Yashvanth Kondi

ykondi.net

Areas of Interest

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

Employment

2022– Aarhus University, Denmark
Postdoctoral Researcher, hosted by Claudio Orlandi

Education

2022 Northeastern University, Boston
PhD in Computer Science at the Khoury College of Computer Sciences
Advisor: abhi shelat
Thesis: *Practical Threshold Elliptic Curve Cryptography From Native Assumptions*

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

Publications

With the exception of undergraduate publications (labelled [-] instead of numbered) all author lists are ordered alphabetically, as is conventional in cryptography.

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

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

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

[7] *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

[6] *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

[5] *Multiparty Generation of an RSA Modulus*
CRYPTO 2020 and Journal of Cryptology, Vol. 35(2)
Megan Chen, Ran Cohen, Jack Doerner, Yashvanth Kondi, Eysa Lee, Schuyler Rosefield, abhi shelat

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

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

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

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

[-] *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

[-] *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

Visits

June–Dec 2020	Novi Research (Facebook), hosted by Valeria Nikolaenko
May–Jul 2019	Aarhus Crypto Group, hosted by Claudio Orlandi
Jan 2016– June 2017	CrIS, Indian Institute of Science, hosted by Arpita Patra

External Reviews

Conferences. EUROCRYPT (2022, 2021, 2020, 2019, 2018), CRYPTO (2022, 2021, 2018), ACM CCS (2022, 2019), ASIACRYPT (2022, 2020, 2019, 2018, 2017), PODC (2021), PKC (2022, 2021, 2019, 2017), TCC (2020, 2019), CT-RSA (2022), SCN (2020)

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

Talks

- *Improved Straightline Extraction in the Random Oracle Model.*
  · Aarhus Crypto 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, MD)
  · 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.