SIGDA Special Interest Group Design Automation
The resource for EDA Professionals

,
Online archive: http://www.sigda.org/publications/newsletter

Comments from the Editors

Dear ACM/SIGDA members,

We are excited to present to you September E-Newsletter. We encourage you to invite your students and colleagues to be a part of the SIGDA newsletter. The newsletter covers a wide range of information from the upcoming conferences and hot research topics to technical news and activities from our community. Get involved and contact us if you want to contribute an article or announcement.

The newly elected ACM SIGDA Executive team is looking for participants to engage with the SIGDA communication team and take leadership roles on restructuring the SIGDA website, communication channels, and outreach activities. We encourage and welcome volunteers to get involved and help us redesign the new image of SIGDA. If you are interested and want to know more, please get in touch with Dr. A. T. Sanial at todri@lirmm.fr.

Happy reading!

Debjit Sinha, Keni Qiu, Editors-in-Chief, SIGDA E-News

To renew your ACM SIGDA membership, please visit http://www.acm.org/renew or call between the hours of 8:30am to 4:30pm EST at +1-212-626-0500 (Global), or 1-800-342-6626 (US and Canada). For any questions, contact acmhelp@acm.org.

SIGDA E-News Editorial Board:

Back to Contents

SIGDA News

(1) "Tesla AI Day Perspectives"
[https://www.eetimes.com/tesla-ai-day-perspectives/]

Tesla’ s AI Day in mid-August featured the introduction of automotive chips, systems and software for machine learning and neural network training. Together, they will advance the training of models destined for self-driving cars.

(2) "Samsung Expands PIM Ambitions"
[https://www.eetimes.com/samsung-expands-pim-ambitions/]

Samsung Electronics Co., Ltd. announced another step in making processing-in-memory (PIM) technology more mainstream. The first successful integration of its PIM-enabled High Bandwidth Memory (HBM-PIM) into a commercialized accelerator system is part of a vision for incorporating PIM technologies into other memory types.

(3) "Intel Brings Chiplets to Data Center CPUs"
[https://www.eetimes.com/intel-brings-chiplets-to-data-center-cpus/]

Intel Corp.’ s fourth-generation Xeon processor, codenamed Sapphire Rapids, consists of four chiplets, the company revealed during its Architecture Day event.

(4) "Emerging Memories Look to Displace NOR, SRAM"
[https://www.eetimes.com/emerging-memories-look-to-displace-nor-sram/]

That’ s according to the annual report released jointly authored by Objective Analysis and Coughlin Associates. It’ s projecting emerging memories to be a $44 billion market by 2031 by displacing incumbent technologies including NOR flash, SRAM, and DRAM, either in the form of standalone memory chips and embedded memories within microcontrollers, ASICs, and even compute processors.

(5) "Vulnerability Disclosure Programs Need to Get Organized"
[https://www.eetimes.com/vulnerability-disclosure-programs-need-to-get-organized/]

Vulnerabilities that create potential security holes in Internet of things (IoT) and industrial control system (ICS) products just keep growing.

(6) "CrossBar Aims to Secure Computing with ReRAM"
[https://www.eetimes.com/crossbar-aims-to-secure-computing-with-reram/]

The company will apply its technology for use in hardware security applications in the form of ReRAM-based cryptographic physical unclonable function (PUF) keys that can be generated in secure computing applications. This is a departure from its usual use as non-volatile semiconductor memory, said CEO Mark Davis in a telephone interview with EE Times, and opens new markets for CrossBar’ s technology.

Back to Contents

"What is" Column

What is Homomorphic Cryptography?

Song Bian,
Assistant Professor,
Department of Informatics,
Kyoto University

The need for data privacy is recently highlighted both in the traditional software regime as well as the emerging hardware domain [1]. Being able to carry out complex computational tasks while preserving data privacy constitutes a novel field of research, and researchers from across the academic discipline work together in envisioning and implementing efficient and secure computing systems. As one of the most promising privacy-preserving computing primitives, homomorphic cryptography attracted major attention over the past decade. Within academia, significant progresses were made since Gentry first realized the idea of fully homomorphic encryption (FHE) [2]. Over the years, FHE schemes evolved in a fast pace, on both the theoretical [3, 4] and the practical levels [5, 6]. In the industry, the Defense Advanced Research Projects Agency (DARPA) has organized the Data Protection in Virtual Environments (DPRIVE) project which involves companies such as Duality Technology, Microsoft and Intel. In addition, many other technology companies such as Google, IBM, Alibaba, etc., are also building their own secure computing solutions over FHE.

