KANAV GUPTA

Cryptology Researcher interested in Secure MPC

@ kanav0610@gmail.com Roorkee, India @kanavgupta99 github.com/kanav99

EDUCATION

Bachelor of Technology

Indian Institute of Technology, Roorkee

July 2017 – May 2021

Major in Computer Science and Engineering
Cumulative GPA : 9.04/10

EXPERIENCES

Research Fellow

Microsoft Research India

July 2021 – Present Bangalore, India

- Part of the team EzPC under the guidance of Dr. Divya Gupta and Dr. Nishanth Chandran.

Internship - SafeNetwork

MaidSafe

Feb 2021 – May 2021 New Delhi, India

- Worked on improving and securing the Self Encryption in the Distributed Network "SafeNetwork"
- Helped in test runs of Safe Network by fixing CLI options and issues faced by users during public testing.

Cryptography Research Assistant

Simula UiB

Sep 2020 – Dec 2020 Bergen, Norway

- Studying Shortest Vector Problem(SVP) in Lattice based cryptography.
- Developing new algorithms for faster lattice enumeration using Obtuse Bases
- Tuning Sieving algorithms like SimHash, GaussSieve for speed using different tricks.

Google Summer of Code 2019

The Julia Language

May 2019 – Aug 2019 Roorkee,India

- Participated in GSoC 2019 with JuliaDiffEq, an organization devoted towards developing the package DifferentialEquations.jl. This package solves most forms of the differential equations in the most optimal way.
- Worked on project "Performance and General Fixes" to develop a toolkit to support the inclusion of different kinds of algorithms in a very optimal way.
- Mentored by Dr. Christopher Rackauckas and Yingbo Ma
- Project Link: GSoC Page

RESEARCH INTERESTS

- Secure Multi Party Computation
- Post Quantum Cryptography
- Side Channel Attacks
- Lightweight Cryptography
- Security in Embedded Systems

CTF PROFILE

- I like to solve Cryptography and Reverse Engineering challenges.
- Bronze medal in NSUCRYPTO Olympiad 2020
- Winner of CSAW Embedded Security Challenge 2020 in India Region and 2nd runner up globally.
- Winner of GitHub Java CTF CodeQL and Chill
- Participated in CCTNS Bug Bounty, organized by Cyber Peace Foundation and National Crime Records Bureau, India
- Placed 5 in CSAW 2019 CTF Final round - India as a part of team SDSLabs at IIT Kanpur
- Placed 12 in CSAW 2018 CTF Qualification Round - India as a part of Team SDSLabs.
- Placed 3 in Brainwaves Hackathon - Cyber Security organized by Société Générale, Banglore
- Winner of SecCon CTF 2019 hosted by Cisco India
- Organizer of BackdoorCTF 2019. Made a couple of challenges.

ACHIEVEMENTS

- Winner of UST Global d3code Hackathon 2019
- Ranked 1 in Regional Mathematics Olympiad 2015, KVS Region
- Selected for KVPY Fellowship 2017 with AIR 161
- Secured AIR 430 in JEE Advanced 2017 and AIR 113 in JEE Main 2017

OPEN SOURCE

SciML - Organization for Scientific Machine Learning

- `https://sciml.ai`
- Part of the organization since November 2018, Now part of Steering Council and maintainer
- I am responsible for the current Non-linear solving capability and custom callbacks in the package

EXPERIENCES (CONTD.)

Student Developer

Joint Seat Allocation Authority, IITR

January 2018 – April 2019 Roorkee,India

- Part of the student team employed by IIT Roorkee(organizing institute of JEE Advanced 2019) to develop the allocation and validation software for the allocation of seats to more than 200,000 students.
- Developed an individual implementation of Deferred Acceptance Algorithm for allocation purposes taking care of different business rules.
- Worked closely with NICSI, New Delhi to cross-verify and release results.

MLH Fellow

Major League Hacking

May 2020 – Aug 2020 New Delhi, India

As part of the inaugural class of MLH Fellows, I contributed to Open Source projects with a team of Fellows under the educational mentorship of a professional software engineer.

PERSONAL PROJECTS

Backdoor

- Website - `https://backdoor.sdslabs.co/`
- Information security platform hosting CTF challenges and competitions, created by SDSLabs.
- Current maintainer of the platform
- Written in PHP, based on the MVC architecture.
- Organised n00bCTF 2019 on Backdoor, a CTF aimed for beginners in information security.

Beast

- Jeopardy-style CTF challenges deployment tool which also manages challenges by packaging them as containers.
- Worked on container security(CR primitives like seccomp, CGroup, etc). Written in Go.

sieve++

- Fastest Lattice Sieve yet. Beats state of art fplll and g6k solvers in some cases.
- Comes packed with common experiments on SVP Challenge Lattices.

Watchdog

- Link - `https://github.com/sdslabs/watchdog`
- A personalized server management tool (and a slack bot) which keeps track of all administrative rights attempts (like sudo and su) on servers and allows/disallows log-in attempts based on public key of user and logs all activity in form of slack messages.
- Binaries written in Rust.

ACTIVITIES

SDSLabs

- Joint Secretary of the technical group since January 2018 which strives to foster technical innovations in campus.
- Have taken several minor and major projects under the group
- Took several public lectures on topics like "Containers under the Hood", "Introduction to Reversing", etc.

Teaching Assistance

- CSN 102 Data Structures - Spring 2020, IIT Roorkee
- CSN 106 Discrete Structures - Spring 2019, IIT Roorkee

REFERENCES

Prof. Sugata Gangopadhyay

@ sugatfma@iitr.ac.in

✉ Department of Computer Science and Engineering, IIT Roorkee

Dr. Chris Rackauckas

@ crackauc@mit.edu

✉ Department of Mathematics, MIT

Dr. Håvard Raddum

@ haavardr@simula.no

✉ Chief Research Scientist, Simula UiB

PUBLICATIONS

Articles

- Gupta, Kanav and Håvard Raddum (2020). *Obtuse Lattice Bases.* arXiv: `2009.00384 [cs.DS]`.