Wei Dai

• 805-364-3141 • weidai@eng.ucsd.edu • http://wdai.us

Education

UNIVERSITY OF CALIFORNIA, SAN DIEGO (UCSD) *Sept. 2016–Present*
DEPARMENT OF COMPUTER SCIENCE AND ENGINEERING (CSE)
Ph.D student, advised by Prof. Mihir Bellare.

UNIVERSITY OF CALIFORNIA, SANTA BARBARA (UCSB) *Aug. 2012–Jun. 2016*

COLLEGE OF ENGINEERING
M.S. Computer Science, advised by Prof. Stefano Tessaro. *Jun. 2016*

COLLEGE OF CREATIVE STUDIES (CCS)
B.S. Computer Science & B.S. Mathematics *Dec. 2015*
Cumulative GPA: 3.91

Research Interests

Broadly in cryptography and theoretical computer science.

Awards

Powell Fellowship, UCSD CSE *2016 / 17–2018 / 19*

Yardi Systems Scholarship, College of Engineering *2014–2015*

Summer Undergraduate Research Fellowship (SURF), CCS *Summer 2014*

Research Affiliations

Currently advised by Prof. Mihir Bellare. *Sept. 2016–Present*

Crypto group at UCSB, advised by Prof. Stefano Tessaro. *Oct. 2015–Jun. 2016*

Koç Lab, with Prof. Çetin Koç & Prof. Ömer Eğecioğlu *2014–2016*

Theses

Master Thesis: *Statistical Methods in Cryptography* *Sept. 2014*
- Application of Rényi divergence in cryptographic applications.
- Tighter bound for the Swap-or-Not cipher.
- Alternative non-adaptive to adaptive blockcipher composition theorem.
- Proposal of lossy deterministic encryption.

Senior Thesis: *Randomness Extractors — An Exposition* *Oct. 2015*
- Surveys literature on randomness extractors.
- Two-source extractors from universal hash functions.

Select Positions & Projects

Taching Assitant
- Automata and Formal Languages (UCSB CS138) *Spring 2016*

Grader
- Advanced Linear Algebra (UCSB Math CS 120) *Winter 2014*
- Parallel and Scientific Programming (UCSB CS 140) *Fall 2015*
- Introduction to Cryptography (UCSB CS 178) *Winter 2016*

Course scheduling system for Sacramento Country Day School *2012–14*
- Implemented heuristic search algorithms for an NP-hard problem.

Fasd. http://github.com/clvv/fasd *2011–Present*
- Shell script that helps with directory naviagtion and file access

- Over 2000 GitHub “stars”

SKILLS

Programming and software tools
- Fluency in: C, C++, Javascript, Python, Unix Shell, LaTeX, git.
- Have worked with: Scala, Ruby, R, parallel libraries (MPI, OpenMP, Intel TBB).
- Familiarity with machine learning: deep learning, Caffe, word2vec.

Fluency in English and Chinese.

EXTRA-CURRICULAR

Staff member at UCSB Excursion Club *2013–2016*
- Leading indoor, outdoor rock climbing and canyoneering trips.
- Teaching basic climbing techniques and rigging for climbing.