sig da Special Interest Group Design Automation
The resource for EDA Professionals

1 May 2021, Vol. 51, No. 5
Online archive: http://www.sigda.org/publications/newsletter

Comments from the Editors

Dear ACM/SIGDA members,

We are excited to present to you May E-Newsletter.

First of all, we would like to remind you of an important thing in our community. Our members have probably received the email notice about SIGDA voting information for the next term. Please kindly go and vote for SIGDA Chair and Executive Committee for the term from 1 July 2021 to 30 June 2024.

We still 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 newsletter is evolving. Please let us know what you think.

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:

Debjit Sinha, E-Newsletter co Editor-in-Chief
Keni Qiu, E-Newsletter co Editor-in-Chief
Xiang Chen, E-Newsletter Associate Editor for SIGDA News column
Yanzhi Wang, E-Newsletter Associate Editor for SIGDA Local chapter news column
Pingqiang Zhou, E-Newsletter Associate Editor for SIGDA Awards column
Wanli Chang, E-Newsletter Associate Editor for SIGDA What is column
Xun Jiao, E-Newsletter Associate Editor for SIGDA What is column
Jayita Das, E-Newsletter Associate Editor for SIGDA Funding opportunities column
Qinru Qiu, E-Newsletter Associate Editor for SIGDA Live column
Yiyu Shi, E-Newsletter Associate Editor for SIGDA Live column
Rajsaktish Sankaranarayanan, E-Newsletter Associate Editor for SIGDA Researcher spotlight column
Xin Zhao, E-Newsletter Associate Editor for SIGDA Paper submission deadline column
Ying Wang, E-Newsletter Associate Editor for SIGDA Technical activities column

Back to Contents

SIGDA News

(1) "Biden Ups Ante to $50 Billion for CHIPS Act"
[https://www.eetimes.com/biden-ups-ante-to-50-billion-for-chips-act/]

US President Joe Biden’ s $2 trillion infrastructure plan announced in April increases the amount of funding that would be allocated to revive the American semiconductor industry to $50 billion.

(2) "TSMC Boosts Capital Budget Again, to $30B"
[https://www.eetimes.com/tsmc-boosts-capital-budget-again-to-30b/]

Taiwan Semiconductor Manufacturing Co. (TSMC) has again raised its 2021 capital expenditure target to $30 billion after customer demand exceeded the company’ s expectations three months ago.

(3) "AMD Keeps Building Momentum Through Q1"
[https://www.eetimes.com/amd-keeps-building-momentum-through-q1/]

AMD reported 2021 first quarter revenue of $3.45 billion, nearly doubling the $1.78 billion it tallied a year ago in Q1 of 2020. On a sequential basis, revenue was up 6% from the immediately preceding quarter.

(4) "Coup de Grace: Nvidia Enters CPU Market"
[https://www.eetimes.com/coup-de-grace-nvidia-enters-cpu-market/]

Nvidia has officially entered the CPU market with Grace, a data center CPU which is designed to accompany GPUs in at-scale AI and high performance computing (HPC) markets.

(5) "Synopsys Tackles SoC Design with Unified Circuit Simulation Flow"
[https://www.eetimes.com/synopsys-tackles-soc-design-with-unified-circuit-simulat...]

With chip design becoming increasingly complex with multiple components and technologies coming together in hyper-convergent integrated circuits (ICs), a single system approach to analyzing the system would be a logical way of simplifying the complexity.

(6) "Mavenir, Xilinx First with Open RAN Support for Massive MIMO"
[https://www.eetimes.com/mavenir-xilinx-first-with-open-ran-support-for-massive-m...]

Open RAN pioneer and cheerleader Mavenir and Xilinx have stolen a march on rivals with an end-to-end massive MIMO portfolio for 4G and 5G networks based on the emerging RAN technology specifications.

(7) "Ice Lake Launch: First Data Center CPU From Intel's Delayed 10nm Process"
[https://www.eetimes.com/ice-lake-launch-first-cpu-from-intels-delayed-10nm-proce...]

Intel has finally launched Ice Lake Xeon CPUs, its first data center CPU family to be built on the integrated device manufacturer's (IDM) delayed 10nm process technology.

(8) "Huang Harangue Heralds AV 'Trillions' "
[https://www.eetimes.com/huang-harangue-heralds-av-trillions/]

Today, the autonomous vehicles (AV) market is more promising than potent. It still has a long way to go before growing into a volume business. But that uncertainty did not stop Jensen Huang, Nvidia's CEO, from touting his company's plan to corner what he describes as a "multi-trillion-dollar transportation ecosystem."

