Ferhat Erata

51 Prospect Street, AKW 203 – New Haven – CT 06511
☎ (203) 833 9448 • ✉ ferhat.erata@yale.edu • 🌐 ferhat.ai

Education

Yale University – *PhD in Computer Science, Programming Languages & Verification* **New Haven, CT, US**
Advisors: Prof. Ruzica Piskac, Prof. Jakub Szefer *Sep. 2019 - Dec. 2024 (expected)*

Yale University – *MSc, MPhil in Computer Science* **New Haven, CT, US**

Ege University – *MSc in Information Technologies* **Bornova, Izmir, TR**

Dokuz Eylul University – *BSc in Computer Science & Industrial Engineering (Double Major)* **Bornova, Izmir, TR**

Work Experience

Amazon Web Services (AWS) **New York, NY, US**
Applied Scientist Intern, Automated Reasoning Group *May 2024 - Present*

- Working on neurosymbolic programming to capture symbolic knowledge and mitigate hallucinations of LLMs in logical reasoning.

Amazon Web Services (AWS) **New York, NY, US**
Applied Scientist Intern, Automated Reasoning Group *May 2023 - Jan. 2024*

- Developed a scheduler framework for randomized testing, model-based testing, and conformance checking of distributed AWS Services in **Rust** programming language. Deployed to the testing workflow of a distributed journal management system.

Amazon Web Services (AWS) **New York, NY, US**
Applied Scientist Intern, Automated Reasoning Group *Jun. 2022 - Jan. 2023*

- Developed a decision procedure in **Rust** programming language for checking linearizability and sequential consistency of distributed systems. Deployed the tool to S3's model-based testing workflows.

Yale University **New Haven, CT, US**
Research Assistant & Teaching Fellow *Sep. 2019 - Present*

- Conducted research on program security analysis for cryptographic **C** code and quantum computers using formal methods and machine learning. Developed a static leakage analysis tool for binaries and a probabilistic symbolic execution engine for **LLVM** IRs. Implemented a tool for automated inference of loop invariants and post conditions in **C/C++** programs
- Worked as Teaching Fellow for *CS423–Operating System* and *CS437–Database Systems* of Prof. Avi Silberschatz.

UNIT Information Technologies R&D Ltd. **Ege University, TR**
Co-founder & Software Engineer *Jan. 2015 - June 2019*

- Developed software engineering tools for *Airbus*, *Daimler*, and *Ford* in European R&D collaborations. Led the ITEA-ModelWriter project (see `https://itea3.org/project/modelwriter.html`) and coordinated a sub-consortium in the ITEA-Assume project (see `https://itea3.org/project/assume.html`). Mainly used **Java** and a formal specification language, **Alloy**.

Programming Languages

Programming: Rust, Python, C/C++, Java, Go, R, Dafny, Alloy **Others**: PyTorch, Scipy, Sympy, Scikit-learn, LLVM, Angr, KLEE

Project & Research Experience

Neurosymbolic Techniques for Abstraction and Reasoning Tasks **2024 - Present**

- Conducting research on discrete program search to automatically solve Abstraction and Reasoning Challenge (ARC) tasks by integrating neural-guided program synthesis with program compression techniques.

Reasoning about Legal Documents using Large Language Models (LLMs) & Theorem Provers **2024 - Present**

- Researching a neurosymbolic approach for logical reasoning of legal documents by combining LLMs with First-Order Logic (FOL) theorem provers, in collaboration with Yale Law School (Prof. Scott Shapiro).

Automated Specification Inference using Machine Learning (ML) & Formal Methods **2023 - 2024**

- Conducted research on the automated inference of nonlinear mixed-integer and real-valued relational properties from programs using machine learning. Applied these techniques to metamorphic property-based testing and formal verification. Explore the tool here: `https://bitween.fun`.

Side-Channel Insecurity of Cryptographic Code and Quantum Computer Security **2019 - 2022**

- Researched on verifying the side-channel insecurity of low-level Post-Quantum Cryptographic code (*EuroS&P 2023* [1]); worked on reverse engineering quantum circuits from power side-channel traces (*CHES 2024* [2], *CCS 2023* [3]); explored detection of quantum computer viruses (*HOST 2023* [4]); developed techniques to model and quantify non-functional behaviors of intermittent programs (*TECS 2023* [5]); surveyed security verification techniques (*JETC 2023* [6]).

Applied Research & Software Development in Aviation and Automative Sectors **2015 - 2019**

- Developed the open-source AlloyInEcore tool that automatically checks correctness of system models (*FSE 2018* [7]) (see `https://modelwriter.github.io/AlloyInEcore/`).
- Developed the open-source Tarski tool that formalizes relationships between sofware development artifacts (*FSE 2017* [8]) (see `https://modelwriter.github.io/Tarski/`).
- Leadership in the development of ModelWriter–Text & Model-Synchronized Document Engineering Platform (*ASE 2017* [9]) (see `https://itea3.org/project/modelwriter.html`).

