

Chaya Ganesh

Present Address

Room No. 311, Sarayu Hostel,
IIT Madras
Chennai 600 036
Phone: 91 9952932611
<http://www.cse.iitm.ac.in/chaya>

Permanent Address

'Shrimatha', #1779,
23rd Cross, MRCR Layout,
Bangalore 560 079
Phone: 91 9986787166
chaya.ganesh@gmail.com

Education	IIT Madras M.S. Computer Science CGPA: 9.4 R.V. College of Engineering (Then affiliated to Visvesvaraya Technological University) B.E. Information Science and Engineering Percentage: 86%, University Gold Medallist. MES College of Arts, Commerce and Science Class XII (Karnataka State board) Percentage: 95.5%, Topped the class in Mathematics and Physics New Public High School Class X (Karnataka State Board) Percentage: 96%, Topped the class in Mathematics	Chennai, India 2009 - Present Bangalore, India 2004 - 2008 Bangalore, India 2004 Bangalore, India 2002
Research Interests	Theoretical Computer Science - Cryptography, Secure Computation, Complexity theoretic questions in cryptography, interplay between game theory and cryptography, Leakage resilience.	
Research and Professional Experience	IIT Madras Guide : Prof C. Pandurangan. <ul style="list-style-type: none">• Survey - Surveyed Secret sharing schemes in the threshold and general access structures.• Communication Complexity of Efficient Two party Computation protocols. Under Review. An analysis of optimal choice of parameters for existing cut-and-choose construction for secure two-party computation.• Current research - Distributed Oblivious Transfer. Microsoft Research, India Research Intern, Mentors : Dr. Vipul Goyal and Dr. Satya Lokam. <ul style="list-style-type: none">• On-Line/Off-Line Leakage Resilient Secure Computation Protocols. Under Review. Explored secure computation protocols in the presence of leakage and gave two protocol constructions. Nortel Networks, India	2009 - Present Sep - Nov 2010 & Jan - Mar 2011 July 2008 - July 2009
	Software Engineer, Nortel Ethernet Routing Switch 8600 Team. <ul style="list-style-type: none">• Part of the command line interface team of the Ethernet Routing Switch. Worked on the design for operability feature, access control policies and management information base.	

- Workshops**
- The Pseudorandomness Workshop at CMI, Chennai, 22 - 25 August 2011. (On Invitation)
 - The Second Annual Mysore Park Workshop in Theoretical Computer Science, 5 - 9 May 2011. (On Invitation)
 - The 2011 School on Approximability conducted by Microsoft Research at IISc, January 2011. (On Invitation)
 - Microsoft Research's Theory Day conducted in January 2010.
- Relevant Coursework**
- Advanced Data Structures and Algorithms.
 - Mathematical Concepts for Computer Science.
 - Topics in Design & Analysis of Algorithms.
 - Parallel and Randomized Algorithms.
 - Advances in Complexity Theory.
 - **Teaching Assistant** for Design and Analysis of Algorithms, and Cryptography and Network Security courses at IITM.
- Projects**
- *iSinc*, Integrated Secure Intranet Communicator - RVCE, Bangalore: June 2008
Developed a communication tool for an intranet with features like encrypted text chat and group conference, notifications, screencast, and implemented the g.711 standard for voice encoding as curriculum final year project.
Language used: C#, .NET framework
 - Frame prediction and image enhancement - Department of Aerospace Engineering, IISc, Bangalore: May 2008
The project involved the video of an electrode arc experiment captured using a low frame rate camera. As part of a two member team, developed the intermediate probable frames using fusion rules. Involved a study of interpolation techniques, implementation of linear interpolation and Block matching algorithm.
Language used: Matlab image processing toolbox.
 - Bluetooth Pairing Security September 2006
A study of the security aspects and vulnerability of the Bluetooth Pairing Protocol. Co-authored a student paper implementing a brute force attack on the pairing scheme. Presented at the 20th Computer Society of India (CSI) Student Convention, won the *Second Best Paper award*.
- Scholastic Achievements**
- Secured *First Rank* and the **University Gold medal** for Information Science and Engineering, 2008.
 - Won the *Best outgoing student* award 2008 awarded by Cognizant for excellent all round performance.
 - Awarded the *Best Student* of the year 2008 awarded by Tata Consultancy Services.
 - Recognized as the *Honeywell Scholar* of the Year 2007 for meritorious academic performance.
- Technical Skills**
- Proficient in C/C++.
 - Working knowledge of L^AT_EX, UNIX Shells, HTML, PHP.
 - Comfortable with Linux and Windows environments.

**Co-Curricular
Activities**

- Won the first prize in *Codebutter*, a 12-hour coding contest at IIIT Bangalore, 2008
- Won the first prize in Programming at ISTE, and other inter-collegiate technical festivals, 2007
- A member of InfinIT, the departmental club, actively participated in its activities, and organised the departmental techno-managerial fest, INFINITY 2007 at RVCE. Was part of the team which organised the Paper presentation event.
- Member of Bangalore .NET Student User Group, have attended the various meets and sessions on .NET and other technologies, also an active member of frequency, the technical club of RVCE.

**Personal
Details**

- Date of Birth: 28th July 1986
- Gender: Female
- Languages Known: English, Kannada and Hindi
- Citizenship: Indian