Tanvir Arafin

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

+1 (202) 594 5489 • marafin@gmu.edu • tanvirarafin.github.io

Education

University of Maryland **Collage Park, MD**
Ph.D., Electrical Engineering *2018*
Dissertation: Hardware-Based Authentication for the Internet of Things

University of Maryland **Collage Park, MD**
M.Sc., Electrical Engineering *2016*

Bangladesh University of Engineering & Technology **Dhaka, Bangladesh**
B.Sc., Electrical & Electronic Engineering *2011*

Professional Appointments

George Mason University **Fairfax, VA**
Tenure-Track Assistant Professor *2022–current*
Department of Cyber Security Engineering
College of Engineering and Computing

Morgan State University **Baltimore, MD**
Tenure-track Assistant Professor *2019–2022*
Electrical and Computer Engineering Department (50%) &
Cybersecurity Assurance and Policy (CAP) Center (50%)

Bloomberg **New York, NY**
Software Engineer *2018–2019*

Bangladesh University of Engineering & Technology **Dhaka, Bangladesh**
Lecturer *2011–2012*

Internships

Cyber Innovation Group, Philips **Andover, MA**
Vulnerability Research Intern *2016–2017*

Security & Privacy Group, Bosch **Pittsburgh, PA**
Research Intern *2016*

Honors & Awards

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*

Awarded Grants, Contracts, & Donations

National Science Foundation (NSF)
An Edge-Based Approach to Robust Multi-Robot Systems in Dynamic Environments,
Role: non-lead PI, Total Award Amount: $600,000, My Share: $95,000 *2022-2025*
Institution: Morgan State University

Maryland Industrial Partnerships(MIPS)
VISPR: A Verified Instruction Secure Processor,
Role: PI, Total Award Amount: $130,000, My Share: $110,000 *2022-2023*
Institution: Morgan State University, Grant Transferred to Dr. Kevin Kornegay

National Science Foundation (NSF)
CyberCorps Scholarship for Service (SFS),
Role: Co-PI, Total Award Amount: $2,200,200, My Share: $265,000 *2021-2026*
Institution: Morgan State University

Applied Research Laboratory for Intelligence and Security (ARLIS)
Cyber-Assessment of AI/ML Tools,
Role: Co-PI, Total Award Amount: $150,000, My Share: $37,500 *2020-2021*
Institution: Morgan State University

NCAE-C Cyber Curriculum and Research Program
Secure Autonomous Navigation Under Adversarial Attacks,
Role: Co-PI, Total Award Amount:$150,000, My Share: $50,000 *2020-2021*
Institution: Morgan State University

NASA Jet Propulsion Lab (NASA-JPL)
Specification-based Anomaly Detection for Embedded Devices *2020*
Role: Co-PI, Total Award Amount: $45,000, My Share: $0

Xilinx University Program
Research Donation *2021*
Award: Xilinx Ultrascale+ Board and Licences

Amazon AWS Educate
Amazon AWS *2020*
Total Award Amount: $1,500

Publications

Book Chapters

[1] **Arafin, Md Tanvir**, Xu, Qian, and Qu, Gang. "Voltage Overscaling Techniques for Security Applications". In: *Approximate Computing*. Springer. In press.

[2] Xu, Qian, **Arafin, Md Tanvir**, and Qu, Gang. "Approximation on Data Flow Graph Execution for Energy Efficiency". In: *Approximate Computing*. Springer. In press.

[3] **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.

[4] **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 Conference Proceedings & Journals

[5] Lu, Zhaojun, Xu, Xueyan, **Arafin, Md Tanvir**, and Zhao, Wehsheng. 2022. "A Holistic Perspective of Security in Emerging Computing-In-Memory: Device, Architecture & System Levels". In: *IEEE Transactions on Emerging Topics in Computing* (*TETC*). To appear.

[6] 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]**.

[7] **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.

[8] 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.

[9] **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

[10] **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.

[11] 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.

[12] **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.

[13] 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%**].

[14] 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.

[15] **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.

[16] 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.

[17] 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%**].

[18] 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.

[19] **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%**].

[20] 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**].

[21] **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%**].

[22] **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%**].

[23] **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.

[24] **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.

[25] **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%**].

[26] **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.

[27] **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%**].

[28] **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.

Journal Articles Under Review

[29] Lu, Zhaojun, **Arafin, Md Tanvir**, Yang, Nathan, and Qu, Gang. "An RRAM Based Computing-In-Memory Architecture and Its Application in Accelerating Transformer Inference". In: *IEEE Internet of Things Journal*. Under review.

