Dina G. Mahmoud

Computer Science PhD Candidate

Computer and Communication Sciences EPFL
PARSA INJ 234 Station 14 CH-1015 Lausanne
(+41) 767080082, (+20) 1001002289
dina.mahmoud@epfl.ch
My Webpage
Linkedin
Google Scholar

Research Interests

I am broadly interested in the heterogeneous computing systems fueling the advances in cloud and embedded computing. These heterogeneous systems provide great opportunities for high-performance power-optimized computing. Security, at all levels, including the hardware and the electrical levels, is essential to ensure efficient systems that guarantee the protection of sensitive data. I, therefore, strive to consider the various architectural aspects and security implications in my research on heterogeneous systems. My work so far has focused on the possibility of electrical-level fault injection in systems incorporating field-programmable gate arrays (FPGAs) and considering the potential multitenancy consistent with cloud computing paradigms. I have investigated the potential for the malicious use of the programmable logic of FPGAs and demonstrated the first FPGA-to-CPU fault-injection exploit.

Education

2019 – present **PhD candidate, Computer & Communication Sciences**, *Ecole Polytechnique Fédérale de Lausanne (EPFL)*, Switzerland.
Thesis: Electrical-Level Fault-Injection Attacks on Heterogeneous FPGA-CPU Systems
Advisors: Dr. Mirjana Stojilović and Prof. Babak Falsafi

2014 – 2019 **Bachelor of Science, Electronics & Communications Engineering**, *The American University in Cairo (AUC)*, Egypt.
GPA: 3.989/4.0 (Dean's Honors List)
Minor: Mathematics
Thesis: Intelligent Battery-Aware Energy Management System for Electric Vehicles
Advisor: Prof. Hassanein Amer

Fellowships & Awards

2020 – present First recipient of the ***Cyber-Defense Campus Doctoral Fellowship*** from armasuisse Science and Technology, fellowship mentor: Dr. Vincent Lenders.

2022 Recipient of the ***Google Generation Scholarship*** for the EMEA region.

2019 Recipient of the ***EDIC Fellowship*** for the first year of doctoral studies at EPFL.

2019 Awarded the ***Zewail Prize for Best Original Essay on a Multidisciplinary Topic***, AUC.

2014 – 2019 Awarded the ***Academic Achievement Scholarship*** for the top admitted students at AUC.

2018 Obtained the ***Highest GPA in the Senior Electronics and Communications Engineering Class***, AUC.

2017 – 2018 ***Outstanding Academic Achievers' Honors Assembly***, AUC.

Employment

2019 – present **Doctoral assistant**, *EPFL*, Switzerland.
Research on electrical-level fault-injection attacks on heterogeneous FPGA-CPU systems (Project link)

- Showed the possibility of leveraging the power consumption of ring oscillators to **remotely inject controlled timing faults** in a multitenant FPGA.
- Demonstrated and evaluated **X-attack**, an exploit combining remote timing faults injection with stealthy hardware Trojans.
- Highlighted the **electrical-level security risks of FPGA-CPU systems** by demonstrating the first fault-injection exploit enabled by an FPGA against a CPU on the same chip.

February – August, 2019 **Research assistant**, *AUC*, Egypt.

- Assisted in research on reliability of FPGA-based systems for machine learning and space applications.
- Mentored students working on their graduation projects.

June – August, 2018 **Summer@EPFL intern**, *EPFL*, Switzerland.
Research on secure FPGAs in the cloud

- Accepted to the Summer Research program (acceptance rate in 2018 was 1.9%).
- Published a research paper showing the feasibility of a fault attack using power waster circuits on Xilinx FPGA, paving the way for more research in the area.

July – August, 2017 **Intern**, *Electrical Systems Engineering Company (ESEC)*, Egypt.
Responsible for troubleshooting and repairing devices (digital low resistance ohmmeters and power analyzers) by interpreting circuits' diagrams and tracing faults using multimeters.

July 2017 **Trainee**, *Engineering for the Petroleum and Process Industries (ENPPI)*, Egypt.
Trained in the Instrumentation Engineering and Telecommunications Systems departments.

Publications

Peer-Reviewed In Conference Proceedings

2022 **Dina G. Mahmoud**, Samah Hussein, Vincent Lenders, and Mirjana Stojilović. FPGA-to-CPU Undervolting Attacks. In *DATE*, March 2022.

