

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 <i>Advisors: Prof. Ruzica Piskac, Prof. Jakub Szefer</i> | New Haven, CT, US 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) <i>Applied Scientist Intern, Automated Reasoning Group</i> ○ Developed a scheduler framework for randomized testing, model-based testing, and conformance checking of distributed AWS Services in Rust programming language. <i>Mentor: Prof. Rupak Majumdar</i> | New York, NY, US May 2023 – Present |
| Amazon Web Services (AWS) <i>Applied Scientist Intern, Automated Reasoning Group</i> ○ Developed a decision procedure in Rust programming languages for checking linearizability of distributed systems. | New York, NY, US Jun. 2022 – Jan. 2023 |
| Yale University <i>Research Assistant & Teaching Fellow</i> ○ 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. | New Haven, CT, US Sep. 2019 – Present |
| UNIT Information Technologies R&D Ltd. <i>Co-founder & Software Research Engineer</i> ○ 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 . | Ege University, TR Jan. 2015 – June 2019 |

Programming Languages

Programming: Rust, C/C++, Go, Python, Java, R, Dafny, Alloy **Others:** PyTorch, Numpy, TensorFlow, Assembly, Angr, KLEE

Project & Research Experience

| | |
|---|-----------------------|
| Fast Specification Inference for Property-based Testing and Formal Verification ○ 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 <i>machine learning</i> with <i>formal techniques</i> . | 2023 – Present |
| Side-Channel Insecurity Research of Cryptographic Code and Quantum Computer Architectures ○ Researched on verifying the side-channel insecurity of low-level Post-Quantum Cryptographic code (<i>EuroS&P</i> 2023 [1]); worked on reverse engineering quantum circuits from power side-channel traces of quantum computer controllers (<i>CHES</i> 2024 [2], <i>CCS</i> 2023 [3]); explored modeling and quantifying non-functional behaviors of intermittent programs (<i>TECS</i> 2023 [4]); contributed to techniques that detect quantum computer virus (<i>HOST</i> 2023 [5]); injects malicious faults (<i>DAC</i> 2024 [6]); and surveyed security verification techniques (<i>JETC</i> 2023 [7]). | 2020 – 2022 |
| Applied Research & Software Development in Aviation and Automotive Sectors ○ Contributed to a static analysis toolchain (<i>COMPSAC</i> 2019 [8]); developed AlloyInEcore tool for automated analysis of system design models (<i>FSE</i> 2018 [9]); developed the Tarski tool for automated analysis of traceability (<i>FSE</i> 2017 [10]); led the development of ModelWriter–Text and model-synchronization engineering platform (<i>ASE</i> 2017 [11]). | 2015 – 2019 |

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 *2023 IEEE 8th 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] Chuanqi Xu, **Ferhat Erata**, and Jakub Szefer. Classification of quantum computer fault injection attacks. In *61st Design Automation Conference (DAC)*, 2024. (under review).
- [7] **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.
- [8] Matthias Kern, **Ferhat Erata**, Markus Iser, Carsten Sinz, Frederic Loiret, Stefan Otten, and Eric Sax. Integrating static code analysis toolchains. In *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, 2019.
- [9] **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.
- [10] **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.
- [11] **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

Grants Awarded Prior to PhD

EU EUREKA – Information Technology for European Advancement (ITEA)

[Project Link]

ASSUME: Affordable Safe & Secure Mobility Evolution

01.09.2015–31.12.2018

- 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 International Industrial R&D Projects Grant Programme, project no. 9150181, with a grant of approximately \$250,000.

EU EUREKA – Information Technology for European Advancement (ITEA)

[Project Link]

ModelWriter: Text & Model-Synchronized Document Engineering Platform

01.10.2015–01.10.2017

- R&D project with with 9 partners from France and Turkey, with ITEA project no: 13028.
- My start-up was awarded by TUBITAK International Industrial R&D Projects Grant Programme, project no: 9140014, with a grant of approximately \$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/>).