MD KAWSER BEPARY

[LinkedIn] [GitHub] [Google Scholar]

Email : mdkawser.bepary@ufl.edu
Mobile : +1-256-417-9343
Address: Gainesville, FL, USA

Area of Interests

- System-on-Chip Design and Verification, Embedded System Application, Hardware Security and Trust, Side-Channel Analysis.

Education

- **University of Florida** — Gainesville, FL
  Doctor of Philosophy (Ph.D.) in Electrical and Computer Engineering — *Jan 2021 - May 2025 (Expected)*
  Advisor: Prof. Mark Tehranipoor — *CGPA: **3.93/4.00***

- **The University of Alabama in Huntsville** — Huntsville, AL
  Master of Science (M.Sc.) in Computer Engineering — *Aug 2019 - Dec 2020*
  Advisor: Prof. M. Tauhidur Rahman — *CGPA: **3.71/4.00***

- **Bangladesh University of Engineering and Technology (BUET)** — Dhaka, Bangladesh
  Bachelor of Science (B.Sc.) in Electrical and Electronic Engineering — *Jul 2014 - Oct 2018*
  *CGPA: **3.51/4.00***

Experience

- **Florida Institute for Cybersecurity (FICS) Research, University of Florida** — Gainesville, FL
  Graduate Research Assistant — *Jan 2021 - Current*
  - Developing a GNN-based power/EM side-channel leakage modeling framework at pre-silicon stage to ensure secure cryptographic designs.
  - Developing a novel PMU-based methodology for detecting browser workloads and cache side-channel attacks to thawrt speculative attacks during runtime.
  - Implemented an automated CAD toolflow to evaluate physical-design aware EM side-channel vulnerability at gate-level, enabling fast security sign-off at pre-silicon.
  - Developed a python-based framework to estimate the IP and SoC-level resiliency against power side-channel threats at RTL as part of a DARPA-funded project in collaboration with Synopsys.
  - Designed security primitive IPs in RTL for device lifecycle management as part of a DARPA-funded AISS project in collaboration with Synopsys.

- **Synopsys Inc.** — Mountainview, CA
  Graduate Technical Intern (Security IP Team), Solutions Group — *May 2023 - Dec 2023*
  - Developed embedded applications for secure boot, TLS communication, and cryptographic services as part of DARPA-funded AISS (Automatic Implementation of Secure Silicon) project.
  - Implemented ASCON lightweight cryptographic application for embedded firmware encryption and authentication as part of secure boot protocol.
  - Integrated ASCON authenticated encryption and hashing hardware module to the Synopsys security engine subsystem and implemented a masking scheme for side-channel resiliency.

- **Department of ECE, University of Florida** — Gainesville, FL
  Graduate Teaching Assistant - Intro to Hardware Security and Trust — *Aug 2022 - Dec 2022*
  - Managed the assignments, projects, and exams and developed tutorials on commercial EDA tools for VLSI design, synthesis, functional and security verification.

- **Department of ECE, The University of Alabama in Huntsville** — Huntsville, AL
  Graduate Research Assistant — *Aug 2019 - Dec 2020*
  - Developed open-source API-based C++ scripts to interface commercial DDR3 DRAM chips deployed on a Xilinx ML605 FPGA board to execute read/write operations with configurable timing parameters.
  - Performed device aging under stress conditions for DRAM modules and analyzed bit-flips due to retention error to explore reliability issues, security vulnerabilities and generate robust signatures.

- **Department of ECE, The University of Alabama in Huntsville** — Huntsville, AL
  Graduate Teaching Assistant - Computer Organization, Intro to Computer Architecture — *Aug 2020 - Dec 2020*
  - Assisted 100+ graduate/undergraduate students with grading homework, quizzes, projects, and exams on concepts of computer organization, architecture, memory hierarchy, assembly language, and MIPS ISA.

Relevant Coursework

- **Computer Engineering**: System-on-Chip Design, VLSI HDL/Modeling, Advanced Computer Architecture, Advanced VLSI, Analog and Digital Electronics, Parallel Programming, Microprocessor and Interfacing
- **Hardware Security**: CAD for Hardware Security Verification, Advanced Hardware Security, Cybersecurity Engineering, Hardware Security and Trust
- **Machine Learning**: Data Mining, Intro to Machine Learning, Probability and Statistics, Linear Algebra

Technical Skills

- **Programming Languages**: Python, C/C++, Rust, MATLAB, RISC-V/MIPS/8086 Assembly
- **Hardware Description Languages**: Verilog, VHDL, SystemVerilog
- **Electronic Design Automation Tools**:
  - **RTL Design and Synthesis**: Synopsys Design Compiler, Xilinx Vivado, Cadence Genus, ABC
  - **Functional Verification**: Synopsys VCS, ModelSim, SystemVerilog Assertion, UVM
  - **Formal Verification**: Cadence JasperGold, Synopsys Formality
  - **Physical Design**: Cadence Innovus, Synopsys ICC2
  - **Other EDA Tools**: Synopsys SpyGlass, PrimeTime, TetraMax, StarRC, HSpice
- **Scripting Languages**: Tcl/Tk, Unix Shell, Bash, Make, CMake, Perl
- **Data Analysis & Machine Learning**: Numpy, SciPy, Pandas, Scikit-learn, Tensorflow, Keras, PyTorch
- **Other Software and Tools**: Proteus, gem5, multi2sim, PAPI, Linux, Git, Perforce, Latex, Minitab

