Semiconductor Research Corporation

Because the future can't wait, we bring the best minds together to achieve the unimaginable

HWS Research Program Annual Review

June 6-9, 2023

Virtual

John Oakley, Science Director
LaDonya Dooley, Research Program Coordinator

https://www.src.org/calendar/e007789/

Thank you!

On Behalf of the SRC,

Thank You!

- To all the industry members for their sponsorship and mentorship
- To all the Principal Investigators & their Students for the great research effort
- To LaDonya Dooley at SRC for the logistical support
- To all of you for being virtual with us!

e-kickoff Reminders

Everyone will be participating virtually

Presenters should remember to speak clearly and keep within the allotted time.

Timing:
30 min (25 min talks with 5 min Q&A)

Presentations and Q&A will be live. Please be mindful, so watch the time to leave 5 minutes for Q&A!!!

Informal Presentations

Please indicate if you want the audience to interrupt with questions. Q/A will occur at the end.

SRC

Reminder: Invoicing and Deliverables

Regular invoicing

Reminder: Send News Items to SRC

- Send noteworthy events and announcements that you and your team are involved in to SRC

- Send this information on a monthly basis. We use what we can in our SRC newsletter and monthly emails to the Advisory Board and liaisons
  - Best Paper Awards (who, award, title of piece, where, when and photos of students/faculty)
  - Papers, posters presentations, and/or conference talks
  - Professional Recognition Awards: IEEE, teaching awards, etc.
  - Professional activities such as workshops, tutorials, and invited talks

More Than 17,000 subscribers!!

- All submissions must have a web link (URL) to the award, paper, etc.
  - If you have your own website that contains information pertaining to your research, share the link with SRC as well

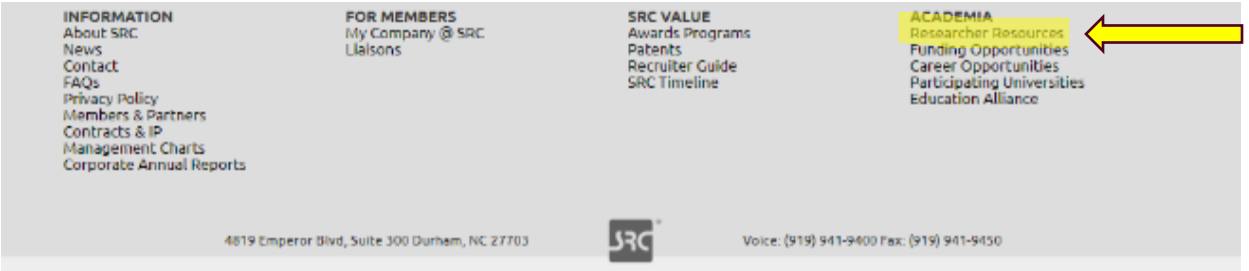
SRC

https://www.src.org/newsroom/newsletter/

Resources that Help Academics Evaluate, Adopt, and Amplify Emerging Member Solutions

Member Resources

- SRC has collected information members provide for the academic community, including education, design, and prototyping
- SRC researchers and students are encouraged to take advantage of these resources in their research and education activities



Member Resources

SRC has collected information members provide for the academic community, including education, design, and prototyping. SRC researchers and students are encouraged to take advantage of these resources in their research and education activities

Intel

- Intel Open Data Center Diagnostic Project
- Intel Academic Compute Resource Environment (ACE)
- Intel Academic Program for oneAPI

Analog Devices

- Active Learning Program
- ADALM-SR1 Hardware
- ADALM-SR1 Switching Regulator Active Learning Module

ARM

ARM Academic Access
ARM Education

- ARM University Program Education Kits
- ARM Education Online Courses
- ARM Education Textbooks and Reference Books

Texas Instruments
Specific tutorial and curriculum for universities include:

- Texas Instruments University Program
- TI Robotics System Learning Kit
- TI Power Management Lab Kit
- TI Experimental Power Electronics Reference and Curriculum
- TI Precision Labs

IBM

- IBM tutorial and curriculum for universities
- IBM Skills Academy
- IBM + Coursera
- IBM PhD Fellowship Program
- IBM Quantum Computing - student opportunities
- IBM AI Hardware

