Srinivasan Raghuraman

Curriculum Vitae

550 Memorial Drive
Cambridge, MA 02139
☎ *+1 (617) 335-9313*
✉ *srini131293@gmail.com, srirag@mit.edu*
🖰 *http://people.csail.mit.edu/srirag*

Research Interests

Cryptography and Complexity Theory

Education

2015–present **Ph. D. in Computer Science**, *MIT*, *GPA – 5/5*.

2011–2015 **B.Tech (Honours) in Computer Science and Engineering, with a Minor in Operations Research**, *Indian Institute of Technology, Madras*, *GPA – 9.9/10* ***Ranked 1st across the Institute***.

2009–2011 **Higher Secondary Examination**, *National Public School, Indiranagar*, Bangalore, 96.8%.

Honours and Awards

Academic

- Received **President of India Prize**, **Bharat Ratna M Visvesvaraya Memorial Prize**, **B Ravichandran Memorial Prize**, **K Srinivasan and Indira Srinivasan Prize**, **Dr Dilip Veeraraghavan Memorial Award**, **Shri Subramanian Prize** and **Shri V Ramachandran Prize** for the best academic performance in the Institute, Computer Science and Humanities.

Olympiads

- Successful at the Indian National Mathematics Olympiad (INMO) 2010, 2011.
- Placed amongst the top 10% of students who appeared for the Indian National Physics Olympiad, Indian National Chemistry Olympiad and Indian National Astronomy Olympiad in 2010.

Scholarships

- **Siebel Scholar**, Class of 2017 – awarded annually for academic excellence and demonstrated leadership to over 90 top students from the world's leading graduate schools.
- **Irwin Mark Jacobs and Joan Klein Jacobs Presidential Fellowship** at MIT.
- **Singapore Technologies (ST)** Engineering Scholarship by Singapore Technologies.
- **Kishore Vaigyanik Protsahan Yojana (KVPY)** Scholarship, a national fellowship for students interested in science by Dept. of Science and Technology, India.
- **National Talent Search (NTS)** Scholarship by National Council of Education Research and Training (NCERT), India.

Publications

PKC '17 *Ran Canetti*, *Srinivasan Raghuraman*, *Silas Richelson*, *Vinod Vaikuntanathan*. **Chosen-Ciphertext Secure Fully Homomorphic Encryption**. *PDF*

CRYPTO '16 *Ranjit Kumaresan*, *Srinivasan Raghuraman*, *Adam Sealfon*. **Network Oblivious Transfer**. *PDF*

PKC '16 *Nishanth Chandran*, *Srinivasan Raghuraman*, *Dhinakaran Vinayagamurthy* (Microsoft Research India). **Reducing Depth in Constrained PRFs: From Bit-Fixing to NC1**. *PDF*

TCC '16-A *Nishanth Chandran*, *Bhavana Kanukurthi*, *Srinivasan Raghuraman*. **Information-Theoretic Local Non-malleable Codes and Their Applications**. *PDF*

CMC '15 *Venkata Padmavati Metta*, *Srinivasan Raghuraman*, *Kamala Krithivasan*. **Small Universal Spiking Neural P Systems with Cooperating Rules as Function Computing Devices**. *PDF*

CMC '15 *Venkata Padmavati Metta*, *Srinivasan Raghuraman*, *Kamala Krithivasan*. **Spiking Neural P Systems with Cooperating Rules**. *PDF*

Manuscripts

Nishanth Chandran, *Srinivasan Raghuraman*, *Dhinakaran Vinayagamurthy*. **Constrained Pseudorandom Functions: Verifiable and Delegatable**. *PDF*

Boneh and Waters left open the question of constructing delegatable constrained pseudorandom functions (constrained PRFs). Boyle, Goldwasser, and Ivan left open the question of constructing verifiable constrained PRFs. In this work, we solved both the questions by constructing constrained PRFs that are verifiable and delegatable.

Undergraduate Thesis

New bounds for hypergraph two-colouring

Prof. Narayanaswamy N S (IIT Madras)

Description The known results are by Erdős, Beck and Radhakrishnan and Srinivasan. The attempt is to study the function $m(n)$ on special kinds of graphs such as matroids, (maximal) outer-planar graphs such as fans, etc., to obtain newer bounds, and attempt at resolving a conjecture from the 1960s.