The basic idea behind homomorphic cryptography is a set of encryption and decryption functions, (Enc,Dec). In addition to the traditional property where any input encrypted with some encryption key cannot be decrypted without the decryption key, a homomorphic encryption scheme includes an additional operator, Eval. For an encryption scheme to be homomorphic, it is important to ensure that f(x)=Dec(Eval(f,Enc(x))), for any input x and some function f. In other words, the evaluation of the function f over the encrypted version of x has to decrypt to f(x), thus permitting functions to be evaluated over ciphertexts. When f is restricted to the addition or multiplication operators, the encryption scheme is referred to as partially homomorphic encryption (PHE) [7]. If f can be arbitrary functions, then the encryption scheme is called FHE. Both PHE and FHE are widely adopted in secure multi-party computing (MPC) [8, 9, 10].

However, FHE (and in general many MPC protocols) faces the significant challenge of seriously degraded performance. For example, even in the most recent FHE application [], a single plaintext bit needs to be encrypted as a 16 Kbytes ciphertext, rendering the evaluations over ciphertexts at least 16,000 times less efficient than that over the plaintexts.

In summary, it is obvious that in the age of big data, private information processing has become an urgent need. While gaps still exist between currently available solutions and practical needs, as data privacy becoming increasingly important in our daily life, it is expected that homomorphic cryptography will play a critical role in an efficient and secure society.

References

[1] Semiconductor Research Corporation, The Decadal Plan for Semiconductors, Accessed on: Aug. 23, 2021. [Online]. Available: https://www.src.org/about/decadal-plan/.
[2] Gentry, C. (2009). A fully homomorphic encryption scheme. Stanford university.
[3] Gentry, C., Sahai, A., & Waters, B. (2013, August). Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In Annual Cryptology Conference (pp. 75-92). Springer, Berlin, Heidelberg.
[4] Chillotti, I., Gama, N., Georgieva, M., & Izabachène, M. (2020). TFHE: fast fully homomorphic encryption over the torus. Journal of Cryptology, 33(1), 34-91.
[5] Chen, H., Laine, K., & Player, R. (2017, April). Simple encrypted arithmetic library-SEAL v2. 1. In International Conference on Financial Cryptography and Data Security (pp. 3-18). Springer, Cham.
[6] Halevi, S., & Shoup, V. (2015, April). Bootstrapping for helib. In Annual International conference on the theory and applications of cryptographic techniques (pp. 641-670). Springer, Berlin, Heidelberg.
[7] Paillier, P. (1999, May). Public-key cryptosystems based on composite degree residuosity classes. In Annual International conference on the theory and applications of cryptographic techniques (pp. 223-238). Springer, Berlin, Heidelberg.
[8] Bian, S., Wang, T., Hiromoto, M., Shi, Y., & Sato, T. (2020). Ensei: Efficient secure inference via frequency-domain homomorphic convolution for privacy-preserving visual recognition. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 9403-9412).
[9] Matsuoka, K., Banno, R., Matsumoto, N., Sato, T., & Bian, S. (2021). Virtual Secure Platform: A Five-Stage Pipeline Processor over TFHE. In 30th USENIX Security Symposium (USENIX Security 21).
[10] Mishra, P., Lehmkuhl, R., Srinivasan, A., Zheng, W., & Popa, R. A. (2020). Delphi: A cryptographic inference service for neural networks. In 29th USENIX Security Symposium (USENIX Security 20) (pp. 2505-2522).

