Identifier 10.1109/TVLSI.2017.2762398

In “Securing the PRESENT Block Cipher Against Combined Side-Channel Analysis and Fault Attacks,” De Cnudde and Nikova perform a hardware implementation of the PRESENT block cipher secured against both side-channel analysis and fault attacks. They also present detailed instructions on the process of successfully achieving a secure Private Circuits II implementation for the data path as well as the control logic.

In “A Flexible Wildcard-Pattern Matching Accelerator via Simultaneous Discrete Finite Automata,” Tsai *et al.* present a simultaneous pattern matching methodology for wildcard patterns by two separated engines to represent discrete finite automata (discrete-FA) for IoT frameworks. The approach obtains scalability for achieving good performance and low space consumption in network security. The authors obtain an energy consumption reduction of up to 48% compared to the energy consumption using a computing system that contains a large memory lookup and comparison overhead.

The problem of IoT hardware security is addressed in “An On-Chip Technique to Detect Hardware Trojans and Assist Counterfeit Identification.” An embedded solution to detect hardware Trojans and counterfeits is presented by Lecomte *et al.*. The proposed method is based on the fingerprinting of the static distribution of the supply voltage over the whole surface of ICs.

In “Chaotic Encrypted Polar Coding Scheme for General Wiretap Channel,” Zhao *et al.* present a cross-layer encryption and coding scheme for wiretap channel in IoT frameworks. In the paper, a onetime-pad encryption and a secure key transmission are constructed by combining chaos stream cipher with the extended multiblock polar coding scheme.

In “ULV-Turbo Cache for an Instantaneous Performance Boost on Asymmetric Architectures,” Wang *et al.* propose a ULV-Turbo cache based on a ULV-selective-ally 8T SRAM (static random access memory) that is able to perform reliable ultralow-voltage operation and provide the speedup function of SRAM rows ally. This has applicability for embedded systems used in IoT hardware. The ULV-Turbo cache proposed by the authors reduces the energy consumption of the entire system by approximately 36%.

The problem of reliability of IoT hardware has been addressed in “Novel Radiation-Hardened-by-Design (RHBD) 12T Memory Cell for Aerospace Applications in Nanoscale CMOS Technology” (published in *IEEE Trans. Very Large Scale Integr. (TVLSI) Syst.,* vol. 25, no. 5, pp. 1593–1600, May 2017, DOI: 10.1109/TVLSI.2016.2645282). Guo *et al.* propose, with respect to 65-nm CMOS commercial process, a novel circuit-level RHBD 12T memory cell that tolerates both single-node an upset and multiple-node upset based on upset physical mechanism behind soft errors together with reasonable layout topology. The proposed 12T cell presented in the paper indicates higher stability during providing fault tolerance capability.

In “Energy-Efficient Side-Channel Attack Countermeasure With Awareness and Hybrid Configuration Based on It,” an energy-efficient countermeasure to side-channel attacks for IoT hardware is presented. Li *et al.* present a low-power-aware special hiding technique for the substitution operation in block ciphers using appropriate feedforward compensation. The technique presented in the paper obtains higher throughput and lower power compared to traditional methods.

In “A Process-Independent and Highly Linear DCO for Crowded Heterogeneous IoT Devices in 65-nm CMOS,” Gorji and Ghaznavi-Ghoushchi present a feedback-assisted digitally controlled oscillator (DCO) that is linear and invariant to process variation for the entire 2.5-GHz frequency band. This has been achieved by appending a dynamic feedback to inner current-controlled oscillator using a frequency-to-current converter.

In “Vulnerability Analysis of Trivium FPGA Implementations,” Potestad-Ordóñez *et al.* address the problem of information security in IoT frameworks. The authors investigate and analyze the vulnerability of Trivium FPGA implementations against fault attacks. They also perform a novel comparison between real and simulated fault injections.

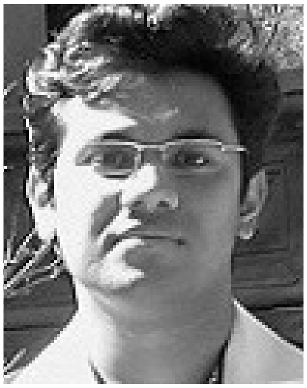
In “Automatic Code Converter Enhanced PCH Framework for SoC Trust Verification,” Guo *et al.* address the problem of IP security in IoT hardware. The authors present a novel integrated formal verification framework to evaluate the trust of system-on-chip (SoC) constructed from untrusted third-party hardware resources. The framework combines an automated model checker with an interactive theorem prover to reduce the time for proving system-level security properties of SoCs. The paper is able to demonstrate system security with reduced verification effort.

