Debajyoti Das
Department of Computer Science das48@purdue.edu
Purdue University +1-7654073262

EDUCATION

- **Purdue University** *West Lafayette, USA*
  PhD student, Department of Computer Science, Freedom Research Lab. *Aug 2015 – present*
  thesis title: Fundamental Constraints and Optimal Constructions of Anonymous Communication Protocols.
- **Indian Institute of Technology Hyderabad** *Hyderabad, India*
  Bachelor of Technology *Aug 2009 – May 2013*

RESEARCH INTERESTS

My research interests lie at the intersection of cryptography and privacy. I design, implement and analyze privacy-preserving systems. My current work focuses on analyzing the fundamental constraints of anonymous communication protocols. The aim is to guide the research community towards techniques that can provide an optimal tradeoff between anonymity and the overhead required to achieve that anonymity.

SELECTED PROJECTS

1. **Security and Performance Analysis of Permissioned Blockchains** *June 2018 – Present*
   This work analyzes the security and performance guarantees of permissioned blockchains. More specifically, we aim to analyze “Proof of Elapsed Time” protocol and propose improvements on the existing protocol. Results are currently under submission.
2. **Anonymity Trilemma** *May 2016 - Present*
   This work analyzes the fundamental lower bounds on anonymous communication protocols in terms of latency and bandwidth overheads. The aim is to confirm the commonly believed trilemma that an anonymous communication protocol can only achieve two out of the following three properties: low bandwidth overhead, low latency overhead and strong anonymity. Results published at IEEE S&P 2018 and PETS 2020.
3. **Building Efficient Anonymous Communication Protocols** *December 2015 – Present*
   This work aims at providing efficient anonymous communication protocols without compromising anonymity guarantees. We explored the path of eliminating expensive real-time operations, by having a precomputation phase; and we proposed "cMix" protocol. The results were published at ACNS 2017.
   Now we are working on building a protocol that provides strong anonymity and has a latency and bandwidth overhead as close as possible to the bounds indicated by the Trilemma work.

RESEARCH/WORK EXPERIENCE

- **Summer Research Intern at Fujitsu Labs America** *June 2018 – August 2018*
  I worked on analyzing the security of permissioned blockchains. More specifically, I worked on analyzing the security and performance guarantees of “Proof of Elapsed Time” protocol (a blockchain implementation using Intel SGX as Trusted Execution Environment).
- **Graduate Research Assistant at Purdue University** *May 2017 – Present*
  I am working as a research assistant under Prof. Aniket Kate in the Freedom Research Lab at Purdue University, West Lafayette campus.

- **Software Developer at Microsoft Corporation, India Development Center** *July 2013 – July 2015*
  DIVISION: Visual Studio
- **Summer Internship at TCS Innovation Labs, Gurgaon, India** *May 2012 – July 2012*
  I worked as a team member in the text mining team. I worked on the project **Collecting User Details for search Applications**. To provide the user more customized search, the activities (search queries, visited links etc.) of all users are collected and analyzed in this project.

TEACHING EXPERIENCE

- **Graduate Teaching Assistant at Purdue University:**
  - CS52800 (Network Security) – Spring 2020
  - CS42600 (Computer Security) – Fall 2016, Spring 2017
  - CS25100 (Data Structures and Algorithms) – Spring 2016
  - CS24000 (Programming in C) – Fall 2015

SELECTED PUBLICATIONS

1. Mic Bowman, *Debajyoti Das*, Avradip Mandal, Hart Montgomery: "**On Elapsed Time Consensus Protocols.**" *Currently under submission*.
2. *Debajyoti Das*, Sebastian Meiser, Esfandiar Mohammadi, Aniket Kate: "**Comprehensive Anonymity Trilemma: User Coordination is not enough**." *20th Privacy Enhancing Technologies Symposium, 2020.*
3. *Debajyoti Das*, Sebastian Meiser, Esfandiar Mohammadi, Aniket Kate: "**Anonymity Trilemma: Strong Anonymity, Low Bandwidth, Low Latency – Choose Two**." *39th IEEE Symposium on Security and Privacy, 2018.*
4. David Chaum, *Debajyoti Das*, Farid Javani, Aniket Kate, Anna Krasnova, Joeri de Ruiter, and Alan T. Sherman: "**cMix: Mixing with Minimal Real-Time Asymmetric Cryptographic Operations**." *15th International Conference on Applied Cryptography and Network Security, 2017.*

TALKS/PRESENTATIONS

- *PoPETS 2020*. Virtual Conference.
  Comprehensive Anonymity Trilemma: User Coordination is not enough.
- FCC 2020. Virtual Conference.
  Anonymity Trilemma: not all is lost for anonymity, but quite a lot is.
- *HotPETs 2019.* Stockholm, Sweden.
  Not all is lost for anonymity – but quite a lot is.
- *IEEE S&P (Oakland) 2018*. San Francisco, USA.
  Anonymity Trilemma: Strong Anonymity, Low Bandwidth, Low Latency – Choose Two.
- *CERIAS Security Seminar 2018*. West Lafayette, USA.
  Anonymity Trilemma: Strong Anonymity, Low Bandwidth, Low Latency – Choose Two.

ACADEMIC SERVICE

- External Reviewer at Eurocrypt 2021.
- External Reviewer at STOC 2019.