Back to Contents

Paper Submission Deadlines

WOSET'21 - Workshop on Open-Source EDA Technology (virtually co-located with ICCAD 2021)
San Diego, CA
Deadline: Sept. 7, 2021
Nov 4, 2021
https://woset-workshop.github.io

ISSCC'22 – IEEE Int'l Solid-State Circuits Conference
San Francisco, CA
Deadline: Sept 8, 2021
Feb 20-24, 2022
http://isscc.org

FPGA’22 – ACM/SIGDA Int’l Symposium on Field-Programmable Gate Arrays
Monterey, CA
Deadline: Sept 13, 2021
Feb 27 - Mar 1, 2022
http://www.isfpga.org

ISQED'22 - Int'l Symposium on Quality Electronic Design
California
Deadline: Sept 14, 2021
April, 2022

http://www.isqed.org

DATE'22 - Design Automation and Test in Europe
Antwerp, Belgium, and online
Deadline: Sept 19, 2021 (Abstracts due: Sept 12, 2021)
Mar 14-23, 2022
http://www.date-conference.com

ISPD’ 22 – ACM Int’ l Symposium on Physical Design
Banff, Alberta, Canada
Deadline: Oct 8, 2021 (Abstracts due: Oct 1, 2021)
Mar 27 - 30, 2022
http://www.ispd.cc

2nd ROAD4NN Workshop: Research Open Automatic Design for Neural Networks (Co-located with DAC 2021)
San Francisco, CA
Dec 5, 2021
https://easychair.org/cfp/ROAD4NN2021

Back to Contents

Upcoming Conferences and Symposia

MLCAD'21 - ACM/IEEE Workshop on Machine Learning for CAD
Virtual Conference
Aug 30 - Sept 3, 2021
https://mlcad.itec.kit.edu/

ASYNC'21 – IEEE Int’ l Symposium on Asynchronous Circuits and Systems
Virtual Conference
Sept 7-10, 2021
http://asyncsymposium.org

IWBDA'21 - Int'l Workshop on Bio-Design Automation
Online
Sept 20-24, 2021
http://www.iwbdaconf.org/2021

PACT'21 - Int'l Conference on Parallel Architectures and Compilation Techniques
Virtual Conference
Sept 26-28, 2021
http://www.pactconf.org

VLSI-SoC’ 21 – IFIP/IEEE Int’ l Conference on Very Large Scale Integration
Virtual conference
Oct 4-8, 2021
http://www.vlsi-soc.com

BioCAS'21 – Biomedical Circuits and Systems Conference
Berlin, Germany
Oct 7-9, 2021
https://2021.ieee-biocas.org/

ESWEEK'21 - Embedded Systems Week (CASES, CODES+ISSS, and EMSOFT)

Virtual Conference
Oct 10-15, 2021
http://www.esweek.org

NOCS'21 – IEEE/ACM Int’l Symposium on Networks-on-Chip (co-located with ESWEEK 2021)
Virtual Conference
Oct 14-15, 2021
https://nocs2021.github.io

MICRO’21 – IEEE/ACM Int'l Symposium on Microarchitecture
Athens, Greece
Oct 16-20, 2021
http://www.microarch.org/micro54

ICCD’21 – IEEE Int’l Conference on Computer Design
Virtual Conference
Oct 24-27, 2021
http://www.iccd-conf.com

BodyNets'21 – Int’l Conference on Body Area Networks
Virtual Conference
Oct 25-26, 2021
http://www.bodynets.org

ICCAD’21 – IEEE/ACM Int’l Conference on Computer-Aided Design
Virtual Conference
Nov 1-4, 2021
http://www.iccad.com

DAC’21 – Design Automation Conference
San Francisco
Dec 5–9, 2021
http://www.dac.com/

FPT'21 - Int'l Conference on Field-Programmable Technology
Auckland, New Zealand
Dec 6-10, 2021
http://icfpt.org

DAForum'21 - SIGDA/IEEE CEDA Ph.D. Forum at DAC 2021
San Francisco, CA
Dec 6, 2021
https://easychair.org/cfp/daforum21

HOST'21 – IEEE Int’l Symposium on Hardware-Oriented Security and Trust
Washington DC
Dec 12-15, 2021
http://www.hostsymposium.org

