

Bo-Yuan Huang

Curriculum Vitae

Contact	Email: bo-yuan.huang@intel.com Phone: (+1) 917-770-2804
Research Interests	Design methodology and functional/security verification of modern computing systems, formal methods, and automated reasoning
Education	<p>Princeton University, USA <i>Ph.D., Electrical and Computer Engineering, 2022</i></p> <p>Thesis: “Instruction-Level Abstraction for Program Compilation and Verification in Accelerator-Rich Platforms” Advisor: Prof. Sharad Malik Committee: Prof. Margaret Martonosi and Prof. Naveen Verma</p> <p>Princeton University, USA <i>M.A., Electrical Engineering, 2017</i></p> <p>National Taiwan University, Taiwan <i>B.S., Electrical Engineering, 2014</i></p>
Experience	
2021 – present	<p>Intel Corporation, Security Research <i>Offensive Security Researcher</i></p> <p>Researching scalable assurance in Trusted Computing and security architectures Researching automated formal verification, fuzzing, and AI-enhanced static analysis</p>
2016 – 2021	<p>Princeton University, Electrical and Computer Engineering <i>Research Assistant</i></p> <p>Advisor: Prof. Sharad Malik Led research in Instruction-Level Abstraction for the specification, verification, and design automation of SW/FW/HW in heterogeneous computer systems Led multi-institutes research on modular and verifiable end-to-end compilation flow for deep-learning applications on accelerator-rich systems</p>
Summer 2019	<p>Microsoft Research, New Security Ventures & Research in Software Engineering <i>Research Intern</i></p> <p>Supervisor: Dr. Patrice Godefroid and Dr. Marina Polishchuk Designed grammar-based fuzzing algorithm with dynamic learning for stateful REST API Implemented REST API data fuzzer for cloud services on top of RESTler</p>
Summer 2018	<p>Microsoft Research, Research in Software Engineering <i>Research Intern</i></p> <p>Supervisor: Dr. Patrice Godefroid and Dr. Barry Bond Designed white-box fuzzing algorithm for attacker-memory-safety of OS kernels Implemented kernel-aware symbolic memory checker on top of SAGE</p>

Summer 2017	Intel Corporation , Security Center of Excellence <i>Security Research Intern</i> Developed formal modeling and verification framework for concurrent firmware Exploited TOC/TOU security vulnerability in an inter-IPs communication protocol
Summer 2016	Intel Corporation , Security Center of Excellence <i>Technical Intern</i> Applied word-level bounded model checking on SoC Secure Boot with QEMU IA semantics
2014 – 2015	Coast Guard Administration <i>Second Lieutenant</i> Designed and developed the first search and rescue procedure assisting system for Taiwan coastal area based on USCG drift theory
2013 – 2014	National Taiwan University , Applied Logic and Computation Lab <i>Undergraduate Research Assistant</i> Advisor: Prof. Jie-Hong Roland Jiang Asynchronous QDI circuit synthesis from signal transition protocols
Summer 2013	TSMC , Advanced Process Transferring Group <i>Software Engineer Intern</i> Developed automation and visualization tools for GDS and design pattern analysis
2012 – 2013	National Taiwan University , Wireless and Mobile Networking Lab <i>Undergraduate Research Assistant</i> Advisor: Prof. Hung-Yu Wei Protocol design and game theoretic solutions for device-to-device radio resource allocation

Teaching Experience

Fall 2018	Princeton ECE 206/COS 306 - Contemporary Logic Design <i>Head Assistant Instructor</i> This course teaches digital logic design and introductory computer organization. I was the head assistant instructor (AI) for this 170-students course. I organized the graduate and undergraduate AI team, taught precepts, held laboratory hours, prepared exam materials, and graded assignments/exams. I received Best Teaching Assistant Award .
Fall 2016, 2017	Princeton ECE 206/COS 306 - Contemporary Logic Design <i>Assistant Instructor</i> × 2

