

Tanvir Arafin

Department of Cyber Security Engineering,
George Mason University, Fairfax, VA 22030

☎ +1 (703) 993 1741 • ✉ marafin@gmu.edu • 🌐 tanvirarafin.github.io

Education

University of Maryland <i>Ph.D., Electrical Engineering</i> Dissertation: Hardware-Based Authentication for the Internet of Things	Collage Park, MD 2018
University of Maryland <i>M.Sc., Electrical Engineering</i>	Collage Park, MD 2016
Bangladesh University of Engineering & Technology <i>B.Sc., Electrical & Electronic Engineering</i>	Dhaka, Bangladesh 2011

Professional Appointments

George Mason University <i>Tenure-Track Assistant Professor</i> Department of Cyber Security Engineering <i>Affiliate Faculty</i> Center of Excellence in C5I	Fairfax, VA <i>current – 2022</i>
Morgan State University <i>Tenure-track Assistant Professor</i> Electrical and Computer Engineering Department <i>Assistant Director</i> Cybersecurity Assurance and Policy (CAP) Center	Baltimore, MD 2022 – 2019
Bloomberg <i>Software Engineer</i>	New York, NY 2019 – 2018
Bangladesh University of Engineering & Technology <i>Lecturer</i>	Dhaka, Bangladesh 2012 – 2011

Internships

Cyber Innovation Group, Philips <i>Vulnerability Research Intern</i>	Andover, MA 2017 – 2016
Security & Privacy Group, Bosch <i>Research Intern</i>	Pittsburgh, PA 2016

Honors & Awards

Best Hardware Demo: 2nd Place

IEEE International Symposium on Hardware Oriented Security and Trust (HOST) 2024

Featured Paper of the Month

IEEE Transactions on Computers (TC) 2022

Best Paper Award

IEEE Asian Hardware Oriented Security and Trust Symposium (Asian HOST) 2018

Best Paper Candidate

ACM Great Lakes Symposium on VLSI (GLSVLSI) 2017

A. James Clark School of Engineering Distinguished Graduate Fellowship

University of Maryland, Graduate School 2012

University Merit Scholarship

Bangladesh University of Engineering and Technology 2011

Students' Honors and Awards

Best Paper Award

7th Annual Sage Memorial Capstone Design Competition,

Students: Blake E Todorowski, Harris Laing, Michael Fox, Rohit Engala 2024
George Mason University

Student Travel Grant Award

2024 IEEE International Conference on Mobility: Operations, Services, and Technologies,

Student: Harris Laing 2024
George Mason University

Awarded Grants, Contracts, & Donations

Virginia Innovation Partnership Authority

Project: Securing Chiplet-based Semiconductor Manufacturing from Untrusted Supply Chains,

Role: PI, Total Award Amount: \$50,000, My Share: \$50,000 2025 – 2024
Institution: George Mason University

National Science Foundation (NSF)

Project: An Edge-Based Approach to Robust Multi-Robot Systems in Dynamic Environments,

Role: PI (non-lead), Total Award Amount: \$600,000, My Share: \$95,000 2025 – 2022
Institution: George Mason University

US Department of Energy: Equipment Donation (DoE)

Program: Laboratory Equipment Donation Program,

Award: LeCroy Oscilloscope and Tectronix Signal Analyzer 2023, 2022
Institution: George Mason University

Xilinx University Program

Program: Research Donation,

Award: Xilinx ACAP and Ultrascale+ Board and Licences

2023, 2022

Institution: George Mason University

Maryland Industrial Partnerships(MIPS)

Project: VISPR: A Verified Instruction Secure Processor,

Role: PI, Total Award Amount: \$130,000, My Share: \$110,000

2023 – 2022

Institution: Morgan State University

National Science Foundation (NSF)

Project: CyberCorps Scholarship for Service (SFS),

Role: Co-PI, Total Award Amount: \$2,200,200, My Share: \$265,000

2022 – 2021

Institution: Morgan State University

Applied Research Laboratory for Intelligence and Security (ARLIS)

Project: Cyber-Assessment of AI/ML Tools,

Role: Co-PI, Total Award Amount: \$150,000, My Share: \$37,500

2021 – 2020

Institution: Morgan State University

NCAE-C Cyber Curriculum and Research Program

Project: Secure Autonomous Navigation Under Adversarial Attacks,

Role: Co-PI, Total Award Amount:\$150,000, My Share: \$50,000

2021 – 2020

Institution: Morgan State University

NASA Jet Propulsion Lab (NASA-JPL)

