Ange-Thierry Ishimwe

Recent PhD Graduate
ange-thierry.ishimwe@colorado.edu
479-320-9300

Teaching and Research Highlight:

- Teaching Assistant for undergraduate and graduate computer architecture courses: led FPGA and VHDL labs, graded assignments and exams, held office hours, redesigned a semester long 32 bit RISC V processor project from Codasip in C to PyMTL in Python, and supported use of architectural simulators such as SimpleScalar.
- Designed hardware defenses against transient execution attacks by enhancing branch and memory dependence predictors to prevent mistraining and built a secure CPU that blocks unsafe memory accesses in the load-store unit(both implemented in Gem5, C++/OOP). Modeled structure latency with CACTI, built synthetic workloads to expose bottlenecks, and used SimPoints to evaluate performance in key regions of interest.
- Extended the Clang/LLVM compiler with custom RISC-V instructions to strengthen memory safety during speculative execution. Implemented LLVM passes that identify expected memory operations at compile time and encode them in custom instructions, enabling processors to distinguish safe and unsafe accesses at runtime.

Featured Publication

- **Ange-Thierry Ishimwe**, Sam McDiarmid-Sterling, Zack McKevitt, and Tamara Silbergleit Lehman. *"SSMR: Statically Detecting Speculation-Safe Memory Regions to Mitigate Transient Execution Attacks."* International Conference on Compiler Construction ***(CC'26)***.

Education

- **Doctoral Candidate in Electrical Engineering**
  University of Colorado Boulder — *May 2026*
  Thesis Title: Mitigating Transient Execution Attacks with Minimal Hardware and Performance Overhead
  Research Area: Computer Architecture, CPU Security, and Compilers
  Advisor: Prof. Tamara Lehman

- **Master of Science in Electrical Engineering**
  University of Colorado Boulder — *May 2022*

- **Honors Bachelor of Science in Computer Engineering**
  University of Arkansas — *May 2020*
  Thesis Title: Identifying Privacy Policy in Service Terms Using Natural Language Processing
  Advisor: Prof. Qinghua Li

Work Experience

Graduate Research Assistant — Fall 2020 - Present

Boulder Computer Architecture Research Lab — Boulder, CO

SSMR: Statically Detecting Speculation-Safe Memory Regions to Mitigate Transient Execution Attacks *(Published at CC 2026)*

Tech Stack*: Clang/LLVM, Gem5, Simpoint, Cacti, C++, RISC-V assembly, LLVM IR*

- Designed a software–hardware co-design defense against Spectre and Meltdown that analyzes target addresses of memory instructions in a modified load-store unit to detect potentially malicious behavior.
- Implemented the defense (SSMR) on the cycle-level accurate gem5 simulator, achieving only a 7% performance overhead.
- Extended the Clang/LLVM compiler with a custom RISC-V instruction to distinguish between safe and unsafe memory operations and mitigate transient execution attacks.
- Designed LLVM analysis and transformation passes to detect potential vulnerabilities in code.
- Benchmarked CPU performance using custom micro-benchmarks and spec cpu2017 workloads to verify overhead and inform design decisions.

SCPC: Securing Cross-Process Collision-Based Transient Attacks *(Work in progress)*
Tech Stack*: Zynq FPGA board, Vivado, systemVerilog, Gem5, Simpoint, Cacti, C++/OOP, X86 assembly*

- Built a functional level model of AMD's Speculative Store Bypass Predictor (SSBP) and integrated it into the gem5 simulator to evaluate a virtualization based defense that isolates prediction structures across processes.

- Applied the same defense to the TAGE-SC-L branch predictor to demonstrate its generalizability.
- Introduced a self-invalidation mechanism to prevent resource monopolization in prediction structures, along with a selective sharing policy that enables safe sharing across benign processes while isolating potentially harmful ones.
- Designed synthetic workloads to stress CPU predictors to identify bottlenecks and compared performance with baseline designs.

Baobab Merkle Tree for Efficient Secure Memory *(Published at CAL 2024)*
Tech Stack*: Gem5, Simpoint, Cacti, C++/OOP, ARM assembly*

- Co-designed and implemented the Baobab Merkle Tree, a secure memory integrity structure that reduces Bonsai Merkle Tree metadata overhead by 2 to 4x.
- Designed an on chip counter memoization table that enables counter sharing while preserving replay attack protection and data integrity guarantees.

Autoprune: Using Machine Learning to Optimize Code Synthesis *(Work in progress)*
Tech Stack*: Clang/LLVM, Scikit-learn, ONNX, Z3, Python, C++*

- Developed a machine learning-based stochastic pruning strategy combined with a state-of-the-art deterministic method to reduce compilation time of souper a superoptmizer by effectively pruning optimization candidates in the LLVM intermediate representation (IR).

