Debajyoti Das

debajyoti.das@esat.kuleuven.be @tutaidas debajyotihotobhaga
https://dedas111.github.io/

Education

- 2015 – 2021 **Ph.D.** Computer Science, Purdue University.
  Thesis supervisor: Aniket Kate.
  Thesis title: *Fundamental Constraints and Provably Secure Constructions of Anonymous Communication Protocols.*
- 2009 – 2013 **B.Tech.** Computer Science and Engineering, Indian Institute of Technology Hyderabad.

Work/Research Experience

- 2021 – · · · · **Postdoctoral Researcher,** COSIC research group, KU Leuven.
  Supervisor: Claudia Diaz.
- 2018 – 2018 **Summer Research Intern,** Fujitsu Labs America.
- 2015 – 2021 **Teaching/Research Assistant,** Department of Computer Science, Purdue University.
- 2013 – 2015 **Software Engineer.** Microsoft India Development Center, Hyderabad, India.
- 2012 – 2012 **Summer Research Intern.** TCS Innovation Labs, Gurgaon, India.

Research Interests

My research interests lie in the intersection of privacy and applied cryptography. My aim is to design, build, and deploy scalable privacy preserving systems based on cryptographic techniques. My current research projects focus on (i) analyzing fundamental constraints for annonymous communication (AC) systems to achieve provable anonymity, (ii) building provably secure, fast and scalable AC protocols, (iii) building efficient privacy preserving storage and computation oursourcing solutions.

Teaching Experience

KU Leuven

- 2022 – 2023 **Lecturer.** Privacy and Big Data.
- 2021 – 2022 **Teaching Assistant.** Privacy and Big Data, Privacy Technologies. Also taught the lecture on Database Security in the course Privacy and Big Data.

Purdue University

- 2015 – 2021 **Teaching Assistant.** Network Security (Spring 2020), Computer Security (Spring 2017, Fall 2016), Data Structure and Algorithms (Spring 2016), Programming in C (Fall 2015).

Other Relevant Experiences

Academic Service

- Member of the technical program committee for ACM CCS 2023.
- Member of the program committee for Annual Privacy Forum 2023.
- Reviewer for STOC 2019, Eurocrypt 2021, ACM TOPS 2021, Africacrypt 2022, PETS 2022 and 2023, ACM CCS 2022.

Other Relevant Experiences (continued)

Invited Talks

2022
- **Visa Research Security Seminar, Palo Alto, USA**. SortingHat: efficient private decision tree evaluation via homomorphic encryption and transciphering.
- **PoPETS, Sydney, Austrailia**. OrgAn: Organizational anonymity with low latency.

2020
- **PoPETS, Virtual Conference**. Comprehensive Anonymity Trilemma: User Coordination is not enough.
- **FCC workshop (affiliated with CSF), Virtual**. Anonymity Trilemma: not all is lost for anonymity, but quite a lot is.

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

2018
- **IEEE S&P, San Francisco, USA.** Anonymity Trilemma: strong anonymity, low bandwidth overhead, low latency – choose two.
- **CERIAS Security Seminar, West Lafayette, USA.** Anonymity Trilemma: strong anonymity, low bandwidth overhead, low latency – choose two.

Research Publications

1. K. Cong, D. Das, G. Nicolas, and J. Park, *Panacea: Non-interactive and stateless oblivious-ram*, Under submission.
2. D. Das, S. Meiser, E. Mohammadi, and A. Kate, *Divide and funnel: A scaling technique for mix-networks*, Cryptology ePrint Archive, Paper 2021/1685, `https://eprint.iacr.org/2021/1685`. URL: `https://eprint.iacr.org/2021/1685`.
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," *Proceedings on Privacy Enhancing Technologies*, vol. 2022, pp. 582–605, Jul. 2022. 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, "Fundamental constraints and provably secure constructions of anonymous communication protocols," Ph.D. dissertation, Purdue University Graduate School, 2021.
7. D. Das, S. Meiser, E. Mohammadi, and A. Kate, "Comprehensive anonymity trilemma: User coordination is not enough," *Proceedings on Privacy Enhancing Technologies*, vol. 2020, pp. 356–383, Jul. 2020. DOI: `10.2478/popets-2020-0056`.
8. 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`.
9. D. Chaum, D. Das, F. Javani, *et al.*, "Cmix: Mixing with minimal real-time asymmetric cryptographic operations," in *ACNS*, 2017. DOI: `10.1007/978-3-319-61204-1_28`.