☎ *+1 (226) 698 6965*
✉ *a2diaa@uwaterloo.ca*
in *abdulrahman-diaa-555300126*
D-Diaa

Abdulrahman Diaa

Education

Sept 2027 **University of Waterloo**, *Ontario*, Canada.
PhD in Computer Science
Supervisor: Prof. Florian Kerschbaum – CrySP Lab

Sept 2023 **University of Waterloo**, *Ontario*, Canada.
MMATH (Thesis) in Computer Science – **GPA: 96.75%**
Thesis: *A (Differentially)-private multiparty instantiation of k-Means*
Supervisor: Prof. Florian Kerschbaum – CrySP Lab

June 2021 **The American University in Cairo**, *Cairo*, Egypt.
Bsc *summa cum laude* (Highest Honors) – **GPA: 4.0/4.0**
Double Major in Computer Engineering and Mathematics
Thesis I: *Mixture of Experts for Human Activity Classification From Images*
Thesis II: *Lattice-based Cryptography and Fully Homomorphic Encryption: A Survey*
Supervisors: Dr. Cherif Salama, Dr. Mohammed Moustafa and Dr. Ahmed El-Guindy

Publications and Preprints

2024 **ArXiv**: **A. Diaa**, T.Humphries and F. Kerschbaum.
FastLloyd: Fed., Accurate, Secure, and Tunable k-Means Clustering with Differential Privacy

2024 **ICLR24**: N. Lukas, **A. Diaa**, L. Fenaux and F. Kerschbaum.
Leveraging Optimization for Adaptive Attacks on Image Watermarks

2024 **USENIX24**: **A. Diaa** L. Fenaux, T. Humphries, M. Dietz, F. Ebrahimianghazani, B. Kacsmar, X. Li, N. Lukas, RA. Mahdavi, S. Oya, E. Amjadian and F. Kerschbaum.
Fast and Private Inference of Deep Neural Networks by Co-designing Activation Functions

2023 **ArXiv**: RA. Mahdavi, **A. Diaa** and F. Kerschbaum.
HE is all you need: Compressing FHE Ciphertexts using Additive HE

2023 **PoPETS23**: S. Sav, **A. Diaa**, A. Pyrgelis, J. Boussat and J. Hubaux.
Privacy-Preserving Federated Recurrent Neural Networks

Industrial Research Experience

Feb 2020 - June 2021 **Dell Technologies**, Cairo, Egypt.
Undergraduate Data Science Research Intern, *Data Office Team*
Reference: Eng. Steve Todd (VP Data Innovation and Strategy)

- Built a (Vertically and Horizontally) split neural network for **federated learning**–PySyft
- Worked on multiple approaches for utilizing bibliomentric data for **technology forecasting**

Jul 2019 - Sept 2019 **Microsoft Advanced Technology Lab in Cairo**, Cairo, Egypt.
Research Software Development Engineering Intern, *Document Knowledge Extraction Team*
Topic: Schema-Inference from Semi-Structured Documents
Supervisor: Eng. Achraf Chalabi (Principal RSDE)

- Built a pipeline that infers a possible schema (list of most relevant headings) governing a given collection of documents — C#, Unsupervised Learning, Natural Language Processing
- Deployed solution on Azure as a web Application — ASP.NET, Azure

Academic Research Experience

Sept 2021 - Present **University of Waterloo**, Ontario, Canada.
Graduate Researcher, *Cryptography, Security and Privacy (CrySP) Lab*
Topic: Accelerated Privacy-Preserving Inference on Neural Networks
Reference: Prof. Florian Kerschbaum

- Developing novel SMPC techniques to accelerate private inference on Deep Neural Networks

July 2021 - Sept 2021 **École Polytechnique Fédérale de Lausanne**, Lausanne, Switzerland.
Research Intern, *Lab for Data Security (LDS)*
Topic: Privacy-Preserving Federated Learning for Recurrent Neural Networks
Reference: Prof. Jean-Pierre Hubaux

