Proceedings of the

IEEE International Symposium on Hardware Oriented Security and Trust (HOST2020)

7 – 11 December 2020 | VIRTUAL CONFERENCE

Part Number: CFP20HOA-ART
ISBN: 978-1-7281-7405-1

Technical support & inquiries

Research Publishing Services

Singapore: t:+65-6492 1137, f:+65-6747 4355

India: t: 044-42178617, 044-24330060

e:enquiries@rpsonline.com.sg

Welcome Message

On behalf of the organizing and steering committees, it is our tremendous pleasure to welcome you to the 2020 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST). HOST 2020 was originally set to take place in San Jose, CA on May 4-7, 2020 for better engagement with companies in Silicon Valley. However, it was postponed due to the COVID-19 pandemic and is taking place in December 7-11, 2020 on the Underline virtual platform. Nevertheless, we expect even greater attendance online as compared to the physical event from the last several years.

IEEE HOST has emerged as a premier event in hardware security encompassing all aspects of research and development in this area of growing significance. The mission of HOST, which is heavily reflected in the HOST 2020 program, can be summarized as follows:

- To be a leading and globally recognized forum that unites researchers, practitioners, and users from the computer security, microelectronics, and EDA communities.
- To disseminate cutting-edge ideas, technologies, and results in areas of overlap between hardware and security – from device, architecture, chip, and systems levels.
- To provide a platform for leaders in industry, government, and academia to share their unique perspectives and to help shape the direction and priorities of the community.
- To address shortages in the security workforce by recruiting and training students from a diverse group for productive careers with prospective employers

IEEE HOST 2020 is a 5-day virtual event. There are 6 tutorials on Monday, December 7th delivered by leading experts from academia and industry on diverse topics such as physical inspection for hardware assurance, AI and deep learning in hardware security, security-aware computer aided design (CAD), and side channel analysis. The tutorial day ends with a student-mentorship networking event, organized by the IEEE Computer Society and HOST, where students interact with industrial sponsors about future careers and employment. The main technical program occurs on December 8-11, and includes 4 keynotes, 1 visionary talk, 3 panels, a record-high 30 technical papers, 22 student hardware demos, 17 posters, and the first ever industrial exhibition. The exhibition includes virtual booths, 2 elevator pitch sessions, and birds-of-feather sessions.

The invited speakers for HOST 2020 showcase some of the most innovative and diverse thinkers in the world on hardware security. Our keynote speakers include David Patterson (UC Berkeley professor, Google distinguished engineer, and RISC-V Foundation Vice-Chair), Rob Aitken (R&D Fellow at ARM), Deirdre Hanford (Chief Security Officer at Synopsys), and Brian Dupaix (Air Force Design Assurance Lead at the AFRL Sensors Directorate and Acting Data Driven Quantifiable Assurance Project Area Lead for the Office of the Secretary of Defense (OSD) Trusted & Assured Micro electronics / MINSEC program).The program also features a visionary talk by Bill Mazzara (Global Vehicle Cyber security Technical Fellow at Fiat-Chrysler Automobiles). This year's program also offers three timely technical panels, “RISC V and Security – Opportunities and Challenges”, “Quantifiable Assurance: The Good, the Bad and the Future and “High-Level Synthesis: Facts, Myths and Fantasies” which include prominent speakers from industry, academia, as well as government.The call for papers of HOST 2020 employed a two-step procedure, where authors first registered their abstracts and subsequently submitted the full manuscripts. For the first time in its history, HOST had two submission deadlines – one on August 15, 2019 and the other on November 15, 2019. In total, we received 110 abstracts. Of those registered abstracts, we received 104 full manuscripts. The HOST 2020 review process consisted of four phases: Round 1, Round 2, Rebuttal, and Deliberation. In Round 1, two reviewers were assigned to each of the manuscripts using the automatic assignment feature in HotCRP (https://hotcrp.com/), which considers TPC member preference as well as conflict of interests (COIs) between the TPC members and authors. Manuscripts with low scores were rejected at the end of Round 1. The surviving manuscripts moved on to Round 2 where they received at least 1 additional review. From those Round 2 assignments, 83% of manuscripts received 4 or more reviews in total. During the Rebuttal phase, thereviews were sent to authors, and the authors submitted a 1000-word response. The Deliberation phase began when the Program Chairs shared rebuttals with the reviewers. The Program Chairs carefully read the reviews and responses, and facilitated online discussions among the reviewers. We were able to achieve consensus on the acceptance status for all papers. This year, each accepted paper received 10 pages (plus references) in the proceedings and a 20-minute video presentation at the conference. The final program has 30 full papers, which represents a 30/104 = 28.8% acceptance rate.

To accommodate term limits, review homogeneity, and HOST's large scope, the HOST 2020 Technical Program Committee (TPC) members were selected using the procedure developed in 2019. The Program Chairs tracked the number of years each candidate has served on the TPC. Past and potential TPC members outline their top ten topics of expertise in hardware and systems security. The past Program Chairs scored past and potential TPC members in terms of participation in HOST, quality of prior reviews, etc. This information was provided to a constrained optimization program. TPC members that maximized a cost function related to the TPC evaluation criteria while meeting constraints on topic areas, diversity, etc. were selected for the HOST 2020 TPC. During the review process, the Program Chairs also recruited additional TPC members as needed.As a virtual event, HOST 2020 offers exciting and innovative ways for attendees, speakers, and sponsors to interact and participate. The Underline platform provides an easy-to-scan schedule containing all of HOST 2020's sessions. The keynote, visionary, and panels take place live on its "main stage" for the most seamless experience for both speakers and attendees. Session moderators manage Q&A both live and through real-time chat. Each session on the main stage is recorded and made available to attendees after the event in case they missed the live session or want to view the session again. 5-minute videos from exhibitors also appear on the main stage in order to introduce the audience to the exhibitors and encourage them to visit their virtual booths. 20-minute videos of accepted papers and 5-minute videos of student hardware demos are available to the attendees "on-demand" before, during, and after the event. Interactive Q&A sessions are held for groups of papers and demos throughout the program. The student poster session uses virtual rooms for each poster where attendees can privately view each poster and speak with the author using video or real-time chat. Networking is viewed as one of the most important aspects of HOST. During sessions and the 30-minute breaks between sessions, attendees can mingle using Gather. Gather offers proximity video chat in 2D interactive spaces and allows attendees to walk in and out of conversations as naturally as at a real conference. To encourage participation in all HOST sessions and breaks, the organizers have developed a unique attendee tracking system. Attendee that show the highest level of participation (i.e., asking questions, attending exhibition, judging competitions, networking during breaks, etc.) each day will be rewarded with prizes and giveaways during and after the event.

HOST 2020 would not be possible, especially in the wake of the pandemic, without the outstanding support and efforts from a variety of sources. First, we are grateful to all our sponsors, including the Gold Sponsors (Cisco, Riscure, and Synopsys), the Silver Sponsors (Arm, Boeing, Intel, NewAE, and Qualcomm), the Exhibitors (Battelle, EDAptive Computing, OneSpin, Rambus, and Tortuga Logic) and the Organizational Sponsors (IEEE, IEEE Computer Society, IEEE Test Technology Technical Council, and IEEE Technical Committee on Security and Privacy). The National Science Foundation (NSF) and Cisco also provided support in the form oftravel grants for domestic and international students, respectively. This year, we were able to support more than 100 students, most of them from underrepresented groups and many who would not have had the opportunity to attend HOST otherwise. Next, we would like to sincerely thank all the volunteers from the organizing committee, steering committee, technical program committee, tutorial committee, awards selection committees (judges), student travel grant committee, and session chairs/moderators. Third, we thank our media partners (JLPEA, Sensors, and IEEE S&P) for publicizing HOST. Fourth, we would like to acknowledge the entire Underline team, especially Darrell Gunter, Daniel Luise, and Jernej Masnec. Last but not least, we'd like to express our gratitude to the IEEE Computer Society for their outstanding efforts and devotion in planning and marketing the event, recruiting and communicating with sponsors, and tracking attendee participation. This includes Paula Anderson, Michelle Tubb, Laura Perry, Regan Pickett, Katherine Mansfield, Georgann Carter, Amir Draquez, Patrick Kellenberger, and Stephen Woods.

Committee

Organizing Committee

General Chairs: Domenic Forte, *University of Florida*
Program Chairs: Yousef Iskander, *Cisco Systems*
Vice-program Chairs: Saverio Fazzari, *Booz Allen Hamilton and* Jim Plusquellic, *UNM*
Finance Chair: Vincent Mooney, *Georgia Tech*
Publicity Chair: Farimah Farahmandi, *University of Florida*
Registration Chair/Vice Finance: Ioannis Savidis, *Drexel University*
Panel Chairs: Rosario Cammarota, *Intel and* Waleed Khalil, *OSU*
Tutorial Chair: Sheng Wei, *Rutgers University*
Hardware Demo Chairs: Fareena Saqib, *University of North Carolina at Charlotte and* Adam Kimura, *Battelle*
Exhibition Chair: Mark Tehranipoor, *University of Florida* and Greg Creech, *GLC Consulting, LLC*
Poster Chair: Kyle Juretus, *Villanova University*
Publications/AV Chair: Mehran Mozaffari Kermani, *University of South Florida*
AV Co-Chair: Robert Karam, *University of South Florida*
Industrial Liaison Chair: Vivek De, *Intel*
European Liaison: Amir Moradi, *Ruhr-Universität Bochum*
Asia-Pacific Liaison: Xiaowei Li, *Chinese Academy of Sciences*
Web Chair: Wei Hu, *Northwestern Polytechnical University*

Steering Committee

Mark Tehranipoor (Chair), *University of Florida*
Jim Plusquellic, *University of New Mexico*
Farinaz Koushanfar, *University of California, San Diego*
Swarup Bhunia, *University of Florida*
Ramesh Karri, *Polytechnic Institute of New York University*
Ryan Kastner, *University of California, San Diego*
Domenic Forte, *University of Florida*
Yousef Iskander, *Cisco Systems*

