Alex Ledger

Resume for Computer Science PhD

(417) 766 9854
a.led1027@gmail.com

Education

2012–2016 **Bachelor of Arts in Math-Computer Science**, *Reed College*.

Undergraduate Thesis

Topic *Implementing Component-Based Garbled Circuits*

Field Cryptography

Advisor Professor Adam Groce

Description Explores methods of secure computation, a cryptographic protocol for allowing two people who do not trust each other to work together. I developed a new technique for chaining components of Yao's garbled circuits, and I implemented the technique in C to achieve an order of magnitude speed up over prior work.

Experience

2016–Present **Assistant Staff**, *MIT Lincoln Lab*, Lexington, MA.
Designed, architected, and implemented a framework for secure computation involving novel cryptographic optimizations, parallelized code, a uniquely tailored test harness, and enhanced developer usability

2016–Present **Student**, *MIT*, Cambridge, MA.
Participated in classes at MIT including Lattice Cryptography with Vinod Vaikuntanathan, Public Ledgers with Silvio Micali, and Multicore Programming with Nir Shavit

2016 **Software Engineer Intern**, *Sailfan*, Portland, OR.
- Researched and developed algorithms and software to detect features in images and compute statistics in domains with a limited training set
- Implemented a RESTful interface for clients to interact with the image processing code

2015–2016 **Math-Computer Science Research Assistant**, *Reed College*, Portland, OR.
- Worked with professor Adam Groce on Oblivious RAM (ORAM), a subfield of cryptography focused on obfuscating a client's access patterns to a server
- Implemented old and new ORAM protocols in C++, wrote cryptographic proofs that the protocols were secure, and published a paper

2016 **Computational Biology Research Assistant**, *Reed College*, Portland, OR.
- Worked with professor Anna Ritz on genomic analysis
- Statistically analyzed genome mapping algorithms and developed methods for detecting and characterizing structual variants

2015–2016 **Artificial Life Lab Research Assistant**, *Reed College*, Portland, OR.
- Worked with professor Mark Bedau on examining whether culture and technology exhibits aspects of evolution, using U.S. patents as a proxy for "technology in culture"
- Employed many statistical and machine learning techniques to analyze the patents database including neural nets, natural language processing techniques, regression models, anomaly detection algorithms, and other network algorithms

2014-2015 **Webmaster of Reed Student Body Website**, *Reed College*, Portland, OR.
Administered a LAMP server and maintained and built Python-Django web applications for the Reed College student body website

2014-2015 **Teaching Assistant**, *Reed College*, Portland, OR.
Teaching Assistant for Math 121, Reed's introduction to computer science course

2014 **Software Engineering Intern**, *The Program PDX*, Portland, OR.
Used C++, OpenFrameworks and video technologies such as the Microsoft Kinect and webcams to construct engaging applications for children's museums and retail stores

Publications

- "Externally Verifiable Oblivious RAM," with Adam Groce and Joshua Gancher. Privacy Enhancing Technologies Symposium (PETS), July 2017.
- "CompGC: Efficient Offline/Online Semi-honest Two-party Computation," with Adam Groce, Alex Malozemoff, and Arkady Yerukhimovich.
- "Haplotype Resolved Assembly and Structural Variant Detection with Long-reads," with Anna Ritz, Oscar Rodriguez, Matthew Pendleton, and Ali Bashir.
- "Implementing Component-Based Garbled Circuits," Undergraduate thesis, Reed College, advised by Adam Groce, 2016.

Computer Skills

Experienced Rust, C, C++, Python, Java, Latex, R, Bash, MongoDB, NoSQL, Linux, Git
Intermediate Clojure, Coq, SQL, Mathematica, Matlab, Haskell

Coursework

- Computer Systems
- Multicore Programming
- Public Ledgers
- Computability and Complexity
- Real Analaysis
- Multivariable Calculus
- 2 years of Economics
- Cryptography
- Lattice Cryptography
- Algorithms and Data Structures
- Probability and Combinatorics
- Abstract Algebra
- Real Analysis
- 2 years of Physics

More Information

Github github.com/aled1027
LinkedIn linkedin.com/pub/alex-ledger/61/ab4/75a

Interests

- Cryptography
- Data Privacy
- Formal Methods
- Asynchronous and Concurrent Systems
- Machine Learning and Artificial Intelligence
- Network and Graph Theory
- Climate Change