Co-Supervision of Undergraduate and Graduate Students

- Intel Intern – Robert Avery (Open Benchmark for Formal Firmware Verification, 2023)
- Intel Intern – Maurille Behemet (AI Security Engine for Threat Modeling, 2023)
- Intel Intern – Fabrizio Cicala (State-aware Fuzzing and Protocol Extraction, 2022)
- Intel Intern – Elijah Bryant (Universal Information Flow Tracking Language, 2022)
- Intel Intern – Isabella Siu (LLVM-based Firmware Instrumentation, 2022)
- REU Program – Sarah Schabar (Crypto-accelerator-rich SoC Analysis, 2021)
- REU Program – Isabella Siu (Secure Bootloader Verification, 2021)
- ECE Junior Thesis – Phoebe Lin (Parallel SAT Solver, 2021)
- CS Visiting Scholar – Yueling Zhang (HDL Synthesis and Hardware Abstraction, 2018)
- ECE Senior Thesis – David Gilhooley (Verified Boot in Trusted Platform Module, 2016)

Awards and Honors

2023	Security Division Recognition Award, Intel
2022	Corporation Quality Award, Intel
2020	ACM TODAES Best Paper Award
2019	Best Teaching Assistant Award, Princeton University
2017, 2018	NSF SSFT Travel Grant
2017	SRC TECHCON Best in Session Award
2016	NSF VMW Full Scholarship, CAV
2015	SEAS Travel Grant, Princeton University
2015	Francis Robbins Upton Fellowship, Princeton University
2014	First Prize: Outstanding Undergraduate Independent Research, NTU
2014	Second Prize: TSMC Special Research Competition
2013	TSMC Undergraduate Research Grant
2013	Ministry of Science and Technology Research Grant
2012	First Prize: TSMC Semiconductor Elite Program
2012	First Prize: Microsoft WP Platform Workshop Innovation Award
2011,2012,2013,2014	President's Awards, NTU

Patent Patrice Godefroid, Bo-Yuan Huang, and Marina Polishchuk. Intelligently fuzzing data to exercise a service. Patent, May 2022. US 11321219 B2.

Publications

Journal Articles

Bo-Yuan Huang, Hongce Zhang, Pramod Subramanyan, Yakir Vizel, Aarti Gupta, and Sharad Malik. Instruction-Level Abstraction (ILA): A Uniform Specification for System-on-Chip (SoC) Verification. *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, 2019. **Best Paper Award.**

Pramod Subramanyan, **Bo-Yuan Huang**, Yakir Vizel, Aarti Gupta, and Sharad Malik. Template-based Parameterized Synthesis of Uniform Instruction-Level Abstractions for SoC Verification. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)*, 2018.

Shih-Tang Su, **Bo-Yuan Huang**, Chih-Yu Wang, Che-Wei Teh, and Hung-Yu Wei. Protocol Design and Game Theoretic Solutions for Device-to-Device Radio Resource Allocation. *IEEE Transactions on Vehicular Technology (TVT)*, 2017.

Conference Proceedings

Bo-Yuan Huang, Hongce Zhang, Aarti Gupta, and Sharad Malik. INVITED: Generalizing the ISA to the ILA: A Software/Hardware Interface for Accelerator-rich Platforms. *Design Automation Conference (DAC)*, 2023.

Priyam Biswas, Sayak Ray, Stephan Heuser, **Bo-Yuan Huang**, Rana Elnaggar, and Jason Fung. Effectiveness of Artificial Intelligence in Detecting Hardware Security Issues: Challenges, Status Quo, and Directions. *Software Professionals Conference (SWPC)*, 2022.

Yu Zeng, **Bo-Yuan Huang**, Hongce Zhang, Aarti Gupta, and Sharad Malik. Generating Architecture Level Abstractions from RTL Designs for Processors and Accelerators. Part I: Determining Architectural State Variables. *International Conference on Computer-Aided Design (ICCAD)*, 2021.

Patrice Godefroid, **Bo-Yuan Huang**, and Marina Polishchuk. Intelligent REST API Data Fuzzing. *ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (FSE)*, 2020.

Bo-Yuan Huang, Hongce Zhang, Aarti Gupta, and Sharad Malik. ILAng: A Modeling and Verification Platform for SoCs using Instruction-Level Abstractions. *International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, 2019.

Yue Xing, **Bo-Yuan Huang**, Aarti Gupta, and Sharad Malik. A Formal Instruction-Level GPU Model for Scalable Verification. *International Conference on Computer-Aided Design (ICCAD)*, 2018.

