Ferhat Yaman

Email: fyaman.dev@gmail.com **Website:** https://ferhatyaman.github.io/

RESEARCH INTERESTS

Hardware Security, Post-Quantum Cryptography, Side-Channel Analysis
Privacy-Preserving Machine Learning, Homomorphic Encryption

EDUCATION

North Carolina State University, Raleigh, NC **Jan 2021 – Aug 2023**

M.Sc. in Computer Engineering

- Advisors: Prof. Samira Mirbagher Ajorpaz, Prof. Aydin Aysu
- **Thesis:** Agent SCA: Advanced Physical Side Channel Analysis Agent with LLMs
- **GPA:** 3.55/4.00, *Summa Cum Laude*

Sabanci University, Istanbul, Turkey **Sep 2014 – May 2020**

B.Sc. in Computer Science and Engineering
B.Sc. in Electronics Engineering
Minor in Neuroscience

- Advisors: Prof. Erkay Savas, Prof. Albert Levi
- **Thesis:** Intrusion Detection Systems with Machine Learning for IoT Devices
- **GPA:** 3.62/4.00, *Summa Cum Laude*

WORK EXPERIENCE

AMD **May 2022 – Present**

Hardware Security Engineer – Product Security Research Team (PSO RD)

- Conducted in-depth evaluations of **Post-Quantum Cryptography (PQC)** algorithms, ensuring optimal efficiency and robustness for next-generation cryptographic systems.
- Architected secure computation frameworks for **machine learning (ML) and artificial intelligence (AI)** on **GPUs**, including the design of a **homomorphic encryption compiler to protect sensitive AI operations.**
- Strengthened the security architecture of **AMD's Secure Encrypted Virtualization and Trusted Execution Environment**, mitigating potential vulnerabilities and enhancing system integrity.
- Designed and implemented test environments to validate **Secure Memory Encryption** and cryptographic components for **system-on-chip (SoC)** platforms, contributing to **FIPS certification** readiness.
- Enhanced the resilience of **cryptographic coprocessors against side-channel attacks (SCA)** by developing advanced models using ChipWhisperer Python libraries and creating **custom SCA models using Riscure Inspector**, driving innovative approaches to secure cryptographic processors and mitigate emerging threats.

Accenture **Jun 2019 – Jul 2019**

Software Engineering Intern

- Contributed to the development of a human resources automation system, streamlining routine HR tasks and enhancing operational efficiency.
- Designed and implemented **RESTful APIs for backend services**, enabling seamless data exchange and improving system functionality. Integrated event-driven and **time-triggered serverless applications** into a microservices architecture, leveraging Microsoft Azure to ensure scalability and reliability.

Vingd **Jan 2019 – Feb 2019**

AI Software Engineering Intern

- Designed and implemented a rule-based security AI bot using Bayesian Networks in Java, and deployed the solution in a containerized environment using Docker for scalability and reliability.

Multinet inventiv **Jul 2018 – Jan 2019**

Software Engineer

- Developed a Fraud Detection and Prevention System leveraging **outlier detection machine learning models** to identify anomalies in large-scale payment datasets using **Weka**.
- Designed and implemented database schemas using **Java Hibernate and Spring Framework**, enabling efficient data management and integration with **backend services.**
- Built and tested **RESTful APIs for machine learning model deployment** and system functionality, ensuring high reliability through **JUnit-based validation.**

RESEARCH EXPERIENCE

Hardware Cyber Threat Research Lab, NC State University **Jan 2021 – July 2022**

Advisor: Dr. Aydin Aysu

- Conducted side-channel analysis (SCA) on deep learning accelerators for edge devices, leveraging the Python TensorFlow framework to uncover vulnerabilities.
- Designed and implemented attack vectors targeting Tensor Processing Units using Riscure Inspector, enhancing the understanding of potential security flaws.
- Optimized solvers for lattice-based cryptography problems, including NP-hard challenges like the Shortest Vector Problem (SVP) and Learning with Errors (LWE), contributing to advancements in PQC

Computer and Information Security Lab, Sabanci University **Sept 2019 – Jan 2021**

Advisors: Prof. Erkay Savas, Prof. Albert Levi

- Optimized **Homomorphic Encryption (HE)** and **Post-Quantum Cryptography** schemes, contributing to advancements in secure computing.
- Developed Python simulations for **prototyped FPGA designs**, enhancing performance and efficiency.
- Built **privacy-preserving machine learning applications** using HE in a Python-based DNN framework.
- Implemented a **secure inference system combining homomorphic encryption and machine learning**, securing a top-5 finish in the **IDASH'20** competition.
- Applied machine learning models to network traffic data for **intrusion detection**, improving security in IoT.

