☎ +91-9800138769
✉ yash.shrivastava@iitkgp.ac.in

Yash Shrivastava

Fourth Year Undergraduate
Computer Science and Engineering

A-211, LBS Hall of Residence
IIT Kharagpur, West Bengal
India - 721302

Publications

- *Provably Secure Key-Aggregate Cryptosystems with Broadcast Aggregate Keys for Online Data Sharing on the Cloud.* Sikhar Patranbis, **Yash Shrivastava**, Debdeep Mukhopadhyay. Accepted in IEEE Transactions on Computers **(TC)**.
- *Parsimonious design strategy for linear layers with high diffusion in block ciphers*. Sikhar Patranbis, Debapriya Basu Roy, **Yash Shrivastava**, Debdeep Mukhopadhyay, Santosh Ghosh. In IEEE International Symposium on Hardware Oriented Security and Trust**(HOST)**, May 2016.
- *Dynamic Key-Aggregate Cryptosystem on Elliptic Curves for Online Data Sharing*. Sikhar Patranbis, **Yash Shrivastava**, Debdeep Mukhopadhyay. In the International Conference on Cryptology in India **(Indocrypt)**, December 2015.

Experience

Apr 2015 - Present

Undergraduate Student — Secure Embedded Architecture Laboratory (SEAL)

Guide: **Dr. Debdeep Mukhopadhyay** — *IIT Kharagpur*

- Worked in the fields of **Key Aggregate Cryptosystems**, **Pairing Based Cryptography**, **Searchable Encryption and Block Ciphers**.
- Proposed and developed scheme for **Two-tier Dynamic Key-Aggregate Cryptosystem** for online data sharing and extended the scheme by incorporating **Aggregate-Key Broadcasting** *(along with a PhD student).*
- Analysed these schemes and explored tradeoffs between runtime, space requirements, scalability and the level of security they provide.
- Implemented the block cipher **PRIDE**, and modified its linear layer to one with parsimonious design strategy.
- Developed program for **Efficient Implementation of Tate-Pairing over Barreto-Naehrig Curves** in C++ using GMP.

May 2016 - July 2016

Research Intern — Big Data Experience Lab (BEL)

Mentor: **Ritwik Sinha** — *Adobe Systems Pvt. Ltd. | Bangalore, India*

- Worked on a project titled "**Enhancing Display Ad Buying**".
- Built a pipelined workflow for forecasting the potential audience size *(number of bid requests and impressions)* and the average cost per impressions. Filed a **patent** application over the same.
- Worked in a team to develop **Big Data Analytics** algorithms efficiently extract and analyse data of Adobe Media Optimizer stored in **Hadoop** cluster.
- Was offered a **full-time position** at Adobe.

May 2015 - July 2015

Software Development Intern — National Digital Library of India

Guide: **Dr. Sandip Chakraborty** — *IIT Kharagpur*

- Developed a **log-in setup** having **role-based access** for NDL portal along with Google Sign-In and secured it against SQL injection and brute force attacks.
- Designed the **PostgreSQL** database schema to store user's details and social activities.

Jan 2014 - Apr 2015

Software Team Member — Autonomous Ground Vehicle Research Group (AGV)

Mentor: **Prof. Debasis Chakraborty** — *IIT Kharagpur*

- Part of the team that designed Eklavya 3.0 (2014) and Eklavya 4.0 (2015), and participated in **Intelligent Ground Vehicle Competition (IGVC)**, held at Oakland University, Michigan.
- Worked on the **motion planning** module, which utilized the terrain map and vehicle location, obtained from sensors (LIDAR, camera, GPS etc.), to plan an optimum path for GPS waypoint navigation and lane navigation.

Academic Projects

July 2015 - Nov 2016

Named Entity Recognition for Twitter with Entity Linking — **Course: Machine Learning**

Guide: **Prof. Pabitra Mitra** — *IIT Kharagpur*

- Developed a Machine Learning based framework for Named Entity Extraction and Recognition *(person, movie, organization, geo-location)* on Twitter.
- Incorporated **entity linking** in the framework to improve disambiguation between entities. Extracted entities were linked to respective articles/categories from DBpedia and Wikipedia using TAGME tool.
- Prepared a dataset of 3000+ tweets with hand annonated entities to be used as gold-standard.

July 2016 - Ongoing

Back to the Roots **Course: Natural Language Processing**

Mentor: **Prof. Pawan Goyal** *IIT Kharagpur*

- Designed a pipeline work-flow for extracting the source word, affix and the sense that affix conveys from a given derived word.
- Developed a **crawler** for Wiktionary to extract gold-standard for source word-derived word pairs along with word's senses.
- Used **k-means clustering** from SciPy and **label propagation algorithm** from Junto to infer the sense of affix from a derived word.

Jan 2015 - Apr 2015

Twitter Analysis using Spark **Course: Database Management System**

Mentor: **Prof. Pabitra Mitra** *IIT Kharagpur*

- Analysed popular **hashtags**, **mentions** etc. by forming hashtag clusters and mention clusters and provided APIs for researchers to use them.
- Integrated **Twitter Streaming API** with **Apache-Spark** and designed efficient ways to store and access data using **PyMongo** and **MongoDB**.

Programming Skills

Proficient	C, C++, Python
Competent	Java, R, Verilog HDL, Assembly, LaTeX
Familiar	C#, PHP

Technical Interests

Cryptography ● Network Security ● Hardware Security ● Robotics ● Data Analytics ● Software Development

Education

2013 - 2018

Indian Institute of Technology Kharagpur **CGPA: 8.73/10 (Till 6th Sem.)**

Integrated Dual Degree (B.Tech + M.Tech) *Kharagpur, India*

2013

Shiv Jyoti Convent School **CGPA: Marks: 92.6% (Overall), 94% (PCM)**

AISCE | Class 12th, CBSE *Kota, India*

2011

St. Thomas Sr. Sec. School **CGPA: 10/10 (School Topper)**

AISSE | Class 10th, CBSE *Mandasaur, India*

Relevant Coursework

(T)heory and (L)aboratory

- Programming and Data Structures (T/L)
- Discrete Structures (T)
- Algorithms - I (T/L)
- Signals and Networks (T/L)
- Switching Circuits (T/L)
- Formal Languages and Automata Theory (T)
- Software Engineering (T/L)
- **Comutational Number Theory (T)**
- Compilers (T/L)
- Computer Organization and Architecture (T/L)
- **Cryptography and Network Security** (T)
- Operating Systems (T/L)
- **Computer Networks (T/L)**
- **Database Management Systems (T/L)**
- **Hardware Security (T)**
- **Machine Learning (T)**
- Natural Language Processing (T)
- Artficial Intelligence (T)
- Theory of Computation (T)
- **Parallel and Distributed Algorithms (T)**

Academic Achievements

- Secured All India Rank 331 **(top 99.8 percentile)** in JEE Advanced 2013.
- One of the 300 **(top 99 percentile)** students selected for National Chemistry Olympiad, 2013.
- Secured a rank of **492** for KVPY fellowship 2013.

Extracurricular Activities

- Part of the team that stood **first** in Software Development during **Inter IIT Tech Meet**, 2016.
- **Senior Editor** at Technology Literary Society, IIT Kharagpur. Was the **Governor** of the society during academic year 2015-16.
- **Student Mentor** at Student Welfare Group, IIT Kharagpur since 2015.