IEEE ACCESS SPECIAL SECTION EDITORIAL:

SECURITY AND RELIABILITY AWARE SYSTEM DESIGN FOR MOBILE COMPUTING DEVICES

It is a well-known fact that design productivity is failing to keep pace with the big increase in the demands of applications and advanced silicon technology, especially in the domain of portable electronics. Moreover owing to the massive complexity of modern systems-on-chip (SoC), complete in-house development is impossible, and thus globalization of the design process has established itself as an inevitable solution for faster and efficient design. In this global design supply chain, the design of mobile computing devices relies heavily on reusable Intellectual Property (IP) cores as a practical solution. However, such IP cores are becoming increasingly vulnerable to malicious activities, attacks and threats. Any form of third party intervention in the design process can raise grave security concerns about the system. Security issues in IP's can be in the form of IP piracy/IP counterfeit or embedded malicious logic or information leakage. The first form of security countermeasure requires anti-piracy methodologies that can nullify false claims of ownership or detect unauthorized pirated designs. The second form of threat, which is often called a 'hardware Trojan', is the deliberate insertion of illicit hardware into the IP design by a rogue designer or vendor, also requires detection/correction strategies as a security countermeasure.

Another important design aspect of mobile computing devices is the reliability of hardware accelerators/custom IP cores. Due to multiple factors, the reliability of digital circuits used as core computation engines in these mobile computing devices poses the risk of malfunction. For example, transient faults occurring due to radiation strikes, permanent faults because of IC packaging, aging of components etc. all lead to adverse effects on the reliability of the system. Moreover, in the present era, scaling of very large scale integration (VLSI) devices is aggressively performed in order to enhance the speed of operation and to lower power consumption. There are multiple mechanisms for achieving this goal such as: (i) reducing device dimensions; (ii) scaling the supply voltage (iii); reducing the frequency of operation etc. However, such actions result in negative consequences for reliability by making the system vulnerable to various faults. The current challenge is to incorporate reliability as a design metric during multi-objective optimization of hardware accelerators/IP cores/application specific processors.

Besides the above, another design aspect for portable electronic devices is performance. Due to the never-ending demands of the consumer electronics market, more and more applications are required to execute simultaneously. This performance is achieved by a combination of hardware accelerators and general purpose processors working in tandem. However, reduction of delay/latency is the key in such a scenario. Therefore, performance enhancement is mandatory besides security and reliability in the consumer electronics market. This special section of IEEE ACCESS journal focuses on the emerging technologies in the area of hardware security and reliability performance enhancement of mobile/smart computing devices. IEEE ACCESS journal is a new multidisciplinary, applications-oriented, all-electronic archival journal continuously presenting the results of original research or development across all of the IEEE's fields of interest. Because of its open access nature, this special section is freely accessible to all readers across the globe. Four high-quality papers have been accepted from prominent groups around the world after rigorous peer-review processes which are discussed in the rest of this guest editorial.

Enhancing performance while ensuring security, is the key to system design that involves smart devices, especially in the internet of things (IoT) domain. Security concerns include external attacks such as eavesdropping, malicious manipulation from an adversary or intellectual property (IP) core maker. So far in the literature, there has not been any work that deals with the hardware architecture of a secure digital camera integrated with a better portable graphics (BPG) compression algorithm that is also suitable for high performance imaging in the IoT. In the invited paper 'Design of a High-Performance System for Secure Image Communication in the Internet of Things' by *E. Kougianos, S. P. Mohanty, G. Coelho, U. Albalawi, and P. Sundaravadivel*, a novel hardware architecture of a quadrotor integrated with a secure BPG compression encoder is proposed. The

authors propose the first ever Simulink based prototype of the SBPG compression algorithm for digital cameras.

Due to globalization in the integrated circuit (IC) design supply chain, trust/security of intellectual property (IP) cores used as components in mobile computing devices imposes a critical challenge. This has led to the domain of IP core protection for anti-theft/piracy as an important subject of research in system design. However there exists very limited effort in handling IP core protection from the vendor's perspective at the behavioral level (during high level synthesis). Tackling IP core protection by embedding the vendor's signature at a higher design abstraction level, ensures that the subsequent lower level design steps are also protected against external attacks such as false claim of ownership and tampering. In the invited paper, 'Exploring Low Cost Optimal Watermark for Reusable IP Cores During High Level Synthesis' by *A. Sengupta and S. Bhadauria,* a novel multi-variable signature encoding for embedding a low cost watermark in an IP core design during high level synthesis that provides enhanced security against typical attacks is proposed. Comparison with a recent technique indicates that this watermark incurs lower embedding cost, lower runtime, and less storage hardware.

