Ferhat Erata

Neuro-Symbolic AI, AI4Code, Automated Reasoning, and Security & Privacy
(203) 833 9448 • ferhat.erata@yale.edu • ferhat.ai • ferhaterata
New Haven – CT 06511

Education

Yale University – PhD in Computer Science — **New Haven, CT, US**
Advisors: Prof. Ruzica Piskac, Prof. Jakub Szefer — *Graduation Date: 05/25*

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

AWS AI – Automated Reasoning Group — **New York, NY, US**
Applied Scientist Intern — *May 2024 - Dec. 2024*

- Working on Neuro-Symbolic AI to capture symbolic knowledge and prevent factual errors caused by LLM hallucinations using mathematically sound Automated Reasoning checks (see Amazon Bedrock Guardrails). Co-inventor, along with Rémi Delmas, of a **US Patent** filed on mitigating LLM hallucinations.

AWS – Automated Reasoning Group — **New York, NY, US**
Applied Scientist Intern — *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.

AWS – Automated Reasoning Group — **New York, NY, US**
Applied Scientist Intern — *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*

- Applied ML and AI techniques to program analysis and security: conducted research on program security analysis for cryptographic C code and quantum computers. Developed a static leakage analysis tool for binaries and a probabilistic symbolic execution engine for LLVM. Implemented a tool for automated inference of program properties in C/C++ programs.
- Worked as Teaching Fellow for *CS423–Operating System* and *CS437–Database Systems* of Prof. Avi Silberschatz.

UNIT Research & Development Ltd. — **Ege University, TR**
Co-founder & Software Engineer — *Jan. 2014 - June 2019*

- Developed software engineering tools for *Airbus*, *Daimler*, and *Ford* in European R&D collaborations. Led the *ModelWriter: Text & Model-Synchronized Document Engineering Platform* project (see `https://itea3.org/project/modelwriter.html`) and coordinated a sub-consortium in the *Assume: Safe & Secure Mobility Evolution* project (see `https://itea3.org/project/assume.html`) and *XIVT: eXcellence In Variant Testing* (see `https://itea3.org/project/xivt.html`). Mainly used Java, C++ and symbolic AI techniques such as finite model finding with Alloy and SAT/SMT solving.

Programming Languages

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

Project & Research Experience

Legal Reasoning using Large Language Models (LLMs) and Theorem Provers — **2024 - Present**

- Researching a Neuro-Symbolic AI 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).

Learning Randomized Reductions and Program Properties — **2023 - Present**

- Introduced a machine learning technique for learning randomized reductions and program invariants. This work is currently under review for (arXiv 2024 [1]). Developed a C language wrapper at `https://bitween.fun`. Applied these techniques to hardware security, private computation, and privacy-preserving machine learning (PPML) (arXiv 2025 [2]).

Side-Channel Insecurity of Cryptographic Code and Quantum Computer Security — **2019 - 2023**

- Researched on verifying the side-channel insecurity of low-level Post-Quantum Cryptographic code (EuroS&P 2023 [3]); worked on reverse engineering quantum circuits from power side-channel traces (CHES 2024 [4], CCS 2023 [5]); developed software countermeasure against physical attacks (ICCAD 2025 [6]); developed techniques to model and quantify non-functional behaviors of intermittent programs (TECS 2023 [7]); surveyed security verification techniques (JETC 2023 [8]).

Applied Research & Software Development in Aviation and Automotive Sectors **2014 - 2019**

- Developed the open-source AlloyInEcore tool that automatically checks correctness of system models (FSE 2018 [9]) (see https://modelwriter.github.io/AlloyInEcore/).
- Developed the open-source Tarski tool that formalizes relationships between software development artifacts (FSE 2017 [10]) (see https://modelwriter.github.io/Tarski/).
- Leadership in the development of ModelWriter–Text & Model-Synchronized Document Engineering Platform (ASE 2017 [11]) (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*

- 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*

- 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, Belgium: Full grant for a short-term scientific mission to visit Modeling, Simulation and Design lab.
- Chalmers University of Technology, Gothenburg, Sweden: Full grant to visit the Division of Formal Methods.

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**, Orr Paradise, Timos Antonopoulos, ThanhVu Nguyen, Shafi Goldwasser, and Ruzica Piskac. Learning randomized reductions and program properties, 2024. (*under review*).

[2] **Ferhat Erata**, Theodoros Trochatos, Barbora Hrda, Yizhuo Tan, and Jakub Szefer. Learning randomized self-reductions for quantum circuit protection. (*under review*).

[3] **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.

[4] **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.

[5] 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.

[6] **Ferhat Erata**, TingHung Chiu, Anthony Etim, Srilalith Nampally, Tejas Raju, Rajashree Ramu, Ruzica Piskac, Timos Antonopoulos, Wenjie Xiong, and Jakub Szefer. Systematic use of random self-reducibility in cryptographic code against physical attacks. In *IEEE/ACM International Conference on Computer-Aided Design* (***ICCAD***), 2024.

[7] **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.

[8] **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.

[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.