Evgeny Manzhosov

New York, NY | 917-392-6355 | e.manzhosov@gmail.com | linkedin.com/in/manzhosov | evmanz.github.io

Research Interests

System security and reliability, distributed systems, compilers, and hardware support for security and privacy.

Profile

My research sits at the intersection of security and reliability, aiming to develop system solutions that ensure high reliability and security guarantees. With a solid foundation in modern computing technologies, my expertise spans from low-level software stack (e.g., memory allocators, code generation) and architecture concepts (e.g., branch prediction, prefetching, memory subsystem, error resiliency) to how modern chips are made (owing to five years of experience in physical design). This comprehensive background enables me to approach problems uniquely, resulting in multiple publications at top conferences such as ISCA and MICRO.

In broad terms, I am interested in security and privacy, computer architecture, distributed systems, and hardware-software co-design.

Education

Columbia University, New York, NY

Ph.D. in Computer Science, advised by Professor Simha Sethumadhavan. — *3/2019 – 9/2024 (est.)*

M. Phil. in Computer Science. — *2/2023*

M.Sc. in Electrical Engineering — *9/2017 – 3/2019*

Technion – Israel Institute of Technology, Haifa, Israel

B.Sc. Electrical Engineering, B.Sc. Physics — *10/2008 – 7/2014*

Honors and Awards

IEEE Micro Top Picks 2022 — 2022

- MUSE ECC and my paper "Revisiting Residue Codes for Modern Memories" was selected as Top Pick for MICRO Top Picks 2022.

Qualcomm Innovation Fellowship — 2020

- Winner of the Qualcomm Innovation Fellowship with proposal "Practical Security for Heterogeneous Systems".

RSA Security Scholar Pitch Off — 2020

- Winner of the 1^{st} RSA Security Scholar Pitch Off competition.

Master of Science Award of Excellence — 2019

- I was awarded Master of Science Award of Excellence by the Department of Electrical Engineering.

Technical Skills

Programming Languages: Python, C/C++, Rust, Tcl
HDL Languages: Verilog, SystemVerilog, VHDL, SystemC
EDA Tools: Synopsys: DC, ICC, ICC2, PrimeTime; Ansys Redhawk
Developer Tools: Git, VS Code
Software: OpenFHE, PyTorch, Or-Tools, LLVM, GEM5, Matlab
ISA: X86 and ARM assembly

Research Experience

Multi-Fault Model Error Correction 10/2023 – Present

- The goal of the project is to design an error correction scheme for deployments at scale as an alternative to "one-fit-all" ECC from CPU vendors.

MUSE ECC 10/2020 – 4/2022

- A novel error correction code designed to encode the metadata with the data while providing ChipKill-level error correction over standard memory interfaces (DDR4, DDR5). For this project, I implemented in Verilog custom low latency (1-2 clock cycles), non-pipelined multipliers, and modulo units for 64 to 160-bit words. In addition, I implemented all the test benches in SystemVerilog, code profiling algorithms in C++, and modified the GEM5 simulator to support variable latency penalty on the memory interface to emulate the impact of ECC.

NoFAT 2020 – 2021

- A novel technique to enable metadata-less memory bounds checks to ensure spatial and temporal memory safety. The NoFAT is built upon binning memory allocators. Hence, with NoFAT we are able to derive base-and-bounds for each object implicitly. To lower the overheads, we implemented custom hardware units to speed up the derivation of the base address for each dereferenced pointer. We use this address later to look up the size of the memory allocation and to determine the upper bound of the object in memory.

ZeRO 2020 – 2021

- A novel technique to ensure pointer integrity with zero performance cost. In ZeRO, pointers are loaded/stored with special instructions and protected in caches with specially encoded metadata.

Name Confusion Architectures 2019

- A novel mitigation for code-reuse attacks in resource-constrained devices (for example, IoT devices) using minimal micro-architectural adjustments and no software changes. For this project, I implemented micro-architectural changes required by the technique to the branch predictors and various pipeline stages of the Out-Of-Order CPU model in the GEM5 architectural simulator.

Tapless Calibration Method 2018

- A new calibration method for silicon photonics switches based on the MZI elements. This method, unlike prior work, does not require tapping the switches to monitor the power. Instead, we leverage the photo-conductance effect to both control and calibrate the switch elements.

Zero-Temperature Coefficient 2012-2013

- Investigating Zero-Temperature Coefficient behavior of CMOS-SOI devices.

Work Experience

Intern at Technology and Research Group, Microsoft, *Redmond, WA* *5/2022 – 8/2022*

- Worked on the scheduling of distributed Machine Learning jobs.

Senior Physical Design Engineer, Cisco Inc., *Caesarea, Israel* *5/2016 – 8/2017*

- I implemented critical path blocks with >10M cells, blocks with HBM2 PHY interfaces, and custom clock structures using ICC2 abstraction flow (divide design to sub-designs and top), Primetime Hyperscale flow, Apache Redhawk DMP flow.

- I drove the development from scratch of a web-based system for monitoring, reporting, and results collection of all Place-and-Route runs. This system allowed engineers to track the impact of design changes on various metrics (e.g., timing closure, DRC errors, and others), compare design versions and create weekly reports in two clicks; significantly enhancing the team's insights into the implementation progress.
- I mentored newly recruited engineers – walk-through Place-and-Route design implementation flows, helped to debug the designs, etc.

