# Albert Kwon

773 609 1213
kwonal@mit.edu
albertkwon.com

## Education

09/13–Present (Expected 02/19) **Massachusetts Institute of Technology**, Cambridge, MA.
Ph.D. Candidate in Electrical Engineering and Computer Science
S.M. in Electrical Engineering and Computer Science — GPA: 4.8/5.0
Advisor: Srini Devadas

09/09–05/13 **University of Pennsylvania**, Philadelphia, PA.
Bachelor of Science in Engineering, with Summa Cum Laude — GPA: 3.98/4.00
Majors: Computer Science, Electrical Engineering

## Work Experience

09/13–Present **Research Assistant**, *CSAIL*, MIT, MA.
- Design and implement systems that improves privacy and anonymity in the cloud using modern cryptography

09/16–12/16 **Technical Intern**, *ProdSec*, Google, CA.
- Designed and implemented applications for CloudProxy, which provides Trusted Execution Environment using TPM
- Performed security audit of CloudProxy code base

09/10-Present **Teaching Assistant**, UPenn/MIT.
- Design and grade assignments and exams, and hold office hours
- List of classes I helped teach:
  - 6.858: Computer Systems Security (Fall 15; MIT)
  - 6.046: Intro. to Algorithms (Spring 15; MIT)
  - CIS320: Intro. to Algorithms (Spring 13; UPenn)
  - CIS380: Operating Systems (Fall 11; UPenn)
  - CIS240: Intro. to Computing Systems (Fall 11; UPenn)
  - CIS110: Intro. to Computer Science (Fall 10; UPenn)

07/13–08/13 **Technical Intern**, BAE Systems, MA.
- Developed a secure processor that could stop majority of the top 10 vulnerabilities and exploits in CVE

## Projects

07/16–Present **Atom**, *github.com/kwonalbert/atom*, in Go.
- Horizontally scalable anonymous communication system
- Supports more than a million users for latency tolerant messaging with strong anonymity
- Publication: **A. Kwon**, H. Corrigan-Gibbs, S. Devadas, B. Ford "Atom: Scalable Anonymity Resistant to Traffic Analysis", arXiv, 2016

10/15–02/16 **Spacemint**, *github.com/kwonalbert/spacemint*, in Go.
- Implementation of proof-of-space and cryptocurrency that use proof-of-space instead of proof-of-work
- Supports up to several terabytes of space

02/15–08/15 **Riffle**, *github.com/kwonalbert/riffle*, in Go.
- An anonymous communication system that has low bandwidth and computation overhead
- Supports up to hundreds of thousands of clients for low-latency messaging and hundreds of clients for high-bandwidth communication with cryptographic guarantees on anonymity
- Publication: **A. Kwon**, D. Lazar, B. Ford, S. Devadas, "Riffle: An Efficient Communication System with Strong Anonymity", in PETS, 2016

01/14–03/15 **ORAM Controller**, *github.com/kwonalbert/oram*, in Verilog.
- Hardware Oblivious Random Access Memory (ORAM) controller that hides memory access patterns and provides memory integrity
- Provides a clean interface to secure any RAM against access pattern leakage with small overhead
- Publication: C. Fletcher, L Ren, **A. Kwon**, M. van Dijk, E. Stefanov, D. Serpanos, S. Devadas, "Techniques for Low-Latency, Low-Area Hardware ORAM Controllers," in FCCM, 2015

## Skills

Languages Go, C, Python, BlueSpec, Java, Matlab, Verilog
OS Linux/Unix