Ferhat Erata

AKW 203, 51 Prospect Street,
New Haven, CT 06511
+1-203-833-9448

https://www.linkedin.com/in/ferhaterata/
https://scholar.google.com/citations?user=UcpqLLYAAAAJ
ferhat.erata@yale.edu

Summary

I am pursuing my PhD in Computer Science at Yale University with a concentration in Programming Languages and Verification, under the guidance of Ruzica Piskac and Jakub Szefer. My recent research focuses on symbolic regression, the dynamic inference of real or integer-valued relational properties from hardware or software implementations, including nonlinear equalities and inequalities, random self-reducible properties, functional equations, and recurrence relations. I integrate machine learning with formal techniques for automated inference at scale. Additionally, I am exploring the application of these properties to enhance areas such as property-based testing, formal verification, self-correcting programs, function synthesis (symbolic regression), software and FPGA security, and privacy-preserving machine learning.

Currently, I am an Applied Scientist Intern with the Automated Reasoning Group at Amazon Web Services (AWS) after completing two full-time internships there. My work aims to improve the reliability of AWS services by creating advanced tools for model-based testing, conformance checking, randomized testing of distributed networked systems, database systems, and cloud services. I also developed a decision procedure to check the linearizability of AWS web services. My implementations primarily use the Rust programming language and are supplemented by black-box techniques.

I have been the lead Teaching Assistant of Avi Silberschatz’s Database Systems class for the last 3 years.

In the past, I worked on verifying the security of low-level Post-Quantum Cryptographic (PQC) code, including C, C++, and binary analysis. I specialized in detecting side-channel vulnerabilities in cryptographic code using formal techniques such as symbolic execution, dynamic analysis, and static analysis. For my master's project at Yale, I developed a probabilistic symbolic execution engine to estimate the power consumption and timing of energy-harvesting, battery-free embedded devices. These devices run programs intermittently, operating only when there is enough harvested ambient energy in their reservoir.

Previously, I worked as a Software Research Engineer on R&D projects within consortia in the aviation and automotive sectors. In these roles, I applied formal methods to both software and system designs.

Professional Experience

Amazon Web Services (AWS), Applied Scientist Intern -- Part Time:
[September 2023 -- January 2024]

- Automated Reasoning Group, New York (https://www.amazon.science/research-areas/automated-reasoning)
- Rust Language: Systematic/Randomized Exploration and Conformance Checking of Distributed Systems.

Amazon Web Services (AWS), Applied Scientist Intern -- Full Time:
[May 2023 -- August 2023]

- Automated Reasoning Group, New York
- Rust Language: Model-based Testing, Systematic Exploration and Conformance Checking of Distributed Systems.
- Mentor: Rupak Majumdar

Amazon Web Services (AWS), Applied Scientist Intern -- Part Time:
[September 2022 -- January 2023]

- Automated Reasoning Group, New York

- Rust Language: Fuzzing of Distributed Message-Passing Systems.

Amazon Web Services (AWS), Applied Scientist Intern -- Full Time:
[June 2022 to August 2022]

- Automated Reasoning Group, New York
- Rust and Go Languages: Developed a decision procedure for checking consistency of distributed systems.
- Mentor: Rupak Majumdar

Yale University, Graduate Teaching Assistant:
[June 2020 -- Present]

- CS423--Principles of Operating System (Instructor: Avi Silberschatz)
- CS437--Database Systems (Instructor: Avi Silberschatz)
- CS440--Advanced Databases (Instructor: Robert Soule)

Yale University, Graduate Research Assistant:
[June 2020 -- Present]

- Member of Rigorous Software Engineering Lab. (Ruzica Piskac https://rose.yale.edu/)
- Member of Computer Architecture and Security Lab. (Jakub Szefer https://caslab.csl.yale.edu/)
- C/C++, LLVM, Rust, and ARM Binaries: Dynamic Analysis, Formal Verification, Property Synthesis, Symbolic Execution, Property-based Testing, Cryptographic Applications, Side-Channel analysis.

COST (European Cooperation in Science and Technology), Management Committee Member:
[December 2017 -- January 2019]

- COST Action IC1402 - Runtime Verification beyond Monitoring (ARVI)
- https://www.cost.eu/actions/IC1402/

COST (European Cooperation in Science and Technology), Management Committee Member:
[January 2015 -- January 2019]

- COST Action IC1404 - Multi-Paradigm Modelling for Cyber-Physical Systems (MPM4CPS)
- https://www.cost.eu/actions/IC1404/

ITEA (Information Technology for European Advancement), Research Engineer, National Consortium Leader:
[January 2019 -- August 2019]

- XIVT Project Consortium (https://itea3.org/project/xivt.html)
- C++ Language: Tool Development using LLVM and KLEE Symbolic Execution Engine.
- I developed AlloyInEcore automated reasoning tool: https://modelwriter.github.io/AlloyInEcore/

- AlloyInEcore: Embedding of First-Order Relational Logic into Meta-object Facility. AlloyInEcore allows the user to specify metamodels with their static semantics, while, using the semantics, it automatically checks the conformance of models with their metamodel, detects inconsistent models, and completes partial models.

