

Education

- Sept 2019 – **Boston University**, *Boston*, Massachusetts, USA.
Present PhD in Computer Science
Dissertation Title: Succinct Communication in Quantum-Prover Protocols
Dean's Fellow, Graduate School of Arts & Sciences, Fall 2019
- June 2019 **The American University in Cairo**, *Cairo*, Egypt.
BSc *summa cum laude* (Highest Honors) – GPA: 3.93/4.00
Double Major in Computer Engineering and Mathematics
Awarded the Ahmed H. Zewail Medal for Excellence in the Sciences and Humanities
- July 2013 **Kafr El-Zayat High School**, *Gharbeya*, Egypt. 99.76%.
Ranked 1st Student Nationwide (1st of $\approx$ 0.5 million students)

Experience Highlights (details provided in later subsections)

- Sep 2019 – **Boston University**, **Boston, MA, USA**
Present *Research & Teaching Fellow, Department of Computer Science*
Areas: Quantum Computing, Cryptography, Complexity Theory, Algorithms, Security, and Privacy.
- Oct 2020 – **envelope.network Inc.**, **Boston, MA, USA**
- March 2022 *Co-founder and Lead Research Engineer, Participated in Boston University Summer Accelerator*
Project: privacy-preserving, fair, and transparent advertising platform
- Summer **Twitter**, **San Francisco, CA, USA**
2019 & Fall *Software Engineering Intern, User Onboarding Backend Team*
2017 Project: who-to-follow account recommendations
- Fall 2018 **École polytechnique fédérale de Lausanne (EPFL)**, **Switzerland**
Visiting Researcher, Decentralized and Distributed Systems (DEDIS) Lab
Project: decentralized framework for privacy-preserving auditable aggregation
- Summer **Twitter**, **Seattle, WA, USA**
2018 *Software Engineering Intern, Platform Security Team*
Project: analytics on content security policy (CSP) violation reports
- Summer **UCLA Institute for Pure and Applied Mathematics (IPAM)**, **Los Angeles, CA, USA**
2017 *Visiting Researcher, Research in Industrial Projects for Students (RIPS)*
Project: facial verification engine sponsored by **GumGum**, an applied computer vision company
- Jan – Mar **Affectiva**, **Cairo, Egypt**
2017 *Machine Learning Scientist (Intern) – Speech, Science Team*
Startup acquired by Smart Eye in 2021 for USD \$73.5 million
- Summer **Microsoft Research**, **Cairo, Egypt**
2015 *Summer Intern Software Development Engineer (SDE), Speaker Recognition Team*
Project: implementation of the Hierarchical multi-Layer Acoustic Model (HiLAM) for speaker verification

Teaching Experience

Graduate Teaching Fellow (Boston University):

- Fall 2025 CAS CS 332 – Elements of the Theory of Computation (with Prof. Leonid Levin)
- Spring 2025 CAS CS 535 – Complexity Theory (with Prof. Leonid Levin)
- Summer 2024 CAS CS 330 – Introduction to Analysis of Algorithms (with Dr. Tiago Januario)
- Spring 2024 CAS CS 530 – Advanced Algorithms (with Prof. Leonid Levin)
- Fall 2023 CAS CS 235 – Algebraic Algorithms (with Prof. Leonid Levin)
- Summer 2023 CAS CS 330 – Introduction to Analysis of Algorithms (with Dr. Tiago Januario)
- Fall 2021 CAS CS 332 – Elements of the Theory of Computation (with Prof. Mark Bun)

Undergraduate Teaching Assistant (The American University in Cairo):

Spring 2019 CSCE 4702 – Secure Systems Engineering

Winter 2018 CSCE 4910 – Big Data Analytics

Fall 2015 MACT 2131 – Discrete Mathematics

Spring 2015 MACT 2123 – Calculus III

Fall 2014 CSCE 2201 – Data Structures and Algorithms

Spring 2014 MACT 1122 – Calculus II

Spring 2014 CSCE 106 – Fundamentals of Computer Science

Peer-Reviewed Publications

Conference Papers

Limited Proxying for Content Filtering Based on X.509 Proxy Certificate Profile. Islam Faisal and Sherif El-Kassas. In *Proc. 11th International Conference on Security for Information Technology and Communications (SECITC 2018)*, LNCS, Bucharest, Romania, November 2018. Springer.

