KESHA HIETALA

KESHA@CS.UMD.EDU

I am interested in compilers, formal verification, program analysis and programming language design, especially as applied to computer security and quantum computing. My thesis research has focused on verifying quantum programs and quantum program optimizations in the Coq proof assistant.

EDUCATION

PhD University of Maryland (College Park), Computer Science — Expected 2022
Dissertation: "A Verified Software Toolchain for Quantum Programming"
Committee: M. Hicks (chair), A. Childs, L. Lampropoulos, R. Rand, X. Wu

MS University of Maryland (College Park), Computer Science — May 2019
Advisor: Michael Hicks

BS University of Minnesota (Twin Cities), Computer Science — May 2016
Graduated Summa Cum Laude
Specialized in Computer Security
Minored in Mathematics and Asian Languages and Literatures (Japanese track)

HONORS AND AWARDS

Distinguished Paper, Symposium on Principles of Prog. Langs. (POPL) 2021
University Fellowship, University of Maryland 2016-2018
NSF Graduate Research Fellowship Honorable Mention, NSF 2016
Outstanding Undergraduate Researcher Award Honorable Mention, CRA 2016
Lando Scholarship, University of Minnesota 2014
Undergraduate Research Opportunities Program Award, Univ. of Minn. 2014
Undergraduate Research Scholarship, University of Minnesota 2013
Dean's List, University of Minnesota 2012-2016
Gold Scholar Award, University of Minnesota 2012
National Merit Scholar, National Merit Scholarship Corporation 2012

PUBLICATIONS

Journal Publications

1. Kesha Hietala, Robert Rand, Shih-Han Hung, Xiaodi Wu, Michael Hicks. "A Verified Optimizer for Quantum Circuits." Proceedings of the ACM Conference on Principles of Programming Languages (POPL). 2021. **Distinguished Paper**.

2. Shih-Han Hung, Kesha Hietala, Shaopeng Zhu, Mingsheng Ying, Michael Hicks, Xiaodi Wu. "Quantitative Robustness Analysis of Quantum Programs." Proceedings of the ACM Conference on Principles of Programming Languages (POPL). 2019.

3. Vaibhav Sharma, Kesha Hietala, Stephen McCamant. "Finding Substitutable Binary Code by Synthesizing Adapters." IEEE Transactions on Software Engineering (TSE). 2019.

Conference Papers

1. Kesha Hietala, Robert Rand, Shih-Han Hung, Liyi Li, Michael Hicks. "Proving Quantum Programs Correct." Proceedings of the Conference on Interactive Theorem Proving (ITP). 2021.

2. Robert Rand, Kesha Hietala, Michael Hicks. "Formal Verification vs. Quantum Uncertainty." 3rd Summit on Advances in Programming Languages (SNAPL). 2019.

3. Andrew Ruef, Kesha Hietala, Arlen Cox. "Volume-Based Merge Heuristics for Disjunctive Numeric Domains." International Static Analysis Symposium (SAS). 2018.

4. Vaibhav Sharma, Kesha Hietala, Stephen McCamant. "Finding Substitutable Binary Code for Reverse Engineering by Synthesizing Adapters." 2018 IEEE 11th International Conference on Software Testing, Verification and Validation (ICST). 2018.

PROFESSIONAL EXPERIENCE

University of Maryland, College Park, MD 2018 – Present
Graduate Research Assistant, Advisor: Michael Hicks

- Designed an intermediate representation for quantum programs (called SQIR) and a semantics amenable to formal verification in the Coq proof assistant.
- Formally verified SQIR implementations of key quantum algorithms and state-of-the-art optimizations over SQIR programs.
- Assisted with the development of a robustness logic for reasoning about quantum programs in the presence of errors.

Microsoft, Remote Summer 2021
Research Intern, Mentors: Sarah Marshall, Nikhil Swamy

- Implemented an embedded language for quantum programming in F*.
- Wrote a plugin for the Q# compiler to convert Q# programs into this embedded language, providing a novel type checking pass to enforce properties like qubit liveness and linearity.

Microsoft Research, Remote Winter 2020
Research Intern, Mentors: Arvind Arasu, Nikhil Swamy

- Assisted with the formalization in F* of FastVer (now Zeta), a high-performance key-value store with data integrity, focusing on connecting an existing high-level proof to a low-level implementation.

