Alexis Korb

alexiskorb@cs.ucla.edu

Research Interests

Cryptography and theoretical computer science

Education

2020-Present **Ph.D. in Computer Science**, UCLA
Advisor: Amit Sahai

2018-2020 **M.S. in Computer Science**, UCLA
Thesis: Limits on the Pseudorandomness of Low-Degree Polynomials over the Integers

2014-2018 **B.S. in Computer Science**, UCLA
Summa Cum Laude

Awards and Honors

2025 UCLA Distinguished Teaching Assistant
UCLA's highest recognition for teaching excellence, awarded to just five students per year across all of UCLA.

2024 UCLA CS Teaching and Education Career Development Award

2022 *Beyond the Csiszár-Körner Bound: Best-Possible Wiretap Coding via Obfuscation* is selected as among the top six papers at CRYPTO 2022 and was consequently specially invited to and published in the *Journal of Cryptology*.

2020 UCLA CS Outstanding Graduating Masters Student

2019 UCLA CS Northrop-Grumman Outstanding TA Award

Professional Research Experience

Summer 2024 **NTT Research, Cryptography and Information Security Lab**
Sunnyvale, CA
Research Intern

Summer 2022 **Simons Institute Summer Cluster: Lattices and Beyond**
University of California Berkeley
Visiting Researcher

Publications

- **Incrementally Verifiable Computation for NP from Standard Assumptions**
  Pratish Datta, Abhishek Jain, Zhengzhong Jin, Alexis Korb, Surya Mathialagan, Amit Sahai
  Crypto 2025
- **Dynamic Bounded-Collusion Streaming Functional Encryption from Minimal Assumptions**
  Kaartik Bhushan, Alexis Korb, Amit Sahai
  Crypto 2025
- **Adaptively Secure Streaming Functional Encryption**
  Pratish Datta, Jiaxin Guan, Alexis Korb, Amit Sahai
  TCC 2025

- **(Multi-Input) FE for Randomized Functionalities, Revisited**
  Pratish Datta, Jiaxin Guan, Alexis Korb, Amit Sahai
  TCC 2025
- **Streaming Functional Encryption**
  Jiaxin Guan, Alexis Korb, Amit Sahai
  Crypto 2023
- **Hard Languages in NP ∩ coNP and NIZK Proofs from Unstructured Hardness**
  Riddhi Ghosal, Yuval Ishai, Alexis Korb, Eyal Kushilevitz, Paul Lou, Amit Sahai
  STOC 2023
- **Beyond the Csiszár-Körner Bound: Best-Possible Wiretap Coding via Obfuscation**
  Yuval Ishai, Alexis Korb, Paul Lou, Amit Sahai
  Crypto 2022, Invited and Accepted to the *Journal of Cryptology*
- **Amplifying the Security of Functional Encryption, Unconditionally**
  Aayush Jain, Alexis Korb, Nathan Manohar, Amit Sahai
  Crypto 2020

Preprints and Manuscripts

- **Building Hard Problems by Combining Easy Ones: Revisited**
  Yael Eisenberg, Christopher Havens, Alexis Korb, Amit Sahai
- **A Note on the Pseudorandomness of Low-Degree Polynomials over the Integers**
  Aayush Jain, Alexis Korb, Paul Lou, Amit Sahai
- **Expanding COVID-19 Symptom Screening to Retail, Restaurants, and Schools by Preserving Privacy Using Relaxed Digital Signatures**
  Brandon Jew, Alexis Korb, Paul Lou, Jeffrey N. Chiang, Ulzee An, Amit Sahai, Eran Halperin, Eleazar Eskin

Patents

- **Adaptively Secure Streaming Functional Encryption System and Method**
  Pratish Datta, Jiaxin Guan, Alexis Korb, Amit Sahai
  U.S. Patent: US-20250274279-A1

Teaching Experience

Fall 2025	**Instructor**, Pepperdine University, COSC 101: Programming Principles I with Python
Summer 2025	**Instructor**, UCLA, CS 180: Introduction to Algorithms and Complexity
Fall 2024	**Instructor**, UCLA, CS 180: Introduction to Algorithms and Complexity
Spring 2025	**TA**, UCLA, CS 33: Introduction to Computer Organization
Spring 2024	**TA**, UCLA, CS 181: Theory of Computing
Winter 2023	**TA**, UCLA, CS 181: Theory of Computing
Fall 2021	**TA**, UCLA, CS 31: Introduction to Computer Science
Winter 2021	**TA**, UCLA, CS 181: Theory of Computing
Spring 2019	**TA**, UCLA, CS 181: Theory of Computing
Winter 2019	**TA**, UCLA, CS 181: Theory of Computing

Varies **Guest Lecturer**, UCLA, CS 180: Introduction to Algorithms and Complexity
- Feb 26, 2025: Dynamic Programming: Shortest Path with Negative Edges
- Feb 24, 2025: Dynamic Programming: Introduction and Sequence Alignment

Varies **Guest Lecturer**, UCLA, CS 181: Theory of Computing
- Feb 21, 2024: Set Cardinality and Cantor's Diagonalization
- Mar 8, 2023: Undecidability and Unrecognizability
- Feb 8, 2023: Introduction to PDAs and Equivalence with CFGs
- Feb 7, 2022: CFL Pumping Lemma and Introduction to Turing Machines

Talks

- **Adaptively Secure Streaming Functional Encryption**
  NTT Research, Cryptography and Information Security Lab - August 2024
- **Streaming Functional Encryption**
  Crypto 2023
- **Hard Languages in NP ∩ coNP and NIZK Proofs from Unstructured Hardness**
  MIT Cryptography and Information Security Seminar - October 2023
  Simons Institute Minimal Complexity Assumptions for Cryptography Workshop - May 2023
  Stanford University Applied Cryptography Group - May 2023
- **Beyond the Csiszár-Körner Bound: Best-Possible Wiretap Coding via Obfuscation**
  Crypto 2022
- **Amplifying the Security of Functional Encryption, Unconditionally**
  Crypto 2020

Service

- Reviewer for Journal of Cryptology
- External Reviewer for Crypto 2025, MFCS 2025, Crypto 2024, TCC 2024, PKC 2024, Eurocrypt 2023, and CCC 2023