

TANZIM MAHFUZ

+2079510990  tanzim.mahfuz@maine.edu  LinkedIn  GitHub
 Google Scholar  ResearchGate  Web of Science

Education

Ph.D. in Electrical and Computer Engineering

University of Maine, Orono, USA

Fall 2022 - Ongoing

Research Assistant, SIEGE Lab, CGPA: 3.76

Master of Science in Computer Engineering

University of Maine, Orono, USA

September 2022 - May 2025

Research Assistant, SIEGE Lab, CGPA: 3.67

Bachelor of Science in Computer Science & Engineering

Jahangirnagar University, Dhaka, Bangladesh

March 2016 - January 2021

CGPA: 3.79, Position: 3rd

Research Interests & Technical Skills

-  **Security & Trust:** Hardware Supply Chain Security (Obfuscation, Side-Channel, Hardware Trojan).
-  **Machine Learning:** Pytorch, Gen AI, Agentic AI, LLM, Langchain, Langgraph.
-  **Software Systems:** Python, Synopsys, C, C++, MATLAB, Java, Debian, Redhat, Docker, Django.

Published Research Articles

- X-DFS: Explainable Artificial Intelligence Guided Design-for-Security Solution Space Exploration**, Tanzim Mahfuz, Swarup Bhunia, Prabuddha Chakraborty, *Published in IEEE Transactions on Information Forensics and Security (TIFS)*, 2024.
 **Impact Factor: 8.7**
 <https://ieeexplore.ieee.org/document/10798618>
- Learning Your Lock: Exploiting Structural Vulnerabilities in Logic Locking**, Prabuddha Chakraborty, Jonathan Cruz, Rasheed Almazawan, Tanzim Mahfuz, Swarup Bhunia, *Published in IEEE Design & Test*, 2024.
 **Impact Factor: 1.9**
 <https://ieeexplore.ieee.org/abstract/document/10400498>
- DERMS Cybersecurity Scenarios, Trends, and Potential Technologies: A Review**, Niroop Sugunaraj, ..., Tanzim Mahfuz, Prabuddha Chakraborty, ..., Prakash Ranganathan, *Published in IEEE Communications Surveys & Tutorials*, 2024.
 **Impact Factor: 50.6**
 <https://ieeexplore.ieee.org/document/10858368>
- SALTY: Explainable Artificial Intelligence Guided Structural Analysis for Hardware Trojan Detection**, Tanzim Mahfuz, Pravin Gaikwad, Tasneem Suha, Swarup Bhunia, Prabuddha Chakraborty, *Published in 43rd IEEE VLSI Test Symposium*, 2025.
 **Core Rank: A**
 <https://ieeexplore.ieee.org/document/11022818>
- POLARIS: Explainable Artificial Intelligence for Mitigating Power Side-Channel Leakage**, Tanzim Mahfuz, Sudipta Paria, Tasneem Suha, Swarup Bhunia, Prabuddha Chakraborty, *Published in 62nd Design Automation Conference*, 2025.
 **Core Rank: A***
 <https://ieeexplore.ieee.org/abstract/document/11132622>
- DISARM: Target Electronic Device Informed Mitigation of Software Runtime Side Channel Vulnerabilities**, Tasneem Suha, Tanzim Mahfuz, Rima Asmar Awad, Prabuddha Chakraborty, *Published in IEEE Transactions on Information Forensics and Security (TIFS)*, 2026.
 **Impact Factor: 8.7**
 <https://ieeexplore.ieee.org/abstract/document/11579425>