The performance of a processor is at the core of mobile computing devices due to numerous applications running in parallel. Though rich literature exists in the area of performance enhancement, no work exists that improves the performance of a parallel processor by a significant margin. In the paper 'Introducing TAM: Time-Based Access Memory' by *N. Mekhiel*, a new memory system is proposed that makes all of its content available to all processors, so that processors do not have to access the shared memory in a sequential order. Rather than having one processor access a single location in the shared memory at a time, it is ensured by compulsion that each location is made available to all processors at a specific time. The proposed memory system is fast and does not utilize decoders for its operation. Significant improvements in performance gain of both single and parallel processors have been achieved by the authors.

A residue generator is an important hardware unit that is responsible for implementing arithmetic codes used in testing arithmetic/logical operations, thus ensuring the reliability of the hardware used in computing devices. The existing design methods for residue generators are oriented to special values of the check base. The paper 'Signature and Residue Testing of Microprogrammable Control Units' by *V. Geurkov*, presents a novel approach to designing residue generators with an arbitrary check base that reduces the probability of error escape. The approach proposed in this paper can be used in fault-tolerant digital designs.

We are pleased with the technical depth and spectrum of this special section, and also confess that it could not cover all the emerging security and reliability aware technologies for mobile computing devices. However, we sincerely thank all the authors and reviewers for the tremendous efforts, and of course the Editor-in-Chief and Staff Members for their great guidance.

ANIRBAN SENGUPTA
Indian Institute of Technology (IIT) Indore, India
Email: asengupt@iiti.ac.in

SARAJU P. MOHANTY
University of North Texas, Denton, USA
Email: Saraju.Mohanty@unt.edu

FABRIZIO LOMBARDI
Northeastern University, Boston, USA
Email: lombardi@coe.neu.edu

MARK ZWOLINSKI
University of Southampton, UK
Email: mz@ecs.soton.ac.uk

Prof. **Anirban Sengupta** is currently an Assistant Professor in Discipline of Computer Science and Engineering at Indian Institute of Technology (I.I.T) Indore, where he directs the research lab on 'Behavioural Synthesis of Digital IP core '. He holds a Ph.D. & M.A.Sc. in Electrical & Computer Engineering from Ryerson University, Toronto (Canada) and is a registered Professional Engineer of Ontario (P.Eng.). He also holds a B.Tech degree from West Bengal University of Technology, India. In the past, he was also affiliated with Indian Institute of Science (IISc) Bangalore as a visiting research scholar. His research interest includes Optimization during Design Space Exploration for Hardware Accelerators, High Level Synthesis, Fault Secured High Level Synthesis, Trojan Security Aware HLS, Hardware Trust in High Level Synthesis, IP core Protection during HLS, Evolutionary Computing during HLS as well as Physical Design using CAD. His research/sponsored projects are funded by Department of Science & Technology (Science & Engineering Research Board), Govt. of India as well as supported by Intel Corporation and Department of Electronics & IT (DEITY), Govt. of India. He has around 100 Publications & Patents which include Journals, Patents and Invited Book Chapters from IEEE, IET, Elsevier, Springer and USPTO/CIPO/IPO. He is owner 11 Patents (granted/published/pending). In the past, his Patents generated funding from Ontario Center of Excellence (OCE), Canada. He had performed industry interactive research extensively for more than 2 years with Calypto, Bluespec, BEECube, Huawei Canada during development of his Ryerson Design Space Exploration Tool arising from his Patent. For his excellence in research, he has been awarded & nominated by Ministry of Training, Colleges and Universities, Ontario for multiple years through OGS as well as by Ryerson University through GREA, RGA and NSERC ICA for consecutive years. He holds editorial positions in 7 IEEE & IET Journals in various capacities such as Associate Editor, Guest Editor and Columnist. He is currently serving as Associate Editor of IET Journal on Computer & Digital Techniques, Associate Editor & Columnist of IEEE Consumer Electronics (M-CE), Associate Editor of IEEE VLSI Circuits & Systems Letter (VCAL) and Associate Editor of IEEE Access Journal. He further serves as Guest Editor of special sections in IEEE Transactions on Consumer Electronics, IEEE Transactions on VLSI Systems and IEEE Access Journals. He is a regular reviewer of IET Journal on Computers and Digital Techniques, IEEE Transactions on VLSI Systems, Elsevier Journal on Swarm and Evolutionary Computation, Elsevier Journal on Applied Soft Computing and Elsevier Journal on Expert Systems. He regularly serves as a member of the Technical Program Committee of IEEE-CS ISVLSI, ACM GLVLSI, IEEE iNIS, IEEE CCECE and ICIT. He has supervised 4 Ph.D. candidates (2 completed and 2 pursuing) and 6 RA/B.Eng. students, many of whom are/were placed in reputed industries and renowned universities.