ITEA (Information Technology for European Advancement), Research Engineer, National Consortium Leader:
[September 2015 -- August 2018]

- ASSUME Project Consortium (https://itea3.org/project/assume.html)
- C++ Language: Tool Development using SAT/SMT solvers.
- I developed Tarski framework: https://modelwriter.github.io/Tarski/

- Tarski: Automated Reasoning about Traces based on Configurable Formal Semantics: For any given artifact (e.g., requirements, architecture models and source code), Tarski allows the user to specify new trace types and their configurable semantics, while, using the semantics, it automatically infers new traces based on existing traces provided by the user, and checks the consistency of traces.

ITEA (Information Technology for European Advancement), Research Engineer, Project Leader:
[October 2014 -- September 2017]

- ModelWriter Project Consortium (https://itea3.org/project/modelwriter.html)
- Java Language: Tool Development using Alloy Specification Language (https://modelwriter.github.io/Tarski/).

- I led the development of ModelWriter framework: https://ieeexplore.ieee.org/document/8115703

- ModelWriter: Text and model-synchronized document engineering platform: We demonstrate how ModelWriter framework can be used to trace the consistency and completeness of technical documents that consist of a set of System Installation Design Principles used by Airbus to ensure the correctness of aircraft system installation. We provide two types of reasoning: reasoning about the meaning of text using semantic parsing and description logic theorem proving; and reasoning about document structure using first-order relational logic and finite model finding.

Education

PhD - Computer Science, Yale University:

- I am a member of the Rigorous Software Engineering (ROSE) Lab, advised by *Ruzica Piskac* (https://rose.yale.edu/) in the Computer Science department. I am also a member of the Computer Architecture and Security Lab (CASLAB), led by *Jakub Szefer* in the Electrical Engineering department (https://caslab.csl.yale.edu/). In the ROSE Lab, I am working on developing novel formal techniques to address hardware-related security problems. These projects are initially specified in collaboration with CASLAB.

MPhil - Computer Science, Yale University:
- Master of Science (MSc) in Computer Science.

MSc - Computer Science, Yale University:
- Master of Philosophy (MPhil) in Computer Science.

MSc - Information Technology, Ege University, Izmir, Turkey:
- Master of Science (MSc), Information Technology.

BSc - Computer Engineering Department, Dokuz Eylul University, Izmir, Turkey:
- Bachelor of Science (BSc), Computer Engineering (Double Major Program).
- Bachelor of Science (BSc), Industrial Engineering.

Publications

[1] Ferhat Erata, Ruzica Piskac, Victor Mateu, and Jakub Szefer. **2023**. “Automated Detection of Single-Trace Side-Channel Vulnerabilities in Constant-Time Cryptographic Binaries” ***8th IEEE European Symposium on Security and Privacy (Euro S&P 2023)***. https://arxiv.org/abs/2304.02102

[2] Xu, Chuanqi, **Ferhat Erata**, and Jakub Szefer. **2023**. "Exploration of Quantum Computer Power Side Channels." ***The 30th ACM Conference on Computer and Communications Security (CCS)***
https://arxiv.org/abs/2304.03315

[3] Xu, Chuanqi, **Ferhat Erata,** and Jakub Szefer. "Classification of Quantum Computer Fault Injection Attacks." arXiv preprint arXiv:2309.05478 (2023). https://arxiv.org/abs/2309.05478

[4] Ferhat Erata, Chuanqi Xu, Ruzica Piskac, and Jakub Szefer. **2024**. Recovering Quantum Circuits from Power Traces using Formal Methods. ***The 31st ACM Conference on Computer and Communications Security (CCS)*** (under submission).

[5] Yusaf Azimi, Fırat, Atıl, Mohammad Celal Çağın Elgün, **Ferhat Erata**, and Cemal Yılmaz. **2023**. "AdapTV: A Model-Based Test Adaptation Approach for End." ***IEEE Access*** https://doi.org/10.1109/ACCESS.2023.3262746.

[6] Ferhat Erata, Shuwen Deng, Faisal Zaghloul, Wenjie Xiong, Onur Demir, and Jakub Szefer. **2022**. "Survey of Approaches and Techniques for Security Verification of Computer Systems". ***ACM Journal on Emerging Technologies in Computing Systems (JETC)*** https://doi.org/10.1145/3564785.