Interactive Oracle Arguments in the QROM and Applications to Succinct Verification of Quantum Computation. Islam Faisal. In *Proc. The Cryptographers' Track at RSA Conference*, San Francisco, California, USA, May 2024.

Other Manuscripts

In Preparation

- 3 **Succinct quantum proofs for MA with multiple unentangled Merlins.** Islam Faisal and Anand Natarajan.
- 4 **Rounding Almost Commuting Hamiltonians.** Islam Faisal, Anand Natarajan, and Alexander Poremba.

Posters

- 5 **Case Studies on the Automated Symbolic Analysis of Voting Protocols.** Islam Faisal. In *AUC Undergraduate Research Exhibition*, Cairo, Egypt, May 2016.
- 6 **Convolutional Neural Networks and Metric Learning for Facial Verification.** Islam Faisal, Andrew Nguyen, Prem Talwai, Surabhi Desai, and Shantanu Joshi. In *Joint Mathematics Meetings Conference*, San Diego, USA, January 2018.

Technical Reports

- 7 **KAIRES: Fully Decentralized Auditable Privacy-Preserving Framework for Aggregation.** Islam Faisal, Eleftherios Kokoris-Kogias, Bryan Ford, and Sherif El-Kassas.
- 8 **Transfer Learning For Emotion Recognition From Speech.** Taniya Mishra, Islam Faisal, and Mohamed Ezzeldin A. Elshaer.
- 9 **Generating Random, Yet Constrained Music.** Muhammad Faisal, Islam Faisal, and Islam Elgamal. Technical report, May 2017.

Pending Patents

- 10 **Speech analysis for cross-language mental state identification.** Taniya Mishra, Islam Faisal, and Mohamed Ezzeldin Abdelmonem Ahmed Mohamed. US Patent App. 16/206,135, June 6 2019.

Academic Research Experience

Research in Computer Science and Applied Mathematics

Sep 2019 – **Boston University, Boston, MA, USA**

Present *Doctoral Researcher, Department of Computer Science*

- Constructed a succinct classical argument protocol for the complexity class *Quantum Merlin-Arthur (QMA)* under complexity-theoretic assumptions and hardness of *LWE* in the Quantum Random Oracle Model (QROM).
- Defined different notions for leakage-resilient zero-knowledge in zero-knowledge proofs on secret-shared in the local and global leakage models;
- Showed a *local leakage resilience* property of an existing zero-knowledge proof system.

Fall 2018 **École polytechnique fédérale de Lausanne (EPFL), Switzerland**

Visiting Researcher, Decentralized and Distributed Systems (DEDIS) Lab

Supervisor: Prof. Bryan Ford

- Designing and implementing a fully-decentralized privacy-preserving machine learning system using blockchains, threshold cryptography, zero-knowledge proofs, secret-sharing, and multi-party computation;
- Preparing a preprint manuscript for submitting to publication;
- Participated in different team meetings and seminars

Summer **UCLA Institute for Pure and Applied Mathematics (IPAM), Los Angeles, CA, USA**

2017 *Visiting Researcher, Research in Industrial Projects for Students (RIPS)*

Supervisor: Dr. Shantanu H. Joshi

- Worked in a team of four students on building a facial verification engine sponsored by **GumGum**, an applied computer vision company;
- Used various mathematical concepts and machine learning tools including Tensorflow, Keras, and Torch;
- Presented the work in the Joint Mathematics Meetings (JMM) Conference

2016 – 2019 **The American University in Cairo, Egypt**

Undergraduate Researcher, Computer Science and Engineering Department

Supervisor: Prof. Sherif El-Kassas

Topics: Formal Methods; Security; Privacy

- Modeled some case studies on the symbolic analysis of voting protocols using the Tamarin prover;
- Worked on designing a limited proxying framework for content filtering that is published in LNCSS

Summer **Center for Informatics Science, Nile University, Giza, Egypt**

2014 *Summer Trainee, Ubiquitous & Visual Computing Group*

- Applied different machine learning topics including classification, clustering, feature selection and ensemble methods using Weka;
- Mentored a new intern and prepared a training manual for future interns

Research in Pure Mathematics

2017 – 2018 **The American University in Cairo, Egypt**

Undergraduate Researcher, Mathematics Department

Supervisor: Dr. Mohammad Sadek

Topics: Number Theory; Elliptic Curves

- Surveyed different variants of the Diophantine Tuples;
- Defined a new variant and proved its non-existence;
- Parameterizing all possible $q \in Q$ for which a given non-zero rational triple (x_1, x_2, x_3) form a $D(q)$ - m -tuple

