Nicolas Alhaddad

Email: nhaddad@bu.edu
LinkedIn: nicolas-alhaddad
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, S. Das, S. Duan, L. Ren, M. Varia, Z. Xiang, and H. Zhang, "Balanced byzantine reliable broadcast with near-optimal communication and improved computation", in *Proceedings of the 2022 ACM Symposium on Principles of Distributed Computing*, ser. PODC'22, Salerno, Italy: Association for Computing Machinery, 2022, pp. 399–417, ISBN: 9781450392624.

[2] N. Alhaddad, S. Das, S. Duan, L. Ren, M. Varia, Z. Xiang, and H. Zhang, "Brief announcement: Asynchronous verifiable information dispersal with near-optimal communication", in *Proceedings of the 2022 ACM Symposium on Principles of Distributed Computing*, ser. PODC'22, Salerno, Italy: Association for Computing Machinery, 2022, pp. 418–420, ISBN: 9781450392624.

[3] R. Issa, N. Alhaddad, and M. Varia, "Hecate: Abuse reporting in secure messengers with sealed sender", in *31st USENIX Security Symposium (USENIX Security 22)*, Boston, MA: USENIX Association, Aug. 2022, pp. 2335–2352, ISBN: 978-1-939133-31-1.

[4] N. Alhaddad, S. Duan, M. Varia, and H. Zhang, *Succinct erasure coding proof systems*, Cryptology ePrint Archive, Report 2021/1500, https://ia.cr/2021/1500, 2021.

[5] 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

MPCH — Remote, USA
Part-time Internship in Cryptography — 2022-2023

- Key Management
- I designed and implemented a novel MPC technique to add, remove and refresh secret shares on top of an open source threshold signature library written in Golang. The protocol supports byzantine failures and assumes honest majority.
- Crypto Wallet
- I designed and implemented a proof of concept (poc) MPC wallet that works on top of the Bitcoin Testnet. The wallet supports non custodial verifiable shares. The poc leverages confidential virtual machines and is written in python.
- DKG, BLS
- I designed and implemented a Distributed Key Generation (DKG) protocol and wrote it in Golang. The design is based on the Pedersen DKG, supports byzantine failures and assumes honest majority. The implementation has been done on the BLS12-381 elliptic curve.

Clabs Remote, USA

Internship in Cryptography Sep-Nov 2021

- Odis++
- I designed and implemented ODIS++, an efficient oblivious message retrieval protocol on the Celo alfajores testnet. In particular, the protocol is used by senders to generate new stealth addresses for receivers. This enables senders to communicate or send funds privately to parties with public addresses. ODIS++ supports delegation; a receiver can delegate the task of detecting a message to a third party while still maintaining confidentiality of the message content.
- Auditable Mixer
- I designed a new distributed trust-less mixer that offers privacy while still being auditable.

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. Andrei Lapets, I formally defined the syntax and semantics of the domain specific query language of conclave. I also worked on static execution cost analysis for static 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. Mayank 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. George 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 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/Mobile Team Manager 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 Lebanon and India. I worked closely with the CTO on managing and designing the infrastructure of Interactive life. I transformed business ideas and requirements into viable code while integrating work between different local and remote members of the team. I helped design, scale, rewrite and automate interactivelife's mobile and web applications, we served more than 30+ apps using our system.

Institute for War & Peace Reporting (IWPR) Beirut, Lebanon

Software engineer/Content Creator 2014

- Cyber-Arabs browser and Cyber-Arabs mobile application
- I compiled a modified version of firefox that connects to IWPR servers as a way to circumvent goeverment censorship. I also created a cross platform mobile application for CyberArabs.

Teaching

- **Instructor** at Boston University — Spring 2023
  Crypto for Data Science(DS453/DS653), co-designed and co-taught the course (link)
- **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:** Android, Cordova, jQuery Mobile, Python-Flask, KnockoutJS, Jquery
- **Cloud Computing:** OpenStack, OpenShift, AWS

Languages

- **English:** Proficient
- **French:** Proficient
- **Arabic:** Native

Interests

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