Technical Program Committee

Adam Duncan, *Naval Surface Warfare Center*
Avesta Sasan, *George Mason University*
Aydin Aysu, *NCSU*
Calvin Chan, *University of New Mexico*
Chengmo Yang, *University of Delaware*
Dmitry Ponomarev, *Binghampton University*
Farhad Merchant, *RWTH Aachen University*
Francesco Regazzoni, *ALaRI Institute of Università della Svizzera italiana*
Francois-Xavier Standaert, *UC Louvain*
Gang Qu, *University of Maryland*
Guru Venkataramani, *George Washington University*
Hai Zhou, *Northwestern*
Ingrid Verbauwhede, *KU Leuven*
Itamar Levi, *UC Louvain*
Jakub Szefer, *Yale University*
Jeyavijayan Rajendran, *Texas A&M University*
Jiafeng Xie, *Villanova University*
Kevin B. Bush, *MIT Lincoln Lab*
Lee Lerner, *GTRI*
Mahida Gul, *Howard University*
Matt French, *USC ISI*

Matthew Areno, *Intel*
Matthew Hicks, *Virginia Tech*
Meng Li, *University of Texas*
Michael Orshansky, *University of Texas*
Naghmeh Karimi, *University of Maryland, Baltimore County*
Prabhat Mishra, *University of Florida*
Rajat Chakraborty, *Indian Institute of Technology, Kharagpur*
Rashmi Jha, *University of Cincinnati*
Ro Cammarota, *Intel*
Ryan Helinski, *Sandia National Lab*
Ryan Kastner, *University of California, San Diego*
Svetla Nikova, *KU Leuven*
Shahin Tajik, *University of Florida*
Swarup Bhunia, *University of Florida*
Taimour Wehbe, *Renesas*
Todd Austin, *University of Michigan*
Ujjwal Guin, *Auburn University*
Vincent Immler
Vivek Venugopal, *USC ISI*
William Diehl, *Virginia Tech*
Xinfei Guo, *University of Virginia*
Yousef Iskander, *Cisco Systems*

Hardware Tutorial Committee

Sheng Wei, *Rutgers University (Chair)*
Yousef Iskander, *Cisco*
Nael Abu-Ghazaleh, *University of California, Riverside*
Xiaolin Xu, *University of Illinois at Chicago*
Adib Nahiyan, *Intel*
Laurent L. Njilla, *AFRL*

Student Travel Grant Committee

Yier Jin, *University of Florida (Chair)*
Gang Qu, *University of Maryland*
Ryan Kastner, *University of California, San Diego*
Domenic Forte, *University of Florida*
Xiaolong Guo, *Kansas State University*

Keynote & Visionary Talk

Keynote I	**Put Up or Shut Up: Advancing Security by Creation, not Criticism**
Date / Time	December 8, 2020 (Tuesday) / 12:30 – 13:15 hrs
Speaker	**David Patterson** *Professor, UC Berkeley*
Co-Chairs	**Jim Plusquellic** and **Saverio Fazzari**

Abstract

When proprietary architectures and proprietary operating systems dominated the information technology industry, the only option available to security experts was to point out the flaws in proprietary hardware-software systems. The hope was that companies would learn from their mistakes, but security remains the Achilles Heel of information technology.

The time for contribution by criticism is past. The security community should evolve to advancing the state of the art by trying to build secure systems and test them in the real world.

Open source operating systems like Linux have been the norm since at least 2010, and in 2020 the RISC-V open instruction set and open source implementations of RISC-V are commercially viable. Open architectures, open-source implementations, and open-source software stacks, plus the plasticity of Field Programmable Gate Arrays (FPGAs) mean engineers can deploy and evaluate novel solutions online and iterate them weekly instead of every few years. While FPGAs are 10× slower than custom chips, such performance is still fast enough to support online users and thus subject security innovations to real attackers.

Moreover, while there are financial incentives for companies to continually increase the complexity of their proprietary architectures, there is little technical reason to do so. The simplicity of the industrial strength RISC-V architecture enabled formal specifications of its instruction set and makes its open source implementations easier to check and enhance.

Finally, proprietary operating systems and architectures limit innovation to employees of those companies, but open operating systems and open architectures allow everyone to innovate.

In 2020, anyone can demonstrate their ideas by enhancing realistic hardware-software systems. It's time for security experts to put up or shut up.

Biography

David Patterson is a UC Berkeley professor of the graduate school, a Google distinguished engineer, and the RISC-V Foundation Vice-Chair. He received his BA, MS, and PhD degrees from UCLA. His Reduced Instruction Set Computer (RISC), Redundant Array of Inexpensive Disks (RAID), and Network of Workstation projects helped lead to multibillion-dollar industries. This work led to about 40 awards for research, teaching, and service plus many papers and seven books. The best known book is Computer Architecture: A Quantitative Approach and the newest is The RISC-V Reader: An Open Architecture Atlas. He and his co-author John Hennessy shared the 2017 ACM A.M Turing Award.

Keynote II	**It's time to tame the wild west of IoT device security**
Date / Time	December 9, 2020 (Wednesday) / 12:00 – 12:45 hrs
Speaker	**Rob Aitken** *R&D Fellow, ARM*
Co-Chairs	**Yousef Iskander** and **Saverio Fazzari**

Abstract

The Internet of Things is increasingly transformingour lives, but IoT devices have often been attractive targets for hackers, not only as gateways to higher value targets but also because low cost devices often lack security features of higher priced systems. Given recent progress in hardware security, we have reached the point where this situation can be addressed. We as a community can define and support standardized capabilities and features of security hardware and on-chip security services. We can also show they can be integrated into designs where cost and time to market are key drivers andprovide standardized mechanisms toconnect them with existing software platforms. This talk looks at how the hardware security community can make that happen and the benefits of doing so.

Biography

Rob Aitken is an Arm Fellow responsible for technology direction at Arm Research. He works onhardware security issues, low power design, and emerging technologies. He has worked on 15+ Moore's law nodes and has published over 100 technical papers on a wide range of topics. Dr. Aitken joined Arm as part of its acquisition of Artisan Components in 2004. Prior to Artisan, he worked at Agilent and HP. He holds a Ph.D. from McGill University in Canada. Dr. Aitken is anIEEE Fellow, and serves on a number of conference and workshop committees.

Keynote III	**The Role of Security and Test in the New Era of Silicon Lifecycle Management**
Date / Time	December 10, 2020 (Thursday) / 12:00 – 12:45 hrs
Speaker	**Deirdre Hanford** *Chief Security Officer, Synopsys*
Co-Chairs	**Domenic Forte** and **Yousef Iskander**

Abstract

At an unprecedented rate, advanced safety and personal applications are becoming commonplace, while the corresponding software, systems and silicon are increasingly interconnected. These trends have raised all aspects of security to a new level of importance, including the secure design and test of each silicon part. Engineering teams typically focus on optimizing power, performance, and area (PPA), but also must meet stringent goals for manufacturing quality, reliability and resiliency. These non-PPA goals are met through the use of advanced test technologies and robust safeguards addressing post-manufacturing defects, such as soft errors and aging-related phenomena. However, improving a design's testability may leave it more vulnerable to attacks and unauthorized access. To address these issues, existing and upcoming technologies will ensure the security and integrity of silicon test data and its access. With enhanced silicon security, new and innovative uses of reliable chip data will arise such as system health monitoring across the entire silicon lifecycle. Cloud-based analysis of silicon metrics, securely gathered from on-chip instruments, will allow pre-emptive actions and optimizations, raising system safety, reliability, and security to unprecedented levels.

Biography

Deirdre serves as the Chief Security Officer for Synopsys. In this role, she works collaboratively to safeguard Synopsys. In addition, she leads efforts to drive industry awareness and enablement for secure design from software to silicon to support our business in EDA, IP and Software Integrity. She previously served as co-general manager of Synopsys' Design Group, responsible for leading the development and deployment of our physical design, implementation, and analog/mixed-signal product lines. Deirdre has held a number of positions at Synopsys since joining the company in 1987, including leadership roles in customer engagement, applications engineering, sales, and marketing.

She earned a B.S.E.E. from Brown University and an M.S.E.E. from UC Berkeley. In 2001, Deirdre was a recipient of the YWCA Tribute to Women and Industry (TWIN) Award and the Marie R. Pistilli Women in EDA Achievement Award. Ms. Hanford served as the Chairman of American Electronics Association in 2008. She currently chairs Brown University's Engineering Advisory Committee and serves on the Engineering Advisory Board for UC Berkeley's College of Engineering. Deirdre also serves on the Board of Directors of Cirrus Logic, Inc

Keynote IV	**Zero Trust Microelectronics: A Model for Hardware Security Evolution**
Date / Time	December 10, 2020 (Thursday) / 15:30 – 16:15 hrs
Speaker	**Brian Dupaix** *Air Force Design Assurance Lead, AFRL*
Co-Chairs	**Saverio Fazzari** and **Domenic Forte**

Biography

Dr. Brian Dupaix currently serves as the Acting Data Driven Quantifiable Assurance Project Area Lead for the Office of the Secretary of Defense (OSD) Trusted &Assured Microelectronics / MINSEC program, managing a research and development budget of over $250M per year. Concurrently, he serves as the Air Force Design Assurance Lead at the AFRL Sensors Directorate in Dayton, Ohio, and is an adjunct professor at The Ohio State University. Dr. Dupaix holds a BS degree Brigham Young University and MS and PhD degrees from The Ohio State University. Prior to joining AFRL, he was a Research Scientist at Ohio State's ElectroScience Laboratory, working on high-speed DACs and ADCs, III-V power-amplifiers, mixed-signal reliability, and trusted electronic components. He also worked in industry, spending 5 years at Honeywell Air Transport Systems, designing digital ASICs for commercial flight and navigation systems and 4 years at Intrinsix creating IP blocks for extensible processors and System-on-Chip ASICs for consumer electronics. He has published over 40 papers and holds five patents with several pending.