2021 **Dina G. Mahmoud**, Beatrice Shokry, Abdallah ElRefaey, Hassanein H. Amer, and Ihab Adly. Runtime Replacement of Machine Learning Modules in FPGA-Based Systems. In *MECO*, June 2021.

2021 Ognjen Glamočanin, **Dina G. Mahmoud**, Francesco Regazzoni, and Mirjana Stojilović. Shared FPGAs and the Holy Grail: Protections against Side-Channel and Fault Attacks. In *DATE*, February 2021.

2020 **Dina G. Mahmoud**, Wei Hu, and Mirjana Stojilović. X-Attack: Remote Activation of Satisfiability Don't-Care Hardware Trojans on Shared FPGAs. In *FPL*, August 2020.

2020 Beatrice Shokry, **Dina G. Mahmoud**, Hassanein H. Amer, Maha Shatta, Gehad I. Alkady, Ramez M. Daoud, Ihab Adly, Manar N. Shaker, and Tarek Refaat. Work-in-Progress: Triple Event Upset Tolerant Area-Efficient FPGA-Based System for Space Applications And Nuclear Plants. In *WFCS*, April 2020.

2019 **Dina Mahmoud** and Mirjana Stojilović. Timing Violation Induced Faults in Multi-Tenant FPGAs. In *DATE*. IEEE, March 2019.

2019 **Dina G. Mahmoud**, Omar A. Elkhouly, Muhammad Azzazy, Gehad I. Alkady, Ihab Adly, Ramez M. Daoud, Hassanein H. Amer, Hany ElSayed, Mark Guirguis, and Mohamed Gamal Abdelshafi. Intelligent Battery-Aware Energy Management System for Electric Vehicles. In *ETFA*, September 2019.

2019 Mahmoud Rumman, **Dina G. Mahmoud**, Ihab Adly, Hassanein H. Amer, Gehad I. Alkady, and Hany ElSayed. Reliable On-Chip Memory for FPGA-Based Systems. In *ICM*, December 2019.

2019 Mina G. Labib, **Dina G. Mahmoud**, Gehad I. Alkady, Ihab Adly, Hassanein H. Amer, Ramez M. Daoud, and Hany M. ElSayed. Heterogeneous Redundancy for PCB Track Failures: An Automotive Example. In *International Conference on Computer Engineering and Systems (ICCES)*, December 2019.

2019 Michael Hanna, Habiba T. Abdelhamid, Kirollos N. Sorour, I. ElAraby, Salma Mahfouz, Yasmeen S. Okasha, **Dina G. Mahmoud**, Gehad I. Alkady, Ramez M. Daoud, Hassanein H. Amer, Hany ElSayed, and Ihab Adly. Smart FPGA-based System for Enhancing Educational Programs. In *Novel Intelligent and Leading Emerging Sciences Conference (NILES)*, October 2019.

2019 Abdallah Gabara, Ramez M. Daoud, Hassanein H. Amer, **Dina G. Mahmoud**, and Hany ElSayed. Fault-Tolerant High-Rate Ethernet-Based Networked Control System. In *Novel Intelligent and Leading Emerging Sciences Conference (NILES)*, October 2019.

2019 Gehad I. Alkady, **Dina G. Mahmoud**, Ramez M. Daoud, Hassanein H. Amer, Manar N. Shaker, Hany M. ElSayed, Magdy S. ElSoudani, Ihab Adly, and Betim Cico. Reliable FPGA-Based Network Architecture for Smart Cities. In *ICM*, December 2019.

2018 **Dina G. Mahmoud**, Gehad I. Alkady, Hassanein H. Amer, Ramez M. Daoud, Ihab Adly, Youssef Essam, Hassan A. Ismail, and Kirollos N. Sorour. Fault Secure FPGA-based TMR Voter. In *MECO*, June 2018.

2017 Malak Y. ElSalamouny, Gehad I. Alkady, Ihab Adly, Ramez M. Daoud, Hassanein H. Amer, Hany ElSayed, **Dina G. Mahmoud**, Hassan A. Ismail, and Hassan H. Halawa. Highly Available FPGA-Based Smart Band for WBAN. In *International Conference on Computer Engineering and Systems (ICCES)*, December 2017.

