Talley Amir

201-414-2830 | talleyamir@gmail.com

Research Interests

- Secure distributed/cloud computing
- Secure multi-party computation
- Zero-knowledge proofs

Education

Yale University | Ph.D. in Computer Science (Aug 2018 - Present)

- Relevant Courses: Advanced Natural Language Processing, Computer Networks, Cryptography & Computer Security
- Cumulative Grade Point Average: 4.00

Brown University | Sc.B. in Applied Mathematics and Computer Science (Sep 2014 – May 2018)

- Relevant Courses: Cryptography (2 terms), Cyber Security & International Relations, Discrete Structures, Information Theory, Intro to Computer Systems, Linear Algebra, Ordinary Linear & Partial Differential Equations, Software Engineering, Statistical Inference I/II, Systems Security, Theory of Computation
- Cumulative Grade Point Average: 3.89

Bergen County Academies | Academy of Visual and Performing Arts (Sep 2010 – Jun 2014)

- Cumulative Grade Point Average: 3.95, Best Composite SAT Score: 2280
- Honors and Awards: National Honor Society, Gold Key Award in Scholastic Art and Writing Competition, Supervisors Award (for highest GPA in the Academy)

Research Experience

Yale University | PhD-Seeking Student (Aug 2018 - Present)
Pursing a PhD in cryptography, have been doing directed reading on robust secret sharing and broadcast encryption schemes. Interested in exploring multi-party computation.

Brown University | Undergraduate Research Assistant (Sep 2017 – Jan 2018)
Assisted in developing a secure cloud computing model that aims to minimize the amount of data leaked to a server that hosts information about a graph.
Advisors: Roberto Tamassia and Esha Ghosh

Teaching & Work Experience

Independent | Tutor (May 2018 - August 2018)
Developed studying strategies for high school students preparing for college entrance examinations; worked with several students in one-on-one sessions to improve performance in SAT and college-level mathematics.

Brown University | Head Teaching Assistant for *CS22: Discrete Structures* (Oct 2016 – May 2018)
Promoted to a leadership position; in addition to UTA duties, I also helped hire and train a team of UTAs, collaborated with the professor to design the course, and managed a staff of 30 TAs.

Ernst & Young | Cyber Security Risk Consultant (Jun 2017 – Aug 2017)
Developed cyber risk assessment tools, attended meetings and workshops for the purpose of strengthening clients' security systems, and drafted reports detailing current news in cyber security as well as metrics and benchmarks for tracking progress in cyber-development projects.

CrowdTangle | Digital Marketing Intern (Jun 2016 – Aug 2016)
Researched and generated lists of social media accounts across various platforms organized by purpose or topic for clients of a rapidly growing tech startup company (procured by Facebook in 2016).

Brown University | Undergraduate Teaching Assistant for *CS22: Discrete Structures* (Jan 2016 – May 2016)
Drafted homework problems, solutions, and grading rubrics, graded weekly problem sets, and held weekly office hours for helping students with assignments and course materials.

Tavlin | Server (Jan 2014 – Aug 2016)
Worked after school in high school and over breaks in college; interacted professionally and amicably with customers and coworkers in a fast-paced restaurant establishment.

Relevant Projects

Yale University CS Department | Cryptography & Systems Security

- Padding Oracle Attack (Python): Used the padding oracle attack to decrypt a message encrypted using a block cipher in CBC mode.

Brown University CS Department | Intro to Computer Systems, Software Engineering, Systems Security

- Flag (Go): Given a poorly secured website, discovered vulnerabilities and designed and executed exploits to steal unauthorized information and escalate privileges (e.g. SQL injection, parameter based access control, file injection, cross-site scripting, etc.).
- Dropbox (Go): Designed and developed a file hosting system which allows multiple users to register for an account and securely authenticate their credentials to upload and download their personal files.

Brown University Mathematics Department | Cryptography

- Primality Testing: Applied Miller-Rabin test to generate large primes from random 1024-bit integers.
- NTru (Java): Wrote a program that encrypts and decrypts messages using NTru scheme given parameters.
- Bitcoin (Java): Implemented a program that, given a list of public keys of the current owners of n coins and a list of t transactions, determines whether each transaction contains a valid ECDSA signature on the Secp256k1 curve, performs the transaction if the signature is valid, and prints the final owners of the n coins in order.

Skills

Languages | First language is English, conversational in Hebrew and Spanish

Programming languages | Java, Python, MatLab, LaTeX, C, Go, JavaScript, Scala, OCaml, HTML

Rubik's cubes | 2x2, 3x3 (Best time: 52 s), 4x4 (Best time: 192 s), 5x5, 6x6