Entrepreneurial Experience

Oct 2020 – **envelope.network Inc., Boston, MA, USA**

March 2022 *Co-founder and Lead Research Engineer, Participated in Boston University Summer Accelerator*

- Co-founded the company to build a **privacy-preserving advertising ecosystem**.
- Co-led the core research project to architect the system with **secure multiparty computation (MPC)**.
- Led architecting and building the system while **managing stacks for different product components** (e.g. **Scala/Vue.js** for full-stack development, **PostgreSQL** for DB, **Slick** for Functional Relational Mapping, **C++** for core cryptography library, and **Javascript** for browser extension).
- Led the team to join the Boston University Summer Accelerator and receive **grant funding of \$10,000**.
- Recruited and managed 8 engineering interns to accelerate the product development in summer 2021.
- Developed the product and business model by interviewing customers and researching the market.
- Led the team to shape the company culture and values, and set up the company environment and tools.

Industrial Experience

2017 - 2019 **Twitter**

Software Engineer (Intern), Platform Security and User Onboarding Backend Teams

Responsibilities shared among the 3 roles:

- Developed software in Scala and used Hadoop and Scalding as well as internal ML libraries;
- Developed unit tests and integration tests as part of a rigorous continuous integration (CI) process;
- Actively participated in team code reviews, deploying and monitoring services, and resolving tech debts;
- Co-organized reading groups on security and machine learning.
- Guided software engineers and fellow interns with tasks and processes I became familiar with.

User Onboarding Backend Team, San Francisco, CA (Summer 2019)

Mentor: Christine Chen, PhD, UIUC

- Worked on calibration of account recommendations for new users between diversity and accuracy;
- Designed and launched an online experiment to A/B test the developed methods with millions of Twitter users;

Platform Security Team, Seattle, WA (Summer 2018)

Mentor: Scott Robinson, BS, MIT

- Took ownership of Twitter's existing content security policy (CSP) violation reporting service which handles millions of reports per second;
- Built an analytics pipeline and visualization dashboard for content security policy (CSP) violation reports;
- Communicated with other teams to improve the process of updating CSP rules.

User Onboarding Backend Team, San Francisco, CA (Fall 2017)

Mentor: Yang Tang, MSc, Tsinghua University

- Trained and evaluated machine learning models for improving who-to-follow account recommendations in profile pages;
- Integrated and deployed ML models online for experimentation with a portion of production traffic;

Jan – Mar **Affectiva, Cairo, Egypt**

2017 *Machine Learning Scientist (Intern) – Speech, Science Team*

Mentors: Taniya Mishra, PhD; Mohamed Ezz, MSc

- Worked directly with the lead speech scientist on emotion recognition from speech;
- Prototyped Affectiva's first multi-class speech emotion classifier;
- Employed transfer learning to adapt a deep Convolutional Neural Network (CNN) for the task of emotion recognition from speech.

Summer **Microsoft Research, Cairo, Egypt**

2015 *Summer Intern Software Development Engineer (SDE), Speaker Recognition Team*

Mentor: Motaz El-Saban, PhD

- Worked on Text-dependent Speaker Verification;
- Implemented the Hierarchical multi-Layer Acoustic Model (HiLAM) for speaker verification;
- Used a variety of speech processing toolkits and models such as HTK, Gaussian Mixture Modeling, MFCC feature extraction and voice activity detection;
- Used a mix of programming languages such as Matlab and C++.

Selected Conferences and Competitions

August 2023 Research in Industrial Projects for Students (RIPS) Reunion Celebration 2023, UCLA Institute for Pure and Applied Mathematics, Los Angeles, CA, USA. August 18, 2023.

August 2023 13th International Conference on Quantum Cryptography, University of Maryland, College Park, MD, USA. August 14 – 17, 2023.
Presented an accepted poster paper.

July 2022 Graduate Summer School on Post-quantum and Quantum Cryptography, UCLA Institute for Pure and Applied Mathematics, Los Angeles, CA, USA. July 25 – 29, 2022.
– Proposed the idea of the summer school to the lead organizer.
– Presented a poster.

