SUJAN KUMAR SAHA

Post-Doctoral Associate, ECE, University of Florida

sujansaha@ufl.edu (352)870-2169 704 SW 16th Ave, Apt 309 Gainesville, FL 32601
https://sujansaha05.github.io/ https://www.linkedin.com/in/sujan-saha-b7010326/
https://scholar.google.com/citations?hl=en&user=cgtLTMEAAAAJ

RESEARCH INTEREST

AI/LLM in System-on-Chip (SoC) Security, AI Hardware Security, Embedded System Security, Re-configurable Computing for Upgradable SoC Security

EDUCATION

Ph.D. in Electrical and Computer Engineering, University of Florida — Gainesville, FL 32603
Advisor: Dr. Christophe Bobda — May 2018 – August 2023

M.Sc. in Computer Engineering, University of California, Riverside — Riverside, CA 92521
Advisor: Dr. Hyoseung Kim — September 2016 – April 2018

B.Sc. in Electrical and Electronic Engineering — Dhaka, Bangladesh
Bangladesh University of Engineering and Technology — January 2006 – December 2010

CURRENT RESEARCH PROJECTS (POSTDOC)

AI/LLM in SoC Security

August 2023 - Present

Institution: University of Florida, **Advisor: Dr. Mark Tehranipoor and Dr. Farimah Farahmandi**
Funding Source: National Science Foundation (**NSF**)

- In this project, we investigate how to use LLM efficiently in different SoC security tasks such as asset identification, threat modeling, vulnerability detection, security property generation for formal verification, etc. by using LLM prompting, Retrieval-Augmented Generation (RAG), and fine-tuning open source LLMs. I am leading this project and working with eleven Ph.D. students to continue the effort. The solutions are available at **Deep-Chip** website. So far, we have published at **DATE 2026, VTS 2025, IEEE Access 2024, HOST 2024, 2025, GoMachtech 2025, MLCAD 2024, 2025 and VLSI-SoC 2024** (Best Paper Candidate).

SoC Security Verification

August 2023 - Present

Institution: University of Florida, **Advisor: Dr. Mark Tehranipoor and Dr. Farimah Farahmandi**
Funding Source: Semiconductor Research Corporation (**SRC**)

- The aim of this project is to develop different pre-silicon security verification methodologies for vulnerabilities detection in SoCs including fuzz and penetration testing, fault injection assessment, hardware emulation based verification, security property based verification etc. I am leading this effort with four PhD students and published at **ASP-DAC 2026, IEEE Design and Test 2025, VLSI-SoC 2025, and GoMactech 2025.**

PAST RESEARCH PROJECTS (PHD AND MASTERS)

Automated Integration of Secure Silicon (AISS)

April 2020 - July 2024

Institution: University of Florida, **Advisor:** Dr. Christophe Bobda and Dr. Mark Tehranipoor
Funding Source: Defense Advanced Research Projects Agency (**DARPA**)

- The goal of this **UF** and **Synopsys Inc.** collaborative research project was to develop a root-of-trust security subsystem for an SoC to enable hardware security functionality. I led the task "**Integration of security IPs into the subsystem**" during my graduate study as Ph.D. student.
- During my post-doctoral tenure, I led the development of **FTR-SE**, an open-source security subsystem featuring a RISC-V co-processor, cryptographic accelerator IPs, silicon lifecycle odometers, and security primitive IPs. I designed and integrated a mailbox IP to enable secure communication between the co-processor and host processor within an SoC. Project released publicly via GitHub.

- Co-developed a time and distance-based security quantification method to assess information leakage vulnerabilities in hardware IPs; integrated into **Synopsys VC SpyGlass tool** and published at **ICCD 2024**. Also proposed a system-level security quantification framework using Common Vulnerability Scoring System (CVSS) techniques, published at **IEEE HOST 2022**.

Multi-tenant cloud FPGA Security

August 2020 - August 2023

Institution: University of Florida, **Advisor:** Dr. Christophe Bobda
Funding Source: National Science Foundation (**NSF**)

- Worked with my colleague to investigate the security and performance issues of multi-tenant cloud FPGAs. We developed an isolation mechanism for secure operation of shared FPGAs in the cloud environment. Published at **IPDPSW 2021, GLSVLSI 2021, ISVLSI 2021 and ACM TRETS 2025**.

