

SHREYA SHARMA

Senior Undergraduate Student at IIT (BHU) Varanasi

@ shreyas.cd.ece17@iitbhu.ac.in

github.com/shreya-28

EDUCATION

Present | Indian Institute of Technology (BHU) Varanasi, India
May 2017 | Department of Electronics Engineering
B.TECH., CURRENT GPA: 9.55/10

PUBLICATIONS

- **Secure and Efficient Federated Transfer Learning**
Shreya Sharma, Choping Xing, Yang Liu, Yan Kang
In IEEE International Conference on Big Data (IEEE - Bigdata'19), Los Angeles, USA. [Link to Paper](#)
- **Privacy-Preserving Deep Learning with SPDZ**
Shreya Sharma, Chaoping Xing, Yang Liu
In Privacy-Preserving Artificial Intelligence (PPAI-20),
Association for the Advancement of Artificial Intelligence Conference (AAAI-20), New York, USA. [Link to Paper](#)

B.TECH. THESIS

Present | **Secure Computation using Silent Preprocessing**
Dec 2019 | Supervisors: [Prof. K. K. Shukla](#) and [Prof. Thomas Schneider](#)
Theme: Generating useful multi-party correlations in the semi-honest setting based on Silent Preprocessing for reduced communication cost.

- Contributing to a scalable high-performance C++ framework for secure multi-party computation (MPC) by ENCRYPTO Group, TU Darmstadt, Germany.
- Analyzing linear-time encodable codes to securely obtain pseudorandom encoded values with a low computational overhead.
- Completed an INTERNSHIP in [Prof. Schneider](#)'s research group ENCRYPTO from April to July, 2020.

RESEARCH EXPERIENCE

Oct 2019 | **Secure Federated Transfer Learning** | REMOTE INTERNSHIP
Aug 2019 | Webank, Shenzhen, China
Supervisor: [Dr. Yang Liu](#) and [Prof. Chaoping Xing](#)

- Designed and implemented a new algorithm for efficiently incorporating Secret Sharing in a federated-system that securely predicts labels for target-domain autoencoder in semi-honest and malicious setting. [Link to Paper](#)
- Achieved 40x improvement in runtimes over prior works.

Jul 2019 | **Privacy-Preserving Deep Learning via SPDZ** | INTERNSHIP
May 2019 | Nanyang Technological University (NTU), Singapore
Supervisor: [Prof. Chaoping Xing](#)

- Used specialized non-linear protocols to efficiently evaluate activation functions like ReLU and sigmoid in two-power rings without loss of accuracy.
- Employed this approach on neural nets for the first time. [Link to Paper](#)

Mar 2019 | **Design of Algebraic Pseudorandom Functions (PRF)** | REMOTE INTERNSHIP
Jan 2019 | Bar Ilan University, Israel
Supervisor: [Prof. Carmit Hazay](#)

- Overcame the challenge of retrieving output from the exponent by designing a novel PRF based on a group structure that allowed for efficient solving of the discrete-log problem.
- Proved a security reduction of this PRF to the DCRA assumption in this group. [Link to Manuscript](#)

Jul 2019 | **Implementing Secure-ML** | INDEPENDENT PROJECT
Dec 2018 | Indian Institute of Technology (BHU) Varanasi
➤ C++ implementation for secure distributed image-classification on joint-data from multiple-parties based on IEEE S&P paper by the same name. [Link to Repository](#)

COURSE PROJECTS

Present Aug 2020	Transliteration for Indian Languages NATURAL LANGUAGE PROCESSING Discerning the problem of transliteration as a machine translation model using statistical methods.
Jul 2020 April 2020	Federated Learning for Classification Task DATA STRUCTURES Implemented decision tree model for classification on joint-data from multiple clients without sharing raw-information using federated learning. Awarded A* grade signifying outstanding performance in the course.
May 2020 Jan 2020	Deep Networks with Internal Selective Attention through Feedback Connections DATA STRUCTURES Explored Deep Attention Selective Network (dasNet) by reproducing the model from state-of-the-art work for breast-cancer classification problem.
March 2020 Jan 2020	VLSI-realisation of Cryptographic Processor MICROPROCESSORS Designed Application Specific Instruction Set Processor (ASIP) for cryptographic applications. Implemented RISC-based ASIP using synthesizable structural verilog.

TECHNICAL SKILLS

Languages	C++, C, Python, Java, Verilog, HTML/CSS, Bash, Latex
Frameworks	Google-Flat Buffers, MP-SPDZ, ABY, FATE, Pytorch, EMP-Toolkit, GNU, GMP, PARI
MOOCs	Cryptography, Networks , Computer Architecture, Operating Systems, Parallel Computing, Algorithms , Discrete Maths

ACHIEVEMENTS & CO-CURRICULAR ACTIVITIES

- > Secured a rank in the **top 1%** of 170,000 applicants in JEE Advanced 2017.
- > Awarded the **DAAD WISE** scholarship in 2020 to pursue summer research internship in Germany
- > Attended **AAAI-20** to present work at PPAI-20 held in conjunction with the conference.
- > Awarded **Google Grace Hopper Celebration Scholarship** to attend GHC 2020.
- > Awarded the **SPARK** research fellowship by IIT Roorkee in 2019.
- > Active member of the global female network **Google - WomenTechmakers** which advocates for gender equality in tech.
- > **Co-ordinator of Spybits**, the annual event on Cyber-security for the Electronics Department, IIT (BHU) Varanasi.
- > **Conducted workshops** teaching cryptography to as a member of Club of Programmers, IIT (BHU) Varanasi.
- > **Content writer for the Literary Club**, guided numerous freshers on writing a verse.
- > **Volunteer work** for [Kashi Utkarsh](#) (Sep 2017 - Present):
 - > Teach elementary level curriculum to local under-privileged children on a weekly basis.
 - > Part of multiple street-plays for raising awareness against issues like smoking in rural neighbourhoods of Varanasi.
 - > Involved in organizing awareness rallies and medical camps for free health check-ups of the poor.