Project: Specification-based Anomaly Detection for Embedded Devices,

Role: Co-PI, Total Award Amount: \$45,000, My Share: \$0

2020

Institution: Morgan State University

Publications

Current Citation Count (Google Scholar): 451

h-Index: 11, i10-index: 13

Erdős Number: 6

Book Chapters

- [1] Ahmed, Fahim and **Arafin, Md Tanvir**. "Attack Detection and Countermeasures at Edge Devices". In: *Smart Cyber-Physical Power Systems: Challenges and Solutions*. Wiley-IEEE series. To appear.
- [2] **Arafin, Md Tanvir**, Xu, Qian, and Qu, Gang. 2022. "Voltage Overscaling Techniques for Security Applications". In: *Approximate Computing*. Springer, pp. 287–311. doi: 10.1007/978-3-030-98347-5_12.
- [3] Xu, Qian, **Arafin, Md Tanvir**, and Qu, Gang. 2022. "Approximation on Data Flow Graph Execution for Energy Efficiency". In: *Approximate Computing*. Springer, pp. 207–232. doi: 10.1007/978-3-030-98347-5_9.

- [4] **Arafin, Md Tanvir** and Qu, Gang. 2021. "Hardware-Based Authentication Applications". In: *Authentication of Embedded Devices*. Springer, pp. 145–181. doi: 10.1007/978-3-030-60769-2_6.
- [5] **Arafin, Md Tanvir** and Qu, Gang. 2017. "Memristor-Based Security". In: *Security Opportunities in Nano Devices and Emerging Technologies*. CRC Press, pp. 55–72. doi: 10.1201/9781315265056-4.

Articles in Refereed Journals.....

- [6] Lu, Z., Wang, X., **Arafin, M.**, Yang, H., Liu, Z., Zhang, J., and Qu, G. Mar. 2024. "An RRAM-Based Computing-in-Memory Architecture and Its Application in Accelerating Transformer Inference". In: *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 32.03, pp. 485–496. doi: 10.1109/TVLSI.2023.3345651.
- [7] Pan, Yuqian, Lu, Zhaojun, Zhang, Haichun, Zhang, Haoming, **Arafin, Md Tanvir**, Liu, Zhenglin, and Qu, Gang. 2022. "ADLPT: Improving 3D NAND Flash Memory Reliability By Adaptive Lifetime Prediction Techniques". In: *IEEE Transactions on Computers*. doi: 10.1109/TC.2022.3214115.
- [8] Zhang, Jiliang, Shen, Chaoqun, Su, Haihan, **Arafin, Md Tanvir**, and Qu, Gang. 2022. "Voltage Over-Scaling-Based Lightweight Authentication for IoT Security". In: *IEEE Transactions on Computers*. doi: 10.1109/TC.2021.3049543. [Featured Paper of the Month, February 2022].
- [9] **Arafin, Md Tanvir** and Qu, Gang. 2018. "Memristors for Secret Sharing-Based Lightweight Authentication". In: *IEEE Transactions on Very Large Scale Integration Systems (TVLSI)* 26.12, pp. 2671–2683. doi: 10.1109/TVLSI.2018.2823714.
- [10] Gao, Mingze, Wang, Qian, **Arafin, Md Tanvir**, Lyu, Yongqiang, and Qu, Gang. 2017. "Approximate Computing for Low Power and Security in the Internet of Things". In: *IEEE Computer* 50.6, pp. 27–34. doi: 10.1109/MC.2017.176.
- [11] **Arafin, Md Tanvir**, Islam, Nazifah, Roy, Sourav, and Islam, Saiful. 2012. "Performance Optimization for Terahertz Quantum Cascade Laser at Higher Temperature Using Genetic Algorithm". In: *Optical and Quantum Electronics* 44.15, pp. 701–715. doi: 10.1007/s11082-012-9590-z.

Articles in Refereed Conference Proceedings.....

