Yashvanth Kondi

ykondi.net
✉ mail at ykondi.net

Research Interests

- Cryptography—Theoretical and Applied.
- Secure Multiparty Computation (MPC) and relevant techniques.
- Zero-knowledge Proofs.

Employment

Nov 2023–present **Principal Scientist**
Silence Laboratories (Employed by Deel).

June 2022–Sep 2023 **Postdoctoral Researcher**
Aarhus University, Denmark. Hosted by Claudio Orlandi.

June 2022–Sep 2023 **Scientific Advisor (Consultant)**
Silence Laboratories.

June 2020–Dec 2020 **PhD Research Intern**
Novi Research (Facebook).

Education

2022 **PhD in Computer Science**
Northeastern University, Boston
Advisor: abhi shelat
Thesis: *Practical Threshold Elliptic Curve Cryptography From Native Assumptions*

2017 **Integrated Master of Technology** (**Bachelor** and **Master**)
International Institute of Information Technology, Bangalore (IIIT-B)
Advisor: Ashish Choudhury
Thesis: *On the Authenticity of Garbling Schemes*
Awarded the Late N. Rama Rao Medal for Student of the Year

Publications

Note. With the exception of undergraduate publications [1,2] all author lists are ordered alphabetically, as is conventional in cryptography.

Manuscripts

[-] *Separating Broadcast from Cheater Identification*
In submission
Yashvanth Kondi, Divya Ravi

Journals

[J2] *Guaranteed Output in O(sqrt(n)) Rounds for Round-Robin Sampling Protocols*
Journal of Cryptology *(to appear)*
Ran Cohen, Jack Doerner, Yashvanth Kondi, abhi shelat

[J1] *Multiparty Generation of an RSA Modulus*
Journal of Cryptology, Vol. 35(2)
Megan Chen, Ran Cohen, Jack Doerner, Yashvanth Kondi, Eysa Lee, Schuyler Rosefield, abhi shelat

Conference Proceedings

[18] *Sometimes You Can't Distribute Random-Oracle-Based Proofs*
CRYPTO 2024
Jack Doerner, Yashvanth Kondi, Leah Namisa Rosenbloom

[17] *Secure Multiparty Computation with Identifiable Abort from Vindicating Release*
CRYPTO 2024
Ran Cohen, Jack Doerner, Yashvanth Kondi, abhi shelat

[16] *Threshold ECDSA in Three Rounds*
IEEE Symposium on Security and Privacy (Oakland) 2024
Jack Doerner, Yashvanth Kondi, Eysa Lee, abhi shelat

[15] *Two-Round Stateless Deterministic Two-Party Schnorr Signatures From Pseudorandom Correlation Functions*
CRYPTO 2023
Yashvanth Kondi, Claudio Orlandi, Lawrence Roy

[14] *Witness-Succinct Universally-Composable SNARKs*
EUROCRYPT 2023
Chaya Ganesh, Yashvanth Kondi, Claudio Orlandi, Mahak Pancholi, Akira Takahashi, Daniel Tschudi

[13] *Threshold BBS+ Signatures for Distributed Anonymous Credential Issuance*
IEEE Symposium on Security and Privacy (Oakland) 2023
Jack Doerner, Yashvanth Kondi, Eysa Lee, abhi shelat, LaKyah Tyner

[12] *Improved Straight-Line Extraction in the Random Oracle Model With Applications to Signature Aggregation*
ASIACRYPT 2022
Yashvanth Kondi, abhi shelat

[11] *Guaranteed Output in O(sqrt(n)) Rounds for Round-Robin Sampling Protocols*
EUROCRYPT 2022
Ran Cohen, Jack Doerner, Yashvanth Kondi, abhi shelat

[10] *Threshold Schnorr with Stateless Deterministic Signing from Standard Assumptions*
CRYPTO 2021
François Garillot, Yashvanth Kondi, Payman Mohassel, Valeria Nikolaenko

[9] *Refresh When You Wake Up: Proactive Threshold Wallets with Offline Devices*
IEEE Symposium on Security and Privacy (Oakland) 2021
Yashvanth Kondi, Bernardo Magri, Claudio Orlandi, Omer Shlomovits

[8] *Non-interactive half-aggregation of EdDSA and variants of Schnorr signatures*

Cryptographers' Track RSA Conference (CT-RSA) 2021
Konstantinos Chalkias, François Garillot, Yashvanth Kondi, Valeria Nikolaenko

[7] *Multiparty Generation of an RSA Modulus*
CRYPTO 2020
Megan Chen, Ran Cohen, Jack Doerner, Yashvanth Kondi, Eysa Lee, Schuyler Rosefield, abhi shelat

[6] *Threshold ECDSA from ECDSA Assumptions: The Multiparty Case*
IEEE Symposium on Security and Privacy (Oakland) 2019
Jack Doerner, Yashvanth Kondi, Eysa Lee, abhi shelat

[5] *Secure Two-party Threshold ECDSA from ECDSA Assumptions*
IEEE Symposium on Security and Privacy (Oakland) 2018
Jack Doerner, Yashvanth Kondi, Eysa Lee, abhi shelat

[4] *Efficient Adaptively Secure Zero-knowledge from Garbled Circuits*
Public Key Cryptography (PKC) 2018
Chaya Ganesh, Yashvanth Kondi, Arpita Patra, Pratik Sarkar

[3] *Privacy-Free Garbled Circuits for Formulas: Size Zero and Information-Theoretic*
CRYPTO 2017
Yashvanth Kondi, Arpita Patra

[2] *Analysis of a Coverstitched Stretch Sensor for Monitoring of Breathing*
International Conference on Sensing Technology (ICST) 2016
Raul I Ramos-Garcia, Fernanda Da Silva, Yashvanth Kondi, Edward Sazonov, Lucy E Dunne

