

Abdulrahman Diaa

✉ a2diaa@uwaterloo.ca • 🌐 abdulrahmandiaa.ca
in abdulrahman-diaa-555300126 • 📍 D-Diaa

Education

University of Waterloo – CrySP Lab

Ontario, Canada
Sept 2021 - Aug 2027

PhD in Computer Science (Sept 2023 - Aug 2027) – **Ongoing**

Thesis: *On the Trustworthiness of Generative Models*

MMath in Computer Science (Sept 2021 - Aug 2023) – **GPA: 96.75%**

Thesis: *Differentially-private multiparty Clustering*

Supervisor: Prof. Florian Kerschbaum

The American University in Cairo

Cairo, Egypt
Sept 2016 - June 2021

Bsc in Mathematics (Sept 2017 - June 2021) – **GPA: 4.0/4.0**

Thesis: *Lattice-based Cryptography and Fully Homomorphic Encryption: A Survey*

Bsc in Computer Engineering (Sept 2016 - June 2021) – **GPA: 4.0/4.0**

Thesis: *Mixture of Experts for Human Activity Classification from Images*

Supervisors: Dr. Ahmed El-Guindy, Dr. Cherif Salama and Dr. Mohammed Moustafa

Awards

2024: CPI Annual Conference Best Poster - CA\$1K	Cybersecurity and Privacy Institute (CPI)
2021-2025: David R. Cheriton Graduate Scholarship - CA\$40K	University of Waterloo
2021-2023: International Masters Award of Excellence - CA\$12.5K	University of Waterloo
2021-2022: Johnston International Entrance Scholarship - CA\$5K	University of Waterloo
2016-2021: Tarek Nour AUC Scholarship - US\$100K	Tarek Nour Communications

Patents

Dell Technologies – Patent No: US 11934487B2 (Granted)	
<i>Splitting Neural Networks on Multiple Edge Devices to Train on Vertically Distributed Data</i>	Mar 2024
Dell Technologies – Application No: US 17/314315 (Pending)	
<i>Data-Driven Index for Identification and Ranking of Companies for a Selected Technology</i>	May 2021
Dell Technologies – Application No: US 17/237400 (Pending)	
<i>Market Basket Analysis for Infant Hybrid Technology Detection</i>	Apr 2021
Dell Technologies – Application No: US 17/160782 (Pending)	
<i>Forecasting Technology Phases Using Unsupervised Clustering with Wardley Maps</i>	Jan 2021

Extra-Curricular Activities

2017: Academic Vice-president	Robotics Club, The American University in Cairo
2017: ROV Control Engineer	Robotics Club, The American University in Cairo
2017: Robotics Instructor	Robotics Club, The American University in Cairo
2017: Content Editor	Geniuses (TV Show)
2016: Helped raise ~4M USD for public schools	Geniuses (TV Show)
2016: Geniuses (TV Show) Team Leader	Al-Bashaer International Schools

Publications and Preprints

- [1] **A. Diaa**, T. Aremu, and N. Lukas. "Optimizing Adaptive Attacks against Content Watermarks for Language Models". In: The 42nd International Conference on Machine Learning. 2025.
- [2] **A. Diaa**, T. Humphries, and F. Kerschbaum. *FastLloyd: Federated, Accurate, Secure, and Tunable k-Means Clustering with Differential Privacy*. 2024. arXiv: 2405.02437 [cs.CR].
- [3] **A. Diaa** et al. "Fast and Private Inference of Deep Neural Networks by Co-designing Activation Functions". In: The 33rd USENIX Security Symposium. 2024.
- [4] N. Lukas, **A. Diaa**, L. Fenaux, and F. Kerschbaum. "Leveraging Optimization for Adaptive Attacks on Image Watermarks". In: The 12th International Conference on Learning Representations. 2024.
- [5] R. Mahdavi, **A. Diaa**, and F. Kerschbaum. *HE is all you need: Compressing FHE Ciphertexts using Additive HE*. 2023. arXiv: 2303.09043 [cs.CR].
- [6] S. Sav, **A. Diaa**, A. Pyrgelis, JP. Bossuat, and JP. Hubaux. "Privacy-Preserving Federated Recurrent Neural Networks". In: The 23rd Privacy Enhancing Technologies Symposium. 2023.