Visionary Talk	**Not Just Security, Hardware Protected Security**
Date / Time	December 11, 2020 (Friday) / 12:00 – 12:30 hrs
Speaker	**Bill Mazzara** *Global Vehicle Cybersecurity Technical Fellow, Fiat-Chrysler Automobiles*
Co-Chairs	**Jim Plusquellic** and **Domenic Forte**

Abstract

This Presentation will make the case for Hardware Protected Security in the Auto Industry. Outlining the use cases which drive the need the points of the newly published SAE standard for hardware Security will be introduced. This presentation will elaborate on the applications of Hardware Protected Security and elaborate on the state of the art in the auto industry.

Biography

Bill Mazzara, a technical fellow of global vehicle cybersecurity, he is the SAE Vehicle Electrical System Hardware Security Subcommittee Chair which has published SAE J3101.
He also serves on the SAE/ISO Joint Working Group for Road Vehicles Cybersecurity Engineering which has published ISO/SAE 21434DIS.

Having begun his career as a test engineer during the infancy of the connected car, Mazzara has witnessed and been a driving force in the evolution of the field being granted 29 related patents in the process. As it became apparent that the lack of cybersecurity was an unfortunate oversight of the connected car, Bill became part of the solution. Mazzara served on the response team charged with addressing what is widely considered one of the automotive industry's first cybersecurity incidents against a passenger vehicle, the incident chronicled in 2010 study by researchers from the Universities of California San Diego and Washington.

A Certified Information Systems Security Professional(CISSP), Mazzara holds a bachelor's degree in Electrical Engineering from the University of Notre Dame in addition to masters' degrees in wireless communications and business administration.

Panel

Wednesday 12/9 2-2:30pm ET:

Panel I: RISC V and Security – Opportunities and Challenges
Moderators:
Radu Teodorescu: *The Ohio State University*
Saverio Fazzari: *Booz Allen Hamilton*
Panelists:
Keith Rebello: *DARPA*
Krste Asanović: *University of California Berkeley*
Jason Oberg: *Tortuga Logic*
David Kohlbrenner, *University of Washington*
Helena Handschuh, *Rambus*

Thursday 12/10 1:30-3pm ET:

Panel II: Quantifiable Assurance: The Good, the Bad and the Future
Moderators:
Jim Plusquellic: *University of New Mexico*
Waleed Khalil: *The Ohio State University*
Panelists:
Matt Casto: *OSD, Casto*
Mike Borza: *Synopsys*
Saverio Fazzari: *Booz Allen Hamilton*
Nicholas D. Pattengale: *Sandia National Laboratories*
Mark Tehranipoor: *University of Florida*

Friday 12/11 3:30-5pm EST:

Panel III: High-Level Synthesis: Facts, Myths and Fantasies
Moderators:
Farimah Farahmandi: *University of Florida*
Mark Tehranipoor: *University of Florida*
Panelists:
John Goodenough: *ARM*
Wally Rhines: *Cornami*
Ryan Kastner: *UCSD*
Hamid Shojaee: *Google*
Luke Duncan: *Centauri*

Technical Programme

Session 1	**Side Channel Attack and Mitigation 1**
Date/Time	December 8, 2020 (Tuesday) / 14:30 – 14:50 hrs
Session Co-Chairs	**Aydin Aysu and Jim Plusquellic**

A Novel Golden-Chip-Free Clustering Technique Using Backscattering Side Channel for Hardware Trojan Detection**
Luong N. Nguyen, Baki Berkay Yilmaz, Milos Prvulovic and Alenka Zajić

Template Attacks Against ECC : practical Implementation Against Curve25519
Antoine Loiseau, Maxime Lecomte and Jacques J. A. Fournier

PARAM: A Microprocessor Hardened for Power Side-Channel Attack Resistance**
Muhammad Arsath K F, Vinod Ganesan, Rahul Bodduna and Chester Rebeiro

BitJabber: The World's Fastest Electromagnetic Covert Channel**
Zihao Zhan, Zhenkai Zhang and Xenofon Koutsoukos

Encoding Power Traces as Images for Efficient Side-Channel Analysis
Benjamin Hettwer, Tobias Horn, Stefan Gehrer and Tim Güneysu

Session 2	**SoC Security**
Date/Time	December 8, 2020 (Tuesday) / 14:30 - 14:50 hrs
Session Co-Chairs	**William Diehl and Dmitry Ponomarev**

Thwarting Control Plane Attacks with Displaced and Dilated Address Spaces
Lauren Biernacki, Mark Gallagher, Valeria Bertacco and Todd Austin

Application-Specific Instruction Set Architecture for an Ultralight Hardware Security Module
Ahmed A. Ayoub and Mark D. Aagaard

Going Deep: Using deep learning techniques with simplified mathematical models against XOR BR and TBR PUFs (Attacks and Countermeasures)
Mahmoud Khalafalla, Mahmoud A. Elmohr and Catherine Gebotys

Bit 2 RNG: Leveraging Bad-page Initialized Table with Bit-error Insertion for True Random Number Generation in Commodity Flash Memory
Wei Yan, Huifeng Zhu, Zhiyuan Yu, Fatemeh Tehranipoor, John Chandy, Ning Zhang and Xuan Zhang

Secure Boot from Non-Volatile Memory for Programmable SoC Architectures
Franz-Josef Streit, Florian Fritz, Andreas Becher, Stefan Wildermann, Stefan Werner, Martin Schmidt-Korth, Michael Pschyklenk and Jürgen Teich

Session 3	**Anti-counterfeit, Anti-tamper and Side-Channel**
Date/Time	December 9, 2020 (Wednesday) / 15:30 - 15:45 hrs
Session Co-Chairs	**Ujjwal Guin and Fareena Saqib**

- **Towards the Avoidance of Counterfeit Memory: Identifying the DRAM Origin**
  B. M. S. Bahar Talukder, Vineetha Menon, Biswajit Ray, Tempestt Neal and Md Tauhidur Rahman

- **Hardware/Software Obfuscation against Timing Side-channel Attack on a GPU**
  Elmira Karimi, Yunsi Fei and David Kaeli

- **Latch-Based Logic Locking****
  Joseph Sweeney, Mohammed Zackriya V, Samuel Pagliarini and Lawrence Pileggi

Session 4	**CAD Tools and Privacy**
Date/Time	December 9, 2020 (Wednesday) / 15:30 - 15:45 hrs
Session Co-Chairs	**Ioannis Savidis and JV Rajendran**

- **CPU and GPU Accelerated Fully Homomorphic Encryption**
  Toufique Morshed, Md Momin Al Aziz and Noman Mohammed

- **ReGDS: A Reverse Engineering Framework from GDSII to Gate-level Netlist**
  Rachel Selina Rajarathnam, Yibo Lin, Yier Jin and David Z. Pan

- **Evaluating Security Specification Mining for a CISC Architecture**
  Calvin Deutschbein and Cynthia Sturton

Session 5	**Side Channel Attack and Mitigation 2**
Date/Time	December 10, 2020 (Thursday) / 12:45 - 13:00 hrs
Session Co-Chairs	**Robert Karam and Lang Lin**

- **RS-Mask: Random Space Masking as an Integrated Countermeasure against Power and Fault Analysis**
  Keyvan Ramezanpour, Paul Ampadu and William Diehl

- **Architecture Correlation Analysis (ACA): Identifying the Source of Side-channel Leakage at Gate-level**
  Yuan Yao, Tarun Kathuria, Baris Ege and Patrick Schaumont

- **MaskedNet: The First Hardware Inference Engine Aiming Power Side-Channel Protection**
  Anuj Dubey, Rosario Cammarota and Aydin Aysu

- **DeepEM: Deep Neural Networks Model Recovery through EM Side-Channel Information Leakage**
  Honggang Yu, Haocheng Ma, Kaichen Yang, Yiqiang Zhao and Yier Jin

Session 6	**Fault Injection**
Date/Time	December 10, 2020 (Thursday) / 12:45 - 13:00 hrs
Session Co-Chairs	**Svetla Nikova and Shahin Tajik**

- **High Precision Laser Fault Injection using Low-cost Components**
  Martin S. Kelly and Keith Mayes

- **Cryptographic Fault Diagnosis using VerFI**
  Victor Arribas, Felix Wegener, Amir Moradi and Svetla Nikova

- **DESIV: Differential Fault Analysis of SIV-Rijndael256 with a Single Fault**
  Aikata, Banashri Karmakar and Dhiman Saha

- **Statistical Ineffective Fault Analysis of GIMLI**
  Michael Gruber, Matthias Probst and Michael Tempelmeier

Session 7	**Reverse Engineering and Physical Attacks**
Date/Time	December 11, 2020 (Friday) / 12:30 - 12:45 hrs
Session Co-Chairs	**Naghmeh Karimi and Ryan Helinski**

- **The Key is Left under the Mat: On the Inappropriate Security Assumption of Logic Locking Schemes**
  M Tanjidur Rahman, Shahin Tajik, M Sazadur Rahman, Mark Tehranipoor and Navid Asadizanjani

- **Lattice PUF: A Strong Physical Unclonable Function Provably Secure against Machine Learning Attacks**
  Ye Wang, Xiaodan Xi and Michael Orshansky

- **Attack of the Genes: Finding Keys and Parameters of Locked Analog ICs Using Genetic Algorithm**
  Rabin Yu Acharya, Sreeja Chowdhury, Fatemeh Ganji and Domenic Forte

Session 8	**IoT Security and HW Security Primitives**
Date/Time	December 11, 2020 (Friday) / 12:30 - 12:45 hrs
Session Co-Chairs	**Jiafeng Xie and Chengmo Yang**

- **A Post-Quantum Secure Discrete Gaussian Noise Sampler**
  Rashmi Agrawal, Lake Bu and Michel A. Kinsy

- **LAHEL: Lightweight Attestation Hardening Embedded Devices using Macrocells**
  Orlando Arias, Dean Sullivan, Haoqi Shan and Yier Jin