HiPC'21 – IEEE Int'l Conference on High Performance Computing, Data, And Analytics
Bangalore, India
Dec 17-20, 2021
http://www.hipc.org

iSES’21 – IEEE Int’l Symposium on Smart Electronic Systems
Jaipur, India

Dec 20-22, 2021
http://www.ieee-ises.org

ASP-DAC'22 - Asia and South Pacific Design Automation Conference
Virtual Conference
Jan 17-20, 2022
http://www.aspdac.com

Back to Contents

Call for Papers

ACM Transactions on Embedded Computing Systems (ACM TECS)
Special Issue on Domain-Specific System-on-Chip Architectures and Run-Time Management Techniques

Guest Editors:
- Umit Y. Ogras, University of Wisconsin (uogras@wisc.edu)
- Radu Marculescu, University of Texas, Austin (radum@utexas.edu)
- Trevor N. Mudge, University of Michigan, Ann Arbor (tnm@umich.edu)
- Michael Kishinevsky, Intel Corporation, (michael.kishinevsky@intel.com)

Domain-specific systems-on-chip (DSSoCs), a class of heterogeneous many-core systems, are recognized as a promising approach to narrow the performance and energy-efficiency gap between custom hardware accelerators and programmable processors. However, fulfilling this promise depends critically on addressing a number of fundamental research questions successfully. To this end, given a target domain, a designer has to come up with a suitable architecture and determine the set of hardware accelerators it must contain. Integrating too many accelerators would increase the design effort and cost. At the same time, leaving out critical accelerators can undermine the system energy efficiency and performance. Typically, a rich set of accelerators can bring the processing times down to nanosecond levels, hence the rest of the system components, such as the on-chip communication, must match the nanosecond level performance as well. DSSoCs must also provide software tools, application programming interfaces (APIs), and accelerator interfaces such that application developers can efficiently utilize them. Finally, a range of runtime management methodologies and algorithms are required to make the best use of the DSSoC resources. For example, existing scheduling algorithms predominantly consider homogenous systems or limited heterogeneity with a handful of types of CPU cores. Schedulers must cope with the increasing level of heterogeneity and a wide range of hardware accelerators by effectively utilizing all chip resources with negligible overhead. Similarly, novel dynamic thermal and power management algorithms are needed to orchestrate the operation of heterogeneous resources.

Starting from these overarching ideas, this special issue calls for research papers that address all aspects of domain-specific architectures, from novel application areas to runtime resource management algorithms and to hardware architecture.

For the full Call for Papers and submission instructions, go to:
https://dl.acm.org/pb-assets/static_journal_pages/tecs/pdf/cfp-domain-specific-s...

Important Dates:
- Open for submissions in ScholarOne Manuscripts: September 1, 2021
- Closed for submissions: October 1, 2021
- Results of first-round of reviews: November 15, 2021
- Submission of revised manuscripts: December 15, 2021
- Results of second-round of reviews: January 15, 2022
- Camera-ready Publication materials due: January 30, 2022

Please direct questions regarding this special issue to Guest Editors: Umit Y. Ogras (uogras@wisc.edu), Radu Marculescu (radum@utexas.edu), Trevor N. Mudge (tnm@umich.edu), Michael Kishinevsky (michael.kishinevsky@intel.com)

Back to Contents

SIGDA Awards

Awards at ISLPED 2021: ACM/IEEE International Symposium on Low Power Electronics and Design: http://www.islped.org/2021/final_program.php#FinalProgram

(1) Best Paper Award
Title: Statistical Optimization of Compute In-Memory Performance Under Device Variation
Authors: Brian Crafton (Georgia Institute of Technology)
Samuel Spetalnick (Georgia Institute of Technology)
Jong-Hyeok Yoon (Daegu Gyeongbuk Institute of Science and Technology)
Arijit Raychowdhury (Georgia Institute of Technology)

(2) Best Design Contest Award
Title: A Low-Power Neural Network Training Processor with 8-bit Floating Point with a Shared Exponent Bias and Fused-Multiply Add Trees
Authors: Jeongwoo Park, Sunwoo Lee, Dongsuk Jeon (Seoul National University)