Peer-Reviewed Journal Articles

2022 **Dina G. Mahmoud**, Vincent Lenders, and Mirjana Stojilović. Electrical-level Attacks on CPUs, FPGAs, and GPUs: Survey and Implications in the Heterogeneous Era. *ACM Computing Surveys*, volume 55, February 2022.

2022 **Dina G. Mahmoud**, David Dervishi, Samah Hussein, Vincent Lenders, and Mirjana Stojilović. DFAulted: Analyzing and Exploiting CPU Software Faults Caused by FPGA-Driven Undervolting Attacks. *IEEE Access*, volume 10, December 2022.

Invited Book Chapters

2023 **Dina Mahmoud**, *Hardware Acceleration*, Trends in Data Protection and Encryption Technologies, V. Mulder, A. Mermoud, V. Lenders, and B. Tellenbach, Eds., Springer Nature Switzerland, pp. 109–11.

2023 **Dina G. Mahmoud**, Ognjen Glamočanin, Francesco Regazzoni, and Mirjana Stojilović, *Practical Implementations of Remote Power Side-Channel and Fault-Injection Attacks on Multitenant FPGAs*, Security of FPGA-Accelerated Cloud Computing Environments, Springer, Forthcoming.

Invited Talks

2023 **X-attack: Remote Activation of SDC Hardware Trojans on Shared Cloud FPGAs** at the CyberAlp Retreat.

2022 **FPGA-to-CPU Undervolting Attacks** at the CyberAlp Retreat.

2022 **FPGA-to-CPU Undervolting Attacks** at the Design, Automation and Test in Europe Conference (conference presentation).

2022 **Remote FPGA-Based Undervolting Attacks** at the Workshop on Security for Custom Computing Machines - IEEE International Symposium on Field-Programmable Custom Computing Machines.

2021 **Attacks and Defenses on FPGA-CPU-GPU Heterogeneous systems** at the CyberAlp Retreat.

2020 **X-Attack: Remote Activation of Satisfiability Don't-Care Hardware Trojans on Shared FPGAs** at the International Conference on Field-Programmable Logic and Applications (FPL) (conference presentation).

Student Supervision

2023 David Dervishi (MSc Thesis).
Supervising David's work on his ongoing MSc thesis targeting the security of cloud FPGAs.

2023 Simone Andreani (BSc Semester Project).
Supervising Simone's work on a project to explore the power consumption of various power-wasting circuits proposed for remote attacks on cloud FPGAs.

2022 Beatrice Shokry (Summer@EPFL intern).
Supervised Beatrice's work on two projects. The first targeted exploring the vulnerability of cloud-based platforms to power-wasting circuits. Her work on the first project resulted in a publication currently under review. The second project continued exploring the clock networks of FPGAs.

2022 David Dervishi (MSc Semester project at EPFL).
Supervised David's work on systematically using dynamic voltage frequency scaling interfaces to map the reaction of baremetal and Linux-based applications on an ARM CPU. This work served as the baseline against which to compare FPGA-to-CPU undervolting attacks and resulted in a peer-reviewed publication.

2022 Pierre Colson (MSc Semester project at EPFL).
Supervised Pierre's work on exploring the clock network of a Zynq-based FPGA platform.

2021 Samah Hussein (Summer@EPFL intern).
Supervised Samah's work on a project exploring the possibility of injecting faults into CPU computation leveraging the power consumption of FPGA circuits on the same chip. This work demonstrated the possibility of such an attack and identified the parameters affecting the attack success. The work was the foundation of two peer-reviewed publications.

Teaching Experience

Fall 2023 **Computer Architecture (Bachelor's)**, *EPFL*, Instructor: Prof. Farshad Khun Jush.
Responsible for adapting the material of previous course to the new course in its first offering.
Guiding students (300+) through weekly labs and programming exercises in VHDL and NIOS assembly.
Overseeing the preparation of the lab materials and the automatic grading system.

Fall 2022 **Computer Architecture I (Bachelor's)**, *EPFL*, Instructor: Dr. Mirjana Stojilović.
Fall 2021 Responsible for guiding and providing help to students through the labs and projects of the course.
Fall 2020 Guided students (300+) through weekly labs involving VHDL and NIOS assembly programming.
Oversaw the preparation of the lab materials and the automatic grading system.