Institute for Infocomm Research, A-STAR **July 2019 – Sept 2019**

Advisors: Dr. Chao Jin, Dr. Ahmad Al Badawi

- Developed and implemented privacy-preserving protocols for Deep Learning models, enhancing data security and model performance.
- Leveraged expertise in Multiparty Computing Security (Homomorphic Encryption, Garbled Circuits) to optimize CNN models, reducing resource usage while maintaining efficiency and security.

Secure Systems Lab, Boston University **July 2017 – Sept 2017**

Advisors: Dr. Manuel Egele

- Conducted research and analysis to identify and mitigate potential security vulnerabilities in digital platforms.
- Analyzed Twitter data for homoglyph character vulnerabilities using Python, identifying potential risks in user interactions. Developed a scalable web scraper system utilizing a 30-node cluster and RabbitMQ

PUBLICATIONS

1. **Yaman, F.**, Mert, A.C., Ozturk, E., Savas E., **"A Hardware Accelerator for Polynomial Multiplication Operation of CRYSTALS-KYBER PQC Scheme"** Design, Automation & Test in Europe Conference & Exhibition *(DATE'21)*
2. Kurian, A., Dubey, A., **Yaman, F.**, Aysu, A. "**TPUXtract: An Exhaustive Hyperparameter Extraction Framework**". IACR Transactions on Cryptographic Hardware and Embedded Systems, *(CHES 2025)*
3. Magara, S.S., Yildirim, C., **Yaman, F.**, Dilekoğlu B., Tutas, F.R., Ozturk, E., Kaya, K., Taştan, O., and E Savas, E., **"ML with HE: Privacy Preserving Machine Learning Inferences for Genome Studies"**. ACM Computer and Communications Security, CCS'21, PPML Workshop
4. Calhoun, A., Ortega, E., **Yaman, F.**, Dubey A., Aysu, A., **"Hands-On Teaching of Hardware Security for Machine Learning"** Proceedings of the Great Lakes Symposium on VLSI, *(ACM GLS-VLSI 2022)*
5. Mert, A.C., **Yaman, F.**, Karabulut, E., Ozturk, E., Savas, E., Aysu, A., **"A Survey of Software Implementations for the Number Theoretic Transform"** SAMOS 2023 International Conference on Embedded Computer Systems

SKILLS

- **Programming Languages:** Python, C / C++, C#, Verilog, Assembly, MATLAB, Java, Unix, SQL
- **Frameworks**:, TensorFlow, PyTorch, Keras, Spring, Hibernate, JUnit
- **Development:** Git, Docker, Perforce, ARM DS5, KVM
- **Security & Analysis**: Riscure SCA, ChipWhisperer, Lascar, eShard, Kali Tools
- **CAD Tools**: Xilinx ISE, Vivado Design Suite

COURSEWORK

North Carolina State University, Raleigh, NC

- Cryptographic Eng. and Hardware Security, Operating Systems, Secure Microprocessor Architecture Design

Sabanci University, Istanbul, Turkey

- Cryptography, Computer Networks and Security, Machine Learning, Digital and Logic System Design

TEACHING EXPERIENCE

North Carolina State University, Raleigh, NC

TA for Cryptographic Engineering and Hardware Security (ECE-592) **Aug 2021 – Dec 2021**

- Instructor: Dr. Aydin Aysu
- Designed and evaluated research projects, graded reports, presentations, homeworks, and held office hours.

TA for Computer Engineering (ECE-290) **Jan 2021 – May 2022**

- Instructor: Prof. Greg Byrd
- Held weekly office hours and helped students to overcome their problems on programming concepts.

Sabanci University, Istanbul, Turkey

TA for Logic and Digital System Design (CS 303, EE 310) **Sept 2018 – May 2020**

- Instructor: Prof. Erkay Savas, Prof. Ilker Hamzaoglu
- Guided students in creating digital systems on FPGA boards and led labs on logic design and Verilog HDL.

TA for Advanced Programming with C++ (CS-201, CS204) **Oct 2016 – Jun 2017**

- Instructor: Prof. Kamer Kaya, Prof. Albert Levi
- Assisted students in developing C++ projects on topics like Classes, Linked Lists, Queues, Heaps, and Trees. Held office hours to support homework, exams, and problem-solving in Object-Oriented Programming (Inheritance, Encapsulation, Polymorphism).