Nishant Kumar

Research Fellow
Microsoft Research India
Advisors: ***Dr.Nishanth Chandran, Dr.Divya Gupta, Dr.Aseem Rastogi & Dr.Rahul Sharma***

Updated: February 9, 2020
t-niskum@microsoft.com | nishant.kr10@gmail.com
Webpage : https://nishkum.github.io
+91-8373908311

Research Interests

Theoretical and Applied aspects of Cryptography and Security

Education

Indian Institute of Technology Delhi — *India*
Bachelor of Technology, Computer Science and Engineering — *July '12 - July '16*
GPA: 9.15/10 (Overall)

Delhi Public School — *India*
All India Senior School Certificate Examination, CBSE, Delhi — *May '12*
Overall: 96.8%

Manuscripts

CrypTFlow: Secure TensorFlow Inference
Nishant Kumar, Mayank Rathee, Nishanth Chandran, Divya Gupta, Aseem Rastogi, Rahul Sharma
In Submission to IEEE Symposium on Security and Privacy (S&P), 2020 [GitHub] [PrePrint]

A Practical Model for Collaborative Databases: Securely Mixing, Searching and Computing
Shweta Agrawal, Rachit Garg, **Nishant Kumar**, Manoj Prabhakaran
In Submission to ACM Conference on Computer and Communications Security (CCS), 2020 [PrePrint]

Work Experience

Microsoft Research Lab — *Bengaluru, India*
Research Fellow, *Cryptography group* — *July '18 - Present*
Working on the EzPC (Easy Secure Multi-Party Computation) project, to construct efficient protocols, and develop tools/techniques, to increase the adoption of Secure Multi-Party Computation (MPC) as a tool, in various privacy-preserving tasks.

Microsoft Corp. — *Hyderabad, India*
Software Engineer, Azure Backup — *July '16 - June '18*
Built an Azure IaaS VM extension to deliver on cloud-native, zero-infrastructure backup solution for workloads hosted in Azure (like SQL Server, SAP Hana etc.). Designed and built key infrastructural components of the extension to support various operations like backup and recovery on any given workload. This service was made generally available to all customers in Azure in April 2019 [Blog Post].

Microsoft Corp. — *Hyderabad, India*
Software Engineering Intern, Data Protection Manager, Azure Backup — *May '15 - July '15*
Worked on secondary backup to Azure in Microsoft Data Protection Manager (DPM) using Point-in-time copy semantics. Designed and developed an OS-level component for change tracking on a volume in the DPM server using bitmaps. An end-to-end working prototype of improved secondary backup to Azure.

Selected Research projects

CrypTFlow: Secure TensorFlow Inference — *July '18 - Present*
Supervisors: Dr.Nishanth Chandran, Dr.Divya Gupta, Dr.Aseem Rastogi & Dr.Rahul Sharma, MSR India [PrePrint]

- *CrypTFlow is an end-to-end system for converting TensorFlow inference code to secure MPC protocols. It is the first system to run very large neural networks, like* Resnet-200 *securely.*
- *Three constituent components:* ***Athos****, an end-to-end compiler from TensorFlow inference code to semi-honest MPC protocols;* ***Porthos****, a semi-honest 3-party computation protocol optimized for ML-like applications; and* ***Aramis****, a novel technique to compile semi-honest protocols to malicious protocols using hardware with integrity guarantees.*
- *Designed and developed Athos and Porthos; responsible for important compute-related optimizations in Porthos.*
- *Code available as open-source at GitHub; working with several product groups for integration in Azure.*

Functionally Encrypted Datastores — *July '15 - July '16, April '18 - Present*
Supervisors: Dr.Shweta Agrawal, IIT Madras & Dr.Manoj Prabhakaran, IIT Bombay [PrePrint]