Publications

- **MK Bepary**, A Basu, S Mohammad, R Hasan, F Farahmandi, M Tehranipoor , "SPY-PMU: Side-channel Profiling of Your Performance Monitoring Unit to Leak Remote User Activity," IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2025. (Under Review)
- **MK Bepary**, T Zhang, J Zhou, F Rahman, F Farahmandi, M Tehranipoor , "Towards Efficient Gate-Level Electromagnetic Side-Channel Leakage Modeling and Vulnerability Assessment," Journal of Hardware and Systems Security, 2024. (Under Review)
- **MK Bepary**, T Zhang, F Farahmandi and M Tehranipoor. "PreSCAN: A Comprehensive Review of Pre-Silicon Physical Side-Channel Vulnerability Assessment Methodologies." Chips 3, no. 3 (2024). (link)
- T Rahman, **MK Bepary**, MSUl Haque, M Tehranipoor and F Rahman, "Design and Security-Mitigation of Custom and Configurable Hardware Cryptosystems," 2023 IEEE 16th Dallas Circuits and Systems Conference (DCAS), Denton, TX, USA, 2023, pp. 1-6. (link)
- **MK Bepary**, F Rahman, F Farahmandi, and M Tehranipoor. "Security Assessment and Modeling of EM Side-channel Leakage at Gate-Level." in Annual GOMACTech Workshop 2023, USA.
- B Ahmed, **MK Bepary**, N Pundir, M Borza, et al. "Quantifiable Assurance: From IPs to Platforms." Cryptology ePrint Archive (2021). (link)
- Co-authored a book chapter titled *"A Survey on CAD for Power Side-Channel Detection"* for the book *"Farimah Farahmandi et al., CAD for Hardware Security, Springer, 2023."*
- Co-authored a book chapter titled *"Counterfeit and Recycled IC Detection"* for the book *"Tehranipoor, M., Pundir, N., Vashistha, N., Farahmandi, F.., Hardware Security Primitives. Springer, 2022."* (link)
- **MK Bepary**, BMSB Talukder, and MT Rahman. "DRAM Retention Behavior with Accelerated Aging in Commercial Chips." Applied Sciences 12, no. 9 (2022): 4332. (link)

Poster Presentations

- Presented a poster titled *"Quantitative Assessment of Power Side-channel Vulnerability at Pre-silicon Stages"* on *2023 Florida Semiconductor Week, Gainesville, FL.* (Jan 2023) (link)
- Presented a poster titled *"Electromagnetic Side-Channel Leakage Modeling and Security Assessment at Pre-Silicon Stages"* on *2022 Trusted and Assurance Microelectronics (TAME) Forum, Columbus, OH.* (Sep 2022) (link)

Selected Academic Projects

- **System-on-Chip (SoC) Design**: Implemented a SoC hardware design using MicroBlaze processor, peripheral IP integration (AXI, APB), bus protocol (APB), and developed baremetal C applications. (2023)
- **Implementation of FPGA Pong Game**: Implemented the hardware design of the VGA controller for monitor and Pong Game controller on a Xilinx FPGA using MicroBlaze processor and I/O peripherals. (2023)
- **Property-based security verification of an RSA controller**: Implemented security properties with SystemVerilog assertions to verify an RSA controller design on Cadence Jasper. (2021)
- **Deep-learning based hand-written character recognition**: Developed a deep convolutional neural network pipeline along with data pre-processing and augmentation techniques using python keras and scikit-learn libraries to classify images of hand-written characters with 98.07% accuracy. (2022) (github)
- **Implementation of an efficient AES crypto engine**: Developed an efficient VHDL implementation of AES 128-bit encryption/decryption engine using pipelined architecture on Xilinx Artix-7 FPGA board. (2020)
- **Performance analysis of cache replacement policies**: Implemented different cache replacement policies (LRU, pseudo-LRU, FIFO, random, MRU, LFU, etc.) on x86 architecture using Gem-5 simulator to analyze the performance improvement on benchmark programs. (2020)
- **Parallel implementation of PCA algorithm**: Developed a parallel implementation of principal component analysis (PCA) algorithm using singular value decomposition (SVD) in OpenMP specification on Alabama Supercomputer to improve performance.(2019)

Honors and Awards

- 1st Place in 2022 IEEE HOST Microelectronics Security Challenge (github), 2022 IEEE HOST Travel Grant, Undergrad Dean's List (2015), Education Board Merit Scholarship (Secondary and Higher Secondary).