Department of Computer Science and Engineering
The American University in Cairo, Egypt
(+20) 1001002289
dina-mahmoud@aucegypt.edu
My Webpage
Linkedin
Google Scholar

Dina G. Mahmoud

Assistant Professor

Education

2019 – 2024 **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 – 2024 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

2024 – Present **Assistant Professor**, *The American University in Cairo*, Egypt.
Research on design of reliable and secure computing systems. Teaching courses on data structures and digital logic design.

2019 – 2024 **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 an AMD 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 *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 *ICCES*, December 2017.

Peer-Reviewed Journal Articles

2024 Dina G. Mahmoud, Beatrice Shokry, Vincent Lenders, Wei Hu, and Mirjana Stojilović. X-Attack 2.0: The Risk of Power Wasters and Satisfiability Don't-Care Hardware Trojans to Shared Cloud FPGAs. *IEEE Access*, volume 12, pages 8983–9011, 2024.

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. *Candidate for Top Picks in Hardware and Embedded Security 2023*.

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.

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.

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 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).

Research Experience

Ecole Polytechnique Fédérale de Lausanne, Switzerland

September, 2019 – August, 2024

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 EVs 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 - DATE - MECO*.