

1200 Dale Ave Apt. 92  
Mountain View, CA 94040  
Ph: +1-650-387-4502

**Arnab Roy**  
arnab@cs.stanford.edu

353 Serra Mall Rm. 490  
Stanford, CA 94305  
Ph: +1-650-725-3110

---

**Education:**

PhD Candidate in Computer Science,  
Stanford University  
2004 – (Thesis defended in Dec. 2008)  
Siebel Scholar 2006  
Course GPA : 4.3 / 4.0

Dual Degree in Computer Science and Engineering,  
[B.Tech.(Hons) and M.Tech.]  
Indian Institute of Technology Kharagpur  
1999 – 2004  
Cumulative GPA : 9.66/10

Pre-college Education:

ISC	1999	Future Foundation School, Kolkata	93.5% aggregate
ICSE	1997	St. Helen School, Kolkata	95.2% aggregate

**Selected Awards and Honors:**

Selected as a student delegate to the 45th International Achievement Summit, June 2006, Los Angeles, California.

Appointed as a **Siebel Scholar**, Class of 2006, conferred on 5 graduate students each from the top 5 Computer Science and top 5 Business schools in United States.

Awarded the **Prime Minister of India Gold Medal** by IIT Kharagpur for best academic performance among all Dual Degree Engineering and Science students graduating in 2004.

Received scholarships from IIT every year for academic performance including the Technology Alumni Association Scholarships for securing the highest Cumulative GPA after 1st and 2nd years (out of approximately 550 students).

Selected for the prestigious Microsoft Research Student Fellowship, summer of 2003. Was unable to attend due to conflict with college schedule.

Awarded a **Gold Medal** and High Distinctions in 1997 & 1998 in International Competition for Schools in Mathematics conducted by ETC, University of New South Wales.

Secured all India 7th position in INMO (Indian National Mathematics Olympiad). Attended the IMO (International Mathematics Olympiad) Training Camps in 1998 & 1999.

Secured 1st position in RMO (Regional Mathematics Olympiad) of the state of West Bengal, India.

**Work Experience:**

Course Assistant at Stanford University for the courses:  
CS155, Spring 2008 - Computer and Network Security  
CS259, Winter 2008 - Security Analysis of Network Protocols  
CS258, Winter 2007 - Introduction to Programming Language Theory

Internship at Microsoft Research, Redmond, Washington, June-September 2008.

Internship at Intel Corporation, Hillsboro, Oregon, June-September 2005.

Internship at National Semiconductor Corporation, Fürstfeldbruck, Germany, May-July 2002.

Summer Research Fellowship offered by Jawaharlal Nehru Centre for Advanced Scientific Research (JNCASR), May-July 2001.

**Book Chapter:**

Arnab Roy, Anupam Datta, Ante Derek, John C. Mitchell, and Jean-Pierre Seifert, "Secrecy Analysis in Protocol Composition Logic", in Formal Logical Methods for System Security and Correctness, IOS Press, 2008. Volume based on presentations at Summer School 2007, Formal Logical Methods for System Security and Correctness, Marktoberdorf, Germany.

**Journal Publications:**

S. K. Panda, Arnab Roy, P. P. Chakrabarti and Rajeev Kumar, "Simulation based verification using temporally attributed boolean logic", ACM Transactions on Design Automation of Electronic Systems, Volume 13, Issue 4 (Sept 2008), Pages:1 - 52.

Anupam Datta, Ante Derek, John C. Mitchell and Arnab Roy, "Protocol Composition Logic", Electronic Notes in Theoretical Computer Science, Volume 172 , 1 April 2007, Pages 311-358. Computation, Meaning, and Logic: Articles dedicated to Gordon Plotkin.

Arnab Roy, S. K. Panda, Rajeev Kumar and P. P. Chakrabarti, "A Framework for Systematic Validation and Debugging of Pipeline Simulators", ACM Transactions on Design Automation of Electronic Systems, Volume 10, Issue 3 (July 2005), Pages: 462 – 491.

**Conference/Workshop Publications:**

John C. Mitchell, Arnab Roy and Mukund Sundararajan, "An Automated Approach for Proving PCL Invariants", in the 3rd International Workshop on Security and Rewriting Techniques, Pittsburgh, June 2008.

Anupam Datta, Joseph Halpern, John C. Mitchell, Riccardo Pucella, and Arnab Roy, "Reasoning about Conditional Probability and Concrete Security in Protocol Proofs (Work in Progress)", in the 4th Workshop on Formal and Computational Cryptography, Pittsburgh, June 2008.

John C. Mitchell, Arnab Roy, Paul Rowe and Andre Scedrov, "Analysis of EAP-GPSK Authentication Protocol", in Proceedings of 6th International Conference on Applied Cryptography and Network Security, New York, June 2008.