- **Protecting RESTful IoT Devices from Battery Exhaustion DoS Attacks**
  Stefan Hristozov, Manuel Huber and Georg Sigl

Tutorials

Tutorial 1	**Physical Inspection for Hardware Assurance**
Date / Time	December 7, 2020 (Monday) / 12:00 – 13:30 hrs
Speaker	**Navid Asadi** *University of Florida*
Chair	**Sheng Wei** *Rutgers University*

Abstract

In this tutorial we will focus on the physical inspections, physical attacks, reverse engineering, counterfeit detection, etc. of electronics from the device to system level using advanced microscopy, failure analysis (FA) techniques combined with image analysis and machine learning. We first introduce the advanced techniques for physical inspection and failure analysis on electronic systems and components. More than five different modules will be discussed here to cover different aspects of the topic. The most recent techniques for physical inspection and attacks are based on the tools and methodologies developed for FA in electronics. FA tools are primarily developed to detect a defect during or after fabrication process, but they have good enough resolution to detect Trojans, extract secret keys, or reverse engineer IC if used maliciously. Such tools include different imaging modalities such as optical microscope, scanning electron microscope (SEM), focused ion beam (FIB), photon emission microscope (PEM), X-ray microscopy (XRM), etc. and probe stations. It is worth mentioning that these attacks require a very sophisticated sample preparation process to expose a targeted area for reverse engineering or other measurements. In this tutorial, the attendees will learn the basics of how such advanced microscopes are working and how they are used for physical inspection approaches including: reverse engineering, counterfeit detection, invasive and semi-invasive attacks, on electronics from device to system level.

Biography

Navid Asadi has received the Ph.D. degree in Mechanical Engineering from University of Connecticut, Storrs, CT, USA, in 2014. He is currently an Assistant Professor with the Electrical and Computer Engineering Department at University of Florida, Gainesville, FL, USA. His current research interest is primary on “Physical Attacks and Inspection of Electronics”. This includes wide range of products from electronic systems to devices. He is involved with counterfeit detection and prevention, system and chip level reverse engineering, Anti reverse engineering, etc. Dr. Asadizanjani has received and nominated for several best paper awards from International Symposium on Hardware Oriented Security and Trust (HOST) and International Symposium on Flexible Automation (ISFA). He was also winner of D.E. Crow Innovation award from University of Connecticut. He is currently the program chair of the PAINE conference and is serving on the technical program committee of several top conferences including International Symposium of Testing and Failure Analysis (ISTFA) and IEEE Computing and Communication Workshop and Conference (CCWC).

Tutorial 2	**Protecting Confidentiality and Integrity of Deep Neural Networks against Side-Channel and Fault Attacks**
Date / Time	December 7, 2020 (Monday)/ 12:00 – 13:30 hrs
Speaker	**Prof. Yunsi Fei**, *Northeastern University* **Prof. Thomas Wahl**, *Northeastern University* **Prof. Xue Lin**, *Northeastern University*

Abstract

Deep learning (DL) has become a foundational means for solving diverse problems ranging from computer vision, natural language processing, and digital surveillance, to finance and healthcare. Security of the deep neural network (DNN) inference engines and trained DNN models on various platforms has become one of the biggest challenges in deploying artificial intelligence. Confidentiality breaches of the DNN model can facilitate manipulations of the DNN inference, resulting in potentially devastating consequences. This tutorial session addresses those security challenges in DNN implementations to promote broader applications of DNNs in security-critical scenarios by ensuring secure execution of DNN inference engines against side-channel and fault injection attacks.

The tutorial starts with a thorough investigation on an adversary's capability to reverse engineer a DNN model implemented on mainstream platforms, including CPU, GPU, FPGA, and ASIC, via passive side channels. Next, we discuss the feasibility of active fault injection attacks, i.e., how to effectively and efficiently disrupt the execution of DNN inference engines. Finally, protection, detection, and hardening mechanisms are proposed for secure execution of DNN inference engines. This tutorial may deepen the understanding of inherent information leakage and fault tolerance of DNN models. The unprecedented rise of DL technology in diverse application domains has rendered secure execution, primarily confidentiality and integrity, a top priority. This tutorial introduces the state-of-the-art on DL implementations, computer architecture and heterogeneous systems, hardware security, and formal methods/verification.

Biography

Yunsi Fei received her BS and MS degrees in Electronic Engineering from Tsinghua University, China in 1997 and 1999, respectively, and her PhD degree in Electrical Engineering from Princeton University in 2004. She is presently a professor of the Electrical and Computer Engineering Department at Northeastern University, and directs the Northeastern University Energy-efficient and Secure System (NUEESS) laboratory. Her recent research focuses on hardware-oriented security and trust, side-channel attack analysis, protection, and evaluation, and secure computer architecture design. She was a recipient of National Science Foundation CAREER award. Her research group has won the best paper award from IEEE MASCOTS'15 and IEEE ICCD'17. She has been on the TPCs of many prestigious conferences in hardware security, computer architecture, and EDA, and is a general co-chair for International Conference on Cryptographic Hardware and Embedded Systems (CHES) 2019. Currently she also serves as the NU site director of a newly established NSF Industry/University Cooperative Research Center (IUCRC) – Center for Hardware and Embedded Systems Security and Trust (CHEST), with its mission as addressing the research challenges that industry faces in this critical area.

Thomas Wahl joined Northeastern University in 2011. He moved to Boston from Oxford University where he was a Research Officer in the Computing Laboratory (now "Department of Computer Science"). Prior to Oxford, Professor Wahl held a postdoctoral position at the Swiss Federal Institute of Technology (ETH) in Zurich. He obtained a PhD in Computer Science from the University of Texas at Austin in 2007. His research concerns formal techniques for ensuring the reliability and security of complex and mission-critical computing systems, specifically in notoriously fragile domains like concurrency and numerical computing. He is also interested in the impact of compiler code transformations on alleged security guarantees made in high-level program representations such as source code. He has co-authored numerous publications on the verification of software. He regularly serves on the program committees of leading conferences in the field of Formal Methods, such as Computer-Aided Verification.

Xue Lin is an assistant professor in the Department of Electrical and Computer Engineering at Northeastern University since 2017. She received her bachelor's degree in Microelectronics from Tsinghua University, China and her PhD degree from the Department of Electrical and Computer Engineering at University of Southern California in 2016. Her research interests include deep learning security and hardware acceleration, machine learning and computing in cyber-physical systems, high-performance and mobile computing systems, and VLSI. Her research work has been supported by NSF CCF, SaTC and CPS programs, Air Force Research Lab, and Office of Naval Research. She got the best paper award at ISVLSI 2014, the top paper award at CLOUD 2014, and TCAD popular paper in 2014.

Tutorial 3	**Electromagnetic and Machine Learning Side-Channel Attacks and Low-overhead Generic Countermeasures**
Date / Time	December 7, 2020 (Monday)/ 12:00 – 13:30 hrs
Speaker	**Prof. Shreyas Sen**, *Purdue University* **Prof. Arijit Raychowdhury**, *Georgia Institute of Technology*

Abstract

Computationally secure Cryptographic algorithms, when implemented on physical hardware leak correlated physical signatures (e.g. power supply current, electromagnetic radiation, acoustic, thermal) which could be utilized to break the crypto engine in linear time. While the existence of such side-channel attacks has been known for decades, the impact of them have been increasing with the proliferation of billions of IoT edge-devices with resource constraints. Recently, it was shown that the AES-256 key could be broken non-invasively in just 5 minutes from a 1-meter distance using EM side-channels. The complexity of breaking AES-256 reduced from ~2256 to ~213 when side-channels are utilized. An attacker does not need to know specific implementation details of the cryptographic device to perform these attacks and extract keys. Going from AES128 to AES 256 only improves protection by 2x when side-channel attacks are employed, making physical side-channel attacks a significant threa.

Existing countermeasures (e.g. algorithmic, masking, power balancing, shielding) generally suffer from high overheads, sometimes performance degradations and often is algorithm specific. Generic low-overhead countermeasures require white-box modeling of the physical emissions and low-level countermeasures. Current statistical techniques for power and EM side-channel attacks during secure computation require multiple traces to be collected; and for low SNR, requires thousands of cycles. Recent advances in Deep Learning based power/EM Side-Channel Analysis (DL-SCA) allows an attack with a single or a few encryptions. Thus DL-SCA increases the attack surface massively, as an attacker who has access to a device for minutes can now attack; instead of hours of possession that were required with previous attacks like CPA. Recent work has shown how training on multiple devices can be used to generalize a DL-SCA machine learning (ML) model and can be used to carry out attack on a new and similar device in a very few encryptions. This puts a huge dent to the security of embedded devices.

In this tutorial, we will cover the following (a) Threats and impacts of physical side-channels (b) In-depth analysis of power side-channel and low-overhead generic power-side channel countermeasure through attenuated signature noise injection (ASNI) using in-line current domain signature attenuation (c) White-box modeling of EM leakage from cryptographic ICs starting from Maxwell's equations and accelerating electrons and analysis of the impact of metal layers on EM information leakage (d) Generic low-overhead EM side-channel countermeasures (e) Intelligent EM sniffing using automated algorithmic automated detection of highest leakage-point (f) Machine-Leaning Side-channel attack and techniques for cross-device DL-SCA and (g) countermeasures for ML-SCA (h) a summary of open problems and future research directions for side-channel attacks and defenses.