7. **DASH: A Meta-Attack Framework for Synthesizing Effective and Stealthy Adversarial Examples**, Abdullah Al Nomaan Nafi, Habibur Rahaman, Zafaryab Haider, Tanzim Mahfuz, Fnu Suya, Swarup Bhunia, Prabuddha Chakraborty, *Published in IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2026.
 **Core Rank: A***
 <https://tinyurl.com/IEEECVPR>
8. **Reducing Wrong Labels using Conflict Score in Distant Supervision for Relation Extraction in Bangla Language**, Tanzim Mahfuz, Tasneem Suha, Md Musfique Anwar, *IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, 2020.
 <https://ieeexplore.ieee.org/document/9411604>
9. **XAI Guided Design-for-Security.**, Tanzim Mahfuz, Swarup Bhunia, Prabuddha Chakraborty, *Published in Government Microcircuit Applications & Critical Technology Conference (GOMACTech)*, 2025. [\[Public release is prohibited\]](#)
10. **Secure and Trustworthy Microelectronics: Vulnerabilities, Solutions, and Trends**, Sriram Prabhakara Rao, , Tanzim Mahfuz, Prabuddha Chakraborty, Prakash Ranganathan *Published in Journal of Hardware and Systems Security*, 2025.
 <https://link.springer.com/article/10.1007/s41635-025-00165-x>
11. **LLM-Orchestrated Agentic AI Framework for SWaP Aware Microelectronics Security**, Tanzim Mahfuz, Tasneem Suha, Prabuddha Chakraborty, *Accepted in Government Microcircuit Applications & Critical Technology Conference (GOMACTech)*, 2026. [\[Public release is prohibited\]](#)
12. **XAI Enabled Power Side-Channel Estimation & Mitigation in Sensitive Digital Hardware**, Tanzim Mahfuz, Tasneem Suha, Prabuddha Chakraborty, *Accepted in Government Microcircuit Applications & Critical Technology Conference (GOMACTech)*, 2026. [\[Public release is prohibited\]](#)
13. **Hardware Aware Mitigation of Timing Side-Channel Vulnerabilities in Critical Infrastructure Software**, Tasneem Suha, Tanzim Mahfuz, Prabuddha Chakraborty, *Accepted in Government Microcircuit Applications & Critical Technology Conference (GOMACTech)*, 2026. [\[Public release is prohibited\]](#)

Patent Applications

1. **Generative AI Based Leakage-Aware Secure Transformations in Digital Hardware**, Tanzim Mahfuz, Tasneem Farhana Suha, Sudipta Paria, Swarup Bhunia, Prabuddha Chakraborty, *Provisional Patent Submitted, App.No.: 63/827,407*. [\[Joint filed with University of Florida\]](#)
2. **Explainable Agentic Framework For Determining Cross PDK Migration Difficulty**, Tanzim Mahfuz, Zafaryab Haider, Timothy Regan, Prabuddha Chakraborty, *Provisional Patent Submitted, App. No.: 64/075,062*. [\[Joint filed with IN2FAB Technology LLC\]](#)

Articles Under Peer Review

1. **LOGIC: An LLM-Orchestrated Agentic Framework for Secure Hardware Design Optimization**, Tanzim Mahfuz, Tasneem Suha, Abdullah Al Nomaan Nafi, Prabuddha Chakraborty, *Submitted in IEEE Transactions on Reliability*, 2026.
2. **MAGE: Conjuring Boolean Masking Gadgets with Large Language Models for Side-Channel Leakage Reduction**, Tasneem Suha, Tanzim Mahfuz, Prabuddha Chakraborty, *Submitted in IEEE Cyber Awareness & Research Symposium*, 2026.
3. **HARP: Measuring Harm Amplification in Multi-Agent LLM Systems**, Md Hafizur Rahman, Zafaryab Haider, Tanzim Mahfuz, Prabuddha Chakraborty, *Submitted in IEEE Symposium on Security and Privacy*, 2026.

Top Journal, Conference Activity as Author

1. **IEEE Transactions on Information Forensics and Security**
 - Number 1 journal in Computer Security & Cryptography Category by Google Metrics.
2. **IEEE/CVF Conference on Computer Vision and Pattern Recognition**
 - Number 1 conference in Engineering & Computer Science and Number 2 conference across all type of research by Google Metrics.
3. **IEEE Communications Surveys and Tutorials**
 - Number 1 journal in Electrical & Electronic Engineering by Google Metrics.
4. **Government Microcircuit Applications & Critical Technology Conference**
 - Number 1 conference in Microelectronic Security For Government of United States.
5. **Design & Automation Conference**
 - Number 1 conference in Hardware Design, Automation by Google Metrics.
6. **IEEE VLSI Test Symposium.**
7. **Journal of Hardware & Systems Security.**

