Debajyoti Das

debajyoti.das@esat.kuleuven.be @tutaidas debajyotihotobhaga
https://dedas111.github.io/ orcid:0000-0002-6777-0566

Education

Aug 2015 – Aug 2021 **Ph.D.** Computer Science, Purdue University.
Thesis supervisor: Aniket Kate.
Thesis title: *Fundamental Constraints and Provably Secure Constructions of Anonymous Communication Protocols.*

Aug 2009 – May 2013 **Bachelor of Technology.** Computer Science and Engineering.
Indian Institute of Technology Hyderabad.

Work/Research Experience

Aug 2021 – · · · · **Postdoctoral Researcher,** COSIC research group, KU Leuven.
Supervisor: Claudia Diaz.

May 2018 – Aug 2018 **Research Intern,** Fujitsu Labs America.

July 2013 – July 2015 **Software Engineer.** Microsoft India Development Center, Hyderabad, India.

Teaching Experience

KU Leuven

Lecturer
- Privacy Technologies (2023-2024, 30 students)
- Privacy and Big Data (2022-2023, more than 300 students)

Teaching Assistant
- Privacy and Big Data (2021-2022), Privacy Technologies (2021-2022)

Guest Lectures
- Database Security and Access Control – Privacy and Big Data (2021-2022)
- Data Anonymization and Differential Privacy – Privacy Technologies (2022-2023)
- Anonymous Communication – Advanced Privacy Technologies (2022-2023)
- Introduction to Privacy – Cybersecurity Basics (2022-2023, 2023-2024)

Purdue University

Teaching Assistant
- Network Security (Spring 2020), Computer Security (Spring 2017, Fall 2016), Data Structure and Algorithms (Spring 2016), Programming in C (Fall 2015)

Guest Lectures
- Proof of Elapsed Time Consensus (Network Security, Spring 2019)
- Unix Access Control (Computer Security, Fall 2016)

Research Interests

My research goal centers around solving people-centric privacy problems and making privacy easily achievable for everyone. My research methodology takes a formal approach towards building privacy preserving systems. With a goal to achieve cryptography-like security guarantees, I take the following approach towards building privacy-preserving systems: (i) identify and propose security definitions that translates to strong privacy guarantees in practice based on rigorous theoretical analysis; (ii) analyze the fundamental requirements to achieve strong guarantees; (iii) based on those analyses, propose more efficient and scalable designs that are deployable in a real-world scenario, accompanied by a rigorous security analysis. My current research efforts attempt to solve problems related to following privacy related domains: (1) building and analyzing anonymous communication systems; (2) building privacy preserving techniques for storage and computation outsourcing based on FHE; (3) formal evaluation of censorship circumvent systems.

Research Publications

Preprints

1. K. Cong, D. Das, G. Nicolas, and J. Park, *Panacea: Non-interactive and stateless oblivious-ram*, Cryptology ePrint Archive, Paper 2023/274, https://eprint.iacr.org/2023/274.

2. D. Das, C. Diaz, A. Kiayias, and T. Zacharias, *Are continuous stop-and-go mixnets provably secure?* Cryptology ePrint Archive, Paper 2023/1311, https://eprint.iacr.org/2021/1685.

Published/accepted Papers

1. D. Das, S. Meiser, E. Mohammadi, and A. Kate, "Divide and funnel: A scaling technique for mix-networks," in *IEEE Computer Security Foundations Symposium (CSF)*, (to appear), 2024. URL: https://eprint.iacr.org/2021/1685.

2. I. B. Guirat, D. Das, and C. Diaz, "Blending different latency traffic with beta mixing," in *Proceedings on Privacy Enhancing Technologies (PETS)*, (to appear), 2024. URL: https://www.esat.kuleuven.be/cosic/publications/article-3681.pdf.

3. K. Cong, D. Das, J. Park, and H. V. Pereira, "Sortinghat: Efficient private decision tree evaluation via homomorphic encryption and transciphering," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2022, pp. 563–577. DOI: 10.1145/3548606.3560702.

4. D. Das, E. Mangipudi, and A. Kate, "Organ: Organizational anonymity with low latency," in *Proceedings on Privacy Enhancing Technologies (PETS)*, 2022, pp. 582–605. DOI: 10.56553/popets-2022-0087.

5. M. Bowman, D. Das, A. Mandal, and H. Montgomery, "On elapsed time consensus protocols," in *22nd International Conference on Cryptology in India (INDOCRYPT 2021)*, 2021, pp. 559–583. DOI: 10.1007/978-3-030-92518-5_25.

6. D. Das, S. Meiser, E. Mohammadi, and A. Kate, "Comprehensive anonymity trilemma: User coordination is not enough," in *Proceedings on Privacy Enhancing Technologies (PETS)*, 2020, pp. 356–383. DOI: 10.2478/popets-2020-0056.

7. D. Das, S. Meiser, E. Mohammadi, and A. Kate, "Anonymity trilemma: Strong anonymity, low bandwidth overhead, low latency - choose two," in *2018 IEEE Symposium on Security and Privacy (S&P)*, 2018, pp. 108–126. DOI: 10.1109/SP.2018.00011.

8. D. Chaum, D. Das, F. Javani, *et al.*, "Cmix: Mixing with minimal real-time asymmetric cryptographic operations," in *15th International Conference on Applied Cryptography and Network Security (ACNS)*, 2017. DOI: 10.1007/978-3-319-61204-1_28.

Other Relevant Experiences

Academic Service

PC Member	IEEE S&P 2024, PETS 2024, ACM CCS 2023, Annual Privacy Forum 2023.
External Reviewer	Eurocrypt 2024, IEEE S&P 2023, ESORICS 2023, PETS 2023 and 2022, ACM CCS 2022, Africacrypt 2022, Eurocrypt 2021, ACM TOPS 2021, STOC 2019.

Invited/Workshop Talks

Feb 2023	Karlsruhe Institute of Technology, Karlsruhe, Germany. OrgAn: Organizational anonymity with low latency.
Nov 2022	Visa Research Security Seminar, Palo Alto, USA. SortingHat: efficient private decision tree evaluation via homomorphic encryption and transciphering.

Other Relevant Experiences (continued)

Sep 2022 — Univeristy of Luebeck, Luebeck, Germany.
OrgAn: Organizational anonymity with low latency.

Jun 2020 — FCC workshop (affiliated with CSF), Virtual.
Anonymity Trilemma: not all is lost for anonymity, but quite a lot is.

Jul 2019 — HotPETS, Stockholm, Sweden.
Not all is lost for anonymity, but quite a lot is.

Apr 2018 — CERIAS Security Seminar, West Lafayette, USA.
Anonymity Trilemma: strong anonymity, low bandwidth overhead, low latency — choose two.

Supervised Theses

Jan 2022 – Jun 2022 — Bachelor's thesis: Olaf Bernhardt. (co-supervised with Esfandiar Mohammadi).
topic: *Split-Streams - Improving on a scalable mixnet functionality*.

Jan 2023 – June 2023 — Master's thesis: Tamalika Ghosh. (co-supervised with Jeongeun Park and Kelong Cong).
topic: *Privacy preserving storage and computation based on FHE*.

Sep 2023 – · · · · — Master's thesis: Oscar Perez Castillo. (co-supervised with Iness Ben Guirat and Lennart Oldenburg).
topic: *Multi-party routing for mixnets*.

PhD students mentored

- Iness Ben Guirat
- Kelong Cong
- Georgio Nicolas

Member on Examination Committee

Nov 2022 – April 2023 — Alex Ternav (Master's thesis, KU Leuven).