(9) "Post GTC 2021 Analysis: Nvidia's Automotive News"
[https://www.eetimes.com/post-gtc-2021-analysis-nvidias-automotive-news/]

Nvidia made so many announcements and offered so much new information about so many different things at its GTC 2021 last week, it's hard to digest it all. Given that, I think it's worth compiling just the news pertaining to the automotive market, and summarizing and analyzing it.

(10) "Foxconn's EV Effort Likely Aimed at Enticing Apple"
[https://www.eetimes.com/foxconns-ev-effort-likely-aimed-at-enticing-apple/]

Foxconn's announcement of an electric vehicle alliance last month is very likely aimed at forming partnerships with companies that have an interest in entering the EV business, and none so much as Apple, according to people close to the world's largest electronics contract manufacturer.

Back to Contents

"What is" Column

What is The Recent Advance in Post-Quantum Cryptography?

Jiafeng (Harvest) Xie
Assistant Professor
Electrical and Computer Engineering Department, Villanova University

The recent advancement in quantum computing has initiated a new round of cryptographic engineering innovation since the existing public-key cryptosystems, such as Rivest Shamir Adleman (RSA) and elliptic curve cryptography (ECC), are proven to be vulnerable to the attacks launched from quantum computers employing Shor's algorithm [1], [2]. It is anticipated that a well-equipped quantum computer will become available in the next 10-15 years, alternative solutions are truly in desperate need. Post-quantum cryptography (PQC) refers to a class of cryptosystems that can resist quantum attacks, and the National Institute of Standards and Technology (NIST) has already started the PQC standardization process. The recent third round PQC finalists include four public-key encryption and three key-establishment algorithms, as well as eight alternative candidates [3].

In the recent second round of the NIST PQC standardization process, as seen from the status report, the selection of the third round PQC finalists is primarily based on the security analysis and considers the potential implementation complexity. In fact, the recent trend in the PQC field has gradually shifted to the implementation of the algorithms on different platforms [4].

Initially, only reference software implementations existed for the candidates, followed by some optimized software implementations. Then, the software/hardware and purely hardware

implementations were reported gradually, though not many [5-6]. This is because: (i) multiple changes in the functionality and parameter values of even well-established candidates, such as Rainbow and McEliece; (ii) the changes brought by the merging of the PQC scheme, e.g., the third round finalist, NTRU, is the merger of the previous NTRUEncrypt and NTRU-HRSS-KEM submissions; (iii) a significant percentage of candidates submitted to previous two rounds of the NIST standardization process has not been selected as finalists or partially broken and this uncertainty potentially hinders the on-going research in the related schemes.

Meanwhile, due to the mathematical and algorithmic complexity of the PQC algorithms and the limited amount of previous work, the workload for a single algorithm, especially for the hardware implementation, can take several months' diligent efforts. The related complexity reduction strategy, as well as the corresponding attack resistance, requires continual investigation. Unique implementation techniques for a certain algorithm under a specific application environment still need a major breakthrough.

Lastly, one has to mention that apart from the on-going NIST PQC standardization process, many aspects of the PQC research such as developing ultra low-complexity lightweight PQC schemes [7-9], are still interesting and underexplored. It is expected in the coming few years that quite a significant amount of work will be paid on this area.

Overall, though PQC field seems to be a little bit "mathematical" to the EDA community, it is highly anticipated that more and more chances will be given to the EDA community, especially in the implementation research and development aspects.

References

[1] W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," Symp. Founda. of Computer Science, pp. 124-134, 1994.
[2] Post-quantum cryptography round 3 submissions. https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions
[3] G. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, J. Kelsey, Y.-K. Liu, C. Miller, D. Moody, R. Peralta, et al., "Status report on the second round of the NIST post-quantum cryptography standardization process," US Department of Commerce, NIST, 202.
[4] J. Xie, K. Basu, K. Gaj, and U. Guin, "Special session: The recent advance in hardware implementation of post-quantum cryptography," 2020 IEEE 38th VLSI Test Symposium (VTS), pp. 1–10, IEEE, 2020.
[5] V. B. Dang, F. Farahmand, M. Andrzejczak, K. Mohajerani, D. T. Nguyen, and K. Gaj, "Implementation and benchmarking of round 2 candidates in the nist post-quantum cryptography standardization process using hardware and software/hardware co-design approaches," Cryptology ePrint Archive: Report 2020/795, 2020.
[6] K. Basu, D. Soni, M. Nabeel, and R. Karri, "NIST Post-Quantum Cryptography- A Hardware Evaluation Study," Cryptology ePrint Archive 2019/047, May 2019.
[7] A. Aysu, M. Orshansky, and M. Tiwari, "Binary Ring-LWE hardware with power side-channel countermeasures," Design, Automation & Test in Europe Conference & Exhibition (DATE). pp. 1253–1258, 2018.
[8] J. Xie, P. He, and W. Wen, "Efficient implementation of finite field arithmetic for binary Ring-LWE post-quantum cryptography through a novel lookup-table-like method," Design Automation Conference (DAC), pp. 1-6, 2021.
[9] P. He, U. Guin, and J. Xie, "Novel low-complexity polynomial multiplication over hybrid fields for efficient implementation of binary Ring-LWE post-quantum cryptography," IEEE JETCAS, pp. 1-6, 2021.