NXP

- Rapid IoT Prototyping Kit

Siemens

- EDA Academic Products

Qualcomm

- University Relations Program

SRC

https://www.src.org/program/grc/guide/researcher/guidelines/

SRC Student Platform on LinkedIn

- What is the **SRC Research Scholars Program?**
  - SRC provides undergrads, graduate students, and postdoctoral researchers with a unique education consisting of traditional course work, cutting-edge research, and direct interaction with the semiconductor industry
  - These Research Scholars work on industry-relevant research with SRC-funded faculty who are recognized experts in their fields
  - Through our extensive community of academics and industry personnel, we nurture the evaluation of the talent pipeline for our industry and beyond
  - Our alumni have become industry leaders and renowned faculty researchers, creating a virtuous cycle where mojo begets mojo

Join Now! And add them to Pillar Science

Get LinkedIn with SRC

SRC uses a special LinkedIn Affiliate page for the SRC Research Scholars Program. Undergrad, graduate students, and postdoctoral researchers participating on SRC research add their SRC Research Scholars experience to their LinkedIn profile. This allows Scholars a way to professionally showcase their talent and experience. It also simplifies how recruiters, engineers, and even other Scholars can find SRC Research Scholars, using either the LinkedIn Search* or LinkedIn Recruiter*.

SRC Research Scholars Program*

By being part of our community, Research Scholars will have a unique opportunity to get to know professionals with careers in the semiconductor industry or government, top researchers in their fields, and other students with similar interests.

SRC encourages all undergrads, graduate students, and postdoctoral researchers to join this program!!!

https://www.src.org/student-center/handbook/linkedin/

Pillar Science Common Issues & Links for Academics

- There are lots of help articles in Pillar Science which can help answer these questions.

- Here's an article about logging into Pillar Science
  - https://semiconductorresearchcorporation.zendesk.com/hc/en-us/articles/11198322803099-How-To-Login-to-Pillar-with-SRC-org-Credentials
- Here's an article about update your profile in Pillar Science
  - https://semiconductorresearchcorporation.zendesk.com/hc/en-us/articles/10330492961563-How-to-Edit-Your-Profile
- Here's an article about adding students, administrators, or other academics to your project
  - https://semiconductorresearchcorporation.zendesk.com/hc/en-us/articles/10330872380187-How-to-add-Students-Admins-or-other-Academics-to-Your-Project
- Here's an article about submitting projects results and deliverables
  - https://semiconductorresearchcorporation.zendesk.com/hc/en-us/articles/11213311626139-How-to-Submit-Project-Results-previously-known-as-publications-
- SRC hosted a live demonstration for academics on January 31, 2023, and the recording is available
  - https://semiconductorresearchcorporation.zendesk.com/hc/en-us/articles/12543067480091-Pillar-Science-Demonstration-for-Academics-Video-Recording-

SRC

https://semiconductorresearchcorporation.zendesk.com/hc/en-us/sections/11359770755483-How-Tos-for-Academics

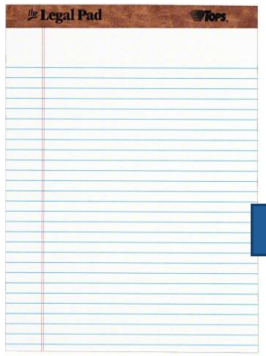
Guidance for Depositing Supporting Code and Data with Pre-Publications

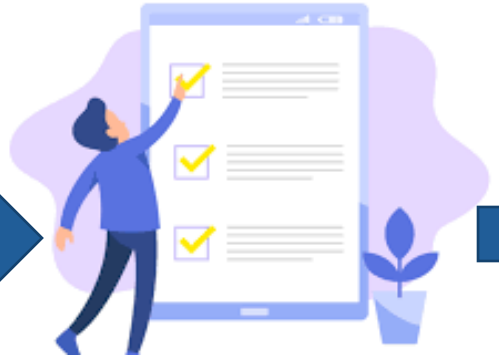
As part of our move to Pillar Science, there is the ability to collect not just the pre-publications PDF's but also arbitrary file formats (.mp4, .ppt, etc.) as well. This new capability enables a new way for SRC programs to facilitate technology transfer to our sponsors.