Awards & Achievements

1. **1st in Cybersecurity Games & Conference, New York University, 2023**, Sudipta Paria, Aritra Dasgupta, Tanzim Mahfuz, Pravin Gaikwad
 - Logic Locking Competition (served as Red Team).
 - Got Travel Grant to participate in-person.
2. **3rd in HeLLO: CTF 2023**, Tanzim Mahfuz, Prabuddha Chakraborty
 - Hardware Obfuscation (served as Red Team).
3. **Prestigious DAC Young Fellowship, 2025**
 - Given by Program Committee of Design Automation Conference (DAC), 2025.
4. **Travel Grant for DAC, National Science Foundation, 2025**
 - Given by NSF Workshop on Hardware Attack Artifacts, Analysis, and Metrics (WHAAAM).
5. **Best Cultural Presentation at Umaine Cultural Fest, 2023**
 - Given by Office of International Program, University of Maine, Orono.
 - Served as President of Bangladesh Students' Association.
6. **Travel Grant, Bangladesh Sweden Trust Fund, 2023**
 - Given by Ministry of Finance, Bangladesh.
7. **Travel Grant, Cyber Awareness and Research Symposium (CARS), 2022**
 - Given by University of North Dakota, USA.
8. **National Science & Technology Fellowship, 2022**
 - Given by Ministry of Science & Technology, Bangladesh.

Professional Certifications

- **IBM Professional Data Science.** (view)
- **Applied Data Science Capstone.** (view)
- **Internet of Things and Embedded Systems.** (view)
- **Arduino Platform and C programming.** (view)

Professional Experiences

Graduate Student Member: Institute of Electrical and Electronics Engineer (IEEE)

ID: 98543655

Instructor: NSF ITEST Semiconductor Summer Camp

July 2025

5 day Camp, Portland, Maine

Reviewer: Journal of Electronic Testing

October 2025

Article about Power Side-Channel Analysis

Reviewer: ACM Transactions on Design Automation of Electronic Systems

June 2025

Article about Hardware Obfuscation

Reviewer: IEEE Transactions on Very Large Scale Integration Systems

January 2025

Article about Hardware Trojan

Reviewer: IEEE Access

February 2025

Article about Hardware Trojan

Judge: Undergraduate Research Judge

April 2024

University of Maine Student Symposium

Software Engineer

July 2021 – April 2022

Robi Axiata Limited, Dhaka

Presentations & Talk

POLARIS: Explainable Artificial Intelligence for Mitigating Power Side-Channel Leakage.

– **Oral:** 62nd Design & Automation Conference, San Francisco, June, 2025.

– **Poster:** The Warren B. Nelms Annual IoT Conference, University of Florida, December, 2025.

– **Poster:** DAC Young Fellowship Program, December, 2025.

SALTY: Explainable Artificial Intelligence Guided Structural Analysis for Hardware Trojan Detection.

– **Oral:** NSF Hardware Assurance Workshop, DAC, June, 2025.

– **Oral:** 43rd IEEE VLSI Test Symposium, Arizona State University, April, 2025.

– **Panel:** WHiSPeS: Wearable Health monitoring Systems for Privacy & Security, UNH, March, 2025.

– **Poster:** Umaine Student Symposium, April, 2025.

Securing Microelectronic Designs from Reverse Engineering using Artificial Intelligence.

– **Poster:** New England Hardware Security Day, Massachusetts Institute of Technology, April, 2025.

– **Poster:** The Roux Institute at Northeastern University, Portland, Maine, January, 2023.

– **Poster:** Cyber Awareness and Research Symposium, University of North Dakota, October, 2022.

Course Projects

- 1. Mobile Robotics: Simulation of a Custom Path Planning for xArm using ROS**
- 2. HCI: EchoMind: An Voice assistant for ESL users and Speech Disorders - View.**
- 3. IoT Home Automation: Small Scale Scenario**
 - Control home appliances using GSM module.
- 4. IoT Smart City Design: Small Scale Scenario**
 - Included smart class, smart transportation, smart kitchen.
- 5. RC car using bluetooth**
 - Included L298N motor driver, Arduino UNO.
- 6. Python: Offline Voice Controlled Desktop Manager - Sample Code.**