Rishab Goyal

Contact Information

Senior Undergraduate Student
Indian Institute of Technology Delhi
New Delhi, India

mobile: +91 9999040044
webpage: www.cse.iitd.ernet.in/~cs1100240
e-mail: cs1100240@cse.iitd.ernet.in

Research Interests

Cryptography and Computer Security

Education

Indian Institute of Technology Delhi, India
Bachelor of Technology, Computer Science and Engineering July 2010 – present
Current GPA: 8.751/10.0
Undergraduate Thesis: Password Authenticated Secret Sharing
Thesis Advisor: Prof. Ragesh Jaiswal (IIT Delhi), Dr. Raghav Bhaskar (Microsoft Research India)

Undergraduate Thesis

Password Authenticated Secret Sharing July 2013 – present
Developing efficient password-authenticated secret sharing scheme to allow users to share secret data among several servers, so that data is decentralized and can be recovered using human-memorable password, but no collusion of servers up to a certain size can mount an off-line dictionary attack on the password or learn anything about the secret

Research Projects

Improve Alternating Direction Method of Mutlipliers (Dr. Dhruv Mahajan)
Microsoft Research India, Bangalore (Summer 2013)

- Developed a novel algorithm to solve convex optimizations efficiently in a distributed setting
- Devised convergence proof and proved it to be more robust with lesser communication overheads
- Implemented the algorithm over Hadoop MapReduce framework

Information Security and Privacy Leaks (Prof. Sanjiva Prasad)
Computer Science and Engineering, IIT Delhi (Fall 2012, Spring 2013)

- Proposed and developed a security analyzer for Android applications to test for malicious behavior, that statically enumerated possible sensitive information flows to an insecure location
- Extended Dorothy Denning's lattice model for secure information flow and George Necula's Proof Carrying Code techniques to develop the analyzer

Privacy Leaks in Android (Prof. Michael Backes, Prof. Matteo Maffei)
Max Planck Institute for Software Systems, Germany (Summer 2012)

- Defined all inference rules necessary for complete structural operational semantics for Dalvik (Android's Virtual Machine), with a focus on security aspects
- Rigorously modelled Android's permission-based security mechanism as well as the inter-process communication

Concurrency Bug Testing Tools (Prof. Sorav Bansal)
Computer Science and Engineering, IIT Delhi (Fall 2013)

- Implemented tools such as CHESS and PCT to detect and reproduce concurrency bugs
- Wrote wrappers over pthreads library to capture, control and search through all interleaving non-determinism systematically and exhaustively

Array Interleaving Compiler Optimization (Prof. Preeti Ranjan Panda)
Computer Science and Engineering, IIT Delhi (Fall 2012)

- Designed an algorithm to look for viable array interleaving opportunities for better cache and vector register access
- Implemented it as a back-end compiler optimization with LLVM as the infrastructure

Other Projects

Zero Knowledge Protocols (Cryptography) (Spring 2013)
Explored and presented existing Zero Knowledge protocols and proof systems including Graph 3-Colorability, Quadratic Residuosity, Zero-Knowledge Proofs of Identity

PintOS (Operating Systems) (Spring 2013)
Implemented system calls for user programs, extended virtual memory and filesystem for the instructional operating system PintOS

Latent Semantic Analysis (Numerical Analysis) (Spring 2012)
Demonstrated better noise reduction and clustering on a database consisting of popular books

Universal Asynchronous Receiver Transmitter (Digital Hardware Design) (Spring 2012)
Designed a hardware-software partitioning on PC and FPGA using UART protocol in VHDL to perform Matrix Multiplication and Systolic Sorting on hardware

Multiplayer Carom (Software Engineering) (Fall 2011)
Wrote a multiplayer carom game played over the network in OpenGL with availability of bots

Automated Course Advisor (Artificial Intelligence) (Fall 2010)
Developed a chatbot based on Prof. Abelson and Prof. Sussman's design on freshmen advisor

Scholastic Achievements

IIT Delhi Semester Merit Award for meritorious academic performance (awarded to 3 students from 80) in freshmen year

Awarded **fellowship** by **Max-Planck-Institute for Software Systems** (Saarbrucken, Germany) under guidance of Prof. Michael Backes for Summer 2012

Selected for **IIT Delhi Student Exchange**, among 30 students from IIT Delhi selected for prestigious Cultural Exchange Programme

Secured **All India Rank 55** in Indian Institute of Technology Joint Entrance Examination (**IIT JEE 2010**) among 0.5 million students

Secured **All India Rank 37** in All India Engineering Entrance Examination (**AIEEE 2010**) among 1 million students

Secured **100%** and 1^{st} **Rank** in Olympiad by **Ramanujam Society** of born Mathematicians 2010

Secured **All India Rank 6** in National Science Talent Search Examination (**NSTSE**) 2010

Awarded Kishore Vigyan Protsahan Yojana (**KVPY** 2009) **fellowship** by Indian Institute of Science, Bangalore

Awarded **National Gold Medal** in Manavsthali Mathematics Olympiad, 2009

Felicitated with **0.1% Silver Medal** certificate of top candidates in National Standard Examination in Physics, 2009

Exhibits selected at **National Science Exhibition** conducted by CBSE consecutively for 2009, 2010

Extra Curriculars

Association for Computer Engineers and Scientists
Leading a team of 10, managing cultural activities of the Computer Science Department, IIT Delhi with over 500 members

Teaching: Over 200 hours of teaching experience at Vidyamandir Classes, an institute for IIT JEE preparation

References

Sanjiva Prasad, Professor, Department of Computer Science and Engineering, Indian Institute of Technology Delhi, sanjiva@cse.iitd.ac.in

Ragesh Jaiswal, Assistant Professor, Department of Computer Science and Engineering, Indian Institute of Technology Delhi, rjaiswal@cse.iitd.ac.in

Raghav Bhaskar, Researcher, Microsoft Research India, Bangalore, rbhaskar@microsoft.com

Dhruv Mahajan, Researcher, Microsoft Research India, Bangalore, dhrumaha@microsoft.com

Matteo Maffei, Associate Professor, Computer Science Department, Saarland University, maffei@cs.uni-saarland.de

Michael Backes, Professor, Computer Science Department, Saarland University, backes@cs.uni-saarland.de