- [12] **Arafin, Md Tanvir**. 2022. "Computation-in-Memory Accelerators for Secure Graph Database: Opportunities and Challenges". In: *27th IEEE/ACM Asia and South Pacific Design Automation Conference (ASP-DAC)*. IEEE.
- [13] Wang, Shuangbao Paul, **Arafin, Md Tanvir**, Osuagwu, Onyema, and Wandji, Ketchiozo. 2022. "Cyber Threat Analysis using Artificial Intelligence and Machine Learning". In: *IEEE 6th International Conference on Cryptography, Security and Privacy (CSP 2022)*. IEEE.
- [14] **Arafin, Md Tanvir** and Kornegay, Kevin. 2021. "Attack Detection and Countermeasures for Autonomous Navigation". In: *2021 55th IEEE Annual Conference on Information Sciences and Systems (CISS)*. IEEE, pp. 1–6. doi: 10.1109/CISS50987.2021.9400224.
- [15] Lu, Zhaojun, **Arafin, Md Tanvir**, and Qu, Gang. 2021. "RIME: A Scalable and Energy-Efficient Processing-In-Memory Architecture for Floating-Point Operations". In: *2021 26th IEEE/ACM Asia and South Pacific Design Automation Conference (ASP-DAC)*. IEEE, pp. 120–125. doi: 10.1145/3394885.3431524. [Acceptance Rate = 30%].
- [16] Xu, Qian, **Arafin, Md Tanvir**, and Qu, Gang. 2021. "Security of Neural Networks from Hardware Perspective: A Survey and Beyond". In: *2021 26th IEEE/ACM Asia and South Pacific Design Automation Conference (ASP-DAC)*. IEEE, pp. 449–454. doi: 10.1145/3394885.3431639.

- [17] **Arafin, Md Tanvir** and Lu, Zhaojun. 2020. "Security Challenges of Processing-in-Memory Systems". In: *Proceedings of the 2020 ACM Great Lakes Symposium on VLSI (GLSVLSI)*, pp. 229–234. doi: 10.1145/3386263.3411365.
- [18] Gao, Jiabao, Wang, Jian, **Arafin, Md Tanvir**, and Jinmei, Lai. 2020. "FABLE-DTS: Hardware-Software Co-Design of a Fast and Stable Data Transmission System for FPGAs". In: *2020 IEEE 33rd International System-on-Chip Conference (SOCC)*. IEEE. doi: 10.1109/SOCC49529.2020.9524764.
- [19] Xu, Qian, **Arafin, Md Tanvir**, and Qu, Gang. 2020. "MIDAS: Model Inversion Defenses Using an Approximate Memory System". In: *2020 IEEE Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*. IEEE, pp. 1–4. doi: 10.1109/AsianHOST51057.2020.9358254. [**Acceptance Rate = 27%**].
- [20] Yimer, Tsion, **Arafin, Md Tanvir**, and Kornegay, Kevin. 2020. "Securing Industrial Control Systems Using Physical Device Fingerprinting". In: *2020 7th IEEE International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*. IEEE, pp. 1–6. doi: 10.1109/IOTSMS52051.2020.9340160.
- [21] **Arafin, Md Tanvir**, Shen, Haoting, Tehranipoor, Mark M, and Qu, Gang. 2019. "LPN-based Device Authentication Using Resistive Memory". In: *Proceedings of the 2019 ACM Great Lakes Symposium on VLSI (GLSVLSI)*, pp. 9–14. doi: 10.1145/3299874.3317970. [**Acceptance Rate = 27%**].
- [22] Jain, Shalabh, Wang, Qian, **Arafin, Md Tanvir**, and Guajardo, Jorge. 2018. "Probing Attacks on Physical Layer Key Agreement for Automotive Controller Area Networks". In: *2018 IEEE Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*. IEEE, pp. 7–12. doi: 10.1109/AsianHOST.2018.8607166. [**Best Paper Award**].
- [23] **Arafin, Md Tanvir**, Anand, Dhananjay, and Qu, Gang. 2017. "A Low-Cost GPS Spoofing Detector Design for Internet of Things (IoT) Applications". In: *Proceedings of the 2017 ACM Great Lakes Symposium on VLSI 2017 (GLSVLSI)*, pp. 161–166. doi: 10.1145/3060403.3060455. [**Best Paper Nominee, Acceptance Rate 24%**].
- [24] **Arafin, Md Tanvir**, Gao, Mingze, and Qu, Gang. 2017. "VOLtA: Voltage Over-Scaling Based Lightweight Authentication for IoT Applications". In: *2017 22nd IEEE/ACM Asia and South Pacific Design Automation Conference (ASP-DAC)*. IEEE, pp. 336–341. doi: 10.1109/ASPDAC.2017.7858345. [**Acceptance Rate = 30%**].
- [25] **Arafin, Md Tanvir**, Stanley, Andrew, and Sharma, Praveen. 2017. "Hardware-based Anti Counterfeiting Techniques for Safeguarding Supply Chain Integrity". In: *2017 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, pp. 1–4. doi: 10.1109/ISCAS.2017.8050605.
- [26] **Arafin, Md Tanvir**, Anand, DM, and Qu, Gang. 2016. "Detecting GNSS Spoofing using a Network of Hardware Oscillators". In: *Proceedings of the 47th Annual Precise Time and Time Interval Systems and Applications Meeting (PTTI)*, pp. 74–79. doi: 10.33012/2016.13135.
- [27] **Arafin, Md Tanvir** and Qu, Gang. 2016. "Secret Sharing and Multi-User Authentication: From Visual Cryptography to RRAM Circuits". In: *Proceedings of the 26th ACM Great Lakes Symposium on VLSI (GLSVLSI)*, pp. 169–174. doi: 10.1145/2902961.2903039. [**Acceptance Rate = 25%**].
- [28] **Arafin, Md Tanvir**, Dunbar, Carson, Qu, Gang, McDonald, N, and Yan, L. 2015. "A Survey on Memristor Modeling and Security Applications". In: *Sixteenth IEEE International Symposium on Quality Electronic Design (ISQED)*. IEEE, pp. 440–447. doi: 10.1109/ISQED.2015.7085466.