- Developed and optimized an SMPC solution for Training Federated Recurrent Networks, utilizing Homomorphic Encryption and Multidimensional Packing for Matrices
- Implemented the solution utilizing LATTIGO library and ONET

Sept 2019 - Jan 2020 **The American University in Cairo**, Cairo, Egypt.
Undergraduate Researcher, *Computer Science and Engineering Department*
Topic: Deep Reinforcement Learning for Traffic Control
Supervisor: Dr. Cherif Salama

- Built a traffic signal-switching agent based on neural networks **(DQN)**— PyTorch, SUMO
- Utilizing minimal state information, the agent beats Fixed-Time and Longest-Queue-First policies

Industrial Engineering Experience

Aug 2018 - Sept 2018 **Nokia EG**, Cairo, Egypt.
Software Engineering Intern

- Developed a windows service to intercept data provider emails and generated reports— C#, SQL

Jul 2017 - Aug 2017 **Microsoft EG**, Cairo, Egypt.
Software Engineering Intern

- Created a Web-API for an ECommerce platform and published it on Azure— C#, MVC

Skills

Languages	Python, GoLang, C++, C#, C, R, Verilog, SQL
Frameworks	Lattigo, CUDA, PyTorch, PySyft, OpenCV, ROS, SUMO, Arduino, QT, ASP.NET
Others	BigQuery, PowerBI

Patents

May 2021 **Data-Driven Index for Identification and Ranking of Companies for a Selected Technology**, Application No: **US 17/314315**.
Filed May 7th, 2021 – Pending

Apr 2021 **Market Basket Analysis for Infant Hybrid Technology Detection**, Application No: **US 17/237400**.
Filed September 22nd, 2021 – Pending

Jan 2021 **Forecasting Technology Phases Using Unsupervised Clustering with Wardley Maps**, Application No: **US 17/160782**.
Filed January 28th, 2021 – Pending

Sept 2020 **Splitting Neural Networks on Multiple Edge Devices to Train on Vertically Distributed Data**, Application No: **US 17/039702**.
Filed September 30th, 2020 – Pending

Awards

2020-2023	David R. Cheriton Graduate Scholarship - CA$20K	*University of Waterloo*
2020-2023	International Masters Award of Excellence (IMAE) - CA$12.5K	*University of Waterloo*
2016-2021	Tarek Nour Sponsorship - US$100K	*Tarek Nour Communications*

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*
2017	Best Interns Project	*Microsoft EG Summer Internship*

Project Highlights

Winter 2022 **On Adaptive and Automated Attacks for Adversarial Example Defenses**, *Advanced Topics in Data Security and Privacy.*

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

Fall 2021 **(Horizontally and Sequentially)-split Federated Recurrent Neural Networks**, *Introduction to Machine Learning.*

Fall 2020 **STM32 Lasertag System: weapon, armor and scoring judge, utilizing IR and Bluetooth communication on an L432KC board**, *Embedded Systems.*

Fall 2019 **Secure peer-to-peer image-sharing service with coherence guarantees and fault-tolerance on UDP sockets**, *Fundamentals of Distributed Systems.*

Fall 2018 **RV32IC-compliant CPU design with memory constraints and privileged instructions support**, *Computer Architecture.*

Teaching Experience

Jan 2021 - June 2021 **The American University in Cairo**, Cairo, Egypt.
Teacher Assistant, *Computer Science and Engineering Department*
Course: Embedded Systems Laboratory
Reference: Dr. Suzanne Safwat

- Provided technical help for the students during lab times.

Sept 2020 - June 2021 **The American University in Cairo**, Cairo, Egypt.
Teacher Assistant, *Mathematics Department*
Course: Linear Algebra
Reference: Dr. Ahmed El-Guindy

- Helped students with understanding the material during office hours

Sept 2017 - Jun 2019 **The American University in Cairo**, Cairo, Egypt.
Teacher Assistant, *Computer Science and Engineering Department*
Course: Programming Fundamentals
Reference: Dr. Howaida Ismail

- Coordinated programming contests and conducted office hours