Institute for Defense Analyses – CCS, Bowie, MD Summer 2017
Summer Researcher, Collaborators: Arlen Cox, Andrew Ruef

- Designed and implemented techniques to compare convex polytopes with the goal of improving the precision of a disjunctive polyhedral analysis.

University of Minnesota, Twin Cities, MN Spring 2016
Undergraduate Research Assistant, Supervisor: Stephen McCamant

University of Minnesota, Twin Cities, MN Spring 2013 – Spring 2014
Undergraduate Research Assistant, Supervisor: Gopalan Nadathur

Undergraduate Internships:

- National Security Agency, *Director's Summer Program* Sums. 2015 & 2016
- MIT Lincoln Laboratory, *Summer Research Program* Summer 2014
- Sandia National Laboratories, *Center for Cyber Defenders* Sums. 2012 & 2013

TEACHING EXPERIENCE

University of Maryland, College Park, MD Fall 2017 & Spring 2018
Graduate Teaching Assistant, Department of Computer Science

- Led a discussion section, graded assignments, developed course material, and held office hours for a junior-level programming languages course.
- Contrasted various programming paradigms and covered topics such as static and dynamic typing, finite automata and context free grammars.

University of Minnesota, Twin Cities, MN Fall 2014 & Spring 2015
Undergraduate Teaching Assistant, Department of Computer Science

- Assisted in discussion sections, graded assignments, and held office hours for a sophomore-level programming languages course.
- Covered programming techniques such as recursion, higher-order functions, lazy and eager evaluation and infinite data objects.

PRESENTATIONS AND INVITED LECTURES

Invited Talk, "Quantum IRs for Formal Verification," QCE 2021 workshop.

Paper Presentation, "Proving Quantum Programs Correct," ITP 2021.

Workshop, "Expanding the VOQC Toolkit," PLanQC 2021.

Paper Presentation, "A Verified Optimizer for Quantum Circuits," POPL 2021.

Workshop, "A Verified Optimizer for Quantum Circuits," PLanQC 2020.

Workshop, "Verified Optimization in a Quantum Intermediate Representation," QPL 2019.

Seminar, "Approaches to Compiling Functional Languages," University of Minnesota, 2016.

SERVICE

Peer-Reviewed Articles for:

- TQC (2020)

Sub-reviewed Articles for:

- OOPLSA (2021)
- PLDI (2020, 2021)
- QCTIP (2020)
- RC (2019)
- Oakland S&P (2017)
- CCS (2017)

Other Service:

- Student volunteer at POPL 2020
- Organizer for UMD's PL reading group, Fall 2018 & Spring 2019
- Project mentor for Girls Talk Math summer camp, 2018 & 2021
- Mentor for Technica hackathon for underrepresented genders, 2018 & 2019

COURSEWORK

Programming Languages and Compilers

- UMN CSCI 5106 – Programming Languages
- UMN CSCI 5161 – Introduction to Compilers
- UMN CSCI 5980 – Special Topics: Advanced Functional Programming
- UMD CMSC 631 – Program Analysis and Understanding
- UMD CMSC 838M – Model Checking
- UMD ENEE 645 – Compilers and Optimization

Computer Security

- UMN CSCI 5271 – Introduction to Computer Security
- UMN CSCI 5471 – Modern Cryptography
- UMN MATH 5248 – Cryptology and Number Theory
- UMD CMSC 818O – Computer and Network Security

Mathematics

- UMN CSCI 5251 – Error-Correcting Codes, Finite Fields, Algebraic Curves

- UMN MATH 5165 – Mathematical Logic I
- UMN MATH 5385 – Introduction to Computational Algebraic Geometry
- UMD CMSC 666 – Numerical Analysis I

Other Computer Science

- UMN CSCI 5521 – Introduction to Machine Learning
- UMD CMSC 858K – Introduction to Quantum Information Processing
- UMD CMSC 714 – High Performance Computing Systems
- UMD CMSC 651 – Analysis of Algorithms

PROGRAMMING LANGUAGES AND TOOLS

Proficient: Python, OCaml, C/C++, Coq, F*

Familiar: F#, Haskell, Ruby, Prolog, Rust, Java

PERSONAL

I enjoy painting, pottery and puzzles.

I am a U.S. Citizen. I have previously held DoD TS/SCI and DOE L clearances.