- *Motivation to increase the efficiency of Functional Encryption (for specific classes of functions) at the cost of allowing the adversary to learn well-defined leakage, with similar tradeoffs between efficiency and security as in Searchable Symmetric Encryption (SSE).*
- *Model partly motivated by the rising security concerns around Aadhaar, a central repository of national identities, including demographic and biometric data, being built by the Government of India.*
- *Model allows multiple data-owners to anonymously outsource data to honest-but-curious non-colluding servers and later allows malicious clients to make search-and-compute queries on the collected data.*
- *Designed and implemented crypto protocols for specific functions in Genome-Wide Association Studies (GWAS).*

Efficient MPC protocols for secure Machine Learning *June '19 - Present*
Supervisors: Dr.Nishanth Chandran & Dr.Divya Gupta, Microsoft Research India

- *Working on constructing efficient (semi-honest and malicious) multi-party computation protocols, for secure inference of ML algorithms in a 2-party setting.*

Selected Other projects

Cryptography in 2-server setting *Jan '15 - May '15*
Supervisors: Dr.Shweta Agrawal, IIT Madras & Dr.Ragesh Jaiswal , IIT Delhi *[Report]*

- *Model whereby a data-owner is interacting with two non-colluding malicious servers. Developed a keyless protocol for supporting Proofs of Retrievability in this setting, and explored how to do function computation efficiently.*

Scheduling policies for Baadal - the IITD academic cloud *Jan '14 - July '14*
Supervisor: Dr.Amit Kumar, IIT Delhi *[Report]*

- *Proposed ways to improve VM scheduling policies used by Baadal, orchestration software for IITD academic cloud.*

Awards and Achievements

- ACM ICPC*: My team (hyperbolicTan) secured rank 18 in ICPC Kharagpur Regionals, 2014.*
- Joint Entrance Examination*: Secured all India rank of 755 in IIT-JEE 2012 among around half a million candidates.*
- Kishore Vaigyanik Protsahan Yojana*: Awarded the prestigious* KVPY *Fellowship Award, 2011, by Govt. of India.*
- CBSE Merit*: Received CBSE Merit Certificate for being among the top 0.1% students in Economics in India.*
- Regional Mathematics Olympiad*: Amongst the top 30 to qualify for RMO-2009, the first stage on the path of becoming part of India's contingent for International Mathematics Olympiad (IMO).*
- Olympiads*: Secured all India ranks of 5 and 30 in National Science Olympiad, organized by Science Olympiad Foundation in 2007 and 2008 respectively.*

Professional Service and Responsibilities

- *Sub-Reviewer for* Asiacrypt *2019,* Indocrypt *2019.*
- *Student volunteer at* TCC *2018.*
- *Organizer, Joint crypto reading group between Microsoft Research India and IISc, Jan - April 2019.*
- *DRI, Stanford Scholar Initiative*
  - *Involved in the creation of short research talks on important papers in different areas of Computer Science, summarizing the novelty of the work, in an effort to disseminate the knowledge to a broader audience.*
  - *As a DRI (Directly Responsible Individual), successfully coordinated and led a team of 3-8 people to create a good research talk. Relevant talks: talk #86, talk #334, talk #223.*
- *Mentor, Avanti Fellows: As part of Avanti Fellows, an NGO that provides students from economically weak sections of India access to mentorship and training to get into good colleges, I mentored two students through their 11th and 12th standards in their preparation for IIT-JEE 2015.*

Open-source contributions

CrypTFlow: Secure TensorFlow inference
Microsoft Research India $\approx 10,000$ *LOC* *[GitHub]*

- *Designed and developed Athos, a compiler (written in Python) from TensorFlow inference code to secure MPC protocols. Athos compiles TensorFlow using 2 Intermediate Languages (IL) - a High-Level Intermediate Language (HLIL) and a Low-Level Intermediate Language (LLIL). Implemented several standard and non-standard optimizations on each IL during compilation. Also, designed and incorporated several optimizations in Porthos (written in C++), a 3-party computation protocol geared for ML-like applications.*