Nicolas Alhaddad

Email: nhaddad@bu.edu
LinkedIn: nicolas-al-haddad-868080a2
GitHub: github.com/nicolas3355

EDUCATION

Boston University — Boston, USA
Ph.D. in Computer Science, Advisor: Mayank Varia, GPA: 4.00/4.00 — 2018–Current

American University of Beirut — Beirut, Lebanon
M.S. in Computer Science (transferred) — 2016–2017

American University of Beirut — Beirut, Lebanon
B.S. in Computer Science — 2012–2016

PUBLICATIONS

[1] N. Alhaddad, M. Varia, and H. Zhang, *High-threshold avss with optimal communication complexity*, Financial Cryptography and Data Security, https://fc21.ifca.ai/papers/93.pdf, 2021.

EXPERIENCE

Boston University — Boston, USA
Software Engineering Fellow/BU Software Application and Innovation Lab (SAIL) — 2018

- Conclave
- Conclave is a query compiler that automatically accelerates analytical queries by transforming a relational query into a combination of scalable, local, cleartext processing and small, isolated Secure multi-party computation (MPC) steps. Working with Prof. Kfoury and Prof. Lapets, I formally defined the syntax and the semantics of the domain specific query language of conclave. I also worked on static execution cost analysis for statically reasoning about functional properties of conclave programs; with the goal of choosing the best conclave back-end based on message complexity performance.
- Conclave Web
- Conclave Web allows multiple analysts/researchers to compute aggregate statistics over datasets uploaded to dataverse without revealing any private data to one another, except for what can be inferred from the output. Conclave web uses conclave to generate the appropriate mpc code and offload to it to containers that run the computation jointly. Conclave web uses openshift and kubernetes for that purpose. Conclave web is currently being deployed on the Massachusetts Open Cloud. I worked with Prof. Varia on designing and implementing the key management system of conclave web.

American University Of Beirut — Beirut, Lebanon
Research Assistant — 2017

- High Performance Surgical Simulation
- I worked with Prof. Turkiyyah on High Performance Surgical Simulation. This project was in collaboration with faculty members from North Carolina University at Chapel Hill and Qatar Robotic Surgery Center. I worked with another researcher on the geometric model for cutting tetrahedral meshes efficiently. We created a mathematical framework for representing, analyzing, and evaluating different nonlinear cuts on the mesh. We brought those ideas to life by creating a C++ library for that purpose.

Interactive life — Beirut, Lebanon
Fullstack Software Engineer — 2015-2017

- Instant generation of native mobile applications with backend support

– Interactivelife is a start-up based in Mercer Island, Washington with a team of developers located in Beirut. The start-up provides instant native mobile and web applications for real-time event-based engagement and content-delivery to users. I was in charge of the mobile team. I helped design, scale, rewrite and automate interactivelife's mobile and web applications.

Institute for War & Peace Reporting (IWPR)   Beirut, Lebanon
Software engineer/Content Creator   2014

- CyberArabs browser
- I compiled a modified version of firefox that connects to IWPR servers as a way to circumvent censorship.
- Cyber-Arabs mobile application
- I created a cross platform mobile application for CyberArabs. The app was basically an rss reader with push notifications.

TEACHING

- **Teaching Fellow** at Boston University   Spring 2020
  Applied Cryptography(CS568)
- **Teaching Fellow** at Boston University   Fall 2019
  Network Security(CS391/CS558)
- **Teaching Fellow** at Boston University   Spring 2019
  Applied Cryptography(CS568)
- **Teaching Fellow** at Boston University   Fall 2018
  Introduction to Computing Systems (CS350)

SKILLS

- **Programming Languages:** Bash, C/C++, Gallina(Coq), Java, Javascript, PHP, Python
- **Web and Mobile Development**

LANGUAGES

- **English:** Full Professional Proficiency
- **French:** Professional Working Proficiency
- **Arabic:** Native

PROJECTS

Selected Projects:

MTD (Bash, Python, Open-Stack, 2018-present)
- Moving Target Defense(MTD) in the cloud. Using proactive security to secure a secret in the cloud.

Liquid voting (Coq, 2019)
- A project that encodes and proves some interesting liquid voting properties in Coq.

INTERESTS

- Applied Cryptography(includes multi-party computation), Zero-knowledge proofs, Smart Contracts
- Distributed Systems/ Blockchains
- Formal Verification/ Model Checking