ISHAAN PREET SINGH

+91 9899785978 | ishaanps92@gmail.com | ishaanpreet.com

RESEARCH INTERESTS

Foundations of Cryptography, Applied Cryptography, Security, Theoretical CS, Technology Policy

EDUCATION

Indian Institute of Technology Delhi, New Delhi *July 2011 - May 2016 expected*
Bachelor and Master of Technology
Computer Science & Engineering

WORK EXPERIENCE

- Teaching Assistant, CSL759: Cryptography and Network Security, IIT Delhi — Fall 2015
- Research Intern, École Polytechnique Fédérale de Lausanne, Switzerland — Summer 2015
- Research Intern, Xerox Research Centre India, Bangalore — Summer 2014
- Student Researcher, Summer Undergraduate Research Opportunity, IIT Delhi — Summer 2013

PUBLICATIONS

- "Assignment Techniques for Crowdsourcing Sensitive Tasks", Elisa Celis, Sai Praneeth Reddy, Ishaan Preet Singh, Shailesh Vaya. *Accepted at CSCW 2016, the 19th ACM Conference on Computer Supported Cooperative Work & Social Computing*

Patents Filed

- "Apparatus and Method for Secure Digital Coupon Verification", 2014*
- "Methods and Systems for Identifying Targeted Content Item for User", 2014*
- "Methods and Systems for Assigning Tasks", 2013*

*Sai Praneeth Reddy, Ishaan Preet Singh, Shailesh Vaya

RESEARCH PROJECTS

Master's Thesis: Cryptography Jan 2015 - Present
with Dr. Shweta Agarwal, IIT Delhi

Attribute Based Encryption for DFAs

- We are trying to create an LWE based ABE scheme for regular languages that allows unbounded length attributes by studying ABE for circuits and ABE for Regular Languages based on bilinear pairings.

Function Hiding in ABEs

- Aimed to extend GSW13's ABE scheme to hide function information according to definitions introduced for function hiding IBE. Tried revealing LWE matrices along with helper matrices to enable propagation through a circuit but discovered that these can be reconstructed revealing the function.

Convergence of Strategies in Networked Multi-Armed Bandits May 2015 - August 2015
with Dr. Elisa Celis, EPFL

- Studied a networked multi armed bandits game, where a player has access to its neighbours' exploration.
- Proved stability of Nash Equilibria, and that Price of Anarchy & Price of Stability would be unbounded.
- Showed that best response dynamics converge to specific Maximum Independent Sets when the network is a tree or has first moves $\in \{0, 0.5, 1\}$. We are trying to extend this and study convergence time.

Discreet Crowdsourcing August 2014 - August 2015
with Dr. Elisa Celis, EPFL and Dr. Shailesh Vaya, XRCI

· Formalised information loss while crowdsourcing tasks with sensitive data and developed task assignment algorithms which give theoretical and experimental guarantees even when workers collude.
· Introduced a hybrid setting which greatly reduces information loss over Amazon Turk-like systems.

Privacy Preserving Marketing May 2014 - August 2014
with Dr. Shaliesh Vaya, XRCI
· Created and implemented efficient oblivious transfer based algorithms to deliver targeted advertisements without revealing information to the server or significantly increasing client side computation.
· Developed a verification system for digital coupons to ensure that they are used only by eligible users.

Evolution of Technology Policy: Internet and Privacy January 2014 - May 2014
with Dr. Ambuj Sagar, IIT Delhi
Developed a timeline evaluating causes behind policy developments related to the Internet, focussing on the net neutrality debate. Assessed the ethical issues & legal framework associated with online privacy.

Algorithms for Subgraphs Induced by Makespan Minimisation May 2013 - Oct 2013
with Dr. Naveen Garg, IIT Delhi
· Designed a deterministic algorithm for finding an induced subgraph of a d-regular r-partite graph a vertex from each partition and maximum degree d?1. This problem was motivated by a reduction from the Makespan Minimisation. We further improved this requirement to an average degree $d/2$ bound.
Received the Summer Undergraduate Research Award, 2013

SCHOLASTIC ACHIEVEMENTS

· Ministry of Human Resource Development Scholarship, Awarded by Government of India 2015
· Charpak Scholarship, Awarded by Government of France 2013
· Summer Undergraduate Research Award, 1 of 2 CS projects awarded, IIT Delhi 2013
· Director's Semester Merit Award for Academic Excellence, IIT Delhi 2011
· All India Rank 124 in IIT JEE, Ranked in Top 0.02% amongst 500,000 students 2011
· Awardee, Indian National Chemistry Olympiad, Selected amongst top 35 in India 2011
· Awardee, Indian National Mathematics Olympiad, Selected amongst top 28 in India 2010, 2011
· NTSE Scholarship, Awarded by NCERT, Government of India 2009

SELECTED COURSEWORK

Cryptography and Network Security, Cryptography for the Cloud, Linear Algebra, Number Theory, Theory of Computation, Current Cryptographic Techniques (Independent Study), Abstract Algebra, Advanced Algorithms, Discrete Mathematics, Clustering Algorithms, Probabilistic Graphic Models

REFERENCES

Dr. Shweta Agarwal
Assistant Professor, Computer Science
Indian Institute of Technology Delhi
shweta@cse.iitd.ac.in

Dr. Shailesh Vaya
Senior Scientist
Xerox Research Centre India, Bangalore
Shailesh.Vaya@xerox.com

Dr. Ambuj Sagar
Professor, Policy Studies
Indian Institute of Technology Delhi
asagar@hss.iitd.ac.in

Dr. L. Elisa Celis
Senior Research Scientist
École Polytechnique Fédérale de Lausanne
elisa.celis@epfl.ch

Dr. Naveen Garg
Professor, Computer Science
Indian Institute of Technology Delhi
naveen@cse.iitd.ac.in