- [29] **Arafin, Md Tanvir** and Qu, Gang. 2015. "RRAM Based Lightweight User Authentication". In: *2015 IEEE/ACM international conference on Computer-Aided Design (ICCAD)*. IEEE, pp. 139–145. DOI: 10.1109/ICCAD.2015.7372561. [**Acceptance Rate = 26%**].
- [30] **Arafin, Md Tanvir** and Islam, Saiful. 2012. "Exploring the Electronic Properties of Relaxed Bilayer Nitrogen-Graphene Alloy using Density Functional Theory". In: *2012 7th IEEE International Conference on Electrical and Computer Engineering*. IEEE, pp. 373–376. DOI: 10.1109/ICECE.2012.6471565.

Ph.D. Thesis.....

- [31] **Arafin, Md Tanvir**. 2018. "Hardware-Based Authentication for the Internet of Things". PhD thesis. University of Maryland, College Park. DOI: 10.13016/M2HH6C88R.

Patents

- [32] Jain, Shalabh, Wang, Qian, **Arafin, Md Tanvir**, and Merchan, Jorge Guajardo. Mar. 2021. *Method to Mitigate Voltage Based Attacks on Key Agreement Over Controller Area Network (CAN)*. US Patent 10,958,680.
- [33] Jain, Shalabh, Wang, Qian, **Arafin, Md Tanvir**, and Merchan, Jorge Guajardo. Feb. 2020. *Method to Mitigate Transients Based Attacks on Key Agreement Schemes Over Controller Area Network*. US Patent 10,554,241.

Invited Talks, Workshops, & Presentation

1. **Ghosts in the Shell: Security Issues in Robotic Operating System**, Hardware Demonstration, *Whiskey and Widgets event for College of Engineering and Computing*, George Mason University, 2024.
2. **Hardware Security @ C5I Center**, Hardware Demonstration, *Center Connect event for College of Engineering and Computing*, George Mason University, 2024.
3. **Design of Secure and Efficient Processing-In-Memory Systems for Large-Scale Applications**, Tutorial Presentation, *34th International System-on-Chip Conference (SOCC)*, 2021.
4. **Hardware Lottery and the Perils of Computer Security**, Invited Talk, Computer Science Department, IT University of Copenhagen, Denmark, 2021.
5. **Autonomous Navigation Under Adversarial Attack**, Abstract Presentation, *49th Annual IEEE Applied Imagery Pattern Recognition (AIPR) Workshop*, 2020.
6. **Physical Unclonable Functions for Security Applications**, Invited Talk, COSC Colloquium Series, Computer Science Department, Morgan State University, 2020.
7. **Guided Reinforcement Learning and Imitation Learning: GRILL-SPICE**, (with Terry Stewart) Telluride Neuromorphic Workshop, 2020.
8. **Hardware Security for IoT devices**, Amazon Graduate Research Symposium, Seattle, Washington, 2017.
9. **Security Data Science: Improving Security with Big Data Techniques**, (with Tudor Dumitras), Maryland Cybersecurity Center(MC2) Annual Symposium, 2014.

