Siddharth Agarwal

Contact Information

Lab 320,
Department of Computer Science and Automation
Indian Institute of Science
Bengaluru, Karnataka, India
Pin - 560012

Phone: +91 8630441276
E-mail: siddharthaga@iisc.ac.in
Linkedin Profile
Personal Website

Research Interests

Foundations of Cryptography, Secure Multiparty Computation, Interactive Proof Systems, Privacy and Security

Education

Indian Institute of Science, Bengaluru, Karnataka, India

MTech(Res), Computer Science and Automation **Aug 2021 - present**
Co-Advisors: Dr. Chaya Ganesh(homepage) and Dr. Bhavana Kanukurthi(homepage)
GPA: 9/10

Birla Institute of Technology & Sciences, Pilani, Rajasthan, India

B.E.(Hons) Computer Science **Aug 2014 - May 2018**
GPA: 8.3/10
Thesis Advisor: Dr. Jennifer J. Ranjani(homepage)
Thesis Topic: A Medical Integrity Verification Algorithm for IoT Applications

Academic Experience

Indian Institute of Science, Bengaluru, Karnataka, India
Graduate Student **Aug 2021 - present**
Worked with **Prof. Bhavana Kanukurthi** and **Prof. Chaya Ganesh** to propose new definitions and practically efficient constructions for **Rational Secure Computation** where the parties evaluate a function in a secure manner such that no information about the other party's input is revealed except the output of the protocol. In this security model, the parties involved in the computation are rational and have well-defined utility functions.

Birla Institute of Technology & Sciences, Pilani, Rajasthan, India
Undergraduate Student **Jan 2018 - May 2018**
Worked with Prof. Jennifer J. Ranjani on a **lossy Watermarking Algorithm** for medical images, where the signature is embedded into the medical image and the receiver can extract the original image and signature from the embedded image such that differences between the extracted image and the original image are imperceptible to the human eye. The extracted signature is used to verify the image authenticity.

Teaching Assistant **August, 2016 - Dec 2016**
Teaching assistant for the course on Data Structure and Algorithms. Duties at various times have included office hours and leading weekly computer lab exercises.

Publications

Siddharth Agarwal and J. Jennifer Ranjani. **Image Integrity Verification via Reversible Predictive Hiding and Elliptic Curve Diffie-Hellman**. International Journal of Innovative Computing and Applications 10, no. 3-4 (2019): 154-163. (link)

Papers in Submission

Siddharth Agarwal, Chaya Ganesh and Bhavana Kanukurthi. **Rational Secure Computation: New Definitions and Constructions**. Submitted to *EUROCRYPT 2024*

Professional Experience

Media.Net, Mumbai, Maharashtra, India

Platform Engineer **July 2018 - July 2021**

Part of Auto Optimisation team in Media.Net. This team is responsible for real-time bidding in *Programatic Advertising* with the goal of optimizing revenue for advertisers and publishers. My role in the team was to design Machine Learning models for accurate predictions of click-through and conversion rates for ad impressions and an API used to fetch predictions for each ad impression.

Academic Services • **Reviewer** for *CSCML 2022* and *TCC 2023*