Omar Sagga

80 Gardner Street, Boston, MA, 02134 ❖ osagga@outlook.com ❖ +1 (512) 960-6033 ❖ github.com/osagga

Education

Bachelor of Arts Computer Science, *Summa Cum Laude* **May 2019**

Boston University, Boston, MA

- Related Coursework: Operating Systems, Applied Cryptography, Distributed Systems, Algorithms and Network Security.
- Dean's List: Spring 2016 – Fall 2018

Experience

Commonwealth Crypto (aka **Arwen)**, Boston, MA

Software Engineer **Jun 2019 - Present**

- Structure internal systems to monitor and track Blockchain changes.
- Integrate backend systems to frontend facing application through C# and Angular frameworks.
- Developed with C# with the use of NBitcoin and BouncyCastle (cryptographic library).

Software Developer, Intern **May 2018 - May 2019**

- Worked on developing a non-custodial cryptocurrency trading platform that utilizes Bitcoin's smart contracts.
- Implemented a Hierarchical Deterministic key generation protocol to derive private keys from an initial private seed.
- Developed with C# with the use of NBitcoin and BouncyCastle cryptographic library.

Boston University Security Group (BUSec), Boston, MA **July 2016 – May 2018**

Research Assistant

- **TumbleBit**
  - Conducted an audit on the cryptography used in the full implementation of TumbleBit, an untrusted Bitcoin-compatible anonymous payment hub (github.com/nTumbleBit/nTumbleBit).
  - Implemented a cryptographic setup protocol for TumbleBit that uses Zero-Knowledge proofs to validate RSA public keys generated by the Tumbler (github.com/osagga/TumbleBitSetup).
  - Developed with C# under the mentorship of Prof. Leonid Reyzin, and Prof. Sharon Goldberg.
- **Securing RPKI protocol (**github.com/yossigi/compress_roas)
  - Analyzed the security problems of using the "maxLength" attribute in RPKI (BGP securing protocol).
  - Presented research results at ACM International **Co**nference on emerging **N**etworking **EX**periments and **T**echnologies (CoNEXT) 2017.
  - Developed a compression algorithm, that utilizes Trie (Prefix Tree), as an alternative to using the "maxLength" attribute and successfully achieved 7~9% compression rate on the number of Route Origin Authorization (ROAs) a BGP router needs to process.
  - Developed with Python in collaboration with Yossi Gilad under the mentorship of Prof. Sharon Goldberg.

Publications

Certifying RSA Public Keys with an Efficient NIZK. Sharon Goldberg, Leonid Reyzin, Omar Sagga, and Foteini Baldimtsi. IACR Cryptology ePrint Archive 2018 (2018): 57.

MaxLength Considered Harmful to the RPKI. Yossi Gilad, Omar Sagga, and Sharon Goldberg. CoNEXT 2017.

Projects

ProxyChat *(Winner at MIT Bitcoin Hackathon)* **March 2018**

- Distributed, end-to-end encrypted Python group chatting application using NuCypher's cryptographic library (pyUmbral).
- Implemented proxy re-encryption on the proxy node to distribute encrypted messages in the chatroom without decryption.

Skills

Programming Languages: C#, Python, C, x86 Assembly, and Java.

Technologies: Cryptography, Blockchain, Git, Linux, and LaTeX.

Achievements and Awards

Outstanding Undergraduate Researcher Award, Honorable Mention **December 2018**

Recognizes undergraduate students in North American universities who show outstanding research potential in an area of computing research.

MIT Bitcoin Hackathon 2018 - NuCypher Sponsor Prize **March 2018**

$5000 to the team (2 members) that best utilizes NuCypher Proxy Re-encryption protocol.

KAUST Gifted Student Program (KGSP) Scholarship - Recipient **August 2014 – May 2019**

Scholarship awarded by the King Abdullah University of Science & Technology (KAUST).

ACM CoNEXT 2017 Student Travel Grant **November 2017**

Financial aid to help eligible and selected students to attend CoNEXT 2017.