Key Performance Indicators (KPI) Process

- KPI instruction video is available: https://www.src.org/src/guide/kpi/

PILLAR SCIENCE





Empty KPI forms On Pillar Science	PIs fill out KPI forms As part of Annual Review	SRC perform qualify control on KPI Forms	Industry verify technology transfers (TTs) + report to SRC	TT Master counts summarized in annual report

We moved KPI process flow to Pillar Science this year and make KPI process visible to SRC members to maximize research experiences with meaningful Technology Transfers.

SRC

https://semiconductorresearchcorporation.zendesk.com/hc/en-us/articles/15056064943771-How-to-edit-and-manage-your-Key-Performancer-Indicators-KPI-card-

Pillar Science Common Issues & Links for Industry

- There are lots of help articles in Pillar Science which can help answer these questions.

- Here's an article about logging into Pillar Science
  - https://semiconductorresearchcorporation.zendesk.com/hc/en-us/articles/11198322803099-How-To-Login-to-Pillar-with-SRC-org-Credentials
- Here's an article about update your profile in Pillar Science
  - https://semiconductorresearchcorporation.zendesk.com/hc/en-us/articles/10330492961563-How-to-Edit-Your-Profile
- Here's an article about adding yourself as a liaison
  - https://semiconductorresearchcorporation.zendesk.com/hc/en-us/articles/10092535189403-How-To-Add-Yourself-As-A-Liaison
- Here's an article about how to find research projects of interest
  - https://semiconductorresearchcorporation.zendesk.com/hc/en-us/articles/9194403647131-Using-Projects-Page
- There was 2 industry demonstrations for industry on February 14 and 21
  - The recordings can be found on the SRC.org website at : https://www.src.org/pillar/

SRC

https://semiconductorresearchcorporation.zendesk.com/hc/en-us/sections/11366772078235-How-Tos-for-Industry

Intellectual Property Statement

- The information provided by researchers during this annual review
  - Is the property of the university and of the researchers presenting this information
  - May include research results sponsored by and provided to the funding members
  - May include intellectual property rights belonging to the university and SRC, to which sponsors may have license rights

- By attending or viewing this review, you are agreeing
  - Not to use this information for purposes unrelated to the review unless and until approved by SRC
  - To keep this information in confidence until the university and SRC have evaluated and secured any applicable intellectual property rights

- After any intellectual property rights have been secured, the SRC encourages the University and researchers to publish and freely disseminate this information and results of the sponsored research program.
  - Worldwide patent rights are waived if publication or public dissemination occurs prior to filing a corresponding U.S. provisional or utility patent application

SRC

https://www.src.org/about/contracts-ip/#ip

General Data Protection Regulation

- Applies to SRC
- Personal data regulations
- Involves privacy notices, consent, and security
- SRC Privacy Policy

https://www.src.org/app/account/guide/privacy-policy/

Agenda – Day 1

- Presentations (30 minutes)
  - 25-minute presentations
  - With 5-minute Q&A (live)

Tuesday, June 6		
11:00 – 11:15 am	Welcome and Introduction	John Oakley / SRC
11:15 – 11:45 am	3064.001: Compiler Designs for Fully Homomorphic Encryption	Anwar Hithnawni / ETHZ – ETH Zurich
11:45 – 12:15 pm	3129.001: Automatic Discovery of Side-Channel Leakage	Michael Schwarz / CISPA Helmholtz Ctr for Information Security
11:45 – 12:15 pm	3199.001: Securing 2.5D/3D ICs Against IP Theft 3198.001: Exploring Hardware-Supported Patching for Resilient System on Chip Architectures	Krishnendu Chakrabarty / Arizona State University
1:15 – 2:00 pm	Break / Poster session (via GatherTown)	
2:00 – 2:30 pm	3194.001: AutoMap: Automated Mapping of Security Properties	Farimah Farahmandi / University of Florida
2:30 – 3:00 pm	3130.001: SPhnQs: Secure and Ultra-Low Energy Post-Quantum Accelerator for Resource Constrained Devices	Eslam Tawfik / Ohio State University – Columbus
3:00 – 3:30 pm	3128.001: Compositional Security Verification of Trusted Execution Environments	Prabhat Mishra / University of Florida
3:30 – 4:00 pm	3127.001: Safe and Secure Operating Systems for Root-of-Trust Silicon	Brad Campbell / University of Virginia - Charlottesville
4:00 – 5:00 pm	TAB Caucus	*Industry-only session*

