ISHRAQ TASHDID

tashdid.ishraq@gmail.com — ishraq.tashdid@ucf.edu — +1 (689) 286-7719
Orlando, FL 32817 — LinkedIn — GitHub

Research Interests

Automated vulnerability reasoning and threat modeling (CWE/CVE/CAPEC); LLM-assisted security analysis across hardware–firmware–software boundaries; formal and property-based security verification; chiplet and SiP authentication; secure SoC design.

Education

University of Central Florida (UCF) *Jan. 2024–Present*
Ph.D. in Computer Engineering (Joint PhD/MS)
Trustee's Doctoral Fellow CGPA: **4.00**/4.00

Bangladesh University of Engineering and Technology (BUET) *Feb. 2017–Jun. 2022*
B.Sc. in Electrical and Electronic Engineering CGPA: 3.48/4.00

Research Experience

Graduate Research Assistant — University of Central Florida *Jan. 2024–Present*

- **LLM-driven threat modeling & automated vulnerability reasoning (DAC 2026):** Built *ATLAS*, a framework that ingests CWE/CVE/CAPEC vulnerability databases, auto-generates structured threat models for any SoC asset, and translates them into formal security properties verified by JasperGold. Detected 39/48 known CWEs across three HACK@DAC benchmarks (> 82% correct property generation). Directly applicable to firmware and software vulnerability workflows that reason over the same threat taxonomies.
- **Automated security property generation & cross-abstraction analysis:** Developed pipelines combining static analysis, AST-level structural reasoning, execution traces, and formal verification feedback to generate precise security assertions with minimal human effort, reducing reliance on manually crafted security rules at every abstraction layer from RTL through system firmware.
- **Chiplet authentication via PUF and MPC (HOST 2026):** Designed *InterPUF*, a distributed authentication framework for reconfigurable System-in-Package (SiP) interposers. Embedded a differential delay PUF in the interconnect fabric and secured evaluation using multi-party computation (MPC), ensuring raw signatures never leave the device. Achieved $< 0.23\%$ area and $< 0.072\%$ power overhead; ML modeling attacks converged at $\sim 47\%$ accuracy (random-guess level).
- **Macro placement automation (MLCAD 2025 — Best Paper Nominee):** Designed human-inspired reinforcement learning frameworks for chip floorplanning to improve post-route routability and reliability in heterogeneous SoCs.

Industry Experience

Hardware Verification Engineer — XCelerium, Irvine, CA *Jan. 2022–Dec. 2023*

- Verified custom **RISC-V** processor implementations at the ISA and **system level** using SystemVerilog, UVM, and cocotb — developing strong familiarity with the hardware-software boundary where firmware executes and privilege/mode transitions occur.
- Verified **AXI memory controllers** and **APB-AXI bridges**, including CDC edge-cases and assertion-based checks on bus-level access control — the same protocol surfaces targeted by firmware and software security assessments.
- Built **Python-driven automation frameworks** for coverage convergence, testbench orchestration, and results analysis, accelerating sign-off across multiple projects.

Selected Publications

- **Ishraq Tashdid**, Tasnuva Farheen, Sazadur Rahman, *"ATLAS: AI-Assisted Threat-to-Assertion Learning for System-on-Chip Security Verification,"* **DAC 2026** (63rd Design Automation Conference), Long Beach, CA, USA. *Accepted.*
- **Ishraq Tashdid**, Tasnuva Farheen, Sazadur Rahman, *"InterPUF: Distributed Authentication via Phys-*

ically Unclonable Functions and Multi-party Computation for Reconfigurable Interposers," **HOST 2026** (IEEE Int'l Symposium on Hardware Oriented Security and Trust), Washington, D.C., USA. *Accepted.*

- **Ishraq Tashdid**, Dewan Saiham, Nafisa Anjum, Tasnuva Farheen, Sazadur Rahman, *"ECOLogic: Enabling Circular, Obfuscated, and Adaptive Logic via eFPGA-Augmented SoCs,"* **ICCD 2025**, Dallas, TX, USA.
- **Ishraq Tashdid**, Tasnuva Farheen, Sazadur Rahman, *"SAFE-SiP: Secure Authentication Framework for System-in-Package Using Multi-party Computation,"* **GLSVLSI 2025**, New Orleans, LA, USA.
- **Ishraq Tashdid**, Tasnuva Farheen, Sazadur Rahman, *"AuthenTree: A Scalable MPC-Based Distributed Trust Architecture for Chiplet-based Heterogeneous Systems,"* **PAINE 2025**, Denver, CO, USA.
- **Ishraq Tashdid**, Valentina Terry, Jordan Merkel, Tasnuva Farheen, Sazadur Rahman, *"BeyondPPA: Human-Inspired Reinforcement Learning for Post-Route Reliability-Aware Macro Placement,"* **MLCAD 2025**, Santa Cruz, CA, USA. **Best Paper Nominee.**
- **Book Chapter (invited):** *LLM for SoC Design and Security* — with UF collaborators, *in preparation*, 2025.

Teaching & Mentoring

Graduate Teaching Assistant — UCF ECE *Spring 2024; Summer & Fall 2025*

- Grading and office hours for Engineering Analysis and Computation; Linear Systems II; Electronics II Lab; Digital Systems Lab.

Undergraduate Mentoring *Aug. 2024–Present*

- Mentored two undergraduate researchers; both earned summer 2025 internships at **AMD** and **Northrop Grumman** and co-authored the MLCAD 2025 Best Paper Nominee.

Invited Talks

Intel AI Forum *Feb. 2026*

Invited talk on *ATLAS*: LLM-driven threat modeling and formal security verification for SoC security — presented to Intel's AI research community.

Florida Semiconductor Summit (FSI) *Feb. 2026*

Invited presentation at the 4th Annual Florida Semiconductor Summit, Rosen Shingle Creek, Orlando, FL. Theme: *Semiconductor Manufacturing in Florida: Power. Progress. Possibilities.*

Honors, Awards & Service

UCF Trustee Doctoral Fellowship (4-year funding), 2024–2028
Best Paper Award Nominee, MLCAD 2025
NSF Travel Grant, IEEE HOST 2025
External Reviewer, IEEE ICCD 2025

Skills

Security & Analysis:	Threat modeling (CWE/CVE/CAPEC), LLM-assisted vulnerability reasoning, assertion-based verification, formal verification (JasperGold), static analysis
Programming:	Python, SystemVerilog, Verilog, C, MATLAB, Assembly
Verification:	UVM, cocotb, pytest, ABV; RISC-V ISA & system-level compliance; AXI/APB bus protocols
EDA & Simulation:	Cadence Innovus / Genus / JasperGold, ModelSim, Quartus Prime, Yosys, PyVerilog