GAYATHRI A GARIMELLA

garimelg at oregonstate dot edu

AREAS OF INTEREST

Interested in efficient cryptographic protocols for Private Set Intersection (PSI), Private Set Union (PSU) and other useful formulations to realize Private Analytics (PA).

More broadly, designing protocols for computing on private data (Secure Computation).

EDUCATION

Ph.D. candidate in Computer Science *advised by Dr. Mike Rosulek* *Sept 2018 - Present*
Oregon State University, Corvallis
Overall GPA: 3.86 (*as of Fall 2020*)

M.Tech in Computer Science *advised by Dr. Ashish Choudhury* *Aug 2013 - Jun 2018*
International Institute of Information Technology, Bangalore
Thesis: Crash-Tolerant Consensus in Directed graphs
Overall GPA: 3.47

B.Tech in Computer Science *Aug 2013 - Jun 2018*
Overall GPA: 3.47

PUBLICATIONS AND MANUSCRIPTS

authors are named alphabetically in this discipline

1. Gayathri Garimella, Payman Mohassel, Jaspal Singh and Mike Rosulek: *Private Set Operations from Oblivious Switching.* PKC 2021
2. Gayathri Garimella, Benny Pinkas, Mike Rosulek, Ni Trieu and Avishay Yanai: *Oblivious Key-Value Stores for Private Set Intersection.* (in submission to CRYPTO 2021)
3. Laasya Bangalore, Ashish Choudhury, Gayathri Garimella: *Round efficient computationally secure multi-party computation revisited.* ICDCN 2019: 292-301
4. Ashish Choudhury, Gayathri Garimella, Arpita Patra, Divya Ravi, Pratik Sarkar: *Crash-Tolerant Consensus in Directed Graph Revisited (Extended Abstract).* SIROCCO 2018.
5. Ashish Choudhury, Gayathri Garimella, Arpita Patra, Divya Ravi, Pratik Sarkar: *Brief announcement: Crash-tolerant Consensus in Directed Graphs Revisited.* DISC 2017: 46:1 - 46:4

Implementation projects

1. **Rust library** for two-party Secure Computation with Covert security and Public verifiability.
   Code hosted at: https://github.com/gayathrigarimella/Public-Verifiability-Covert.git
2. **C++ library** for two-party computation on the intersection of sets to learn cardinality of intersection, union, intersection, cardinality-sum, private-id.
   Code hosted at: https://github.com/gayathrigarimella/PSI-analytics.git

RELEVANT COURSEWORK

Oregon State University: *Introduction to Cryptography, Theory of Computation, Analysis of Algorithms, Graph Theory, Advanced Algorithms, Abstract algebra*

International Institute of Information Technology: *Computing on Private Data, Introduction to Modern Cryptography, Approximation Algorithms, Computational Geometry, Multi-agent Systems*

TECHNICAL SKILLS

Proficient in Rust, C++, Python and comfortable with SQL, Github, linux platforms.

EXPERIENCE

Professional activities

1. EECS Graduate Curriculum Committee : student member (CS dept) — Jan 2021 - present
2. Sub-reviewer — CRYPTO 2021
3. Sub-reviewer — Indocrypt 2020

Teaching

1. Teaching Assistant (OSU) : CS517 - Complexity theory (Graduate) — Spring 2020
2. Teaching Assistant (IIIT-B) : CS716 - Computing on Private Data — Fall 2017

Academic achievements:

1. Passed PhD Qualifying Exam — Nov 2019
2. Graduate Assistantship at Oregon State University — Sept 2018 - Present
3. Selected for the Summer Research Fellowship by Indian Academy of Science — Summer 2016
4. Received Dean's Merit List — Fall 2013

Internships:

1. Visitor at CrIS Lab, IISc, Bangalore *advised by Prof. Arpita Patra* — Summer 2016, 2017
2. Intern at Natural Language Processing Lab, IISc, Bangalore *advised by Prof. Veni Madhavan* — Summer 2015

Presentations:

1. *Round efficient computationally secure Multi-party computation Revisited.* ICDCN, Bangalore, India. January 2019.

Workshops and Conferences: Had the opportunity to attend -

1. CRYPTO, Santa Barbara, USA — Aug 2019
2. Indocrypt, Chennai, India — Dec 2017
3. NMI School and workshop on MPC, IIT-Bombay, India — Mar 2017

LANGUAGES

Fluent in English, Telugu, Hindi and Kannada.