September Arab Security Conference 2020 (Virtual Event)

2020 Presented a talk titled: Achieving More by Knowing Less: Decentralized Infrastructures and Secure Multiparty Computing Protocols

- Feb 2020 MIT's interdisciplinary Quantum HACKathon (iQuHACK)
 - Mentored a team of high school students to use IBM's Qiskit to prototype Qryptos: Quantum Framework for Secret-Shared-Output Secure Assisted Computation (Presentation available here)
- July 2020 Invited to Institute for Advanced Study (IAS)/Park City Mathematics Institute (PCMI) Graduate Summer School: Number Theory Informed by Computation (Cancelled due to COVID-19)
- Jan 2020 Attended two boot camps at the Simons Institute at UC Berkeley supported by Boston University:
 - Lattices: Algorithms, Complexity, and Cryptography Boot Camp
 - The Quantum Wave in Computing Boot Camp
- Aug 2019 The 39th Annual International Cryptology Conference (CRYPTO 2019). *Santa Barbara, CA, USA*. Supported by Twitter to travel to the conference.
- Aug 2019 28th USENIX Security Symposium. *Santa Clara, CA, USA*.
Gave a lightning talk about our ongoing work building a fully decentralized framework for machine learning.
- Nov 2018 11th International Conference on Security for Information Technology and Communications (SECITC 2018). *Bucharest, Romania*.
Presented our paper "Limited Proxying for Content Filtering Based on X.509 Proxy Certificate Profile"
- Aug 2018 Arithmetic Geometry, Number Theory, and Computation. *MIT, Cambridge, MA, USA*.
- May 2018 The 13th Annual AUC Mathematics Competition. *Cairo, Egypt*.
Groups Round Winner.
- 2017, 2018 The Annual Conference for Excellence in Undergraduate Research, Entrepreneurship and Creative Achievement (EURECA). *AUC, Cairo, Egypt*.
- Jan 2018 Joint Mathematics Meetings (JMM). *San Diego, California, USA*.
 - Supported by AUC and UCLA's IPAM to travel to the conference.
 - Presented an oral presentation and a poster on our work on facial verification during the summer at IPAM.
- Jul 2015 Black-Box Optimization Competition at the Genetic and Evolutionary Computation Conference (GECCO). *Madrid, Spain*.
- Oct 2013 Intel Science Competition - Arab World 2013. *Amman, Jordan*.
- Mar 2013 Intel Bibliotheca Alexandrina Science and Engineering Fair. *Alexandria, Egypt*.

--- Honors and Awards

- 2019 Dean's Fellowship, Graduate School of Arts & Sciences, Boston University
- 2019 ETH Zürich Direct Doctorate in Computer Science Scholarship (declined)
- 2019 École doctorale Informatique et Communications (EDIC) Fellowship, EPFL (declined)
- 2019 Graduated *summa cum laude* (Highest Honors), The American University in Cairo
- 2019 Ahmed H. Zewail Medal for Excellence in the Sciences and Humanities, AUC's Centennial Graduation Commencement
- 2018 AUC Annual Mathematics Competition Groups Round 1st Place
- 2017 CSCE Exemplary Student
- 2013–2019 Dean's List for outstanding academic achievement
- 2013 Top Ranked Student Nationwide in High School (1st of approx. 1/2 million students)
- Mar 2013 Intel Excellence in Computer Science Award – Awarded by Intel Foundation at the Intel Bibliotheca Alexandrina Science and Engineering Fair

--- Grants

- 2021 \$10,000 Award - Boston University Summer Accelerator

2015–2018 AUC University Undergraduate Research Travel Grants UG#1810898, UG#1711739, UG#1504427
2014 AUC University Undergraduate Research Mini Grant UG#1404292
2013–2019 University Public Schools Scholarship – Full-tuition undergraduate scholarship

Academic Service & Extracurricular Activities

Fall 2019 – Organizing the Quantum Cryptography Reading Group at Boston University.
Present
Fall 2023 Mentor, Boston University Undergraduate Research Opportunities Program.
Fall 2022, Judge, Boston University Spark! Demo Day.
Fall 2025
2019-2020 Mentored a team of undergraduates working on a senior project on verifiable distributed computing.
Spring 2018 Organized the AUC Security and Privacy Reading Group
2015 Arabic Managing Editor, The Insider AUC
2013, 2018 Academic Committee Member, Computer Science and Engineering Association
2011–2013 Founding Chair, KZ High School Tech-Club