Access Control on Hardware Accelerator IPs in SoC

May 2018 - March 2020

Institution: University of Florida, **Advisor:** Dr. Christophe Bobda
Funding Source: Air Force Research Lab (**AFRL**)

- Developed a security framework to enable access control on hardware accelerator IPs in SoCs to prevent illegal access from software applications. Published at **AsianHOST 2020**. The dynamic policy update mechanism is developed to change the access control policies at run-time. Published at **GoMachtech 2021**.
- Contributed to the development of Python tool "MeXT-SE" that automatically generates the proposed security module [27] in HDL and the Tcl script that create Zynq SoC with the module in Xilinx Vivado tool.

Spatio-Temporal GPU management for Real-Time Systems

September 2016 - April 2018

Institution: University of California, Riverside, **Advisor:** Dr. Hyoseung Kim
Funding Source: Department Graduate Fellowship

- Developed a GPU management framework for Real-Time systems to increase GPU utilization and schedulability of the tasks. Published at **RTCSA 2019**.

WORK EXPERIENCE

Post-Doctoral Associate, FICS Research, ECE, University of Florida

August 2023 – Present

Advisor: Dr. Mark Tehranipoor and Dr. Farimah Farahmandi

Gainesville, FL 32603

- My job responsibilities include the supervision of Ph.D. students for multiple projects, writing research proposals for future grants, organizing seminars and workshops, and coordinating with research collaborators.

Graduate Research Assistant, University of Florida

May 2018 – August 2023

Advisor: Dr. Christophe Bobda

Gainesville, FL 32603

- Conducted research on secure integration of SoC IPs, focusing on hardware-level isolation techniques and runtime monitoring architectures for FPGA-based SoCs. Contributed significantly to the DARPA AISS program, NSF Cloud FPGA Security project, and AFRL-funded hardware access control initiative. Responsibilities included developing design specifications, creating FPGA prototypes, performing experiments, authoring research articles, publishing in peer-reviewed venues, and presenting findings at leading conferences.

Synopsys Inc.

June 2022 – November 2022

Technical Intern, Solution R&D Group

Sunnyvale, CA 94085

- Developed the provisioning firmware application of Watermarked IP in Security Engine Sub-system being developed for the DARPA AISS project.
- Designed, and implemented the MailBox IP and tested it in the Zynq SoC platform for inter processor communication used in the AISS project.

Xilinx Inc. (Now AMD-Xilinx)

June 2021 – December 2021

Design Engineering Intern, DFX Silicon Design

San Jose, CA 95124

- Developed two software tools using perl for automating the debug and test process of Xilinx FPGA chips

TEACHING EXPERIENCE

Adjunct Lecturer, ECE Department, University of Florida — Fall 2024

Course: EEL5764 - Computer Architecture

Instructor, ECE Department, University of Florida — Summer 2023

Course: EEL3834 - Programming I for Electrical Engineers

Graduate Teaching Assistant, ECE, University of Florida — Spring 2023

Course: System-on-Chip Design, Instructor: Dr. Christophe Bobda

Graduate Teaching Assistant, ECE, University of California, Riverside — Fall 2017

Course: Data Acquisition, Instrumentation, and Process Control, Instructor: Dr. Hyoseung Kim

PROFESSIONAL SERVICES

- Serving as a major contributor in Microelectronic Security Training (MEST) center. Responsibilities include moderating monthly webinars, planning certificate programs, and developing training modules.
- Served as TPC member of ACM Great Lake Symposium on VLSI (GLSVLSI) Conference 2025.
- Served as a committee member for the IEEE Computer Society Upsilon Pi Epsilon Honor Society Award 2025, 2026 contributing to the evaluation and selection of award recipients.
- Served as TPC member of IEEE International Symposium on Hardware Oriented Security and Trust (HOST) 2024.
- Served as Local Arrangement Chair of 32nd IEEE International Symposium on Field-Programmable Custom Computing Machines (FCCM) 2024.
- Served as TPC member of Brief presentation at 30th IEEE Real-Time and Embedded Technology and Application Symposium (RTAS) 2024.
- Worked as reviewer and sub-reviewer of multiple journals and conferences including Proceedings of the IEEE, IEEE Access, TCAD, TPDS, ACM TRETS, DAC, FCCM, FPL, FPT, Codes+ISSS, ASAP, and AsianHOST.