[30] Pan, Yuqian, Zhang, Haichun, Zhang, Haoming, **Arafin, Md Tanvir**, Liu, Zhenglin, Lu, Zhaojun, and Qu, Gang. "ADLPT: Improving 3D NAND Flash Memory Reliability by Adaptive Lifetime Prediction Techniques". In: *IEEE Transactions on Computers*. Under review.

[31] Xu, Qian, **Arafin, Md Tanvir**, and Qu, Gang. "An Approximate Memory based Defense against Model Inversion Attacks to Neural Networks". In: *IEEE Transactions on Emerging Topics in Computing (TETC)*. Under review.

Ph.D. Thesis

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

Patents

[33] 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.

[34] 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. **Design of Secure and Efficient Processing-In-Memory Systems for Large-Scale Applications**, Tutorial Presentation, *34th International System-on-Chip Conference (SOCC)*, 2021.
2. **Hardware Lottery and the Perils of Computer Security**, Invited Talk, Computer Science Department, IT University of Copenhagen, Denmark, 2021.
3. **Autonomous Navigation Under Adversarial Attack**, Abstract Presentation, *49th Annual IEEE Applied Imagery Pattern Recognition (AIPR) Workshop*, 2020.
4. **Physical Unclonable Functions for Security Applications**, Invited Talk, COSC Colloquium Series, Computer Science Department, Morgan State University, 2020.

5. **Guided Reinforcement Learning and Imitation Learning: GRILL-SPICE**, (with Terry Stewart) Telluride Neuromorphic Workshop, 2020.
6. **Hardware Security for IoT devices**, Amazon Graduate Research Symposium, Seattle, Washington, 2017.
7. **Security Data Science: Improving Security with Big Data Techniques**, (with Tudor Dumitras), Maryland Cybersecurity Center(MC2) Annual Symposium, 2014.

Teaching

Courses Taught

- **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	F 2019, SP 2020, F 2020, SP 2021, SP 2022

- **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

New Course Designed

- EEGR 745: Advanced Digital VLSI Design

Courses Revised

- EEGR 760: Advanced Topics in Computer Engineering
- EEGR 480: Introduction to Cyber Security

Mentoring

Doctoral Thesis Committee Chair

- Chongkon Zaman — Expected Graduation: 2023
- Olufemi Agunbiade — Expected Graduation: 2024

Master's Dissertation Committee Chair

- Jose Dominguez — Expected Graduation: 2022

Doctoral Thesis Committee Member

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

Undergraduate Senior Design Project Supervisor

- Ashia Mccalla, Gerald Amory, Maryline Ivana Happy, Jose Dominguez-Cortez, Robert Hill, Antwaan Thomas, Faizat Kaffo, Malik Smith, Anthony Turner, Fitsum Tadasse, Reuben Macintosh

Professional Service

Grant Review Committee Member

Panelist, National Science Foundation (NSF) *2022*
Technical Reviewer, Maryland Industrial Partnerships (MIPS) *2021*

Conference Technical Program Committee Member

IEEE Asia and South Pacific Design Automation Conference (ASP-DAC) *2021, 2022*
IEEE International System-on-Chip Conference (SOCC) *2020, 2021*
IEEE Asian Hardware Oriented Security and Trust Symposium (AsianHOST) *2021*

Conference Organizing Committee Member

Publication Chair, IEEE Asian Hardware Oriented Security and Trust Symposium *2021*

Conference Session Chair

IEEE International System-on-Chip Conference (SOCC) *2020, 2021*
IEEE Asian Hardware Oriented Security and Trust Symposium *2021*
IEEE Asia and South Pacific Design Automation Conference (ASP-DAC) *2020*

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)

University Service

Assistant Director, Cybersecurity Assurance & Policy Center *2019 – current*
Member, SGS Policy & Procedures Committee, Morgan State University *2020 – current*

Departmental Service

Graduate Coordinator, ECE Department, Morgan State University *2020 – current*
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 –current*
Member, Cyber Defense Education (CAE-CDE) Re-designation Committee *2020, 2021*
USENIX Campus Representative, Morgan State University *2020 – current*

Affiliation

Member, Institute of Electrical and Electronics Engineers (IEEE) *2008 – current*
Member, USENIX: The Advanced Computing Systems Association *2020 – current*
Member, Sigma Xi, the Scientific Honorary Society *2019 – current*

Student Member, IEEE Communication Society *2010-2015*

References

Available upon request.

Last updated on August 8, 2022