Back to Contents

Technical Activities

1. “Emerging Memories Look to Displace NOR, SRAM”

Emerging memories are projected to be a $44 billion market by 2031, likely displacing NOR flash, SRAM, and DRAM...
[https://www.eetasia.com/emerging-memories-look-to-displace-nor-sram/]

2. “Intel process and architecture updates; AI in EDA attracting investors; Foxconn to add SiC and MEMS offering”

Catching up on some of the news from the last four weeks or so, Intel stands out with its late-July and mid-August announcements which we will briefly recall below...
[https://www.edacafe.com/nbc/articles/1/1861465/Intel-process-architecture-update...;-AI-EDA-attracting-investors;-Foxconn-add-SiC-MEMS-offering-by-Roberto-Frazzoli]

3. “Research Alliances Grow to Learn How 6G Will Play Out”

Many 6G research initiatives are appearing around the world as the significance of our dependence on fast, reliable networks is highlighted by the pandemic....
[https://www.eetimes.eu/research-alliances-grow-to-learn-how-6g-will-play-out/]

Job Openings:
----
1. University of Nottingham Department of Computer Science

Job Title: Assistant Professor in Computer Science

Description: £36914 to £49553 per annum (pro-rata if applicable) depending on skills and experience.

Salary progression beyond this scale is subject to performance. We are looking for people who complement our strengths by contributing new expertise in either: (i) our identified strategic growth areas, such as Embodied Intelligent Systems (Robotics and Cyber Physical Systems), Digital Health, Cyber Security and/or Computational Intelligence; or (ii) other areas across the whole span of computer science including (but not limited to) our existing research groups. See our recruitment microsite https://www.nottingham.ac.uk/jobs/currentvacancies/computer-science-opportunitie... for more information on our School’s vision, research strengths, and role within the university strategy. For successful international applicants, we provide financial support for your visa and the immigration health surcharge, plus an interest-free loan to help cover the cost of immigration-related expenses for any dependants accompanying you to the UK. For more information please see the our webpage on Financial support for visas and the immigration health surcharge.

2. Tokyo Institute of Technology School of Engineering, Japan

Job Title: Professor

Description: The successful candidate will be required to engage in education, research and administration for the Department of Systems and Control Engineering (Advanced measurement group AI applied measurement field, and Interdisciplinary Research Group/Super Bio Robotics Group). Please include details for each category. State if it was a keynote or invited lecture. For items a. and b., include the number of citations for , the total number of citations h-index, and name of database* used. Please download the template file from: http://www.jinjika.jim.titech.ac.jp/jobposting/apply_data_2021sce_professor1.xls.... Please send your application to: koubo_R3_3_at_sc.e.titech.ac.jp (please replace "_at_" with "@") The subject of the e-mail should be “Application for Professor of SCE”.

3. University of Maryland, USA

Job Title: Assistant Professor in Electrical and Computer Engineering

Description: The University of Maryland has made the safety of our students, faculty and staff, and our surrounding communities a top priority. As part of that commitment, the University System of Maryland (USM) recently announced that students, faculty, and staff on USM campuses this fall, including UMD, are required to be vaccinated against COVID. As a prospective and/or a new employee at UMD, you will be required to comply with the University’s vaccination protocol. Proof of full vaccination will be required before the start of employment in order to work at any University of Maryland location. Prospective or new employees may seek a medical or religious exemption to the vaccination requirement at return.umd.edu and must have an approved exemption prior to the start of their employment. An application should include a cover letter, curriculum vitae, a list with contact information of three references, examples of research achievements including three significant publications, a research statement (up to three pages, not including references), and a statement of teaching philosophy (up to two pages). The cover letter should include up to five concise keywords that best describe the applicant’s research expertise and areas of strength, and include URLs of Google Scholar, ORCID, and/or other weblinks outlining his/her work. Inquiries can be directed to ece@umd.edu . Posting Date: 08/09/2021; Open Until Filled Yes; Best Consideration Date: 12/01/2021.

Back to Contents

Notice to Authors

Notice to Authors

This newsletter is a free service for current SIGDA members and is added automatically with a new SIGDA membership.
Circulation: 2,700