Spring 2022 **Information, Calcul, Commuincation (ICC) (Bachelor's)**, *EPFL*, Instructor: Dr. Mirjana
Spring 2021 Stojilović.
Spring 2020 Responsible for the programming part of the course.
Guided students (300+) through weekly programming exercises in C and Python.
Launched automated grading platform for students in the C and Python courses.
Oversaw the preparation of lab exercises and programming assignments.

Spring 2019 **Microcontroller System Design Lab (Bachelor's)**, *AUC*, Instructor: Dr. Ramez Daoud.
Guided students through execution of laboratory experiments and helped them find causes of their errors by teaching them the troubleshooting approaches.

Spring 2019 **Digital Logic Design Lab (Bachelor's)**, *AUC*, Instructor: Dr. Ihab Talkhan.
Guided students through learning the basics of digital logic circuits and VHDL design.
Aided students in learning to troubleshoot to locate the sources of errors in the lab experiments.

Fall 2016 **Digital Logic Design (Bachelor's)**, *AUC*, Instructor: Prof. Hassanein Amer.
Spring 2017 Undergraduate teaching assistant for the course responsible for holding review sessions for the students.
Clarified concepts to students and guided them in figuring out how to solve digital logic design problems.

Research Experience

Ecole Polytechnique Fédérale de Lausanne, Switzerland

September, 2019 – present
Electrical-Level Fault-Injection Attacks on Heterogeneous FPGA-CPU Systems.
Exploring and developing attacks targeting fault injection against FPGA-based systems and demonstrating how the effects can propagate to CPUs within the same heterogeneous system.

Advisors: **Dr. Mirjana Stojilović**, *Scientist, School of Computer and Communication Sciences*, EPFL
Prof. Babak Falsafi, *Professor, School of Computer and Communication Sciences*, EPFL

CYD Mentor: **Dr. Vincent Lenders**, *Executive Director, Cyber-Defence Campus*, armasuisse

June, 2018 – August, 2018
Introducing Timing Violation Induced Faults in Multi-Tenant FPGAs.
Exploring the potential for building and carefully controlling malicious circuit designed to lower the on-chip voltage and inject faults into the operation of neighboring circuits within a multi-tenant FPGA.

Advisor: **Dr. Mirjana Stojilović**, *Scientist, School of Computer and Communication Sciences*, EPFL

The American University in Cairo, Egypt

January, 2017 – August, 2019
Reliability and Fault-Tolerance of FPGA-based Circuits.
Investigated the reliability of FPGA-based systems used in industrial, automotive, and space applications. Designed circuits for better reliability of FPGA-based systems for various applications.

Advisor: **Prof. Hassanein Amer**, *Professor, Dept. of Electronics & Communications Engineering*, AUC

February, 2018 – December, 2018
Drive Cycle Classification for Intelligent Battery-Aware Energy Management System for Electric Vehicles.
Exploring power management techniques for electric vehicles and implementing driving cycle classification using NN Toolbox in MATLAB. Developing a hardware prototype using Arduino microcontroller and Zynq board.

Advisor: **Prof. Hassanein Amer**, *Professor, Dept. of Electronics & Communications Engineering*, AUC

Professional Service

2021 – present **Member**, *Technical Program Committee*, IEEE International Conference on Emerging Technologies and Factory Automation (ETFA).

2019 – present **Student Member**, *ACM SIGARCH - WiCARCH - IEEE*.
Reviewer, *IEEE TVLSI - FCCM - FPGA - FPL*.

Extracurriculars

2021 Mentor for school girls and Speaker at **Coding Club des Filles**.

2021 Hopper at the **Virtual Grace Hopper Celebration (vGHC)**, providing session reviews and acting as a professional viewer.

2021 Speaker for **Toi aussi, crée ton appli**, introducing 21 girls aged 12 to 16 to the basics of logic circuits and their security.

2018 Student Representative on the **Research and Creativity Convention (RCC)** Organizing Committee.

2017 Member and Copilot on the **Robotics AUC ROV** team, contributing to building the control system of a remotely operated vehicle (ROV) and chosen by the team of 21 members to act as copilot during the regional competition. Won 7th place among 19 entries.

2016 – 2017 Intermediate Program Head for the **Robotics Club** at AUC.

2016 Physics Team Head for **Egyptian Researchers**, writing articles on topics in Physics to be published on Facebook and editing the team members' articles.

2015 – 2016 Basic Technical Head for the **Robotics Club** at AUC, teaching new members basics of Arduino programming and connecting digital circuits.