# Ferhat Yaman

www.linkedin.com/in/ferhatyaman/

fyaman@ncsu.edu

Website: ferhatyaman.github.io
Phone: +1(919)3481090

## EDUCATION

**North Carolina State University**, Raleigh, NC — Jan. 2021 – Dec 2022(Exp.)
M.S. Computer Engineering, HECTOR Lab, Advisor: Dr. Aydin Aysu
**Coursework:** Cryptographic Eng. and Hardware Security, Compiler Design, Microprocessor Architecture, Operating Systems

**Sabanci University**, Istanbul, Turkey — Sept. 2014 – Jun. 2020
B.S. Computer Science, Double Major in B.Eng. Electronic Engineering, Minor in Psychology, 2020 (**GPA: 3.61**)
**Coursework:** Cryptography, Computer Networks and Security, Machine Learning, Digital and Logic System Design

**Hong Kong University of Science and Technology**, Hong Kong — Jan. 2018 - Jun. 2018
Exchange Student on Electronic Engineering and Computer Science, 2018

## WORK EXPERIENCES

*AMD – Hardware Security Intern* — May 2022 - Present
- Working on **side-channel analysis** of Crypto Coprocessors and **mitigation techniques such as masking**

*NC State University, HECTOR Lab – Hardware Security Researcher / Advisor: Dr. Aydin Aysu* — Jan 2021 - Present
- Working on **side-channel analysis** on deep learning accelerators on edge devices
- Working on solver for lattice crypto NP-Hard problems such as **shortest vector problem (SVP), learning with error (LWE)**

*Sabanci University, CISEC Lab – Hardware Security Researcher / Advisor: Dr. Erkay Savas* — March 2020 – Jan 2021
- Worked on optimizations of **Homomorphic Encryption (HE)** and **Post-Quantum Cryptography** schemes
- Worked on privacy-preserving machine learning algorithms by using HE

*A-STAR, Institute for Infocomm Research – Security Research Intern* — July 2019 – Sept. 2019
- Worked on implementation of privacy preserving protocols on Deep Learning and improvement of those protocols
- Applied knowledge of **Multiparty Computing Security** (HE, GC) to CNN models with using less resources

*Accenture – Software Engineering Intern* — June 2019 – July 2019
- Implemented RESTful APIs at backend of product and integrated event and time triggered serverless applications

*Multinet Inventiv - Software Engineering Intern* — July 2018 – Jan. 2019
- Worked on Fraud Detection and Prevention System which uses microservices and machine learning to identify fraud
- Implemented REST microservices (Spring), unit and integration tests (Junit) and designed MSSQL database, front-end web application using Primefaces on java environment

## PROJECTS

*Differential Power Analysis of Deep Neural Networks - Advisor: Dr. Aydin Aysu* — Feb. 2021 – Present
- Conducting DPA on real deep learning accelerators and trying to recover secret parameters

*Secure Tumor Classification using Homomorphic Encryption - Advisor: Prof. Erkay Savas* — Oct. 2020 – Nov. 2020
- Implemented an inference by using homomorphic enc. and machine learning algorithms. **Placed 5th in IDASH20 competition**

*Intrusion Detection System on IoT Devices - Bachelor's Thesis* — Sept. 2018 – Sept. 2019
- Implemented Machine Learning models on network traffic data to identify intrusions with *Prof. Albert Levi*
- Created different network traffics for different scenarios using 6-LoWPAN, RPL protocols and implemented different attacks

## PUBLICATIONS

1. **F Yaman,** AC Mert, E Ozturk, E Savas . "A hardware accelerator for polynomial multiplication operation of CRYSTALS-KYBER PQC scheme". Design, Automation & Test in Europe Conference & Exhibition *(DATE). 2021*
2. ŞS Mağara, C Yıldırım, **F Yaman,** B Dilekoğlu, FR Tutaş, E Öztürk, K Kaya, Ö Taştan, and E Savaş. **"ML with HE: Privacy Preserving Machine Learning Inferences for Genome Studies"**. *ACM CCS 2021* Privacy Preserving Machine Learning Workshop. 2021

## HONOR AND AWARDS

**Graduate Merit Award and Graduate Student Support Plan –** *NC State University* — Apr. 2020
**Singapore International Pre-Graduate Award (SIPGA) –** *A-STAR* — May. 2019

## SKILLS

**Proficient in** C++, Python, Unix, Java, Verilog HDL, C#
**Familiar with** JavaScript, HTML, CSS, SQL

**Technologies:** Git, Riscure SCA, TensorFlow, Keras, Spring, Hibernate, Docker, TDD, Kali Tools