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, M. Varia, and Z. Yang, *Haven++: Batched and packed dual-threshold asynchronous complete secret sharing with applications*, Cryptology ePrint Archive, Paper 2024/326, https://eprint.iacr.org/2024/326, 2024.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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 — 2022-2024

- Designed and implemented a novel Multi-Party Computation (MPC) technique to manage (add, remove and refresh) secret shares in a Golang-based open-source threshold signature library, enhancing protocol resilience against Byzantine failures.
- Developed a proof of concept (POC) MPC wallet for Bitcoin Testnet, featuring non-custodial verifiable shares, leveraging confidential virtual machines and written in Python
- Implemented a Distributed Key Generation (DKG) protocol in Golang, based on the Pedersen DKG, compatible with BLS12-381 elliptic curve, ensuring robustness against Byzantine failures.

Clabs — Remote, USA
Full-time Internship in Cryptography — Sep-Nov 2021

- Created ODIS++, an efficient oblivious message retrieval protocol on the Celo alfajores testnet, enabling private communication and fund transfers to public addresses. The protocol also supports delegation; a receiver can delegate the task of detecting a message to a third party while still maintaining confidentiality of the message content.
- Designed a distributed, trustless, auditable mixer offering enhanced privacy features for users.

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

- 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. 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 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.

Interactive life Beirut, Lebanon
Full Stack Software Engineer/Mobile Team Manager 2015-2017

- 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

- Developed a custom browser based on Firefox to circumvent government censorship. The browser was distributed to journalists on the field.
- Developed a cross platform mobile application for IWPR's CyberArabs. The mobile application was deployed on the Google Play Store.

Teaching

- **Teaching Fellow** at Boston University Spring 2024
  Blockchains and their Applications(CS595)
- **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), Golang, Java, Javascript, PHP, Python
- **Web and Mobile Development:** Android, Cordova, jQuery Mobile, Python-Flask, KnockoutJS, Jquery
- **Cloud Computing:** OpenStack, OpenShift, AWS

Languages

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

Interests

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