TALK, POSTER AND DEMONSTRATION

- **Lasp: Llm assisted security property generation for soc verification**
  Avinash Ayalasomayajula, Rui Guo, Jingbo Zhou, **Sujan Kumar Saha**, Farimah Farahmandi
  In Oral session of International Symposium on Machine Learning for CAD (MLCAD), 2024
- **A Hardware/Software Framework for System-on-FPGA Security**
  Sujan Kumar Saha, and Christophe Bobda
  In Oral session of Security for Custom Computing Machine (SCCM) Workshop, 2023
- **Metrics for Assessing Security of System-on-Chip**
  Sujan Kumar Saha, Joel Mandebi Mbongue, and Christophe Bobda
  In Open Poster session of Hardware Oriented Security and Trust (HOST) Symposium, 2022
- **System-Level Design of Secure System-on-Chips**
  Sujan Kumar Saha and Christophe Bobda
  In Open Demo session of Technical Demo Conference (TDC), 2021 at Florida Institute of Cybersecurity (FICS)
- **MeXT-SE: A Design Tool to Generate Secure MPSoCs**
  Md Jubaer Hossain Pantho, **Sujan Kumar Saha** and Christophe Bobda
  In Open Demo session of Hardware Oriented Security and Trust (HOST) Symposium, 2020
- **FPGA Accelerated Embedded System Security Through Hardware Isolation**
  Sujan Kumar Saha and Christophe Bobda
  In Oral presentation session of Asian Hardware Oriented Security and Trust (AsianHOST) conference 2020, and open poster session of Annual Warren B. Nems IoT Conference, 2019 at University of Florida

AWARDS AND HONORS

- **Wilson and Marie Collins Endowment for graduate fellowship award**, Summer 2023
  ECE Department, University of Florida
- **Deans Distinguished Fellowship**, Fall 2016 - Fall 2017
  ECE Department, University of California, Riverside

- **Merit Scholarship**, Year 2006 - Year 2009
  Comilla Education Board, Bangladesh
  In top 1% in nationwide Higher Secondary Certificate Examination

PUBLICATIONS

Book Chapter:

[1] C. Bobda, J. M. Mbongue, **S. K. Saha**, and M. K. Ahmed. "Domain isolation and access control in multi-tenant cloud FPGAs". In: *Security of FPGA-Accelerated Cloud Computing Environments*. Springer, 2023, pp. 29–55.

Patent:

[2] M. Tehranipoor, S. Saha, **S. K. Saha**, F. Farahmandi, F. Rahman, H. Al-Shaikh, and K. Z. Azar. *Gray-box Hardware Penetration Testing Framework for Hardware Security Verification*. **US patent** filed (under review). **2025**.

Journals:

[3] H. Al Shaikh, S. Saha, **S. K. Saha**, K. Z. Azar, F. Farahmandi, and M. Tehranipoor. "Rethinking System-on-Chip Verification for Secure Cross-layer Interactions". In: *IEEE **Design & Test*** (**2025**).

[4] P. E Calzada, Z. Ibnat, T. Rahman, K. Kandula, D. Lu, **S. K. Saha**, F. Farahmandi, and M. Tehranipoor. "VerilogDB: The Largest, Highest-Quality Dataset with a Preprocessing Framework for LLM-based RTL Generation". In: *arXiv preprint arXiv:2507.13369* (**2025**).

[5] R. Guo, A. Ayalasomayajula, H. Li, J. Zhou, **S. K. Saha**, and F. Farahmandi. "SVAgent: AI Agent for Hardware Security Verification Assertion". In: *arXiv preprint arXiv:2507.16203* (**2025**).