In “Multiradix Trivium Implementations for Low-Power IoT Hardware,” low-power IoT hardware design problem is addressed. Mora-Gutiérrez *et al.* propose low-power multiradix Trivium implementations based on the use of parallelization techniques to reduce dynamic power consumption. The paper shows that designs offer dynamic power savings of 31%–45% with radix-1 and radix-2 when compared with the current Trivium and 15% with radix-8.

We are pleased with the technical depth and spectrum of this special section, though we readily confess that many aspects of the hardware security problems are not addressed here. We sincerely thank all the authors and reviewers for their timely efforts, and the Editor-in-Chief and IEEE Staff for their guidance.

Anirban Sengupta
IIT Indore
Indore, India
E-mail: asengupt@iiti.ac.in

Sandip Kundu
University of Massachusetts Amherst
Amherst, MA, USA
E-mail: kundu@umass.edu



Anirban Sengupta (M'09–SM'17) received the Ph.D. and M.A.Sc. degrees in electrical and computer engineering from Ryerson University, Toronto, ON, Canada.

He is an Assistant Professor of Computer Science and Engineering at IIT Indore, Indore, India, where he directs the Research Laboratory on "CAD for Consumer Electronics Security and Reliability." He is a registered Professional Engineer of Ontario (P.Eng.). His research/sponsored projects are supported by industries such as Intel Corporation and VividSparks IT Solutions. He has 130 publications and patents, with the bulk of them in IEEE and IET periodicals. Several of his patents have been cited by IBM, Siemens Corporation, Qualcomm, STC.UNM, and Siemens Aktiengesellschaft. His patents generated funding from the Ontario Center of Excellence (OCE), Toronto, ON, Canada. Several of his IEEE publications have appeared in the "Top 50 Most Popular Articles" from the IEEE Periodicals. He has supervised in excess of 15 candidates, including 4 Ph.D.s, many of whom are/were placed in academia and industry.

Dr. Sengupta is a recipient of the Sir Visvesvaraya Faculty Research Fellow Award from the Ministry of Electronics & IT and the Best Research Paper Award 2017 by IIT Indore. He was awarded the prestigious IEEE Distinguished Lecturer by the IEEE Consumer Electronics Society in 2017, as well as the Outstanding Associate Editor Award from the IEEE Computer Society Technical Committee on VLSI (TCVLSI) Letter Editorial Board of IEEE Computer Society in 2017. He was awarded the highest rating of "excellent" by the expert committee of the Department of Science and Technology based on the performance (output) in an externally funded project in 2017. He currently serves as a Senior Editor, an Associate Editor, an Editor, and a Guest Editor of several IEEE Transactions/Journals, Elsevier, and IET Journals, including the IEEE TRANSACTIONS ON AEROSPACE AND ELECTRONIC SYSTEMS, the IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, IEEE ACCESS, *IET Journal on Computer and Digital Techniques*, *Elsevier Microelectronics Journal*, IEEE CONSUMER ELECTRONICS MAGAZINE, and IEEE VLSI CIRCUITS AND SYSTEMS LETTERS. He also serves as a Guest Editor for the IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, the IEEE TRANSACTIONS ON VLSI SYSTEMS, and IEEE ACCESS. He is the Technical Program Chair of the 36th IEEE International Conference on Consumer Electronics 2018 in Las Vegas, the 15th IEEE International Conference on Information Technology 2016, the 3rd IEEE International Symposium on Nanoelectronic and Information Systems 2017, and the 2019 IEEE International Symposium on VLSI in Florida. He holds an external affiliation as "Honorary Chief Scientist" at VividSparks IT Solutions Pvt. Ltd.

Sandip Kundu (S'85–M'86–SM'94–F'07) received the Ph.D. degree from the University of Iowa, Iowa City, IA, USA, in 1988.

He spent 17 in industry before joining academia in 2005. He started his career at IBM Research, New York City, NY, USA, as a Research Staff Member, and then worked at Intel Corporation, Santa Clara, CA, USA, as a Principal Engineer before joining the University of Massachusetts Amherst (UMass Amherst), Amherst, MA, USA. He is a Program Director of the CNS Division, CISE Directorate, National Science Foundation, Alexandria, VA, USA, on leave from UMass Amherst, where he is currently a Professor with the Electrical and Computer Engineering Department. He has authored or coauthored nearly 250 research papers in VLSI design and test, holds several key patents including ultra-drowsy sleep mode in processors, and has given more than a dozen tutorials at various conferences.

Prof. Kundu is a fellow of the Japan Society for Promotion of Science, a Senior International Scientist of the Chinese Academy of Sciences, and was a Distinguished Visitor of the IEEE Computer Society. He is currently an Associate Editor of the IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING. He served as an Associate Editor for the IEEE TRANSACTIONS ON COMPUTERS, the IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, and *ACM Transactions on Design Automation of Electronic Systems*. He was been the Technical Program Chair/General Chair of multiple conferences including the ICCD, ATS, ISVLSI, DFTS, and VLSI Design Conference.