Biography

Shreyas Sen is an Assistant Professor in ECE, Purdue University and the inventor of the ElectroQuasistatic Human Body Communication, for which is the recipient of the MIT Technology Review top10 Indian Inventor Worldwide under 35 (MIT TR35 India) Award. Dr. Sen's current research interests span circuits/systems for Internet of Things (IoT), Biomedical and Hardware Security. He has over 5 years of industry research experience in Intel Labs, Qualcomm and Rambus. Dr. Sen is a recipient of the NSF CRII Award, AFOSR Young Investigator Award, Google Faculty Research Award, Intel Quality Award for industrywide impact on USB-C type and multiple best-paper awards. He has co-authored 2 book chapters, over 130 journal and conference papers and has 14 patents granted/pending. In 2018, Dr. Sen was chosen by MIT Technology Review as one of the top 10 Indian Inventors Worldwide under 35 (MIT TR35 India Award), for the invention of using the Human Body as a Wire, which has the potential to transform healthcare, neuroscience, and human-computer interaction. Dr. Sen is a recipient of the AFOSR Young Investigator Award 2017, NSF CISE CRII Award 2017, Google Faculty Research Award 2017, HKN Outstanding Professor Award, Intel Labs Divisional Recognition Award 2014 for industry-wide impact on USB-C type, Intel PhD Fellowship 2010, IEEE Microwave Fellowship 2008, GSRC Margarida Jacome Best Research Award 2007, Best Paper Awards at CICC 2019, HOST 2017, 2018 and 2019, ICCAD Bestin-Track Award 2014, VTS Honorable Mention Award 2014, RWS Best Paper Award 2008, Intel Labs Quality Award 2012, SRC Inventor Recognition Award 2008 and Young Engineering Fellowship 2005. He serves/has served as an Associate Editor for IEEE Design & Test, Executive Committee member of IEEE Central Indiana Section, ETS and Technical Program Committee member of DAC, CICC, DATE, ISLPED, ICCAD, ITC, VLSI Design, IMSTW and VDAT. Dr. Sen is a Senior Member of IEEE.

Arijit Raychowdhury is currently a Professor in the School of Electrical and Computer Engineering at the Georgia Institute of Technology where he joined in January, 2013. He received his Ph.D. degree in Electrical and Computer Engineering from Purdue University (2007) and his B.E. in Electrical and Telecommunication Engineering from Jadavpur University, India (2001). His industry experience includes five years as a Staff Scientist in the Circuits Research Lab, Intel Corporation, and a year as an Analog Circuit Designer with Texas Instruments Inc. His research interests include low power digital and mixed-signal circuit design, design of power converters, sensors and exploring interactions of circuits with device technologies. Dr. Raychowdhury holds more than 25 U.S. and international patents and has published over 80 articles in journals and refereed conferences. He serves on the Technical Program Committees of DAC, ICCAD, VLSI Conference, and ISQED and has been a guest associate-editor for JETC. He has also taught many short courses and invited tutorials at multiple conferences, workshops and universities. He is the winner of the Intel Labs Technical Contribution Award, 2011; Dimitris N. Chorafas Award for outstanding doctoral research, 2007; the Best Thesis Award, College of Engineering, Purdue University, 2007; Best Paper Awards at the International Symposium on Low Power Electronic Design (ISLPED) 2012, 2006; IEEE Nanotechnology Conference, 2003; SRC Technical Excellence Award, 2005; Intel Foundation Fellowship, 2006; NASA INAC Fellowship, 2004; M.P. Birla Smarak Kosh (SOUTH POINT) Award for Higher Studies, 2002; and the Meissner Fellowship 2002. Dr. Raychowdhury is a Senior Member of the IEEE.

Tutorial 4	**CAD for Security**
Date / Time	December 7, 2020 (Monday)/ 14:00 – 16:45 hrs
Speaker	**Prof. Mark Tehranipoor**, *University of Florida* **Prof. Farimah Farahmandi**, *University of Florida*

Abstract

The growing complexity of system-on-chips (SoCs) and the ever-increasing cost of IC fabrication have forced the semiconductor industry to shift from a vertical business model to a horizontal model. In this model, time-to-market and manufacturing costs are lowered through outsourcing and design reuse. To be more specific, SoC designers obtain licenses for third party intellectual property (3PIPs) and integrate them with their in-house IPs to design a specific SoC. To further reduce the cost, they may also outsource the SoC design to contract design houses, foundries, and assemblies for synthesis, DFT insertion, GDSII development, fabrication, test, and packaging. With most of these entities involved in design, manufacturing, integration, and distribution located across the globe, SOC design houses no longer have the ability to monitor the entire process and ensure security and trust.

Moreover, designers are not knowledgeable about all vulnerabilities in the design, and the countermeasures to address them. Unfortunately, existing tools do not help with the alleviating the magnitude of the problem. The tools are developed to optimize designs against power, performance, and area, while security is completely ignored. In fact, in some cases, tools and designers unintentionally create vulnerability in a circuit through security-unaware design processes/practices. These issues and the lack of trust and control have led to a large number of vulnerabilities. Hence, it is imperative to develop computer-aided design (CAD) tools with security in mind to identify and address vulnerabilities through design life-cycle.

To protect the SoC from such vulnerabilities, academic and industry researchers have proposed many design-for-security and security assessment/validation techniques, e.g., information flow tracking, side-channel leakage analysis, IP encryption, logic obfuscation, design-for-anti-counterfeit, etc. These techniques can be applied to detect vulnerabilities in ASIC and FPGA design flows. Some of these techniques are currently being evaluated by industry and are expected to be adopted in the near future. However, recent literature has pointed out to some of the limitations of these approaches. Therefore, it is crucial to have an in-depth understanding of the security provided by different techniques and understand their limitations.

The goal of this tutorial is to present (i) the threat posed by each entity in the SoC supply chain, (ii) vulnerabilities introduced during various stages of design life-cycle, (iii) CAD tools and methodologies for security assessment, (iv) Countermeasure tools and methodologies for addressing each vulnerability, and (vi) challenges and research roadmap ahead.

Biography

Mark M. Tehranipoor is currently the Intel Charles E. Young Preeminence Endowed Professor in Cybersecurity at the Department of Electrical and Computer Engineering, the University of Florida. His current research projects include: hardware security and trust, electronics supply chain security, IoT security, and reliable and testable VLSI design. Prof. Tehranipoor has published over 400 journal articles and refereed conference papers and has given about 200 invited talks and keynote addresses since 2006. In addition, he has 4 patents, and has published 11 books and 22 book chapters. He is a recipient of 13 best paper awards and nominations, the 2009 NSF CAREER award, the 2014 MURI award, the 2008 IEEE Computer Society (CS) Meritorious Service Award, the 2012 IEEE CS Outstanding Contribution, the 2010 and 2016 IEEE TTTC/CS Most Successful Technical Event for cofounding and chairing HOST Symposium, the 2009 and 2014 UConn ECE Research Excellence Award, and the 2012 UConn SOE Outstanding Faculty Advisor Award.

He serves on the program committee of more than a dozen leading conferences and workshops. Prof. Tehranipoor served as the guest editor for JETTA, IEEE Design and Test of Computers, and IEEE Computer Society Computing Now. He served as Program Chair of the 2007 IEEE Defect-Based Testing (DBT) workshop, Program Chair of the 2008 IEEE Defect and Data Driven Testing (D3T) workshop, Co-program Chair of the 2008 International Symposium on Defect and Fault Tolerance in VLSI Systems (DFTS), General Chair for D3T-2009 and DFTS2009, and Vice-general Chair for NATW-2011. He co-founded a new symposium called IEEE International Symposium on Hardware-Oriented Security and Trust (HOST) (http://www.hostsymposium.org/) and served as HOST-2008 and HOST-2009 General Chair and continue to serve as Chair of the Steering Committee for HOST. He also co-founded IEEE Asian-HOST (http://asianhost.org/). Further, he co-founded Journal on Hardware and Systems Security (HaSS) (http://www.editorialmanager.com/hass). He is also a co-founder of TrustHub (http://www.trust-hub.org/). He served as associate Editor-in-Chief (EIC) for IEEE Design and Test of Computers from 2012-2014. He is currently serving as an Associate Editor for IEEE Design and Test of Computers, an Associate Editor for JETTA, an Associate Editor for Journal of Low Power Electronics (JOLPE), an Associate Editor for ACM Transactions for Design Automation of Electronic Systems (TODAES). He has served as an IEEE Distinguished Speaker and an ACM Distinguished Speaker from 2010-2013.

Prior to joining University of Florida, Dr. Tehranipoor served as the founding director of the Center for Hardware Assurance, Security, and Engineering (CHASE) and the Comcast Center of Excellence in Security Innovation (CSI) at the University of Connecticut. Prof. Tehranipoor is a Fellow of the IEEE, Golden Core Member of IEEE Computer Society, and Member of ACM and ACM SIGDA. He is also a member of Connecticut Academy of Science and Engineering (CASE).

Farimah Farahmandi is an assistant professor in the Department of Electrical and Computer Engineering at the University of Florida. She received her Ph.D. from the Department of Computer and Information Science and Engineering at the University of Florida, 2018. She received her B.S. and M.S. from the Department of Electrical and Computer Engineering at the University of Tehran, Iran in 2010 and 2013, respectively. Her research interests include computer-aided design (CAD) for hardware security, formal verification, and post-silicon validation and debug. Her research has resulted in two books, seven book chapters, and several publications in premier ACM/IEEE journals and conferences. Her research has been recognized by several awards including IEEE System Validation and Debug Technology Committee Student Research Award, Gartner Group Info-Tech Scholarship, and a nomination for the Best Paper Award in IEEE Asia and South Pacific Design Automation Conference (ASPDAC), 2017. She has actively collaborated with various research groups (IBM, Intel, and Cisco) that has led to several joint publications. She currently serves as an Associate Editor of IET Computers & Digital Techniques. She also has served on many technical program committees as well as organizing committees of premier ACM and IEEE conferences. Her research has been sponsored by SRC, AFRL, DARPA, and Cisco. She is a member of IEEE and ACM.

Tutorial 5	**Property Driven Hardware Security**
Date / Time	December 7, 2020 (Monday)/ 14:00 – 16:45 hrs
Speaker	**Prof. Ryan Kastner**, *University of California, San Diego* **Dr. Nicole Fern**, *Tortuga Logic*

Abstract

There are a large and growing number of hardware specific security vulnerabilities. Meltdown, Spectre, Foreshadow, TLBleed, and countless other attacks expose architectural flaws with implications on the security of computing devices ranging from cloud services to embedded devices. With the dramatic increase in hardware security flaws reported, it is clear that we have reached a time where hardware has become an attractive attack surface that can be exploited with potentially large consequences. To mitigate these attacks we must make security a first class citizen in the hardware design process.

