Prashant Nalini Vasudevan

NUS Presidential Young Professor
Dept. of Computer Science
National University of Singapore

✉ *prashant@comp.nus.edu.sg*
www.comp.nus.edu.sg/~prashant

Employment

July 2021 – Present
Assistant Professor (NUS Presidential Young Professor)
Department of Computer Science
National University of Singapore

Sep 2018 – Apr 2021
Postdoctoral Researcher in EECS
University of California Berkeley
Host: Sanjam Garg

Education

Aug 2018
PhD in Computer Science
Massachusetts Institute of Technology
Thesis: Fine-Grained Cryptography
Advisor: Vinod Vaikuntanathan

Aug 2015
SM in Computer Science
Massachusetts Institute of Technology
Thesis: A Study of Efficient Secret Sharing
Advisor: Vinod Vaikuntanathan

May 2013
BTech in Computer Science and Engineering
Indian Institute of Technology Madras
Thesis: Determinantal Complexity Under Restrictions
Advisor: Jayalal Sarma

Professional Service

Program Committees
CRYPTO 2024, PKC 2024, TCC 2022, EUROCRYPT 2021, INDOCRYPT 2020, EUROCRYPT 2020, TCC 2019

Reviewing
FOCS, STOC, EUROCRYPT, CRYPTO, TCC, SODA, ICALP, ASIACRYPT, CCC, ITCS, INDOCRYPT, IEEE Transactions on Information Theory, Journal of Cryptology

Publications

CCS 2023 Control, Confidentiality, and the Right to be Forgotten
Aloni Cohen, Adam Smith, Marika Swanberg, and Prashant Nalini Vasudevan

CRYPTO 2022 Collision-Resistance from Multi-Collision-Resistance
Ron D. Rothblum, Prashant Nalini Vasudevan

PETS 2022 Deletion Inference, Reconstruction, and Compliance in Machine (Un)Learning
Ji Gao, Sanjam Garg, Mohammad Mahmoody, Prashant Nalini Vasudevan

EUROCRYPT 2021 Public-Coin Statistical Zero-Knowledge Batch Verification against Malicious Verifiers
Inbar Kaslasi, Ron D. Rothblum, Prashant Nalini Vasudevan

TCC 2020 Batch Verification for Statistical Zero Knowledge Proofs
Inbar Kaslasi, Guy N. Rothblum, Ron D. Rothblum, Adam Sealfon, Prashant Nalini Vasudevan

SCN 2020 Tight Verifiable Delay Functions
Nico Döttling, Sanjam Garg, Giulio Malavolta, Prashant Nalini Vasudevan

CRYPTO 2020 Nearly Optimal Robust Secret Sharing against Rushing Adversaries
Pasin Manurangsi, Akshayaram Srinivasan, Prashant Nalini Vasudevan

EUROCRYPT 2020 Formalizing Data Deletion in the Context of the Right to be Forgotten
Sanjam Garg, Shafi Goldwasser, Prashant Nalini Vasudevan

ITCS 2020 Cryptography from Information Loss
Marshall Ball, Elette Boyle, Akshay Degwekar, Apoorvaa Deshpande, Alon Rosen, Vinod Vaikuntanathan, Prashant Nalini Vasudevan

TCC 2019 Statistical Difference Beyond the Polarizing Regime
Itay Berman, Akshay Degwekar, Ron Rothblum, Prashant Nalini Vasudevan

CRYPTO 2019 Leakage Resilient Secret Sharing and Applications
Akshayaram Srinivasan, Prashant Nalini Vasudevan

ITCS 2019 Placing Conditional Disclosure of Secrets in the Communication Complexity Universe
Benny Applebaum, Prashant Nalini Vasudevan

SODA 2019 XOR Codes and Sparse Random Linear Equations with Noise
Andrej Bogdanov, Manuel Sabin, Prashant Nalini Vasudevan

CRYPTO 2018 From Laconic Zero-Knowledge to Public-Key Cryptography
Itay Berman, Akshay Degwekar, Ron Rothblum, Prashant Nalini Vasudevan

CRYPTO 2018 Proofs of Work from Worst-Case Assumptions
Marshall Ball, Alon Rosen, Manuel Sabin, Prashant Nalini Vasudevan

EUROCRYPT 2018 Multi Collision Resistant Hash Functions and their Applications
Itay Berman, Akshay Degwekar, Ron Rothblum, Prashant Nalini Vasudevan

FOCS 2017 On the Power of Statistical Zero Knowledge
Adam Bouland, Lijie Chen, Dhiraj Holden, Justin Thaler, Prashant Nalini Vasudevan
Invited to the special issue of SICOMP for FOCS 2017

CRYPTO 2017 Conditional Disclosure of Secrets: Amplification, Closure, Amortization, Lower-bounds, and Separations
Benny Applebaum, Barak Arkis, Pavel Raykov, Prashant Nalini Vasudevan

STOC 2017 Average-Case Fine-Grained Hardness
Marshall Ball, Alon Rosen, Manuel Sabin, Prashant Nalini Vasudevan

CCS 2016 Improvements to Secure Computation with Penalties
Ranjit Kumaresan, Vinod Vaikuntanathan, Prashant Nalini Vasudevan

CRYPTO 2016 Fine-Grained Cryptography
Akshay Degwekar, Vinod Vaikuntanathan, Prashant Nalini Vasudevan

ASIACRYPT 2015 Secret Sharing and Statistical Zero Knowledge
Vinod Vaikuntanathan, Prashant Nalini Vasudevan

Manuscripts

Control, Confidentiality, and the Right to be Forgotten
Aloni Cohen, Adam Smith, Marika Swanberg, Prashant Nalini Vasudevan
(Preliminary version presented at the UpML and TPDP workshops at ICML 2022)

Teaching

Aug-Dec 2022 CS3230: Design and Analysis of Algorithms
National University of Singapore

Aug-Dec 2021 CS6230: Topics in Information Security (Probabilistic Proof Systems)
National University of Singapore