

# Abhiram Kothapalli

Department of Electrical Engineering and Computer Science  
University of California, Berkeley  
Soda Hall, 345 Le Roy Ave, Berkeley, CA 94709  
akothapalli@berkeley.edu

## Summary

---

Abhiram Kothapalli is a postdoctoral scholar at University of California, Berkeley hosted by Sanjam Garg. He earned his Ph.D. at Carnegie Mellon University in Computer Science advised by Bryan Parno. Abhiram's research develops fundamental technologies aimed at scaling expressive privacy and integrity guarantees across the internet.

## Professional Appointments

---

**Postdoctoral Scholar**, University of California, Berkeley, CA, USA 09/24 – Present  
Department of Electrical Engineering and Computer Science  
Host: Sanjam Garg

## Education

---

**Carnegie Mellon University**, Pittsburgh, PA, USA 08/18 – 05/24  
Ph.D. in Computer Science  
Dissertation: A Theory of Composition for Proofs of Knowledge  
Advisor: Bryan Parno

**University of Illinois**, Urbana-Champaign, IL, USA 08/15 – 05/18  
B.S. in Computer Science, B.S.LAS in Mathematics  
Advisors: Andrew Miller, Nikita Borisov

## Research Experience

---

**Microsoft Research**, Redmond, WA, USA 01/21 – 04/21  
Research Intern, Mentor: Srinath Setty

**Sandia National Laboratories**, Livermore, CA, USA 05/18 – 08/18  
Research Intern, Center for Cyber Defenders

**Sandia National Laboratories**, Albuquerque, NM, USA 05/17 – 08/17  
Research Intern, Center for Cyber Defenders

**Information Trust Institute**, Urbana-Champaign, IL, USA 05/16 - 08/16  
Research Intern, Mentor: Andrew Miller

## Conference Publications

---

- [1] S. Garg, M. Hajiabadi, D. Kolonelos, A. Kothapalli, and G. V. Policharla, “A framework for witness encryption from linearly verifiable SNARKs and applications,” in *Annual International Cryptology Conference*, Springer Nature Switzerland Cham, 2025, pp. 504–539.
- [2] J. Kim, A. Kothapalli, O. Chardouvelis, R. S. Wahby, and P. Grubbs, “ALPACA: Anonymous blocklisting with constant-sized updatable proofs,” in *2025 IEEE Symposium on Security and Privacy (SP)*, IEEE, 2025, pp. 3364–3382.
- [3] A. Kothapalli and S. Setty, “HyperNova: Recursive arguments for customizable constraint systems,” in *Annual International Cryptology Conference*, Springer Nature Switzerland Cham, 2024, pp. 345–379.
- [4] A. Kothapalli and S. Setty, “NeutronNova: Folding everything that reduces to zero-check,” *Cryptology ePrint Archive*, 2024.
- [5] A. Kothapalli and B. Parno, “Algebraic reductions of knowledge,” in *Annual International Cryptology Conference*, Springer Nature Switzerland Cham, 2023, pp. 669–701.
- [6] V. Goyal, A. Kothapalli, E. Masserova, B. Parno, and Y. Song, “Storing and retrieving secrets on a Blockchain,” in *IACR International Conference on Public-Key Cryptography*, Springer International Publishing Cham, 2022, pp. 252–282.
- [7] A. Kothapalli, S. Setty, and I. Tzialla, “Nova: Recursive zero-knowledge arguments from folding schemes,” in *Annual International Cryptology Conference*, Springer, 2022, pp. 359–388.
- [8] I. Tzialla, A. Kothapalli, B. Parno, and S. Setty, “Transparency dictionaries with succinct proofs of correct operation,” in *NDSS 2022*, Apr. 2022.
- [9] A. Kothapalli and R. Mitchell, “Regex-based linkography abstraction refinement for information security,” in *Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics*, 2018, pp. 1–7.
- [10] A. Kothapalli, A. Miller, and N. Borisov, “Smartcast: An incentive compatible consensus protocol using smart contracts,” in *International Conference on Financial Cryptography and Data Security*, Springer International Publishing Cham, 2017, pp. 536–552.

## Professional Activities

---

**Program Committee**, 47th IEEE Symposium on Security and Privacy (Oakland) 2025

**Program Committee**, 45th Annual International Cryptology Conference (Crypto) 2025

### External Reviewer

Oakland 2023, Asiacrypt 2024, Crypto 2024, Oakland 2024, ITCS 2024, FC 2024, PKC 2024, ITC 2025, Eurocrypt 2025

## Research Funding Awards

---

**Research Fellowship**, Anaxi Labs – 130,000 USD 09/24-09/25

<b>Doctoral Fellowship</b> , Protocol Labs – 80,000 USD	08/22-05/24
<b>Illinois Cybersecurity Scholar</b> , National Science Foundation – 120,000 USD	08/16-05/18

### Selected Invited Talks

---

<i>Zero-Knowledge Folding Schemes</i> University of Illinois at Urbana-Champaign, Security and Privacy Seminar	August 2025
<i>Transformations on SNARKs from Recursion</i> UC Berkeley, Simons Institute Proofs Reading Group	July 2025
<i>Witness Encryption from Linearly Verifiable SNARKs and Applications</i> Eurocrypt 2025 2nd Workshop on Laconic Cryptography	May 2025
<i>Recursive Proofs of Knowledge</i> UC Berkeley, CS276 – Graduate Cryptography	November 2024
<i>NeutronNova: Folding Everything that Reduces to Zero-Check</i> UC Berkeley, Security Seminar	November 2024
	Bay Area Crypto Day November 2024
<i>Zero-Knowledge Folding Schemes</i> UC Berkeley, Theory Seminar	November 2024
<i>Recent Advancements in High-Performance Proof System Design</i> UC Berkeley, Cryptography Seminar	November 2024
<i>HyperNova: Recursive Arguments for Customizable Constraint Systems</i> Crypto 2024	August 2024
A16z	July 2024
Protocol Labs	May 2023
CMU Crypto Seminar	May 2023
<i>Algebraic Reductions of Knowledge</i> Crypto 2023	August 2023
CMU Crypto Seminar	December 2022
<i>SuperNova: Proving Universal Machine Executions without Universal Circuits</i> Delendum	March 2023
<i>Nova: Recursive Zero-Knowledge Arguments from Folding Schemes</i> Stanford University, Applied Cryptography Seminar	November 2022
Crypto 2022	August 2022
<i>Monadic Composition of Argument Systems</i> PLCrypt Workshop	August 2022

*Poppins: A Direct Construction for Asymptotically Optimal zkSNARKs*  
Protocol Labs

August 2019

*SmartCast: An Incentive Compatible Consensus Protocol Using Smart Contracts*  
FC 2017, First Workshop on Trusted Smart Contracts

April 2017