Arnab Roy, Anupam Datta and John C. Mitchell, "Formal Proofs of Cryptographic Security of Diffie-Hellman-based Protocols", in Proceedings of 3rd Symposium on Trustworthy Global Computing, November 2007.

Arnab Roy, Anupam Datta, Ante Derek and John C. Mitchell, "Inductive Proofs of Computational Secrecy", in Proceedings of 12th European Symposium On Research In Computer Security, September 2007.

Arnab Roy, Anupam Datta, Ante Derek, John C. Mitchell, "Inductive Trace Properties for Computational Security", in ACM SIGPLAN and IFIP WG 1.7 7th Workshop on Issues in the Theory of Security, March 2007.

S. K. Panda, Arnab Roy, P. P. Chakrabarti and Rajeev Kumar, "Simulation based verification using temporally attributed boolean logic", in Proceedings of the 20th Int. Conf. VLSI Design/ 6th Int. Conf. Embedded System, Bangalore, January 2007. IEEE CS Press.

Arnab Roy, Anupam Datta, Ante Derek, John C. Mitchell, Jean-Pierre Seifert, "Secrecy Analysis in Protocol Composition Logic", in Proceedings of 11th Annual Asian Computing Science Conference, Tokyo, December 2006.

Anupam Datta, Ante Derek, John C. Mitchell, Arnab Roy, Vitaly Shmatikov, Mathieu Turuani and Bogdan Warinschi, "Computationally Sound Compositional Logic for Security Protocols", in the 2nd Workshop on Formal and Computational Cryptography, Venice, June 2006.

### **Manuscripts:**

Yuri Gurevich and Arnab Roy, "Operational Semantics for DKAL: Application and Analysis", Microsoft Research Technical Report, Dec. 2008.

Arnab Roy, Anupam Datta, Ante Derek, John C. Mitchell, "Inductive Trace Properties for Computational Security", in review for Journal of Computer Security.

Changhua He, Mukund Sundararajan, Arnab Roy, Anupam Datta, Ante Derek, John C. Mitchell, "A Modular Correctness Proof of TLS and IEEE 802.11i", in review for ACM Transactions on Information and System Security.

### **Other Research Literature:**

M.Tech. Thesis: "Framework for Simulation-based Verification of Microprocessor Pipeline Simulators", May 2004. Advisors : Prof. P. P. Chakrabarti and Prof. Rajeev Kumar.

B.Tech. Thesis: "Automated Generation of Cycle Callable Simulators for Architectural Design Space Exploration", May 2003. Advisors : Prof. P. P. Chakrabarti and Prof. Rajeev Kumar.

Technical Report: Arnab Roy, N.R. Satish and Rajeev Kumar, "CR16C+ Cycle Callable Simulator: Modeling of the CR16C+ Core and its interaction with a high performance pipelined bus", August 2002. (Technical Report for National Semiconductor Corporation).

### **Selected Talks:**

"Computational Protocol Composition Logic" – invited guest lecture at Carnegie Mellon University, Pittsburgh – Oct 2007

"Security Protocols Research" – discussion session as an invited panelist at the 2nd Franco-Japanese Computer Security Workshop, Tokyo – Dec 2006

"Formal Analysis of Security Protocols in Protocol Composition Logic" – invited talk at Intel Corporation, Bangalore, India – November 2005

"Formal Methods in Security" – at Intel Corporation, Hillsboro, Oregon – March 2005

Talks at conference venues on most of my authored papers.

### **Other activities:**

Co-ordinator of the Stanford Security Lunch, 2006-07.

Was the head and instructor of the AI group of KRAIG (Kharagpur Robotics & AI Guild). Was actively interested in robotics and participated in robotics competitions at IIT.

Was a Think-Tank committee member of the BitWise 2k3. BitWise is an online time-constrained algorithm intensive international programming contest conducted annually by the CSE Department Society of IIT Kharagpur.

### **References:**

Prof. John C. Mitchell  
(Advisor – Stanford University)  
<http://theory.stanford.edu/people/jcm/mitchell@cs.stanford.edu>

Dr. Yuri Gurevich  
(Mentor – Microsoft Research)  
<http://research.microsoft.com/~gurevich/gurevich@microsoft.com>

Dr. Jean-Pierre Seifert  
(Mentor – Intel Corporation,  
now at Samsung)  
[j.seifert@sisa.samsung.com](mailto:j.seifert@sisa.samsung.com)

Prof. Partha P. Chakrabarti  
(Advisor - IIT Kharagpur)  
<http://www.facweb.iitkgp.ernet.in/~ppchak/ppchak@cse.iitkgp.ernet.in>