All Times in ET

SRC

https://www.src.org/calendar/e007789/

Agenda – Day 2

- Presentations (30 minutes)
  - 25-minute presentations
  - With 5-minute Q&A (live)

All Times in ET

Wednesday, June 7		
11:00 – 11:15 am	Welcome and Introduction	John Oakley / SRC
11:15 – 11:45 am	3043.001: Efficient and Secure Lattice-based Post-Quantum Public-Key Cryptography (PQC) in Hardware: NIST's PQC Standardization and Beyond	Sujoy Sinha Roy / Technische Universität Graz
11:45 – 12:15 pm	3126.001: Real-Time Edge-based Security Monitoring and Reasoning	Mohsen Imani / University of California - Irvine
12:15 – 12:45 pm	3125.001: Secure and Programmable Open-Source Rot Augmented with IC Design Techniques for Side-Channel Attack Mitigation	Dennis M. Sylvester, Mehdi Saligane / University of Michigan – Ann Arbor
12:45 – 1:15 pm	3124.001: An Evolutionary AI-based Fuzz Testing for Extensive SoC Security Verification	Mark M. Tehranipoor / University of Florida
1:15 – 1:30 pm	Break	
1:30 – 2:00 pm	Industry Talk: Semiconductor Security Technology Adoption: Overcoming Resistance	Jean-Phillipe Martin / Intel
2:00 – 2:30 pm	3067.001: Detection and Prevention of Aging Attacks Targeting Electromigration	Linda Milor / Georgia Institute of Technology
2:30 – 3:00 pm	3065.001: Exploring Hardware-Supported Patching for Resilient System on Chip Architectures	Benjamin Tan / NYU Tandon School of Engineering
3:00 – 3:30 pm	3063.001: Reconfigurable Hardware for Secure IC Packaging using Nano-electromechanical Systems	Navid Asadi / University of Florida
3:30 – 4:00 pm	3062.001: Latch-Based Circuit Design for Power Analysis Attack and Delay Mitigation	Jennifer L. Dworak Students: Laskshmi Ramakrishnan, Nihu Rao / Southern Methodist University
4:00 – 5:00 pm	TAB Caucus	*Industry-only session*

https://www.src.org/calendar/e007789/

Agenda – Day 3

- Presentations (30 minutes)
  - 25-minute presentations
  - With 5-minute Q&A (live)

All Times in ET

Thursday, June 8		
11:00 – 11:15 am	Welcome / Introduction	John Oakley / SRC
11:15 – 11:45 am	**3061.001**: Metrics for Logic Circuit Security	Ronald D. Blanton / Carnegie Mellon University
11:45 – 12:15 pm	**3060.001**: Security Assurance for Multi-tenant Accelerators	Sandip Ray / University of Florida
12:15 – 12:45 pm	**3059.001**: Securing End-to-End Systems through Hardware Accelerated Homomorphic Encryption and Analytics in a Post-Quantum World	Arijit Raychowdhury, Zach Ellis (student) / Georgia Institute of Technology
12:45 – 1:15 pm	**2998.001**: Efficient Hardware Accelerator for Fully Homomorphic Encryption	Keshab K. Parhi, Weihang Tan (student) / University of Minnesota
1:15 – 2:00 pm	Break / Poster Session (via GatherTown)	
2:00 – 2:30 pm	**2997.001**: Fully Homomorphic Encryption Accelerated with Processing-In-Memory	Tajana S. Rosing / University of California – San Diego
2:30 – 3:00 pm	**2996.001**: Analog-Inspired Low Energy Secure and Trustworthy Wireless Transceivers for IoT Trusted Communications	Seyed Hossein Miri Lavasani / Case Western Reserve University
3:00 – 3:30 pm	**2995.001**: Thwarting Microarchitectural Replay Attacks	Josep Torrellas, Neil Zhao (student) / University of Illinois – Urbana-Champaign
3:30 – 4:00 pm	**2993.001**: Automatically Generating Information Flow Properties	Cynthia K. Sturton / University of North Carolina – Chapel Hill
4:00 – 5:00 pm	TAB Caucus	*Industry-only session*