Physical Design Engineer, Apple, *Haifa, Israel* *3/2013 – 5/2016*

- RTL2GDS of low power and high std cell count designs with multiple voltage domains and clock domain crossings – floorplanning, placement, clock tree synthesis, timing closure, DRC/LVS clean up, formal verification, etc.
- In addition, on a day-to-day basis, I was developing and supporting project Place-and-Route flows for the top and block levels. It included things such as power grid flow scripts, power switch and tap insertion flows for multi-voltage area designs, running regressions to validate flow stability, and helping team members with flow-related issues.
- At last, I was responsible for Full Chip Power Delivery Analysis using Apache Redhawk suite. I was running Static/Dynamic IR Drop analysis, resolving full-chip, integration, and block-level issues, and support of partition owners.

Physical Design Engineer (part-time), Intel, *Haifa, Israel* *7/2011 – 3/2013*

- I set up and maintained simulation environments for Apache RedHawk: simulations scripts, scenarios, post-processing. In addition, I did Static IR Drop, Dynamic IR Drop, and Power-UP simulations on a block/full-chip level.

Workshops and Talks

1. **Manzhosov, E.** and Simha Sethumadhavan. "Amplification of Errors by Encryption". 2^{nd} *Workshop on Data Integrity and Secure Cloud Computing (DISCC). In Conjunction with the* 56^{th} *International Symposium on Microarchitecture (MICRO 2023).*

Conference Publications

1. **Manzhosov, E.**, and Sethumadhavan, S., "Polymorphic Error Correction". **To Appear in:** *57th IEEE/ACM International Symposium on Microarchitecture (MICRO), November, 2024*.

2. **Manzhosov, E.**, Hastings, A., Pancholi, M., Piersma, R., Tarek Ibn Ziad, M., and Sethumadhavan, S., 2022, October. "Revisiting Residue Codes for Modern Memories". *2022 55th IEEE/ACM International Symposium on Microarchitecture (MICRO)*, 2022, pp. 73-90. **Top Pick in Micro Top Picks 2023**.

3. Tarek Ibn Ziad, M., Arroyo, M.A., **Manzhosov, E.**, Kemerlis, V.P., and Sethumadhavan, S., 2021, September. "WiP: Securing Resource-Constrained Processors with Name Confusion". In *2021 IEEE Symposium on Secure and Private Execution Environment Design* (SEED).

4. Tarek Ibn Ziad, M., Arroyo, M.A., **Manzhosov, E.**, Kemerlis, V.P., and Sethumadhavan, S., 2021, September. "EPI: Efficient Pointer Integrity For Securing Embedded Systems". In *2021 IEEE Symposium on Secure and Private Execution Environment Design* (SEED).

5. Tarek Ibn Ziad, M., Arroyo, M.A., **Manzhosov, E.**, Piersma, R. and Sethumadhavan, S., 2021, June. "No-FAT: Architectural support for low overhead memory safety checks". In *2021 ACM/IEEE 48th Annual International Symposium on Computer Architecture* (ISCA) (pp. 916-929). IEEE.

6. Tarek Ibn Ziad, M., Arroyo, M.A., **Manzhosov, E.** and Sethumadhavan, S., 2021, June. "ZeRØ: Zero-overhead resilient operation under pointer integrity attacks". In *2021 ACM/IEEE 48th Annual International Symposium on Computer Architecture* (ISCA) (pp. 999-1012). IEEE.

7. Abrams, N.C., Cheng, Q., Glick, M., **Manzhosov, E.**, Jezzini, M., Morrissey, P., O'Brien, P. and Bergman, K., 2020. "Design considerations for multi-chip module silicon-photonic transceivers". *In Metro and Data Center Optical Networks and Short-Reach Links III* (Vol. 11308, p. 113080I). International Society for Optics and Photonics.

8. Gazman, A., **Manzhosov, E.**, Bahadori, M., Anderson, E., Zhu, Z., Shen, Y. and Bergman, K., 2018, September. "Topology Agnostic Solution for Tapless Calibration of Silicon Photonic Mach-Zehnder Based Switches". In *2018 European Conference on Optical Communication* (ECOC) (pp. 1-3). IEEE.

9. Malits, M., Svetlitza, A., **Manzhosov, E.**, Rotman, N. and Nemirovsky, Y., 2012, November. "The influence of thermoelectric effects on the self-heating of nanometer CMOS-SOI devices". In 2012 IEEE 27th Convention of Electrical and Electronics Engineers in Israel (pp. 1-5). IEEE.

Journal Publications

1. Shen, Y., Meng, X., Cheng, Q., Rumley, S., Abrams, N., Gazman, A., **Manzhosov, E.**, Glick, M.S. and Bergman, K., 2019. "Silicon photonics for extreme scale systems". *Journal of Lightwave Technology*, 37(2), pp.245-259.

2. Gazman, A., **Manzhosov, E.**, Browning, C., Bahadori, M., London, Y., Barry, L. and Bergman, K., 2018. "Tapless and topology agnostic calibration solution for silicon photonic switches". *Optics express*, 26(25), pp.32662-32674.