[6] Z. Ibnat, P. E. Calzada, R. M. Ihtemam, **S. K. Saha**, J. Zhou, F. Farahmandi, and M. Tehranipoor. "DeepV: A Model-Agnostic Retrieval-Augmented Framework for Verilog Code Generation with a High-Quality Knowledge Base". In: *arXiv preprint arXiv:2510.05327* (**2025**).

[7] M. K. Ahmed, M. Panoff K., J. M. Mbongue, **S. K. Saha**, E. N. Tchinda, P. E. Mbua, and C. Bobda. "Multi-Tenant Cloud FPGA: A Survey on Security, Trust, and Privacy". In: *ACM Transactions on Reconfigurable Technology and Systems(**TRETS**)* 18.2 (**2025**), pp. 1–44.

[8] D. Saha, S. Tarek, H. A. Shaikh, K. T. Hasan, P. S. Nalluri, Md. A. Hasan, N. Alam, J. Zhou, **S. K. Saha**, M. Tehranipoor, and F. Farahmandi. "SV-LLM: An Agentic Approach for SoC Security Verification using Large Language Models". In: *arXiv preprint arXiv:2506.20415* (**2025**).

[9] D. Saha, S. Tarek, K. Yahyaei, **S. K. Saha**, J. Zhou, M. Tehranipoor, and F. Farahmandi. "Llm for soc security: A paradigm shift". In: ***IEEE Access*** (**2024**).

Conferences:

[10] M. A. Hasan, D. Saha, K. T. Hasan, N. Alam, A. Uddin, **S. K. Saha**, M. Tehranipoor, and F. Farahmandi. "LAsset: An LLM-assisted Security Asset Identification Framework for SoC Verification". In: *Accepted at **DATE***. **2026**.

[11] B. Ahmed, **S. K. Saha**, and J. Liu. "Modified bus invert encoding to reduce capacitive crosstalk, power and inductive noise". In: *2015 2nd International Conference on Electrical Information and Communication Technologies (**EICT**)*. IEEE. **2015**, pp. 95–100.

[12] B. Ahmed, **S. K. Saha**, J. Zhou, S. Aftabjahani, M. Tehranipoor, and F. Farahmandi. "Continuity in Security: Leveraging LLM for Translating Security Properties Across Hardware Designs". In: *2024 IFIP/IEEE 32nd International Conference on Very Large Scale Integration (**VLSI-SoC**)*. IEEE. **2024**, 1–6, **Best paper candidate**.

[13] M. K. Ahmed, **S. K. Saha**, and C. Bobda. "Trusted IP solution in multi-tenant cloud FPGA platform". In: *2022 IEEE 8th World Forum on Internet of Things (**WF-IoT**)*. IEEE. **2022**, pp. 1–6.

[14] A. Ayalasomayajula, R. Guo, J. Zhou, **S. K. Saha**, and F. Farahmandi. "Lasp: Llm assisted security property generation for soc verification". In: *Proceedings of the 2024 ACM/IEEE International Symposium on Machine Learning for CAD **(MLCAD)***. **2024**, pp. 1–7.

[15] A. Ayalasomayajula, H. Li, H. Al-Shaikh, **S. K. Saha**, and F. Farahmandi. "TDM: Time and Distance Metric for Quantifying Information Leakage Vulnerabilities in SoCs". In: *2024 IEEE 42nd International Conference on Computer Design (**ICCD**)*. IEEE. **2024**, pp. 130–133.

[16] P. Bhowmik, M.J.H. Pantho, **S. K. Saha**, and C. Bobda. "Attention-Based Secure Feature Extraction in Near Sensor Processing: Work-in-Progress". In: *2020 International **CODES+ ISSS** Conference*. IEEE. **2020**, pp. 21–23.

[17] P. Bhowmik, Md J. H. Pantho, **S. K. Saha**, and C. Bobda. "A Reconfigurable Layered-Based Bio-Inspired Smart Image Sensor". In: *2019 IEEE Computer Society Annual Symposium on VLSI (**ISVLSI**)*. IEEE. **2019**, pp. 169–174.

