ANASUYA ACHARYA

Postdoctoral Researcher at Aarhus University Interested in Cryptography

@ anasuyahirai@gmail.com +45 52742305 Aarhus, Denmark
in www.linkedin.com/in/anasuyaacharya anasuyaacharya.github.io/

PUBLICATIONS

Conference Proceedings

- Acharya, Anasuya, Karen Azari, Mirza Ahad Baig, Dennis Hofheinz, and Chethan Kamath (2025). "Securely Instantiating 'Half Gates' Garbling in the Standard Model". In: *PKC 2025, May 12-15, 2025*. Røros, Norway: Springer, pp. 37–75.
- Acharya, Anasuya, Karen Azari, and Chethan Kamath (2025). "On the Adaptive Security of Free-XOR-Based Garbling Schemes in the Plain Model". In: *EUROCRYPT 2025, May 4-8, 2025*. Madrid, Spain: Springer, pp. 214–244.
- Acharya, Anasuya, Carmit Hazay, Vladimir Kolesnikov, and Manoj Prabhakaran (2025). "Towards Building Efficient SCALES Protocols". In: *ASIACRYPT 2025, December 8-12, 2025*. Melbourne, Australia: Springer.
- Acharya, Anasuya, Carmit Hazay, and Muthuramakrishnan Venkitasubramaniam (2025). "On Achieving "Best-in-the-Multiverse" MPC". in: *TCC 2025, December 1-5, 2025*. Aarhus, Denmark: Springer.
- Acharya, Anasuya, Carmit Hazay, Vladimir Kolesnikov, and Manoj Prabhakaran (2024). "Malicious Security for SCALES - Outsourced Computation with Ephemeral Servers". In: *CRYPTO 2024, August 18-22, 2024*. Santa Barbara, USA: Springer, pp. 3–38.
- Acharya, Anasuya, Tomer Ashur, Efrat Cohen, Carmit Hazay, and Avishay Yanai (2023). "A New Approach to Garbled Circuits". In: *ACNS 2023, June 19-22*. Kyoto, Japan: Springer, pp. 611–641.
- Acharya, Anasuya, Carmit Hazay, Oxana Poburinnaya, and Muthuramakrishnan Venkitasubramaniam (2023). "Best of Both Worlds - Revisiting the Spymasters Double Agent Problem". In: *CRYPTO 2023, August 20-24, 2023*. Santa Barbara, USA: Springer, pp. 328–359.
- Acharya, Anasuya, Carmit Hazay, Vladimir Kolesnikov, and Manoj Prabhakaran (2022). "SCALES - MPC with Small Clients and Larger Ephemeral Servers". In: *TCC 2022, November 7-10, 2022*. Chicago, USA: Springer, pp. 502–531.
- Prabhakaran, Manoj M., Anasuya Acharya, and Akash Trehan (2019). "An Introduction to the CellTree Paradigm". In: *ICISS 2019, Volume 11952 LNCS, 16-20 December 2019*. Hyderabad, India: Springer.
- Sanyashi, Tikaram, Anasuya Acharya, and Bernard Menezes (2019). "Plaintext Recovery Attacks and their Mitigation in an Application Specific SHE Scheme". In: *PDCAT 2019, 5-7 December 2019*. Gold Coast, Australia: IEEE Xplorer.
- Patil, Vishwas, Anasuya Acharya, and R. K. Shyamasundar (2018). "Landcoin: A Land Management System using Litecoin Blockchain Protocol". In: *SDLT3 2018, 12 November 2018*. Gold Coast, Australia.

EDUCATION

Ph.D. in Computer Engineering

Bar Ilan University

July 2025 Ramat Gan, Israel

CGPA: 86.94 / 100

M.Tech. in Computer Science and Engineering (CSE)

IIT Bombay

July 2020 Mumbai, India

CGPA: 9.54 / 10

B.Tech. in CSE

NIT Trichy

May 2017 Tiruchirappalli, India

CGPA: 8.06 / 10

ACHIEVEMENTS

GATE (Graduate Aptitude Test for Engineering)
Score of 791 and AIR (All India Rank) 231 in the GATE Computer Science and Information Technology paper in February 2017

AP (Advanced Placement Exam)
Scored 3/5 in Physics C Mechanics, Computer Science A, Calculus AB in May 2012

AAT (National Award of Academic Aptitude and Achievement Test)
Scored 99 percentile in quantitative aptitude in May 2007

SOFTWARE SKILL SET

LaTeX | GIT | Linux(Ubuntu)

Java | C | C++ | SEBOL | JavaScript | Python | PHP | MATLAB

SERVICE

Workshops and Talks

- *Maliciously Secure SCALES Protocols* (2024). Cryptography in the Blockchain Era (CIBE) 2024, 23-27 June 2024, Bertinoro, Italy.
- *Maliciously Secure SCALES Protocols* (2024). Theory and Practice of Multi-Party Computation Workshop (TPMPC) 2024, 3-6 June 2024, TU Darmstadt, Germany.
- *SCALES: MPC with Small Clients and Larger Ephemeral Servers* (2023). ACE Conference (Algorand Centres of Excellence) 2023, 10-12 January 2023, Hotel Arts, Barcelona.
- *SCALES: MPC with Small Clients and Larger Ephemeral Servers* (2022). Theory and Practice of Multi-Party Computation Workshop (TPMPC) 2022, 7-10 June 2022, Aarhus University, Denmark.
- *CellTree: A new Paradigm for Distributed Data Repositories* (2019). Talk, 28 June 2019, IIT Bombay, Mumbai, India.

Organizing

- *39th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science* (2019). 11–13 December 2019, IIT Bombay, Mumbai, India.
- *ACM India Grad Cohort 2018* (2018). 6-7 July 2018, IIT Bombay, Mumbai, India.

EXPERIENCE

Research Assistant

Information Security Research and Development Center (ISRDC)

July 2017 – July 2020 | Mumbai, India

A three year scholarship student and Research Assistant in ISRDC, IITB.

IT Intern

Atreus Global

May – June 2016 | Jakarta, Indonesia

Java developer for SAP installation, integration and documentation.

Research Intern

Indian Statistical Institute

December 2015 – January 2016 | Kolkata, India

Research intern in cryptography under Prof. Shubhamoy Maitra, studying and attempting cryptanalysis of the RC4 stream cipher.

Systems Engineering Intern

P.T. Yokogawa Indonesia

May – June 2015 | Jakarta, Indonesia

Involved in installation project of DCS (Distributed Control Systems) in industrial production plants.

IT Intern

P.T. Indorama Synthetics

December 2014 – January 2015 | Purwakarta, Indonesia

Developer, tester and debugger for PHP based applications, and performed data analysis using Oracle BI.

LANGUAGES

English
Hindi
Bengali
Japanese
Mandarin
Bahasa Indonesia

EXTRA-CURRICULAR

JLPT N2
HSK 3
TEFL
BMC @ HMI

HOBBIES

Trekking | Learning Languages | Writing | Crash Coursing

REFEREES

Prof. Carmit Hazay

bar Ilan University

Ramat Gan, Israel
carmit.hazay@biu.ac.il
+972-3-738-4672
https://www.eng.biu.ac.il/hazay/
PhD Thesis Supervisor

Prof. Manoj M. Prabhakaran

IIT Bombay

Mumbai, India
mp@cse.iitb.ac.in
+91-22-2576-7709
www.cse.iitb.ac.in/~mp/
Masters Thesis Supervisor