[1] *An Interdisciplinary, Dialogic Approach to Develop an Electronic Device to Enhance Freedom and Mobility of Women in Public Spaces in the Indian Context - Illustrated by the Case of Convers[t]ation*
IEEE GHTC-SAS 2014
Yashvanth Kondi, Daksh Varshneya, Sruthi Krishnan, Madhav Rao

Activities

Supervision

- **Internship supervision** at Silence Laboratories:
  · Sriram Sridhar, PhD student at UC Berkeley (Summer 2024)
  · Nidhish Bhimrajka, Master's student at IIIT Bangalore (Spring 2024)
  · Supreeth Varadarajan, Master's student at IIIT Bangalore (Spring 2024)
- **Student supervision** at Aarhus University:
  · Mie Krogh, Jakob Lauritsen, and Tobias Duus, Bachelor's project (Ivan Damgård as primary supervisor, Spring 2023)

Service

Program Committees. Financial Cryptography 2025, TPMPC (2025, 2023), EUROCRYPT 2024.

External Conference Reviews. CRYPTO (2024, 2023, 2022, 2021, 2018), EUROCRYPT (2023, 2022, 2021, 2020, 2019, 2018), ACM CCS (2022), ASIACRYPT (2023, 2022, 2020, 2019, 2018, 2017), PODC (2021), PKC (2022, 2021, 2019, 2017), TCC (2023, 2020, 2019), ACNS (2023), CT-RSA (2022), SCN (2020)

Journal Reviews. Journal of Cryptology, IEEE Transactions on Information Forensics & Security

Organizing Committee. DeCompute Conference (2024, 2023), Information-Theoretic Cryptography Conference (ITC) 2023.

Talks

- *Separating Broadcast from Cheater Identification.*
  · Trust Lab Seminar, IIT Bombay (Mumbai)
- *Towards Practical MPC for Restaking: Separating Broadcast from Cheater Identification.*
  · DeCompute 2024 (Singapore)
- *Sometimes You Can't Distribute Random-Oracle-Based Proofs.*
  · CRYPTO 2024 (Santa Barbara)
  · Nordicrypt Summer 2023 (Aarhus)
- *Separating Broadcast from Cheater Identification: The ECDSA Case.*
  · Cryptography in the Blockchain Era Workshop (Bertinoro)
- *Verifiable Randomness and Threshold Signing.*
  · 3-Rand Web3 Randomness Workshop (Online)
- *Threshold ECDSA in Three Rounds.*
  · Theory and Practice of Multiparty Computation 2024 (Darmstadt)
  · IEEE Symposium on Security and Privacy 2024 (San Francisco)
  · Visa Research Seminar (Online)
  · Brown Cryptography Seminar (Providence)
  · DeCompute 2023 Conference (Singapore)
  · JP Morgan AlgoCRYPT Seminar (Online)
  · Aarhus Cryptography Seminar (Aarhus)
- *Threshold ECDSA with Identifiable Abort: The Case for Honest Majority.*
  · Encrypt London (London)
- *Two-Round Stateless Deterministic Two-Party Schnorr Signatures From Pseudorandom Correlation Functions.*
  · CRYPTO 2023 (Santa Barbara)
- *An Overview of Threshold ECDSA Signing Protocols.*
  · a16z Crypto Seminar (Online)
- *Composable Non-interactive Zero-knowledge Proofs in the Random Oracle Model.*
  · Chalmers University of Technology (Gothenburg)
- *Witness-Succinct Universally-Composable SNARKs.*
  · Technion (Haifa)
- *Improved Straightline Extraction in the Random Oracle Model.*
  · ASIACRYPT 2022 (Taipei)
  · Aarhus Crypto Summer Day 2022 (Aarhus)
- *Guaranteed Output in O(sqrt(n)) Rounds for Round-Robin Sampling Protocols.*
  · Theory and Practice of Multiparty Computation 2022 (Aarhus)
- *Threshold Schnorr with Stateless Deterministic Signing from Standard Assumptions.*
  · CRYPTO 2021 (Online)
  · NIST Workshop on Multi-Party Threshold Schemes 2020 (Online - short talk)
- *Practical Threshold Cryptography from Native Assumptions.* (papers [3,4,5,8])
  · IIIT Bangalore Samvaad (Online seminar)
- *Refresh When You Wake Up: Proactive Threshold Wallets with Offline Devices.*
  · IEEE Symposium on Security and Privacy 2021 (Online)

· Cornell Tech (Online)
· Theory and Practice of Blockchains 2020 (Online)

- *Non-interactive half-aggregation of EdDSA and variants of Schnorr signatures.*
  · Cryptographers' Track RSA Conference 2021 (Online)
- *Multiparty Generation of an RSA Modulus.*
  · CRYPTO 2020 (Online)
- *Threshold ECDSA from ECDSA Assumptions.*
  · DC Area Crypto Day (Washington DC)
  · BUSec Seminar (Boston University)
  · IEEE Symposium on Security and Privacy 2019 (San Francisco)
  · NIST Threshold Cryptography Workshop 2019 (Gaithersburg)
  · Aarhus Crypto Summer Day (Aarhus)
- *Efficient Adaptively Secure Zero-knowledge from Garbled Circuits.*
  · Public Key Cryptography 2018 (Rio De Janeiro)
- *Privacy-Free Garbled Circuits for Formulas: Size Zero and Information-Theoretic.*
  · CRYPTO 2017 (Santa Barbara)
  · New England Security Day 2017 (poster - Boston)
  · Northeastern Theory seminar (Boston)

Teaching (TA)

Fall 2020: CY 2550 Introduction to Cybersecurity at Northeastern University.
Fall 2016: CS/NC-716 Computing on Private Data at IIIT-Bangalore.