Property driven hardware security is a design methodology to assess the safety and security of hardware designs. It enables security experts to describe how the hardware should (or should not) function. These security properties are formally specified using languages that map to models that are easy to verify using existing design tools. There are three fundamental elements for any hardware security design flow. First, security experts need expressive languages to specify these security properties. Second, these properties should map to models to describe the security related behavior of a hardware design. Finally, hardware security design tools verify that the hardware design meets these properties using formal solvers, simulation, and emulation.

This tutorial looks at the elements of a property driven hardware security design methodology. A property driven hardware security design methodology starts with expressive security models that enable one to specify safety and security properties related to confidentiality, integrity, availability, separation, isolation, side channels, real-time operation, and Trojans. These models provide a formal way to specify the desired security of the hardware. Hardware security verification tools evaluate that the hardware design meets these security properties. These tools help the hardware designer find the source of security flaws and provide an assessment of their potential risks. Information flow and statistical models provide the necessary expressive power for specifying these properties, while also leveraging existing hardware verification tools for formal analysis, simulation, and emulation.

Biography

Dr. Ryan Kastner is a professor in the Department of Computer Science and Engineering at the University of California, San Diego.. He received a PhD in Computer Science (2002) at UCLA, a Masters degree in engineering (2000) and Bachelor degrees (BS) in both Electrical Engineering and Computer Engineering (1999) from Northwestern University. He spent the first five years after his PhD as a professor in the Department of Electrical and Computer Engineering at the University of California, Santa Barbara.

Professor Kastner leads the Kastner Research Group whose current research interests fall into three areas: hardware acceleration, hardware security, and remote sensing. He is the co-director of the Wireless Embedded Systems Graduate Program — a specialized Masters degree targeting individuals working in local industries. He co-directs the Engineers for Exploration Program, which pairs undergraduates in research experiences with domain scientists in archaeology, conservation, and cultural heritage. He is the cofounder of the company Tortuga Logic that develops hardware security solutions based upon technology developed in his research group.

Dr. Nicole Fern is a senior hardware security engineer at Tortuga Logic whose primary role is providing security expertise and defining future features and applications for the product line. Before joining Tortuga Logic in 2018 she was a postdoc at UC Santa Barbara. Her research focused on the topics of hardware verification and security. She received her undergraduate degree in Electrical Engineering from The Cooper Union for the Advancement of

Science and Art in 2011 and her Ph.D. from the Electrical and Computer Engineering department at UC Santa Barbara in 2016.

Tutorial 6	**Security Issues in AI and Their Impacts on Hardware Security**
Date / Time	December 7, 2020 (Monday)/ 14:00 – 16:45 hrs
Speaker	**Prof. Gang Qu**, *University of Maryland, College Park* **Dr. Rosario Cammarota**, *Intel AI Research* **Dr. Pin-Yu Chen**, *IBM Research Trusted AI Group* **Dr. Lin Yuan**, *Waymo*

Abstract

Hardware security and trust has gained a lot of attention in the past two decades and many related topics have gained attention from both government and industry. These include hardware Trojan, physical unclonable function, intellectual property (IP) protection, trusted IC and EDA tools as well as supply chain in general. Recently, artificial intelligence (AL) and machine learning (ML) has been growing at a pace that we have never seen before and now it has made its impact on literally everywhere from our daily life to homeland security. This tutorial will address two key problems: (1) what are the major security (or robustness) challenges facing the AI/ML community? (2) how AI/ML affect the development of hardware security and trust? More specifically, we will focus on trust in AI/ML, IP protection in AI.ML adversarial robustness in deep learning, preservation of user privacy in inference models, the best AI/ML practices in industry, and the challenges and opportunities for hardware security in the ear of AI/ML.

Biography

Gang Qu is a professor in the Department of Electrical and Computer Engineering at the University of Maryland, College Park. He has worked extensively in the area of hardware security with more than 200 publications and delivered more than 100 invited talks. He has also contributed in building the hardware security and trust community. Notably, he has been involved in HOST from its first edition and served as the TPC chair in 2018 and general chair in 2019. He also co-founded the AsianHOST which is in its 4th year now. He has organized as chair or cochair for about 10 other conferences and workshops, as well as founded or chaired hardware security tracks. The book based on his dissertation, Intellectual Property Protection in VLSI Designs: Theory and Practice is the first of its kind. He has developed a MOOC of Hardware Security on Coursera that has attracted tens of thousands of students all over the world.

Rosario Cammarota is a Principal Scientist at Intel AI Research, where he grows the effort in privacy-preserving computing, with a focus on AI systems. He holds the grade of IEEE Senior Member. He serves as program committee members for venues of international prestige in hardware and system security such as DAC, ICCAD, HOST and NDSS. He serves as Editorial Board Member for the Springer International Journal of Parallel Programming, and as Associate Editor for the Springer Journal on Hardware and System Security. He is a prolific inventor and one of the recipients of the Semiconductor Research Corporation Mahboob Khan Outstanding Industry Liaison Awards in 2017, 2018 and 2019.

Pin-Yu Chen is a Principal Scientist at Intel AI Research, where he grows the effort in privacypreserving computing, with a focus on AI systems. He holds the grade of IEEE Senior Member. He serves as program committee members for venues of international prestige in hardware and system security such as DAC, ICCAD, HOST and NDSS. He serves as Editorial Board Member for the Springer International Journal of Parallel Programming, and as Associate Editor for the Springer Journal on Hardware and System Security. He is a prolific inventor and one of the recipients of the Semiconductor Research Corporation Mahboob Khan Outstanding Industry Liaison Awards in 2017, 2018 and 2019.s currently a research staff member at IBM Thomas J. Watson Research Center, Yorktown Heights, NY, USA. He is also affiliated with the MIT-IBM Watson AI Lab and is a co-PI of MIT-IBM projects. Dr. Chen's recent research is on adversarial machine learning and robustness analysis of neural networks. His research interest includes graph and network data analytics and their applications to data mining, machine learning, signal processing, and cyber security. He was the recipient of the Chia-Lun Lo Fellowship from the University of Michigan Ann Arbor. He received the NIPS 2017 Best Reviewer Award, and was also the recipient of the IEEE GLOBECOM 2010 GOLD Best Paper Award and several conference travel grants. Dr. Chen is currently on the editorial board of PLOS ONE. He is a workshop co-chair of “Signal Processing for Adversarial Machine Learning” at GlobalSIP 2018 and “Adversarial Learning Methods for Machine Learning and Data Mining” at KDD 2019.

Lin Yuan Lin Yuan is a Staff Software Engineer at Waymo. His work focuses on developing the machine learning platform for the perception and planning tasks for autonomous driving vehicles. Before joining Waymo, he was working at Amazon AI on large scale distributed learning. He is a committer and major contributor to the Apache deep learning framework MXNet and LFAI distributed learning library Horovod. He received his Ph.D. in Computer Engineering from the University of Maryland, College Park.

Hardware Demos

Session	**Student Hardware Demo Q&A Session 1**
Date/Time	Tuesday, December 8, 2020 / Time: 15:45 - 16:20 hrs
Session Co-Chairs	**Hassan Salmani** and **Fareena Saqib**

- **Attack of the Genes: Finding Keys and Parameters of Locked Analog ICs using Genetic Algorithm**
  Rabin Yu Acharya, Sreeja Chowdhury, Fatemeh Ganji and Domenic Forte

- **Hardware Demo of Thermistor and Solar Cell Based PUFs via a PUF based Controller Area Network Security Framework**
  Carson Labrado and Himanshu Thapliyal

- **SOLOMON: An Automated Framework for Detecting Fault Attack Vulnerabilities in Hardware**
  Milind Srivastava, Patanjali slpsk, Indrani Roy, Chester Rebeiro, Aritra Hazra, and Swarup Bhunia

- **Demo of Fingerprinting Cloud FPGAs**
  Shanquan Tian, Wenjie Xiong, Ilias Giechaskiel, Kasper Rasmussen and Jakub Szefer

Session	**Student Hardware Demo Q&A Session 2**
Date/Time	Tuesday, December 8, 2020 / Time: 15:45 - 16:20 hrs
Session Co-Chairs	**Wenjie Che** and **Adam Kimura**

- **RASC v2: Enabling Remote Access to Side-Channels and Leveraging FPGA Acceleration for Real-Time Side-Channel Monitoring**
  Yunkai Bai, Andrew Stern, Jungmin Park, Domenic Forte and Mark Tehranipoor

- **Side-channel Power Resistance for Encryption Algorithms using Dynamic Partial Reconfiguration (SPREAD)**
  Ivan Bow, Jithin Joseph, F. Saqib, C. Patel, R. Robucci and J. Plusquellic

- **SCNIFFER: Fully Automated, Low-cost, Efficient EM SCA Attack**
  Josef A Danial, Debayan Das and Shreyas Sen

- **Power Delivery Network based Board-Level Security Measurement and Side-Channel Attack**
  Huifeng Zhu, Xiaolong Guo, Xuan Zhang and Yier Jin
- **Statistical Ineffective Fault Analysis using FOBOS Glitch Generator**
  Abubakr Abdulgadir, Keyvan Ramezanpour, William Diehl, Paul Ampadu and Jens-Peter Kaps
- **Runtime Trust Evaluation Using On-Chip EM Sensors**
  Jiaji He, Leibo Liu, Xiaolong Guo and Yier Jin

Session	**Student Hardware Demo Q&A Session 3**
Date/Time	Wednesday, December 9, 2020 / Time: 16:15 - 16:45 hrs
Session Co-Chairs	**Mehran Mozaffari Kermani** and **Adam Kimura**