Bo-Yuan Huang, Sayak Ray, Aarti Gupta, Jason Fung, and Sharad Malik. Formal Security Verification of Concurrent Firmware in SoCs using Instruction-Level Abstraction for Hardware. *Design Automation Conference (DAC)*, 2018.

Bo-Yuan Huang, Yi-Hsiang Lai, and Jie-Hong Roland Jiang. Asynchronous QDI Circuit Synthesis from Signal Transition Protocols. *International Conference on Computer-Aided Design (ICCAD)*, 2015.

Workshop Proceedings

Bo-Yuan Huang, Steven Lyubomirsky, Thierry Tambe, Yi Li, Mike He, Gus Smith, Gu-Yeon Wei, Aarti Gupta, Sharad Malik, Zachary Tatlock. From DSLs to Accelerator-Rich Platform Implementations: Addressing the Mapping Gap. *ASPLOS Workshop on Languages, Tools, and Techniques for Accelerator Design (ASPLOS-LATTE)*, 2021.

Hongce Zhang, **Bo-Yuan Huang**, Yue Xing, Aarti Gupta, Sharad Malik. Hardware-Software Interface Specification for Verification in Accelerator-Rich Platforms. *ASPLOS Workshop on Languages, Tools, and Techniques for Accelerator Design (ASPLOS-LATTE)*, 2021.

Bo-Yuan Huang, Hongce Zhang, Pramod Subramanyan, Yakir Vizel, Aarti Gupta, and Sharad Malik. Instruction-Level Abstraction (ILA): Democratizing Instructions for SoCs. *SRC TECHCON*, 2017. **Best in Session Award.**

Bo-Yuan Huang, Shih-Tang Su, Chih-Yu Wang, Che-Wei Teh, and Hung-Yu Wei. Resource Allocation in D2D Communication - A Game Theoretic Approach. *IEEE ICC Workshop on M2M Communications for Next Generation IoT (ICC-M2M)*, 2014.

Talks & Tutorials

- | | |
|-----------|---|
| Sep. 2022 | Tutorial — Formal Information Flow Verification for Hardware CWEs. <i>Design & Testing Technology Conference (DTTC)</i> |
| Sep. 2022 | Panel — Back to the Future: Scopes and Opportunities of AI in Hardware Security. <i>Design & Testing Technology Conference (DTTC)</i> |
| June 2022 | Tutorial — Generalizing the ISA to the ILA: A Software/Hardware Interface for Accelerator-rich Platforms. <i>International Symposium on Computer Architecture (ISCA)</i> |
| May 2022 | Tutorial — Generalizing the ISA to the ILA: A Software/Hardware Interface for Accelerator-rich Platforms. <i>Annual Symposium of the Applications Driving Architectures (ADA) Center</i> |
| May 2021 | Invited Talk — Instruction-Level Abstraction & ILAng: A Modeling and Verification Platform for SoCs. <i>Paul G. Allen School of Computer Science & Engineering, University of Washington.</i> (Host: Prof. Luis Ceze) |

April 2021 Invited Talk — Instruction-Level Abstraction for Accelerator-rich Architectures' Specification and Verification. *Graduate Institute of Electronics Engineering, National Taiwan University.* (Host: Prof. Chien-Mo Li)

April 2021 Invited Talk — Instruction-Level Abstraction for Software Development and Verification in Accelerator-rich Computing Systems. *Security and Privacy Lab, Intel Labs.* (Host: Dr. Carlos V. Rozas)

Professional Service

2023 ASPLOS (TPC), ICCAD (TPC), and FMCAD (TPC)

2020 CAV (APC)

External reviewer CAV, DAC, DATE, ICC, ICCAD, FMCAD, and IEEE TCAD

Community Service

2022, 2023 Program Manager, Princeton-Intel Research Experience for Undergraduate Program

2021 Mentor, Princeton-Intel Research Experience for Undergraduate Program

2019 – 2021 Mentor, ReMatch Undergraduate Summer Research Program

2017 – 2019 Mentor, Princeton Early Career Mentoring Program

2017 – 2019 Speaker & Mentor, Graduate Student Orientation Workshop Series

2017 – 2018 Vice President, Princeton Association of Taiwanese Students

This curriculum vitae was last updated on 16th July, 2023.