Other Research Experience

Practically Implementable Dynamic Proofs of Retrievability

Nishanth Chandran, *Satyanarayana V. Lokam* (Microsoft Research India)

Description In this work, we designed a practical dynamic proof of retrievability (dynamic PoR) scheme. What we envision is a generic extension to a static PoR with tunable parameters to achieve desired factor of storage on both the client as well as the server, which provides high throughput with low client and server storage.

Professional Experience

Summer 2013 **HCL Infosystems Pvt. Ltd.** *Industrial Training*

This summer intern involved implementation of storage for secure, real-time extension and high availability.

Summer 2013 **Acceletrade Technologies** *Industrial Training*

This summer intern involved Statistical Arbitrage Analysis using Co-Integration and Principal Component Analysis. I developed of an application to automate High Frequency Trading (HFT).

Summer 2012 **SAP Labs**

The work involved exposing HANA stored procedures as REST services and consuming the same using JSF/JSP UI, developing several pages for Janyaa, a non-profit based in U.S and re-designing the back-end for ChariTra.

Workshops and Schools

January 2016 **Second Desert Workshop in Cryptography**

Discussion of recent results in foundations of cryptogtaphy and the possibility of cryptography with low complexity.

March 2014 **XRCI Open 2014** *Xerox Research Centre India (XRCI)*

An open innovation symposium with several talks on big data, machine learning, *etc*.

January 2014 **ITCSC-INC Winter School 2014** *Chinese University of Hong Kong*

A workshop themed '**Fourier Transforms**' with talks on applications to boolean functions, communication, probability.

Talks and Presentations

Conference Talks

- **“Information-Theoretic Local Non-malleable Codes and Their Applications”**, by *Nishanth Chandran, Bhavana Kanukurthi, Srinivasan Raghuraman* – Thirteenth IACR Theory of Cryptography Conference (TCC 2016-A), Tel Aviv, Israel. *January 2016*
- **“Small Universal Spiking Neural P Systems with Cooperating Rules”**, by *Venkata Padmavati Metta, Srinivasan Raghuraman, Kamala Krithivasan* – The 15th International Conference on Membrane Computing (CMC-15), Prague, Czech Republic. *August 2014*
- **“Spiking Neural P Systems with Cooperating Rules”**, by *Venkata Padmavati Metta, Srinivasan Raghuraman, Kamala Krithivasan* – The 15th International Conference on Membrane Computing (CMC-15), Prague, Czech Republic. *August 2014*

MIT

- **Network Oblivious Transfer**, by *Ranjit Kumaresan, Srinivasan Raghuraman, Adam Sealfon, CRYPTO 2016*. *March 2016*
- **Constrained Pseudorandom Functions: Verifiable and Delegatable**, by *Nishanth Chandran, Srinivasan Raghuraman, Dhinakaran Vinayagamurthy*. *September 2015*

Microsoft Research[1]

- **“On Notions of Security for Deterministic Encryption, and Efficient Constructions without Random Oracle”**, by *Alexandra Boldyreva, Serge Fehr, Adam O’Neill, CRYPTO 2008*. *June 2014*
- **“Better Security for Deterministic Public-Key Encryption: The Auxiliary-Input Setting”**, by *Zvika Brakerski, Gil Segev, CRYPTO 2011*. *June 2014*
- **“Proofs of Retrievability via Hardness Amplification”**, by *Yevgeniy Dodis, Salil P. Vadhan, Daniel Wichs, TCC 2009*. *May 2014*

tMeet[2], IITM

- **Spiking Neural P Systems with Cooperating Rules** – Introduction to the notion of Spiking Neural P Systems with Cooperating Rules and proof of universality. *April 2014*
- **Network Oblivious Transfer**, by *Ranjit Kumaresan, Srinivasan Raghuraman, Adam Sealfon, CRYPTO 2016*. *August 2016*

Extra-curricular Activities

- Selected to represent IIT Madras for the onsite event in the ACM ICPC regionals, 2013.
- Carnatic vocalist for 15 years; playing Veena and Piano for 4 years; Concert Choir, Chamber Choir and A Cappella for 1 year
- Interacted with approximately 200 colleges in Tamil Nadu (including National Service Scheme (NSS), IIT Madras) for participation in the charity oriented initiative of SAP Labs entitled ChariTra.

[1] These talks were given as a part of Cryptography Reading Group at Microsoft Research, Bangalore.

[2] These talks were given as a part of the weekly Theory meet, called *tMeet*, at IIT-Madras.