

Abdulrahman Diaa

+1 (226) 698 6965 • a2diaa@uwaterloo.ca • d-diaa.github.io
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: *Privacy-preserving Vector Databases*

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

Publications and Preprints

- [1] **A. Diaa**, T. Aremu, and N. Lukas. *Optimizing Adaptive Attacks against Content Watermarks for Language Models*. 2024. arXiv: 2410.02440 [cs.CR].
- [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.

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 Sponsorship - US\$100K	Tarek Nour Communications

Patents

Dell Technologies – Patent No: US 11934487B2 (Granted)

Splitting Neural Networks on Multiple Edge Devices to Train on Vertically Distributed Data Mar 2024

Dell Technologies – Application No: US 17/314315 (Pending)

Data-Driven Index for Identification and Ranking of Companies for a Selected Technology May 2021

Dell Technologies – Application No: US 17/237400 (Pending)

Market Basket Analysis for Infant Hybrid Technology Detection

Apr 2021

Dell Technologies – Application No: US 17/160782 (Pending)

Forecasting Technology Phases Using Unsupervised Clustering with Wardley Maps

Jan 2021

Research Experience

Cybersecurity Researcher

Airbus Defence and Space – VCX

Topic: Practically-optimal Batch Private Information Retrieval

Supervisor: 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

Supervisor: 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

Supervisor: 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

Supervisor: Eng. Achraf Chalabi

Cairo, Egypt

Jul 2019 - Sept 2019

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

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

Computer Architecture

RV32IC-compliant CPU design with memory constraints and privileged instructions support

Fall 2018

Honors

2021: President Cup	<i>The American University in Cairo</i>
2016-2021: Dean's list of Academic Standing	<i>The American University in Cairo</i>
2020: Challenge Coin for Innovation	<i>Dell Technologies</i>
2019-2020: Finalist	<i>Egyptian Collegiate Programming Contest</i>
2017: Best Interns Project	<i>Microsoft EG Summer Internship</i>
2016: Best Player Cup	<i>Geniuses (TV-Show), Season 1</i>

Teaching Experience

Teacher Assistant <i>University of Waterloo</i> Course: Privacy, Cryptography, Network, and Data Security Reference: <u>Thomas Humphries</u>	Ontario, Canada <i>Jan 2023 - Apr 2023</i>
Teacher Assistant <i>The American University in Cairo</i> Course: Embedded Systems Laboratory Reference: <u>Dr. Suzanne Safwat</u>	Cairo, Egypt <i>Jan 2021 - June 2021</i>
Teacher Assistant <i>The American University in Cairo</i> Course: Linear Algebra Reference: <u>Dr. Ahmed El-Guindy</u>	Cairo, Egypt <i>Sept 2020 - June 2021</i>
Teacher Assistant <i>The American University in Cairo</i> Course: Programming Fundamentals Reference: <u>Dr. Howaida Ismail</u>	Cairo, Egypt <i>Sept 2017 - Jun 2019</i>

Engineering Experience

Software Engineering Intern <i>Nokia EG</i>	Cairo, Egypt <i>Aug 2018 - Sept 2018</i>
Software Engineering Intern <i>Microsoft EG</i>	Cairo, Egypt <i>Jul 2017 - Aug 2017</i>

Other Roles

2018-2019: Student Technology Assistant	<i>C. of Learning & Teaching, The American University in Cairo</i>
2015-2017: A-Levels Teacher Assistant	<i>Al-Bashaer International Schools</i>

Skills

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

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