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 - Apr. 2025 (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 2023 - Present*

- Developed a scheduler framework for randomized testing, model-based testing, and conformance checking of distributed AWS Services in **Rust** programming language. *Mentor*: Prof. Rupak Majumdar

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 languages for checking linearizability of distributed systems.

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

- Researched on program security analysis for cryptographic **C/C++** code using formal methods and machine learning.
- Worked as Teaching Fellow to help design and lead lab sessions, hold office hours and proctor exams for *CS423–Principles of Operating System* and *CS437–Database Systems* of Prof. Avi Silberschatz, and *CS440–Advanced Databases* of Prof. Robert Soule.

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

- Applied formal methods to both software and system engineering in several international R&D collaborations in Europe. I 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`). I mainly used **Java** and formal languages such as **Alloy**.

Programming Languages

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

Project & Research Experience

Fast Specification Inference for Property-based Testing and Formal Verification **2023 - Present**

- Researching on the automated inference of nonlinear real-valued relational properties, such as equalities, inequalities, random self-reducible properties from programs for security verification and property-based testing. This work, which is currently under review for conference submissions, involves the integration of *machine learning* with *formal techniques*.

Side-Channel Insecurity of Cryptographic Code and Quantum Computer Security **2020 - 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 of quantum computer controllers (*CHES 2024* [2], *CCS 2023* [3]); explored modeling and quantifying non-functional behaviors of intermittent programs (*TECS 2023* [4]); contributed to techniques that detect quantum computer virus (*HOST 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: CORE: 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

EU EUREKA – 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.

EU EUREKA – 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.

Fellowships and Scholarships

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

European Cooperation in Science and Technology – *Short-Term Scientific Mission Grants* **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/`).

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] **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.

[5] 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.

[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.

Professional Service

Management Committee Member **2015 - 2019**
European Cooperation in Science and Technology (COST)

- 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/`)

Program Committee Member **2019 - 2023**

- Computer Aided Verification (CAV 2023)—Artifact Evaluation
- Verification, Model Checking, and Abstract Interpretation (VMCAI 2023)—Artifact Evaluation
- Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2024)—Artifact Evaluation
- International Workshop on Multi-Paradigm Modelling for Cyber-Physical Systems (MPM4CPS)

Journal Reviewer **2022 - 2023**

- Journal of Automated Reasoning
- IEEE Computer Architecture Letters