

## Education

- 05/15–Present **Massachusetts Institute of Technology**, Cambridge, MA.  
Ph.D. Candidate in Electrical Engineering and Computer Science  
Advisor: Srini Devadas
- 09/13–05/15 **Massachusetts Institute of Technology**, Cambridge, MA.  
S.M. in Electrical Engineering and Computer Science  
Thesis: Riffle : An Efficient Communication System with Strong Anonymity  
Advisor: Srini Devadas  
GPA: 4.8/5.0
- 09/09–05/13 **University of Pennsylvania**, Philadelphia, PA.  
Bachelor of Science in Engineering, with Summa Cum Laude  
Majors: Computer Science, Electrical Engineering  
Advisor: André DeHon  
GPA: 3.98/4.00

## Research Interests

Security and Privacy; Applied Cryptography; Anonymity; Distributed Systems; Cryptocurrency

## 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
- 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
- 05/11-05/13 **Research Assistant**, *Implementation of Computation Group*, UPenn, PA.  
◦ Implemented hardware support for pointers with bounds (Fat Pointers) to prevent attacks such as buffer overflows  
◦ Designed and implemented a novel router that helps mitigate denial-of-service and without sacrificing throughput

## Publications

- 1 **A. Kwon**, D. Lazar, B. Ford, S. Devadas, “Riffle: An Efficient Communication System with Strong Anonymity”, in PETS, 2016
- 2 **A. Kwon**, M. Al-Sabah, D. Lazar, S. Devadas, M Dacier, “Circuit Fingerprinting Attacks: Passive Deanonimization of Tor Hidden Services”, in USENIX Security, 2015
- 3 L. Ren, C. Fletcher, **A. Kwon**, E. Stefanov, E. Shi, M. van Dijk, S. Devadas, “Constants Count: Practical Improvements to Oblivious RAM”, in USENIX Security, 2015
- 4 X. Yu, S. K. Haider, L. Ren, C. Fletcher, **A. Kwon**, M. van Dijk, S. Devadas, “PrORAM: Dynamic Prefetcher for Oblivious RAM,” in ISCA, 2015
- 5 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
- 6 C. Fletcher, L. Ren, **A. Kwon**, M. van Dijk, S. Devadas, “Freecursive ORAM: [Nearly] Free Recursion and Integrity Verification for Position-based Oblivious RAM,” in ASPLOS, 2015
- 7 **A. Kwon**, K. Zhang, P. Lim, Y. Pan, J. Smith, A. DeHon, “ROTORouter: Router Support for Endpoint-Authorized Decentralized Traffic Filtering to Prevent DoS Attacks,” in ICFPT, 2014
- 8 **A. Kwon**, U. Dhawan, J. Smith, T. F. Knight Jr., A. DeHon, “Low-Fat Pointers: Compact Encoding and Efficient Gate-Level Implementation of Fat Pointers for Spatial Safety and Capability-based Security,” in CCS, 2013
- 9 U. Dhawan, **A. Kwon**, E. Kadric, C. Hritcu, B. C. Pierce, J. M. Smith, A. Dehon, G. Malecha, G. Morrisett, T. F. Knight, A. Sutherland, T. Hawkins, A. Zyxnfryx, D. Wittenberg, P. Trei, S. Ray and G. Sullivan, “Hardware Support for Safety Interlocks and Introspection,” in AHNSW, 2012

---

## Teaching

- Fall 15 **6.858: Computer Systems Security**, *Teaching Assistant*, MIT.  
Instructors: Frans Kaashoek and Robert Morris
- Spring 15 **6.046: Introduction to Algorithms**, *Teaching Assistant*, MIT.  
Instructors: Erik Demaine, Srin Devadas, Nancy Lynch
- Spring 13 **CIS320: Introduction to Algorithms**, *Teaching Assistant*, UPenn.  
Instructors: Rajiv Gandhi and Sanjeev Khanna
- Fall 12 **CIS380: Operating Systems**, *Teaching Assistant*, UPenn.  
Instructor: Boon Thau Loo
- Fall 11 **CIS240: Introduction to Computer Systems**, *Teaching Assistant*, UPenn.  
Instructor: C.J. Taylor
- Fall 10 **CIS110: Introduction to Computer Science**, *Teaching Assistant*, UPenn.  
Instructor: Jean Griffin
- Spring 10 **CIS192: Python Programming**, *Teaching Assistant*, UPenn.  
Instructor: Constantine Lignos

---

## Projects

- 07/16–Present **Atom**, [github.com/kwonalbert/atom](https://github.com/kwonalbert/atom), in Go.
  - Horizontally scalable anonymous communication system
  - Supports more than a million users for latency tolerant messaging with strong anonymity
- 10/15–02/16 **Spacemint**, [github.com/kwonalbert/spacemint](https://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](https://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
- 01/14–03/15 **ORAM Controller**, [github.com/kwonalbert/oram](https://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
- 05/11–08/13 **SAFE Processor**, in *Bluespec*.
  - Secure processor that supports privilege separation, memory safety, and dynamic information flow tracking
  - Optimized to run on modern FPGAs at 200MHz
- 07/12–07/13 **ROTORouter**, in *Bluespec+Verilog*.
  - A router that aims to mitigate Denial-of-Service attacks by filtering malicious packet
  - Supports packet filtering at line-rate with extremely low false positive rate.

---

## Honors and Awards

- 2013-2014 **Shillman Fellowship**, MIT.
- 2013 **Undergraduate Research Award**, *Honorable Mention*, Computing Research Association.
- 2013 **A. Atwater Kent Prize**, UPenn.
- 2013 **Hugo Otto Wolf Memorial Prize**, UPenn.
- 2012 **Stuart Eichert, Jr. Memorial Prize**, UPenn.
- 2011 **Manfred Altman Memorial Award**, UPenn.

---

## Skills

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