[18] C. Bobda, H. Ishebabi, P. Mahr, J. M. Mbongue, and **S. K. Saha**. "MeXT: A flow for multiprocessor exploration". In: *2019 IEEE High Performance Extreme Computing Conference (**HPEC**)*. IEEE. **2019**, pp. 1–7.

[19] C. Bobda, T. Whitaker, J. M. Mbongue, and **S. K. Saha**. "Synthesis of hardware sandboxes for trojan mitigation in systems on chip". In: *2019 IEEE High Performance Extreme Computing Conference (**HPEC**)*. IEEE. **2019**, pp. 1–6.

[20] Z. Ibnat, P. E Calzada, D. Saha, H. Al-Shaikh, **S. K. Saha**, J. Zhou, F. Farahmandi, and M. Tehranipoor. "Trusting the Machine: How Secure is LLM-Generated RTL Code?" In: *2025 ACM/IEEE 7th Symposium on Machine Learning for CAD (**MLCAD**)*. IEEE. **2025**, pp. 1–8.

[21] M. M. M. Rahman, **S. K. Saha**, M. Tehranipoor, and F. Farahmandi. "Automating Security Monitoring Event Generation for SoCs Using Large Language Models". In: *Accepted at Annual **GOMACTECH** Conference*. **2026**.

[22] J. M. Mbongue, **S. K. Saha**, and C. Bobda. "A security architecture for domain isolation in multi-tenant cloud FPGAs". In: *2021 IEEE Computer Society Annual Symposium on VLSI (**ISVLSI**)*. IEEE. **2021**, pp. 290–295.

[23] J. M. Mbongue, **S. K. Saha**, and C. Bobda. "Domain Isolation in FPGA-Accelerated Cloud and Data Center Applications". In: *Proceedings of the 2021 on Great Lakes Symposium on VLSI (**GLSVLSI**)*. **2021**, pp. 283–288.

[24] J. M. Mbongue, **S. K. Saha**, and C. Bobda. "Performance study of multi-tenant cloud FPGAs". In: *2021 IEEE International Parallel and Distributed Processing Symposium Workshops (**IPDPSW**)*. IEEE. **2021**, pp. 168–171.

[25] **S. K. Saha**, B. Ahmed, and J. Liu. "A survey on interconnect encoding for reducing power consumption, delay, and crosstalk". In: *2015 2nd International Conference on Electrical Information and Communication Technologies (**EICT**)*. IEEE. **2015**, pp. 7–12.

[26] **S. K. Saha**, M. K. Ahmed, and C. Bobda. "A Hardware/Software Architecture for System-on-Chip Security". In: *2023 Annual **GOMACTECH** Conference*. **2023**.

[27] **S. K. Saha** and C. Bobda. "FPGA Accelerated Embedded System Security Through Hardware Isolation". In: *2020 IEEE Asian Hardware Oriented Security and Trust Symposium (**AsianHOST**)*. IEEE. **2020**, pp. 1–6.

[28] **S. K. Saha** and C. Bobda. "System-on-Chip (SoC) Security through Dynamic Policy Enforcement in Hardware Accelerators". In: *2021 Annual **GOMACTECH** Conference*. **2021**.

[29] **S. K. Saha**, A. N. Butka, M. K. Ahmed, and C. Bobda. "OpenTitan based multi-level security in FPGA system-on-chips". In: *2023 IEEE International Conference on Field Programmable Technology (**FPT**)*. IEEE. **2023**, pp. 302–303.

[30] **S. K. Saha** and J. Liu. "Byte-Based Partial-Match instruction and data compression for high-performance and low-power interconnects". In: *2016 14th IEEE International New Circuits and Systems Conference (**NEWCAS**)*. IEEE. **2016**, pp. 1–4.

[31] **S. K. Saha**, J. M. Mbongue, and C. Bobda. "Metrics for Assessing Security of System-on-Chip". In: *2022 IEEE International Symposium on Hardware Oriented Security and Trust (**HOST**)*. IEEE. **2022**, pp. 113–116.

[32] **S. K. Saha**, Y. Xiang, and H. Kim. "STGM: Spatio-Temporal GPU Management for Real-Time Tasks". In: *2019 IEEE 25th International **RTCSA** Conference*. IEEE. **2019**, pp. 1–6.