Teaching

Courses Taught

George Mason University

- CYSE 499/580: Hardware and Cyber Physical Systems *SP 2023*
- CYSE 465: Transportation System Design *SP 2024, F2023, F2022*

Morgan State University

- EEGR 760: Advanced Topics in Computer Engineering *SP 2020*
- EEGR 745: Advanced Digital VLSI Design *F 2021*
- EEGR 480: Introduction to Cyber Security *F 2019, F 2020*
- EEGR 463: Digital Electronics *SP 2022, SP 2021, F 2020, SP 2020, F 2019*

Bangladesh University of Engineering & Technology

- Introduction to Electrical Engineering *SP 2012*
- VLSI I Laboratory *SP 2012, F 2011*
- Microprocessor & Interfacing Laboratory *F 2011*
- Electronics Laboratory *F 2011*

Mentoring & Advisement

Ph.D. Thesis Advisement

George Mason University

- Yanze Wu
- Fahim Ahmed

Undergraduate Senior Design Project Sponsor

George Mason University

- Project: Securing Robust Multi-Robot Systems in Dynamic Environments
Students: Blake E Todorowski; Michael Lane Fox ; Harris E Laing; Kirthan Gaddam;
Anosh A Mian *2024 – 2023*
- Project: Émpistos: Trusted Embedded Processing and Optimizations for Edge AI Security
Students: Zack Francis Wagner; AlRaheeq Al Rawas; Anay Gulati; Maximilian A Karen;
Bradford Williams *2024 – 2023*

Doctoral Thesis Committee Member

Morgan State University

- Latha Suravasi, Khir Henderson, Greig Richmond, Edmund Smith, Tsion Yimer

Undergraduate Senior Design Project Supervisor

Morgan State University

- Maryline Ivana Happy; Jose Dominguez-Cortez; Robert Hill *2022 – 2021*
- Ashia Mccalla; Gerald Amory *2022 – 2021*
- Antwaan Thomas; Faizat Kaffo *2021 – 2020*

o Malik Smith; Anthony Turner	2021 – 2020
o Fitsum Tadasse; Reuben Macintosh	2021 – 2020

Professional Service

Grant Review Committee Member	
Panelist, National Science Foundation (NSF)	2024 – 2022
Technical Reviewer, Maryland Industrial Partnerships (MIPS)	2021
Conference Technical Program Committee Member	
IEEE Design and Automation Conference (DAC)	2024 – 2023
IEEE Asia and South Pacific Design Automation Conference (ASP-DAC)	2023 – 2021
IEEE International System-on-Chip Conference (SOCC)	2024, '23, '21, '20
IEEE Asian Hardware Oriented Security and Trust Symposium (AsianHOST)	2024 – 2021
Conference Organizing Committee Member	
Publication Chair, IEEE Asian Hardware Oriented Security and Trust Symposium	2024 – 2021
Conference Session Chair	
IEEE Asia and South Pacific Design Automation Conference (ASP-DAC)	2022, '20
IEEE International System-on-Chip Conference (SOCC)	2021, '20
IEEE Asian Hardware Oriented Security and Trust Symposium	2021
Journal Reviewer	
IEEE Transactions on Computer-Aided Design of ICs and Systems (TCAD)	
IEEE Transactions on Very Large Scale Integration Systems (TVLSI)	
IEEE Network Magazine	
Integration, the VLSI Journal (Elsevier)	
Computer & Security (Elsevier)	
Journal of Hardware and Systems Security (Springer)	

Departmental Service

George Mason University	
Chair, Ph.D. Proposal Committee , CYSE Department	2024 – 2023
Member, Department Handbook Committee , CYSE Department	2024 – 2023
Member, Grievance Committee , CYSE Department	2024 – 2023
Chair, Graduate Committee , CYSE Department	SP 2023
Member, Advertisement Committee , CYSE Department	SP 2023
Member, Departmental Tenure-Track Hiring Committee , CYSE Department	2023 – 2022
Member, Departmental Term-Track Hiring Committee , CYSE Department	2023 – 2022
Chair, Colloquium Committee , CYSE Department	F 2022
Member, Graduate Committee , CYSE Department	F 2022

Morgan State University

Graduate Coordinator , ECE Department, Morgan State University	2020 – 2022
Undergraduate Coordinator , ECE Department, Morgan State University	2019 – 2020
Member , Curriculum Development Committee, Ph.D. in Secure Embedded Systems	2020
Member , Faculty Development Committee, ECE Department,	2019 – 2022
Member , Cyber Defense Education (CAE-CDE) Re-designation Committee	2020, 2021
USENIX Campus Representative , Morgan State University	2020 – 2022

Affiliation

Member, Institute of Electrical and Electronics Engineers (IEEE)	<i>current</i> – 2008
Member, USENIX: The Advanced Computing Systems Association	2022 – 2020
Member, Sigma Xi, the Scientific Honorary Society	2023 – 2019
Student Member, IEEE Communication Society	2015 – 2010

Citizenship Status

US Permanent Resident, Citizen of Bangladesh.

References

Available upon request.