Prof. Saraju P. Mohanty (SM'08) is a Professor at the Department of Computer Science and Engineering (CSE), University of North Texas (UNT), where he directs the NanoSystem Design Laboratory (NSDL). He obtained a Ph.D. in Computer Engineering from the University of South Florida (USF) in 2003, a Master's degree in Systems Science and Automation (SSA) from the Indian Institute of Science (IISc), Bangalore, India in 1999, and a Bachelor's degree (Honors) in Electrical Engineering from Orissa University of Agriculture and Technology (OUAT), Bhubaneswar, India in 1995. Prof. Mohanty's research is in "Low-Power High-Performance Secure Electronic Systems". Prof. Mohanty's research has been funded by National Science Foundation (NSF), Semiconductor Research Corporation (SRC), and Air Force. Dr. Mohanty is an inventor of 4 US patents. Prof. Mohanty is an author of 200 peer-reviewed journal and conference articles, and 3 books. The publications are well-received by the world-wide peers with a total of 2500 citations leading to an h-index of 25 and i10-index of 67 (from Google Scholar). His latest book titled Nanoelectronic Mixed-Signal System Design is published by McGraw-Hill in 2015 is a best seller. This book received 2016 PROSE (Professional &

Scholarly Excellence) Award for best Textbook in Physical Sciences & Mathematics from the Association of American Publishers (AAP). Prof. Mohanty has been serving on the editorial board of several peer-reviewed international journals or transactions. He currently serves on the editorial board of 6 peer-reviewed international journals, including IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), ACM Journal on Emerging Technologies in Computing Systems (JETC), and IET Circuits, Devices & Systems Journal (CDS). He is the Editor-in-Chief of the IEEE Consumer Electronics Magazine. He serves as a founding Editor-in-Chief (EiC) of the VLSI Circuits and Systems Letter (VCAL). He has been serving as a guest editor for many prestigious journals including ACM Journal on Emerging Technologies in Computing Systems (JETC) and IEEE Transactions on Emerging Topics in Computing (TETC). Prof. Mohanty currently serves as the Chair of Technical Committee on Very Large Scale Integration (TCVLSI), IEEE Computer Society (IEEE-CS) to oversee a dozen of IEEE conferences. He serves on the organizing and program committees of several international conferences. He serves on the steering committee of the IEEE-CS Symposium on VLSI (ISVLSI). He is the founder conference chair for the IEEE International Symposium on Nanoelectronic and Information Systems (IEEE-iNIS). He was a conference chair for the IEEE-CS Symposium on VLSI (ISVLSI) 2012 and 2014. Prof. Mohanty is a senior member of IEEE and ACM. Prof. Mohanty has supervised 8 Ph.D. dissertations and 24 M.S. theses; seven of these advisees have received outstanding student awards at UNT. He has received Honors Day recognition as an inspirational faculty at the UNT for multiple years. He has also received UNT Provost's Thank a Teacher recognition for multiple years. More about his biography, research, education, and outreach activities can be obtained from his website: http://www.smohanty.org.

Prof. Fabrizio Lombardi (M'81–SM'02-F'09) graduated in 1977 from the University of Essex (UK) with a B.Sc. (Hons.) in Electronic Engineering. In 1977 he joined the Microwave Research Unit at University College London, where he received the Master in Microwaves and Modern Optics (1978), the Diploma in Microwave Engineering (1978) and the Ph.D. from the University of London (1982). He is currently the holder of the International Test Conference (ITC) Endowed Chair at Northeastern University, Boston. During 2007-2010 Dr. Lombardi was the Editor-In-Chief of the IEEE Transactions on Computers. Currently he is the Editor-In-Chief of the IEEE Transactions on Nanotechnology and the IEEE Transactions on Emerging Topics in Computing and serves as an elected Member of the Board of Governors of the IEEE Computer Society. His research interests are nano manufacturing/computing, VLSI design and fault/defect tolerance of digital systems. He has extensively published in these areas and coauthored/edited seven books.

Prof. **Mark Zwolinski** received the B.Sc. degree in electronic engineering and the Ph.D. degree in electronics from University of Southampton, Southampton, U.K., in 1982 and 1986, respectively. He is currently a Professor in the Dept .of Electronics and Computer Science, University of Southampton. He has authored two textbooks and has co-authored a third. He has written over 190 papers in the areas of EDA and test. His current research interests include high-level synthesis, fault tolerance, and behavioral modeling and simulation. He has supervised 30 PhD students to completion. Prof. Zwolinski is also a Fellow of IET and BCS and Senior Member of IEEE and ACM.