Grants Awarded

NSF – U.S. National Science Foundation, Secure & Trustworthy Cyberspace Program **[Award Link]**
SaTC: Automatic Detection and Repair of Side Channel Vulnerabilities in Software Code *Jul. 2023 – Jun. 2026*

- Contributed to the proposal writing and partly working on the project as a PhD student. Award no: 2245344; amount: $600,000

EUREKA – EU. Information Technology for European Advancement (ITEA) **[Project Link]**
ASSUME: Affordable Safe & Secure Mobility Evolution *Sept. 2015 – Dec. 2018*

- R&D project with 38 partners from Canada, Germany, Portugal, Sweden, and Turkey, with ITEA project no. 17039.
- My start-up was awarded by TUBITAK Intl. Industrial R&D Projects Grant Programme. Project no: 9150181, amount: $250,000.

EUREKA – EU. Information Technology for European Advancement (ITEA) **[Project Link]**
ModelWriter: Text & Model-Synchronized Document Engineering Platform *Nov. 2015 – Nov. 2017*

- R&D project with with 9 partners from France and Turkey, with ITEA project no: 13028.
- My start-up was awarded by TUBITAK Intl. Industrial R&D Projects Grant Programme. Project no: 9140014, amount: $300,000.

Leadership and Awards

Yale University – *Full Scholarship for PhD* **Aug. 2019 - Aug. 2025**
Awarded a full scholarship for doctoral studies in Computer Science

Short-Term Scientific Missions – *European Cooperation in Science and Technology* **Jun. 2018 – Sep. 2018**

- University of Antwerp, Antwerp, Belgium: Full grant for a short-term scientific mission to visit Modelling, Simulation and Design lab (MSDL) `http://msdl.uantwerpen.be`.
- Chalmers University of Technology, Gothenburg, Sweden: Full grant to visit the Division of Formal Methods (`https://chalmersformalmethods.github.io/`).

Management Committee Member – *European Cooperation in Science and Technology* **2015 - 2019**

- Action IC1404 - Multi-Paradigm Modelling for Cyber-Physical Systems (MPM4CPS) (`https://www.cost.eu/actions/IC1404/`)
- Action IC1402 - Runtime Verification beyond Monitoring (ARVI) (`https://www.cost.eu/actions/IC1402/`)

Selected Publications

[1] **Ferhat Erata**, Ruzica Piskac, Victor Mateu, and Jakub Szefer. Towards automated detection of single-trace side-channel vulnerabilities in constant-time cryptographic code. In *IEEE European Symposium on Security and Privacy* (***EuroS&P***), 2023.

[2] **Ferhat Erata**, Chuanqi Xu, Ruzica Piskac, and Jakub Szefer. Quantum circuit reconstruction from power side-channel attacks on quantum computer controllers. *IACR Transactions on Cryptographic Hardware and Embedded Systems* (***TCHES***), 2024.

[3] Chuanqi Xu, **Ferhat Erata**, and Jakub Szefer. Exploration of power side-channel vulnerabilities in quantum computer controllers. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (***CCS***), 2023.

[4] Sanjay Deshpande, Chuanqi Xu, Theodoros Trochatos, Hanrui Wang, **Ferhat Erata**, Song Han, Yongshan Ding, and Jakub Szefer. Design of quantum computer antivirus. In *International Symposium on Hardware Oriented Security and Trust* (***HOST***), 2023.

[5] **Ferhat Erata**, Eren Yildiz, Arda Goknil, Kasim Sinan Yildirim, Jakub Szefer, Ruzica Piskac, and Gokcin Sezgin. Etap: Energy-aware timing analysis of intermittent programs. *ACM Transactions on Embedded Computing Systems* (***TECS***), 2023.

[6] **Ferhat Erata**, Shuwen Deng, Faisal Zaghloul, Wenjie Xiong, Onur Demir, and Jakub Szefer. Survey of approaches and techniques for security verification of computer systems. *ACM Journal on Emerging Technologies in Computing Systems* (***JETC***), 2023.

[7] **Ferhat Erata**, Arda Goknil, Ivan Kurtev, and Bedir Tekinerdogan. AlloyInEcore: embedding of first-order relational logic into meta-object facility. In *Proceedings of the Symposium on the Foundations of Software Engineering* (***ESEC/FSE***), 2018.

[8] **Ferhat Erata**, Arda Goknil, Bedir Tekinerdogan, and Geylani Kardas. A tool for automated reasoning about traces based on configurable formal semantics. In *Proceedings of the Foundations of Software Engineering* (***ESEC/FSE***), 2017.

[9] **Ferhat Erata**, Claire Gardent, Bikash Gyawali, Anastasia Shimorina, Yvan Lussaud, Bedir Tekinerdogan, Geylani Kardas, and Anne Monceaux. ModelWriter: Text and model-synchronized document engineering platform. In *Proceedings of the Automated Software Engineering* (***ASE***), 2017.