[7] Ferhat Erata, Arda Göknil, Sinan Yıldırım, Eren Yıldız, Ruzica Piskac, Jakub Szefer, and Gökçin Sezgín. **2022**. "Energy-aware Timing Analysis of Intermittent Programs". ***ACM Transactions on Embedded Computing Systems (TECS)*** https://dl.acm.org/doi/10.1145/3563216.

[8] Sanjay Deshpande, Chuanqi Xu, Theodoros Trochatos, Hanrui Wang, **Ferhat Erata**, Song Han, Yongshan Ding, and Jakub Szefer. **2023**. "Design of a Quantum Computer Antivirus". ***IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*** https://doi.org/10.1109/HOST55118.2023.10133711

[9] Fırat, Atıl, Mohammad Yusaf Azimi, Celal Çağın Elgün, **Ferhat Erata**, and Cemal Yılmaz. "Model-based test adaptation for smart TVs." In *Proceedings of the **3rd ACM/IEEE International Conference on Automation of Software Test (AST)***, pp. 52-53. 2022. https://doi.org/10.1145/3524481.3527237

[10] Jalil Morris, Obi Nnorom Jr., Anisul Abedin, **Ferhat Erata**, and Jakub Szefer. **2021.** "Deep Freezing Attacks on Capacitors and Electronic Circuits", in *Proceedings of the International Conference on **Security, Privacy and Applied Cryptographic Engineering (SPACE)***, December. https://doi.org/10.1007/978-3-030-95085-9_10 (**Best Student Paper Award**). http://cse.iitkgp.ac.in/conf/SPACE2021/best_papers.php

[11] Mert Ozkaya and **Ferhat Erata. 2020**. "Understanding practitioners' challenges on software modeling: A survey." ***Journal of Computer Languages*** 58: 100963. https://doi.org/10.1016/j.cola.2020.100963.

[12] Mert Ozkaya and **Ferhat Erata**. **2019**. A Survey on the Practical Use of UML for Different Software Architecture Viewpoints. ***Information and Software Technology***. https://doi.org/10.1016/j.infsof.2020.106275

[13] Bedir Tekinerdogan and **Ferhat Erata. 2019**. Automated Reasoning Framework for Traceability Management of System-of-Systems. ***Science of Computer Programming*** https://doi.org/10.1016/j.scico.2020.102416

[14] Ferhat Erata, Arda Goknil, Ivan Kurtev, and Bedir Tekinerdogan. **2018**. "AlloyInEcore: Embedding of First-Order Relational Logic into Meta-Object Facility for Automated Model Reasoning", in *Proceedings of the 26th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (**ESEC/FSE'18**)*, November 4–9, 2018, USA. ACM. https://doi.org/10.1145/3236024.3264588

[15] Ferhat Erata, Claire Gardent, Bikash Gyawali, Anastasia Shimorina, Yvan Lussaud, Bedir Tekinerdogan, Geylani Kardas and Anne Monceaux. **2017**. Modelwriter: Text and model-synchronized document engineering platform. In Proceedings *of 32th IEEE/ACM International Conference on Automated Software Engineering, (**ASE'17**)*. Urbana-Champaign, IL, USA, 2017, 928–933. DOI: https://doi.org/10.1109/ASE.2017.8115703

[16] Ferhat Erata, Arda Goknil, Bedir Tekinerdogan, and Geylani Kardas. **2017**. A tool for automated reasoning about traces based on configurable formal semantics. In *Proceedings of the 2017 11th Joint Meeting on Foundations of Software Engineering (**ESEC/FSE'17**)*. https://doi.org/10.1145/3106237.3122825

[17] Matthias Kern, **Ferhat Erata**, Stefan Otten, Eric Sax, Markus Iser, Carsten Sinz, and Frederic Loiret. **2019**. Integrating Static Code Analysis Toolchains. In *Proceedings of the IEEE 43rd Annual Computer Software and Applications Conference (**COMPSAC'19**)*. https://doi.org/10.1109/COMPSAC.2019.00080

[18] Ferhat Erata, Moharram Challenger, Bedir Tekinerdogan, Anne Monceaux, Eray Tuzun, and Geylani Kardas. **2017**. Tarski: a platform for automated analysis of dynamically configurable traceability semantics. In *Proceedings of the ACM SIGAPP Symposium on Applied Computing (**SAC'17**), Programming Languages Track*. ACM, New York, NY, USA, 1607-1614. https://doi.org/10.1145/3019612.3019747

Service

Journal of Automated Reasoning (IF: 1.532).
• Reviewer • https://www.springer.com/journal/10817