- **REFaaS: Remote Exploitation of FPGA-as-a-Service Platforms**
  Nitin Pundir, Fahim Rahman, Farimah Farahmandi and Mark Tehranipoor
- **FPGA Bitstream Camouflaging**
  Ali Shuja Siddiqui, Yutian Gui, Geraldine Shirley Nicholas and Fareena Saqib
- **High-level Synthesis Vulnerabilities: Information Leakage and Control Flow Violations**
  Md Rafid Muttaki and Nitin Pundir
- **Machine Learning Techniques in Side-channel Analysis**
  Yutian Gui, Ali Shuja Siddiqui, Fareena Saqib and Chaitanya Mukund Bhure
- **MeXT-SE: A Design Tool to Generate Secure MPSoCs**
  Md Jubaer Hossain Pantho, Sujan Saha and Christophe Bobda
- **Machine Learning Bluetooth Transmission State Operation Verification via Monitoring the Transmission Pattern**
  Abdelrahman Elkanishy, Abdel-Hameed Badawy and Paul Furth

Session	**Student Hardware Demo Q&A Session 4**
Date/Time	Wednesday, December 9, 2020 / Time: 16:15 - 16:45 hrs
Session Co-Chairs	**Aydin Aysu** and **Fareena Saqib**

- **Detecting Recycled SoCs by Exploiting Aging Induced Biases in Memory Cells**
  Wendong Wang, Ujjwal Guin and Adit Singh

- **End-to-End Traceability of ICs in Component Supply Chain for Fighting Against Recycling**
  Yuqiao Zhang and Ujjwal Guin

- **Hardware Demonstration of Watermarking of NAND Flash Memory Chips**
  Mohammad Sadman Sakib, Aleksandar Milenković and Biswajit Ray

- **SPARTA: Laser Probing Approach for Trojan Detection**
  Andrew Stern, Shahin Tajik, Farimah Farahmandi and Mark Tehranipoor

- **Current based Remote PCB Authentication using JTAG Architecture**
  Shubhra Deb Paul and Swarup Bhunia

- **Automated Design and Synthesis of Secure System-on-Chip Architectures**
  Atul Prasad Deb Nath, Kshitij Raj, Swarup Bhunia and Sandip Ray

List of Posters

1. HawkEye: A Threat Detector for Intelligent Surveillance Cameras Powered with AI Models

Speaker: **Mathias Echi**, *Prairie View A&M University*

Abstract

In this paper, we present a prototype implementation of systems, such as Hawk-Eye, an AI powered threat detector for smart surveillance cameras. Hawk-Eye is able to develop on central servers hosted in the cloud as well as on surveillance cameras. It enables the initial analysis of the captured images to take place on-site, which reduces the communication overheads and enables swift security actions. At the cloud side, Mask R-CNN model was build that can detect suspicious objects in an image. At the camera side, CNN model was build that can consume a stream of images directly from an on-site webcam, classify them, and displays the results to the user via a GUI-friendly interface. Finally, we evaluated our system using various performance metrics such as classification time and accuracy. Our experimental results showed an average overall prediction accuracy of 94% on our dataset.

2. A post-quantum secure Gaussian noise sampler

Speaker: **Rashmi Agrawal**, *Boston University*

Abstract

While the notion of achieving "quantum supremacy" maybe debatable, rapid developments in the field of quantum computing is heading towards more realistic quantum computers. As practical quantum computers start becoming more feasible, the requirement to have quantum secure cryptosystems becomes more compelling. Due to its many advantages, lattice-based cryptography has become one of the key candidates for designing secure systems for the post-quantum era. The security of lattice-based cryptography is governed by the small error samples generated from a Gaussian distribution. Hence, the Gaussian distribution lies at the core of these cryptosystems. In this paper, we present the hardware design implementation of three different sampling algorithms including rejection, Box-Muller, and the Ziggurat method for the Gaussian Sampler. Our goal is to provide concrete recommendations for future use and adoption in various cryptosystems based on sampling efficiency, hardware cost, and throughput. The key feature of our design implementation is that it performs high-precision sampling to meet the NIST's recommended security level of 112-bits or higher for the postquantum era, which most existing hardware implementations fail to do. Furthermore, our design implementation is highly optimized for FPGA-based implementation and is also generic so that it can be seamlessly integrated into most cryptosystems. Synthesis results are obtained using Vivado design suite for a Xilinx Zynq-7010 CLG400ACX1341 FPGA board.

3. RASC v2: Enabling Remote Access to Side-Channels and Leveraging FPGA Acceleration for Real-Time Side-Channel Monitoring

Speaker: **Yunkai Bai**, *University of Florida*

Abstract

Nowadays, IoT devices face many threats like hardware trojans and malware attacks. However, the traditional side-channel based defend mechanism has limitations due to large and expensive experiment setups. In this case, RASC is proposed. RASC is a miniature platform that minimizes the traditional side-channel analysis system into two tiny PCBs. Moreover, RASC can communicate with the security house remotely via Bluetooth. This Poster includes the content of the RASC and two experiments we have done about RASC. The first experiment is AES cracking experiment, and it proves the attack capability of the RASC. The second experiment is the malware detection

experiment, and it proves the defense capability of the RASC. In the future, we will use RASC to do the disassembly experiment and let it process data internally.

4. ReGDS: A Reverse Engineering Framework from GDSII to Gate-level Netlist

Speaker: **Rachel Selina Rajarathnam**, *University of Texas at Austin*

Abstract

With many fabless companies outsourcing integrated circuit (IC) fabrication, the extent of design information recoverable by any third-party foundry remains clouded. While traditional reverse engineering schemes from the layout employ expensive high-resolution imaging techniques to recover design information, the extent of design information that can be recovered by the foundry remains ambiguous. To address this ambiguity, we propose ReGDS, a layout reverse engineering (RE) framework, posing as an inside-foundry attack to acquire original design intent. Our framework uses the layout, in GDSII format, and the technology library to extract the transistor-level connectivity information, and exploits unique relationship-based matching to identify logic gates and thereby, recover the original gate-level netlist. Employing circuits ranging from few hundreds to millions of transistors, we validate the scalability of our framework and demonstrate 100% recovery of the original design from the layout. To further validate the effectiveness of the framework in the presence of obfuscation schemes, we apply ReGDS to layouts of conventional XOR/MUX locked circuits and successfully recover the obfuscated netlist. By applying the Boolean SATisfiability (SAT) attack on the recovered obfuscated netlist, one can recover the entire key and, thereby, retrieve the original design intent. Thus ReGDS results in accelerated acquisition of the gate-level netlist by the attacker, in comparison to imaging-based RE schemes. Our experiments unearth the potential threat of possible intellectual property (IP) piracy at any third-party foundry.

5. Boosting Entropy and Enhancing Reliability for Physically Unclonable Functions

Speaker: **Ricardo Ivan Valles Novo**, *New Mexico State University*

Abstract

Physically Unclonable Functions (PUFs) are emerging hardware security primitives that leverage random variations during chip manufacturing process to generate unique secrets. The security level of generated PUF secrets is mainly determined by its unpredictability feature which is typically evaluated using the metric of entropy bits. In this poster, we present a novel entropy boosting technique that significantly improves the upper bound of PUF entropy bits from the scale of log2(N!) up to O(N^2). We also propose a reliability-enhancing scheme to compensate for the impact on reducing reliability by saving a significant portion of potential reliable response bits. Experimental results based on a published large-scale RO PUF frequency dataset validated that the proposed technique significantly boosts PUF entropy bits from the scale of O(N·log2(N)) up to approach the new upper bound of O(N^2) with a comparable reliability, and the reliability-enhancing technique saves 4x more on the percentage of reliable response bits.

6. PARAM: A Microprocessor Hardened for Power Side-Channel Attack Resistance

Speaker: **Muhammad Arsath K F**, *Indian Institute of Technology Madras*

Abstract

The power consumption of a microprocessor is a huge channel for information leakage. While the most popular exploitation of this channel is to recover cryptographic keys from embedded devices, other applications such as mobile app finger-printing, reverse engineering of firmware, and password recovery are growing threats. Countermeasures proposed so far are tuned to specific applications, such as crypto-implementations. They are not scalable to the large number and variety of applications that typically run on a general purpose microprocessor. In

this paper, we investigate the design of a microprocessor, called PARAM with increased resistance to power based side-channel attacks. To design PARAM, we start with identifying the most leaking modules in an open-source RISC V processor. We evaluate the leakage in these modules and then add suitable countermeasures. The countermeasures depend on the cause of leakage in each module and can vary from simple modifications of the HDL code ensuring secure translation by the EDA tools, to obfuscating data and address lines thus breaking correlation with the processor's power consumption. The resultant processor is instantiated on the SASEBO-GIII FPGA board and found to resist Differential Power Analysis even after one million power traces. Compared to contemporary countermeasures for power side-channel attacks, overheads in area and frequency are minimal.

7. FPGA Bitstream Camouflaging

Speaker: **Geraldine Shirley Nicholas**, *UNCC*

Abstract

Reconfigurable logic enables architectural updates for embedded devices by providing the ability to reprogram partial or entire device. However, this flexibility can be leveraged by the adversary to compromise the device boot process by modifying the bitstream or the boot process with physical or remote access of the device placed in a remote field. We propose a novel multilayer secure boot mechanism for SoCs with a two-stage secure boot process. The first stage uses device bound unique response as a key to decrypt application logic. The security function is extended at runtime by integrating intermittent architecture and application locking mechanism to reveal correct functionality.

8. Implementation of Secure Shell for Presentation Software using Raspberry Pi

Speaker: **Keith Ghant**, *Alabama A&M University*

Abstract

As many generations of computers were progressed for many decades, computers became somehow smaller and the interactive terminals was more user-friendly.

The idea of this terminal interface is that it has a high-level trust between the central computer and all the networks since the network were used to isolate from another physically.

The idea of SSH is that it can be used to file transfers, secure logins, and secure the connection between two parties.