SRC

https://www.src.org/calendar/e007789/

Agenda – Day 4

- Presentations (30 minutes)
  - 25-minute presentations
  - With 5-minute Q&A (live)

Friday, June 9		
11:00 – 11:15 am	Welcome / Introduction	John Oakley / SRC
11:15 – 12:15 pm	2992.001 / 2991.001: IP Protection through Secure and Private Function Evaluation - WPI	Fatemeh Ganji, Dev Mehta (student) / Worcester Polytechnic Institute Domenic Forte / University of Florida
12:15 – 12:45 pm	2990.001: Physical-Layer Identification and Authentication for Wireless IoT Devices	Taiyun Chi / Rice University
12:45 – 1:45 pm	TAB Caucus	*Industry-only session*

All Times in ET

https://www.src.org/calendar/e007789/

Thank You!

Opens?

John Oakley
Science Director
John.Oakley@src.org

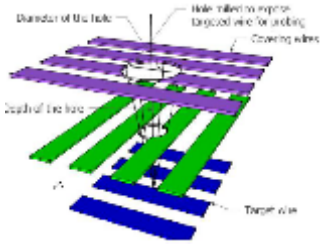
Hardware Security Research Program

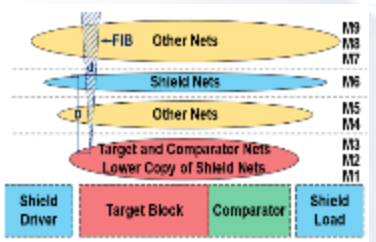
- The Hardware Security (HWS) Research Program is focused on developing strategies, techniques, and tools to provide assurance that electronic systems will perform as intended. Such assurance is a function of processes and tools integrated across all steps of design, manufacture, and distribution. In order to build a technological foundation that business and government can use to make systems that are trustworthy and secure, there is a need for fundamental, multidisciplinary research that spans architecture, design and manufacture.

- Current Research Portfolio is focused on:
  - Security Metrics and Hardware Security Properties
  - Taxonomy of Security Attacks/Flaws (like side channels)
  - Counterfeit Detection and Avoidance
  - Enabling Security by Design
  - Security Verification and Validation

Future Research Directions:

- New Research focus areas will include:
  - Handling for Dynamics Created by Future Artificial Intelligence devices
  - Real-time Attack Awareness and Mitigation Strategies
  - Novel approaches to End-to-End Security Solutions that eliminates the diverse communication method and inherent complexities.





https://www.src.org/program/grc/hws/

SRC Liaison Program

Maximizing the Value of Participation

Move Yourself, Your Company and the Next Generation Forward

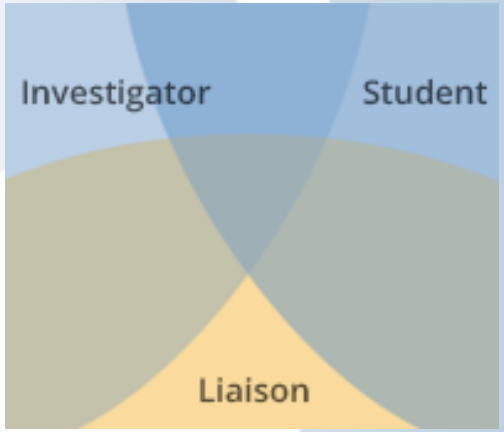
Develop the Workforce

- Provide relevant guidance for industry challenges
- Prepare students to enter industry or pursue future academics

Contribute to Research

- Encourage technology exchange between university and industry
- Bridge the conventional gap between academia and industry

Expectation to have regular PI-Liaisons calls at least one every 4-8 weeks



Academia Contributes to Industry

- Provide an out of the box approach to current problems which enhance industry research and development enables a differentiated product for the marketplace
- Provide an outside perspective adding diversity to the thought process of how best to attack a challenge

Access New Technology

- Gain valuable insights into problems and solutions that will ultimately impact industry competitiveness
- Provide an effective way to deliver actionable research results directly into their companies

Identify the Best

- Identify the most compelling research from current and recent research

SRC

https://www.src.org/liaison/