IEEE Computer Architecture Letters (IF: 2.118).
• Reviewer • https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=10208

International Conference on Computer Aided Verification (CAV) 2023.
• PC member (AE) • http://www.i-cav.org/2023/organisation/

24th International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI 2023):
• PC member (AE) • https://popl23.sigplan.org/committee/VMCAI-2023-papers-artifact-evaluation-committee

International Workshop on Multi-Paradigm Modelling for Cyber-Physical Systems (MPM4CPS):
• PC member • http://msdl.uantwerpen.be/conferences/MPM4CPS/2023/50_committees

FedCSIS:
• PC member (Software, System and Service Engineering) • https://fedcsis.org/sessions/s3e/committee

Courses

AWS Machine Learning University
- Introduction to Program Verification in Dafny.
- Introduction to Solvers.
- ML for Leaders Generative AI
- Techniques – Mathematical Fundamentals for Machine Learning

Yale University Graduate Course
- Object-Oriented Programming
- Software Analysis and Verification
- Language-Based Security
- Intro to Database Systems
- Principles Of Operating Systems
- Introductory Statistics
- Intro to Probability Theory
- Compilers and Interpreters
- Cryptography and Computer Security

Activities

SSFT Summer School 2023 - Menlo College, Atherton, CA, USA [May 24 - 28, 2023]
Twelfth Summer School on Formal Techniques (Received Scholarship)

PLDI 2019 - Phoenix, Arizona, USA [June 22-28, 2019]
Programming Language Design and Implementation (Student Volunteer)

SAT/SMT/AR Summer School 2019 - Instituto Superior Técnico, University of Lisbon, Portugal [July 3-6, 2019]
International Summer School on Satisfiability, Satisfiability Modulo Theories, and Automated Reasoning

SSFT Summer School 2019 - Menlo College, Atherton, CA, USA [May 18-25, 2019]
Ninth Summer School on Formal Techniques (Received Scholarship)

FaceTAV 2018 - Facebook London, London, UK [November 28-29, 2018]
Facebook Testing & Verification Symposium (Participation)

ESEC/FSE 2018 - Lake Buena Vista, Florida, USA [November 6-9, 2018]
The ACM SIGSOFT Symposium on the Foundations of Software Engineering (Paper Presentation, Volunteering)

Short-Term Scientific Mission - Chalmers University of Technology, Gothenburg, Sweden [4-22 June 2018]
Formal Methods Division - Efficient Runtime Verification for Recursive Data Structures (Received Full Grant)

DeepSpec Summer School 2018 - Princeton University, New Jersey, USA [16-27 July 2018]
DeepSpec Summer School on Verified Systems (Interactive Proof Assistant Coq) (Received Full Grant)

Workshop on the Future of Alloy - CSAIL Lab, MIT, Cambridge, Massachusetts, USA [30 April - 1 May 2018]
Speaker - "*AlloyInEcore: Deep Embedding of First-Order Relational Logic into Meta-Object Facility*"

Short-Term Scientific Mission - University of Antwerp, Antwerp, Belgium [23-29 September 2018]
Systems and software Modeling Group / Modeling, Simulation and Design Lab (Received Full Grant)

2nd ARVI COST School on Runtime Verification, France [19-21 March 2018]
Winter School on Runtime Verification (Received Travel and Accommodation Grant)

WSCR 2017 - ETH Zurich, Switzerland [13 - 14 October 2017]
Workshop on Software Correctness and Reliability (Participation)

ESEC/FSE 2017 - Paderborn, Germany [4 - 8 September 2017]
The ACM SIGSOFT Symposium on the Foundations of Software Engineering (Paper Presentation)

SC^2 Summer School 2017 - MPI Informatics, Saarbrucken, Germany [31 July - 4 August 2017]
Satisfiability Checking (SAT/SMT) and Symbolic Computation Summer School (Registration Grant)

WSCR 2016 - ETH Zurich, Switzerland [7 - 8 October 2016]
Workshop on Software Correctness and Reliability (Participation)

VTSA Summer School 2016 - University of Liège, Belgium [29 August - 2 September 2016]
Verification Technology, Systems & Applications (Participation)

SMT Workshop 2016 - University of Coimbra, Portugal [1 - 2 July 2016]
14th International Workshop on Satisfiability Modulo Theories (Participation)

ICJAR 2016 - University of Coimbra, Portugal [27 - 30 June 2016]
International Joint Conference on Automated Reasoning (Participation)

SAT/SMT/AR Summer School 2016 - Instituto Superior Técnico, University of Lisbon [22-25 June 2016]
International Summer School on Satisfiability, Satisfiability Modulo Theories, and Automated Reasoning