9. Scalable Adaptive Trusted Transceivers

Speaker: **Michael Kines**, *Ohio State University*

Abstract

the exponential growth of Internet of Things (IoT) devices, cyberattacks take center stage eroding consumer trust and leaking private information. Hardware Trojans inserted by untrusted foundries can broadcast private keys over wireless carriers, power supply side-channels can leak private information, and IoT sensors can easily be spoofed. Trusted hardware is a viable solution; however, it often comes at a significant cost in energy and silicon area, and designs do not adapt to changing requirements. Our approach incorporates scalable performance in transmission range, throughput, power, and trust, to best adapt to the temporal needs of the application space.

10. Hardware/Software Obfuscation against Timing Side-channel Attack on a GPU

Speaker: **Elmira Karimi**, *Northeastern University*

Abstract

GPUs are increasingly being used in security appli- cations, especially for accelerating encryption/decryption. While GPUs are an attractive platform in terms of performance, the security of these devices raises a number of concerns. One vulnerability is the data-dependent timing information, which can be exploited by adversary to recover the encryption key.

Memory system features are frequently exploited since they create detectable timing variations. In this paper, our attack model is a coalescing attack, which leverages a critical GPU microarchitectural feature - the coalescing unit. As multiple concurrent GPU memory requests can refer to the same cache block, the coalescing unit collapses them into a single memory transaction. The access time of an encryption kernel is dependent on the number of transactions. Correlation between a guessed key value and the associated timing samples can be exploited to recover the secret key.

In this paper, a series of hardware/software countermeasures are proposed to obfuscate the memory timing side channel, making the GPU more resilient without impacting performance. Our hardware-based approach attempts to randomize the width of the coalescing unit to lower the signal-to-noise ratio. We present a hierarchical Miss Status Holding Register (MSHR) design that can merge transactions across different warps. This feature boosts performance, while, at the same time, secures the execution. We also present a software-based approach to permute the organization of critical data structures, significantly changing the coalescing behavior and introducing a high degree of randomness. Equipped with our new protections, the effort to launch a successful attack is increased up to 1433X × 178X, while also improving encryption/decryption performance up to 7%.

11. Thwarting Control Plane Attacks with Displaced and Dilated Address Spaces

Speaker: **Lauren Biernacki**, *University of Michigan*

Abstract

To maintain the control-flow integrity of today's machines, code pointers must be protected. Exploits forge and manipulate code pointers to execute arbitrary, malicious code on a host machine. A corrupted code pointer can effectively redirect program execution to attacker-injected code or existing code gadgets, giving attackers the necessary foothold to circumvent system protections. To combat this class of exploits, we employ a Displaced and Dilated Address Space (DDAS), which uses a novel address space inflation mechanism to obfuscate code pointers, code locations, and the relative distance between code objects. By leveraging runtime re-randomization and custom hardware, we are able to achieve a high-entropy control-flow defense with performance overheads well below 5% and similarly low power and silicon area overheads. With DDAS in force, attackers come up against 63 bits of entropy when forging absolute addresses and 18 to 55 bits of entropy for relative addresses, depending on the distance to the desired code gadget. Moreover, an incorrectly forged code address will result in a security exception with a probability greater than 99.996%. Using hardware-based address obfuscation, we provide significantly higher entropy at lower performance overheads than previous software techniques, and our re-randomization mechanism offers additional protections against possible pointer disclosures.

12. Circuit Masking Theory to Standardization, A Comprehensive Survey for Hardware Security Researchers and Practitioners

Speaker: **Ana Covic**, *University of Florida*

Abstract

Sensitive data, such as firmware and cryptographic keys, can be extracted by mounting physical attacks, e.g., photon emission analysis, micro-probing, etc. These attacks can be launched on an integrated circuit (IC) through either the frontside (i.e., passivation) or backside (i.e., silicon substrate). Unlike frontside attacks confronting obstacles from the upper metal layers, through backside attacks, access to transistors and logic gates can be granted. Our previous work has proposed a backside metal shield connected to inner-logic using through-silicon-vias (TSVs), which made backside attacks significantly more complex. However, it has also hindered failure analysis, a critical step for process and design engineers. In this work, we aim to complement physical countermeasures with provable security approaches that increase the number of simultaneous probes needed to perform probing. Commonly applied mathematical models for probing attacks have employed randomized bits to mask the input and modified computations. As the number of masks increases, the number of probes needed to extract one bit of secret data increases exponentially, assuming noise-free conditions. There are two paths that have been investigated for circuit masking transformations. Firstly, the noise present in probed data can be considered, allowing for the application of side-channel attack models and associated security verification tools. Secondly, in addition to security, the composability of implemented clusters of gates has been investigated for the higher number of random masks. Furthermore, when implementing masking schemes, another challenge to face is the presence of glitches, which inherently happen in logic circuits and reduce the effectiveness of random masks. The goal of our survey is to relate the notion of masking with physical backside attack countermeasures. To this end, our first milestone is to unify provable probing and side-channel models in order to develop and realize more practical countermeasures.

13. Parallel Attack on Logic Locking

Speaker: **Danielle Duvalsaint**, *Carnegie Mellon University*

Abstract

Logic locking is a design-for-trust technique used to prevent potential threats in the design chain. Many different techniques for logic locking have been introduced, making it difficult to compare the security of the different techniques. This poster will discuss an ATPG based approach that can be used to characterize multiple types of locked circuits. This approach derives key values from locked circuits using ATPG, effectively telling a designer how strong their lock is. Experiments show this approach is effective at measuring the security of multiple lock types and that the analysis can be scaled to simulate an attacker with increased resources.

14. Hardware Constructions for Error Detection of Lattice-based Cryptosystems Utilized in Secure Post-Quantum Cryptographic Architectures

Speaker: **Ausmita Sarker**, *University of South Florida*

Abstract

With the potential advent of quantum computers, public-key cryptographic algorithms will be broken. We cannot wait till such compromising attacks break our security, especially in deeply-embedded hardware systems. The steady progress in quantum computing has motivated standardization by the NIST (Round2: March 2019). Ideal lattices, one class of lattice-based cryptosystems, is based on worst-case hardness of lattice problem, and provides realizable execution, higher efficiency, and low parameter size. Implementations of cryptographic primitives can fall victim to active hardware side-channel attacks, whose secure, efficient, and high error coverage countermeasures are proposed in this work. Ring-learning with error (Ring-LWE) is a popular worst-case lattice problems with a practical key size and O(n.lgn) complexity. Ring polynomial multiplier is the most rigorous computation of ring-LWE, somewhat homomorphic encryption (SHE), fully homomorphic encryption (FHE) and other emerging cryptographic structures.

15. GRAPh Probability for Logic Locking Evaluation (GRAPPLLE)

Speaker: **Christopher Taylor**, *Ohio State University*

Abstract

With the reduction of U.S. based IC fabrication facilities, the risk of IP theft and malicious modifications has increased. Logic locking has been a proposed solution, which causes a chip to operate incorrectly, obscuring its function and increasing the difficulty to insert a change that operates off a desired trigger. The effectiveness of any logic locking technique depends on the design chosen, the amount of camouflage inserted or key length, and the specific location of the inserted cells. Measuring the security added is done using a Boolean Satisfiability Problem (SAT) solver, and the time to break is the metric. This attack requires the use of a fully functional chip (oracle) and relies solely on the input and output data through functional testing. This attack model ignores the underlying structure that exists in a design, the vast amount of repetition, as well as design reuse. We propose GRAPh Probability for Logic Locking Evaluation (GRAPPLLE) a structure attack, based on localized repetition that does not require the use of an oracle. By generated subgraphs around locked elements in a design, we are able to predict with some confidence the correct keys through subgraph similarity located within the same circuit.

16. Deep Learning Analysis in Colon Histopathology Images

Speaker: **Yu Shen**, *Cornell University*

Abstract

Recent success in Deep Learning has changed various fields of study including biomedical image analysis. Traditionally, these analysis consist of hand-crafted feature extraction followed by applying classical computer vision methods. However, with accumulation of digital histopathological images, analysis techniques based on deep learning would ease the increasing workloads on pathologists. In this study, we categorized the state-of-the-art deep learning methods for colon cancer diagnosis in different segmentation applications(Nuclei and Gland). Furthermore, we introduce an original work for gland instance segmentation using Mask-RCNN on colon tissue, and apply boolean analysis to reveals a new gene expression pattern on the glandular epithelium cells.

17. Toward Consortium-Based Blockchain Infrastructures, Enabling Modeling, Detecting, Tracking of Counterfeit Integrated Circuits

Speaker: **Jason Vosatka**, *University of Florida*

Abstract

The electronics supply chains are vulnerable to counterfeit integrated circuits (ICs), as unauthenticated components and subsystems must pass through numerous untrusted entities before reaching their final installation. Moreover, the unknown and unverifiable supply routes across the world makes component-level 'chain-of-custody' knowledge an unworkable problem. We propose initial steps toward a consortium-based blockchain infrastructure to provide traceability and provenance of authentic and counterfeit ICs. We propose initial steps toward a modeling and metrics method enabling empirical calculations of relative risk through quantitative, data-driven confidence levels of authentication.

Corporate Sponsors

Gold

CISCO

riscure
driving your security forward

SYNOPSYS®
Silicon to Software™

Silver

arm

BOEING

intel

NewAE Technology

Qualcomm

Exhibitor Sponsors

BATTELLE
It can be done

ECI EDAPTIVE COMPUTING, INC.

onespin
assuring IC integrity

Rambus

SYNOPSYS®
Silicon to Software™

riscure
driving your security forward

Tortuga Logic

Organizational Sponsors

IEEE

IEEE COMPUTER SOCIETY

tttc™

IEEE TC on Security & Privacy

NSF

Media Partners

Journal of *Low Power Electronics and Applications*
an Open Access Journal by MDPI

sensors
an Open Access Journal by MDPI

IEEE SECURITY & PRIVACY

Student Travel Grant Sponsor

NSF

CISCO

Student Hardware Demo Session

CISCO

cryptography
an Open Access Journal by MDPI

Author Index