Research Experience

Cybersecurity Researcher

Airbus Defence and Space – VCX

Topics: Practical Batch Private Information Retrieval and Privacy-preserving DBSCAN

Reference: Dr. Erik-Oliver Blass

München, Germany

Jan 2025 - July 2025

Research Intern

École Polytechnique Fédérale de Lausanne – Lab for Data Security (LDS)

Topic: Privacy-preserving Federated Learning for Recurrent Neural Networks

Reference: Prof. Jean-Pierre Hubaux

Lausanne, Switzerland

July 2021 - Sept 2021

Undergraduate Data Science Research Intern

Dell Technologies – Data Office Team

Topics: Technology Forecasting and Distributed Neural Networks

Reference: Eng. Steve Todd

Cairo, Egypt

Feb 2020 - June 2021

Undergraduate Researcher

The American University in Cairo

Topic: Deep Reinforcement Learning for Traffic Control

Reference: Dr. Cherif Salama

Cairo, Egypt

Sept 2019 - Jan 2020

Research Software Development Engineering Intern

Microsoft Advanced Technology Lab in Cairo – Document Knowledge Extraction Team

Topic: Unsupervised Clustering for Schema-Inference from Semi-Structured Documents

Reference: Eng. Achraf Chalabi

Cairo, Egypt

Jul 2019 - Sept 2019

Academic Service

2025: Workshop Reviewer

1st Workshop on GenAI Watermarking (WMark@ICLR)

2025: Artifact Reviewer

34th USENIX Security Symposium

2024: Journal Reviewer

Transactions on Knowledge and Data Engineering (TKDE)

Engineering Experience

Software Engineering Intern

Nokia EG

Cairo, Egypt

Aug 2018 - Sept 2018

Software Engineering Intern

Microsoft EG

Cairo, Egypt

Jul 2017 - Aug 2017

Project Highlights

Recent Advances on Foundation Models

Optimizing Adaptive Attacks Against Watermarked Language Models Winter 2024

Advanced Topics in Data Security and Privacy

On Adaptive and Automated Attacks for Adversarial Example Defenses Winter 2022

Reinforcement Learning

Multi-Agent Reinforcement Learning for Large-Scale Traffic Control Winter 2022

Introduction to Machine Learning

(Horizontally and Sequentially)-split Federated Recurrent Neural Networks Fall 2021

Fundamentals of Distributed Systems

Secure peer-to-peer image-sharing service with coherence guarantees and fault-tolerance on UDP Fall 2019

Teaching Experience

Teacher Assistant

University of Waterloo

Ontario, Canada

Jan 2023 - Apr 2023

Course: Privacy, Cryptography, Network, and Data Security

Reference: Thomas Humphries

Teacher Assistant

The American University in Cairo

Cairo, Egypt

Jan 2021 - June 2021

Course: Embedded Systems Laboratory

Reference: Dr. Suzanne Safwat

Teacher Assistant

The American University in Cairo

Cairo, Egypt

Sept 2020 - June 2021

Course: Linear Algebra

Reference: Dr. Ahmed El-Guindy

Teacher Assistant

The American University in Cairo

Cairo, Egypt

Sept 2017 - Jun 2019

Course: Programming Fundamentals

Reference: Dr. Howaida Ismail

Other Roles

2018-2019: Student Technology Assistant

C. of Learning & Teaching, The American University in Cairo

2015-2017: A-Levels Teacher Assistant

Al-Bashaer International Schools

Other Honors

2021: President Cup

The American University in Cairo

2016-2021: Dean's list of Academic Standing

The American University in Cairo

2020: Challenge Coin for Innovation

Dell Technologies

2019-2020: Finalist

Egyptian Collegiate Programming Contest

2016: Best Player Cup

Geniuses (TV-Show), Season 1

Skills

Languages: Python, GoLang, C++, C#, C, Rust, R, Verilog, SQL

Frameworks: Lattigo, CUDA, PyTorch, PySyft, OpenCV, ROS, SUMO, Arduino, QT, ASP.NET