[33] D. Saha, **S. K. Saha**, J. Zhou, M. Tehranipoor, and F. Farahmandi. "Enhancing Hardware Security: Detecting Vulnerabilities in HDL Codes Using Fine-Tuned Large Language Model". In: *Accepted at Annual **GOMACTECH** Conference*. **2025**.

[34] D. Saha, K. Yahyaei, **S. K. Saha**, M. Tehranipoor, and F. Farahmandi. "Empowering hardware security with llm: The development of a vulnerable hardware database". In: *2024 IEEE International Symposium on Hardware Oriented Security and Trust (**HOST**)*. IEEE. **2024**, pp. 233–243.

[35] S. Saha, A. Alhurubi, T. Rahman, H. A. Shaikh, **S. K. Saha**, F. Farahmandi, and M. Tehranipoor. "GEmFuzz: Uncovering System-Level Vulnerabilities in SoCs via Emulation-Based Grey-Box Fuzzing". In: *Accepted at **ASP-DAC***. **2026**.

[36] S. Saha, A. Alhurubi, T. Rahman, **S. K. Saha**, F. Farahmandi, and M. Tehranipoor. "Emulation-based Fuzzing for System-level Vulnerability Detection". In: *Accepted at Annual **GOMACTECH** Conference*. **2026**.

[37] Md. S. U. I. Sami, J. Zhou, **S. K. Saha**, F. Rahman, F. Farahmandi, and M. Tehranipoor. "SAP: Silicon Authentication Platform for System-on-Chip Supply Chain Vulnerabilities". In: *2024 IEEE International Symposium on Performance Analysis of Systems and Software (**ISPASS**)*. IEEE. **2024**, pp. 109–119.

[38] S. Tarek, D. Saha, **S. K. Saha**, and F. Farahmandi. "BugWhisperer: Fine-Tuning LLMs for SoC Hardware Vulnerability Detection". In: *2025 IEEE 43rd VLSI Test Symposium (**VTS**)*. IEEE. **2025**, pp. 1–5.

[39] S. Tarek, D. Saha, **S. K. Saha**, M. Tehranipoor, and F. Farahmandi. "Socurellm: An llm-driven approach for large-scale system-on-chip security verification and policy generation". In: *2025 IEEE International Symposium on Hardware Oriented Security and Trust (**HOST**)*. IEEE. **2025**, pp. 335–345.

[40] S. Tarek, D. Saha, **S. K. Saha**, M. Tehranipoor, and F. Farahmandi. "Threat2SVA: Threat Model and CWE-Aware Security Assertion Generation Using LLM". in: *Accepted at Annual **GOMACTECH** Conference*. **2026**.

[41] A. Uddin, **S. K. Saha**, F. Farahmandi, and M. Tehranipoor. "Case Study: Fault-Injection Vulnerability Assessment at RTL Level". In: *2024 IEEE Physical Assurance and Inspection of Electronics (**PAINE**)*. IEEE. **2024**, pp. 1–7.

SKILLS

Software Programming Language: C, C++, Python, Perl, CUDA C
Hardware Programming Language: Verilog, VHDL, SystemC
Scripting Language: Linux shell, Tcl
Revision Control: Github, GitLab
Tools: Xilinx Vivado, Petalinux, Intel Quartus, ModelSim, Synopsys Design Compiler, VCS, CoreTools, Platform Architect, Gem5, MATLAB

REFERENCES

Mark M. Tehranipoor
Professor, Chair, ECE
University of Florida
Email:*tehranipoor@ece.ufl.edu*

Christophe Bobda
Professor, ECE
University of Florida
Email:*cbobda@ece.ufl.edu*

Farimah Farahmandi
Associate Professor, ECE
University of Florida
Email:*farimah@ece.ufl.edu*

Li-C Wang
Professor, ECE
UC Santa Barbara
Email:*licwang@ece.ucsb.edu*

Waleed Khalil
Professor, ECE
Ohio State University
Email:*khalil.18@osu.edu*