Back to Contents

Paper Submission Deadlines

VLSI-SoC’21 – IFIP/IEEE Int’l Conference on Very Large Scale Integration
Singapore
Deadline: May 3, 2021
Oct 5-7, 2021
http://www.vlsi-soc.com

IWLS'21 - International Workshop on Logic & Synthesis
Virtual conference
Deadline: May 10, 2021 (Abstracts due: May 10, 2021)
Jul 19-21, 2021
https://www.iwls.org

HOST'21 – IEEE Int’l Symposium on Hardware-Oriented Security and Trust
Washington DC
Deadline: May 11, 2021 (Abstracts due: Apr 27, 2021)
Dec 12-15, 2021
http://www.hostsymposium.org

BodyNets'21 – Int’l Conference on Body Area Networks
Virtual Conference
Deadline: May 13, 2021
Oct 25-26, 2021
http://www.bodynets.org

ICCAD’21 – IEEE/ACM Int’l Conference on Computer-Aided Design
Virtual Conference
Deadline: May 28, 2021 (Abstracts due: May 21, 2021)
Nov 1-4, 2021
http://www.iccad.com

FPT'21 - Int'l Conference on Field-Programmable Technology
Auckland, New Zealand
Deadline: Jul 19, 2021 (Abstracts due: Jul 12, 2021)
Dec 6-10, 2021
http://icfpt.org

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

ISLPED'21 Design Contest - The International Symposium on Low Power Electronics and Design
Virtual Conference
Deadline: May 15, 2021
July 26 – 28, 2021
http://www.islped.org/2021

Special Issue on Neuromorphic Computing Technologies - IEEE Transactions on Computers
Submission deadline: October 15, 2021 (submission site will be open 2 weeks before the deadline)
Scheduled to appear: July 2022
https://www.computer.org/digital-library/journals/tc/call-for-papers-special-iss...

Back to Contents

Upcoming Conferences and Symposia

FCCM' 21 - The 29th IEEE International Symposium On Field-Programmable Custom Computing Machines
Orlando, FL
May 9 – May 12, 2021
https://www.fccm.org/

RTAS'21 – 27th IEEE Real-Time and Embedded Technology and Applications Symposium
Nashville, USA
May 18-21, 2021
http://2021.rtas.org

MDTS'21 – IEEE Microelectronics Design & Test Symposium
Virtual workshop
May 18-21, 2021
http://natw.ieee.org

ISCA' 21 – Int' l Symposium on Computer Architecture
Valencia, Spain
May 22 – 26, 2021
https://iscaconf.org/isca2021/

ISCAS'21 – IEEE Int'l Symposium on Circuits and Systems
Daegu, Korea
May 23-26, 2021
http://iscas2021.org

LCTES' 21 – ACM Int' l Conference on Languages Compilers, Tools and Theory of Embedded Systems
Virtual conference
Jun 20-25, 2021
https://pldi21.sigplan.org/home/LCTES-2021

GLSVLSI' 21 – ACM Great Lakes Symposium on VLSI
Virtual Conference
Jun 22-25, 2021
http://www.glsvlsi.org

ICDCS'21 – IEEE Int'l Conference on Distributed Computing Systems
Virtual
Jul 7 - 10, 2021
https://icdcs2021.us/

ISVLSI' 21 – IEEE Computer Society Annual Symposium on VLSI
Tampa, Florida
Jul 7-9, 2021
http://www.ieee-isvlsi.org

DAC' 21 – Design Automation Conference
San Francisco
Jul 11–15, 2021
http://www.dac.com/

ISED' 21 – 10th Int' l Symposium on Embedded Computing & System Design
Kollam, India
Jul 16-18, 2021
http://isedconf.org

ISLPED’ 21 – ACM/IEEE Int’ l Symposium on Low Power Electronics and Design
Hybrid Zoom/Boston, MA
Jul 26-28, 2021
http://www.islped.org

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

ESWEEK'21 - Embedded Systems Week (CASES, CODES+ISSS, and EMSOFT)
Virtual Conference
Oct 10-15, 2021
http://www.esweek.org

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

Back to Contents

SIGDA Partner Journal

What is Security Threat in Approximate Computing Systems?

