WEI DAI

Department of Computer Science & Engineering
University of California, San Diego
9500 Gilman Drive, La Jolla, CA, USA.

E-mail: weidai@eng.ucsd.edu
Web: https://cseweb.ucsd.edu/~weidai

Last updated: October 11th, 2021

RESEARCH INTERESTS

Design and analysis of cryptographic protocols, especially regarding applications to security, scalability, and privacy of blockchains.

EDUCATION

Ph.D. Computer Science (expected Dec. 2021). Sep. 2016 – Present
College of Engineering. University of California, San Diego (UCSD).
Advisor: Prof. Mihir Bellare.

M.S. Computer Science. Dec. 2015 – Jun. 2016
College of Engineering. University of California, Santa Barbara (UCSB).
Advisor: Prof. Stefano Tessaro.
Thesis title: *Statistical Methods in Cryptography*

B.S. Computer Science & B.S. Mathematics Aug. 2012 – Dec. 2015
College of Creative Studies. UCSB.
Summa cum laude. Cumulative GPA: 3.91
Thesis title: *Randomness Extractors—An Exposition*

EMPLOYMENT

NTT Research Jun. 2021 – present
Research Intern. Supervisor: Dr. Tatsuaki Okamoto and Dr. Go Yamamoto

University of California, San Diego Jun. 2016 – Jun. 2021
Research Assisstant & Teaching Assisstant

University of Washington Jun. – Sep. 2019
Research Intern. Supervisor: Prof. Stefano Tessaro.

Visa Research Jun. – Sep. 2018
Research Intern. Supervisor: Dr. Atul Luykx.

AWARDS

Powell Fellowship 2016 – 2019
College of Engineering. University of California, San Diego.

Yardi Systems Scholarship 2014 – 2015
College of Engineering. University of California, Santa Barbara.

Summer Undergraduate Research Fellowship Jun. 2014 – Sep. 2014
College of Creative Studies. University of California, Santa Barbara.

Conference Publications

[1] Mihir Bellare and Wei Dai. Defending against key exfiltration: Efficiency improvements for big-key cryptography via large-alphabet subkey prediction. In Bhavani M. Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu, editors, *ACM CCS 2017*, pages 923–940. ACM Press, October / November 2017.

[2] Mihir Bellare and Wei Dai. The multi-base discrete logarithm problem: Tight reductions and non-rewinding proofs for Schnorr identification and signatures. In Karthikeyan Bhargavan, Elisabeth Oswald, and Manoj Prabhakaran, editors, *INDOCRYPT 2020*, volume 12578 of *LNCS*, pages 529–552. Springer, Heidelberg, December 2020.

[3] Mihir Bellare, Wei Dai, and Lucy Li. The local forking lemma and its application to deterministic encryption. In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part III*, volume 11923 of *LNCS*, pages 607–636. Springer, Heidelberg, December 2019.

[4] Mihir Bellare, Wei Dai, and Phillip Rogaway. Reimagining secret sharing: Creating a safer and more versatile primitive by adding authenticity, correcting errors, and reducing randomness requirements. *PoPETs*, 2020(4):461–490, October 2020.

[5] Wei Dai, Viet Tung Hoang, and Stefano Tessaro. Information-theoretic indistinguishability via the chi-squared method. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part III*, volume 10403 of *LNCS*, pages 497–523. Springer, Heidelberg, August 2017.

[6] Wei Dai, Stefano Tessaro, and Xihu Zhang. Super-linear time-memory trade-offs for symmetric encryption. In Rafael Pass and Krzysztof Pietrzak, editors, *TCC 2020, Part III*, volume 12552 of *LNCS*, pages 335–365. Springer, Heidelberg, November 2020.

Other Professional Activities

Conference Talks
INDOCRYPT2020, ASIACRYPT 2019, ACM CCS 2017

Sub-reviewer
ITC2021, CRYPTO 2019, CRYPTO 2018, ASIACRYPT 2017, CRYPTO 2017, STOC 2016

Teaching Assisstantships

- Modern Cryptography (UCSD CSE207): Spring 2021
- Introduction to Modern Cryptography (UCSD CSE107): Fall 2018, Spring & Fall 2020
- Theory of Computation (UCSD CSE105, UCSB CS138): Spring 2016, Winter 2021

Personal

Citizenship: US
Languages: English, Chinese