

Ashutosh Kumar

Curriculum Vitae

404 Westwood Plaza
Los Angeles, CA 90095
☎ +1 (310) 254 8257
✉ a@ashutoshk.com
🌐 www.ashutoshk.com

Publications

- 2018 *Non-Malleable Secret Sharing* - **STOC** 2018
Vipul Goyal and Ashutosh Kumar
- 2018 *Non-Malleable Secret Sharing for General Access Structures* - **CRYPTO** 2018
Vipul Goyal and Ashutosh Kumar
- 2018 *On the Price of Proactivizing Round-Optimal Perfectly Secret Message Transmission* - **IEEE Transactions on Information Theory** 2018 (Conference version in ICITS 2015)
Ravi Kishore, Ashutosh Kumar, Chiranjeevi V and Kannan Srinathan
- 2015 *Work Efficient Algorithms for Large Graph Exploration on Emerging Heterogeneous Architecture* - **Journal of Parallel and Distributed Computing** 2015
Dip S. Banerjee, Ashutosh Kumar, Meher Chaitanya, S. Sharma and Kishore Kothapalli

Manuscripts

- 2018 *Leakage-Resilient Secret Sharing*
Ashutosh Kumar, Raghu Meka and Amit Sahai
- 2018 *Non-Malleable Commitments from Non-Malleable Extractors*
Vipul Goyal, Ashutosh Kumar, Sunoo Park, Silas Richelson and Akshayaram Srinivasan

Education

- 2017 – **Ph.D. (MS Ongoing)**, COMPUTER SCIENCE, UCLA, GPA : 4.0/4.0.
Advisors: Prof. Rafail Ostrovsky and Prof. Amit Sahai
Awarded Dean's GSR Fellowship for year 2018-2019
- 2010 – 2014 **B.Tech.**, COMPUTER SCIENCE AND ENGINEERING, IIIT Hyderabad, GPA: 8.6/10.0 .
Undergraduate Research Award, Dean's List Award and Academic Distinction (top 15%)

Experience

- Summer 2018 **Research Intern**, MICROSOFT RESEARCH, India.
Mentor: Dr. Neeraj Kayal
- 2015 – 2017 **Research Fellow**, MICROSOFT RESEARCH, India.
Mentor: Prof. Vipul Goyal
- 2014 – 2015 **Software Engineer**, MICROSOFT, India.
- Summer 2013 **Software Engineering Intern**, GOOGLE, India.
- 2013 – 2014 **Teaching Assistant**, IIIT HYDERABAD.
Courses: Data Structures; IT Workshop

Talks

- 2018 *New Frontiers in Secret Sharing* - Southern California Theory Day
- 2018 *Non-Malleable Secret Sharing* - STOC 2018
- 2018 *Non-Malleable Secret Sharing* - Microsoft Research India

Professional Service

- 2016–2018 **External Reviewer**, STOC, CCC, CRYPTO, EUROCRYPT, JOURNAL OF CRYPTOLOGY, TCC, ASIACRYPT, FST&TCS, PKC, CANS.