The ACM Transactions on Design Automation of Electronic Systems would like to invite you to read a literature review “Security Threat Analyses and Attack Models for Approximate Computing Systems: From Hardware and Micro-architecture Perspectives” by Dr. Qiaoyan Yu at the University of New Hampshire in the April 2021 issue. The full literature review may be found at the following link: https://dl.acm.org/doi/10.1145/3442380.

Approximate Computing (AC) techniques trade accuracy for performance improvement and energy efficiency, being increasingly attractive in various computation-intensive applications. Different than conventional computing, AC allows the computation to deviate from the reference or deterministic execution behaviors. Thus, AC has emerged as a new paradigm of computing systems, especially for applications such as image processing, audio recognition, information search, and artificial intelligence.

Approximation mechanisms have been successfully developed in system design, software, storage elements, and circuits for arithmetic accelerators. Most research efforts on approximate computing focus on developing new approximation mechanisms and implementation methods, rather than examining the security vulnerabilities of AC systems. Until recently, researchers [1, 2, 3, 4] start to notice that the utilization of approximate computing techniques could facilitate the adversary to create new attack surfaces to compromise computing systems. For instance, the work [5] shows that voltage- or frequency-overscaled approximate computations can reveal the identity of the approximate computing device. The work [2] introduces the new security threats originated from approximate memories, where a configuration signal in approximate DRAM is used as a trigger to degrade the performance of the system or cause a denial of service. Another recent work [6] highlights that the boundary between precise and approximate modules could be leveraged to develop a new attack surface on future computing systems.

A comprehensive study on security challenges brought by various approximation techniques is conducted in the work [7]. As concluded, it is imperative to investigate the security threats on AC systems due to the following reasons: (1) as different abstraction layers have diverse approximation

mechanisms, it is difficult to formulate the security problem in a systematic manner; (2) there does not exist a unified framework to standardize the procedure for discovering the security vulnerabilities of AC systems; (3) because AC systems can inherently tolerate errors with respect to precise operations or allow the output to deviate from the original specification, the metrics adopted for functional verification are typically based on the average accuracy. The statistical average accuracy leaves intelligent attackers a room to immerse the attack effect in the inherently tolerable errors. The work [7] further proposes four kinds of unique attacks that could harm the reliability, integrity and security of AC systems: building covert channel attack, error compensation attack, tampering error resilience mechanism attack, and accelerating error propagation attack. Those attacks are generalized at a high level and demonstrated in arithmetic units, memory, and practical applications. Moreover, the general guideline for feasible defense methods is suggested to inspire more researchers in the approximate computing community.

The ACM Transactions on Design Automation of Electronic Systems (TODAES), the premier ACM journal in design and automation of electronic systems and a closer partner of SIGDA, has a new Editorial Board since June 1, 2020. It is calling for submission of Special Issue proposals as well as tutorials, surveys and the newly established Designer Notes. You can find TODAES' s updated scope at https://dl.acm.org/journal/todaes/about.

[1] W. Liu, F. Lombardi, and M. Shulte. 2020. "A Retrospective and Prospective View of Approximate Computing," in Proc. IEEE 108 (03 2020), pp. 394–399.
[2] P. Yellu, N. Boskov, M. A. Kinsy, and Q. Yu. 2019. "Security Threats in Approximate Computing Systems," in Proc. GLSVLSI' 19, pp. 387–392.
[3] F. Regazzoni, C. Alippi, and I. Polian. 2018. "Security: The Dark Side of Approximate Computing?" in Proc. ICCAD' 2018, pp. 1–6.
[4] Y. Wang, J. Dong, Q. Xu, and Z. Lu. 2020. "Is It Approximate Computing or Malicious Computing?" in Proc. GLSVLSI' 2020, pp. 333–338.
[5] S. Keshavarz and D. Holcomb. 2017. "Privacy leakages in approximate adders," in Proc. 2017 IEEE International Symposium on Circuits and Systems (ISCAS), pp. 1–4.
[6] P. Yellu, L. Buell, D. Xu, and Q. Yu. 2020. "Blurring Boundaries: A New Way to Secure Approximate Computing Systems," in Proc. GLSVLSI' 2020, pp. 327–332.
[7] P. Yellu, L. Buell, M. Mark, M. Kinsy, D. Xu, and Q. Yu, "Security Threat Analyses and Attack Models for Approximate Computing Systems: From Hardware and Micro-Architecture Perspectives," ACM Trans. Des. Autom. Electron. Syst. 26, 4, Article 32 (February 2021), 31 pages.

Back to Contents

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