Undergraduate Research Assistant Spring 2020
Computer Systems Laboratory — Fayetteville, AR

SPAR-2: A SIMD Processor Array for Machine Learning in IoT Devices *(Published at FPL 2021)*
Tech Stack*: Zynq FPGA board, Vivado, HLS, Verilog, C*

- Aided in designing and building a custom array processor for FPGA IoT edge devices that accelerates matrix-matrix multiplications for various Machine Learning (ML) and Artificial Intelliigence (AI) algorithms.
- Implemented the array processor as a Processor-In-Memory and packed 16,384 processing elements achieving high performance through concurrent computations and reduced communication latencies on a Zynq FPGA board.
- Obtained speedups of 24.51x compared to High-Level Synthesis equivalent design and 1.75x over similar past custom designs running RNN and LSTM neural network benchmarks for ML and AI.

Teaching

Computer Organization (ECEN 3593) *Fall 2021*
Teaching Assistant for Prof. Tamara Lehman in undergraduate course at the University of Colorado Boulder.
Converted a RISC-V 32-bit pipelined processor used in teaching labs from C to Python, and held weekly office hours.

Advanced Computer Architecture (ECEEN 5593) *Spring 2021*
Teaching Assistant for Prof. Tamara Lehman in graduate course at the University of Colorado Boulder.
Held weekly office hours to help students with questions and aided in preparing and grading homework and exams.

Digital Design (CSCE 2114) *Spring 2020*
Teaching Assistant for Prof. Pat Parkerson in undergraduate course at the University of Arkansas.
Conducted two labs per week, graded exams and homeworks, and held weekly office hours.

Skills

Programming Languages: C/C++, Java, Python, Verilog, VHDL, RISCV, X86, ARM
Simulators and Frameworks: Gem5, Vivado, CLANG/LLVM, Valgrind, perf, CACTI, Simpoint, QEMU
ML Platforms: ONNX, TensorFlow, Scikit-learn

Publications

C7 **SCPC: Securing Cross-Process Collision-Based Transient Attacks**
AT Ishimwe, Mujahid Al Rafi, T Lehman, Hyeran Jeon
Under review at International Conference on Parallel Processing (ICPP 2026)

C6 **SSMR: Statically Detecting Speculation Safe Memory Regions to Mitigate Transient Execution Attacks** *January 2026*
AT Ishimwe, S McDiarmid-Sterling, Z McKevitt, T Lehman
International Conference on Compiler Construction (CC)
https://dl.acm.org/doi/abs/10.1145/3771775.3786272

C5 **Autoprune: A Stochastic Candidate Pruning Strategy for Souper** *November 2025*
AT Ishimwe, K Heewoo, J Izraelevitz, T Lehman
arXiv
https://arxiv.org/abs/2509.16497

C4 **Baobab Merkle Tree for Efficient Secure Memory** *January 2024*
S Thomas, K Workneh, **AT Ishimwe**, Z McKevitt, P Curlin, R Bahar, J Izraelevitz, T Lehman
IEEE Computer Architecture Letters (CAL)
https://ieeexplore.ieee.org/document/10417116

C3 **A Customizable Domain-specific Memory-centric FPGA Overlay for Machine Learning Applications** *August 2021*
A Panahi, S Balsalama, **AT Ishimwe**, JM Mbongue, D Andrews
International Conference on Field-Programmable Logic and Applications (FPL)
https://ieeexplore.ieee.org/document/9556381

C2 **SPAR-2: A SIMD Processor Array for Machine Learning in IoT Devices** *June 2020*
S Basalama, A Panahi, **AT Ishimwe**, D Andrews
International Conference on Data Intelligence and Security (ICDIS)
https://ieeexplore.ieee.org/document/9323000

C1 **Identifying Privacy Policy in Service Terms Using Natural Language Processing** *Spring 2020*
AT Ishimwe
Undergraduate Honors Thesis, University of Arkansas
https://scholarworks.uark.edu/cgi/viewcontent.cgi?article=1083&context=csceuht

Posters

SMAD: Efficiently Defending Against Transient Execution Attacks *Spring 2023*
AT Ishimwe, Tamara Silbergleit Lehman
Workshop for graduate students studying computer architecture and related fields
https://web.mit.edu/yarch2023/

VulnerabiliTree: A Taxonomy of Hardware and Software Computer Attacks for Heuristic Hacking Defense *Fall 2021*
Sylvia Llosa, **AT Ishimwe**, Tamara Silbergleit Lehman
Workshop on Hardware and Architectural Support for Security and Privacy
https://haspworkshop.org/2021/program.html

Awards

Dean's Graduate Fellowship award *Fall 2020*
Electrical, Computer & Energy Excellence Fellowship *Fall 2020*
Brewer Family Entrepreneurship $1000 competition winner *Fall 2019*
Dean's List *Spring 2017 - Fall 2018*
Chancelor's List *Fall 2016*