Pramod Subramanyan

Contact Information

RM 507, Department of of Computer Science and Engineering
Indian Institute of Technology, Kanpur.
Kanpur, Uttar Pradesh, INDIA - 208016

Email: spramod@cse.iitk.ac.in
Phone: +91-512-259-2025
Web: `http://cse.iitk.ac.in/users/spramod`

Education

Princeton University, Princeton, NJ.

Ph.D. Department of Electrical Engineering, 2011-2016.

Thesis: Deriving Abstractions to Address Hardware Platform Security Challenges advised by Professor Sharad Malik.

Indian Institute of Science, Bangalore.

M.Sc. (Engg.), Supercomputer Education and Research Center, 2008-2011.

Thesis: Efficient Redundant Execution in Chip Multiprocessors advised by Professor Virendra Singh.

R. V. College of Engineering, Bangalore.

B.E., Electronics and Communication Engineering, 2002-2006.

Book Chapters

- "Verifying Security Properties in Modern SoCs using Instruction-Level Abstractions", Pramod Subramanyan and Sharad Malik. *Hardware IP Security and Trust*, edited by Prabhat Mishra, Swarup Bhunia and Mark Tehranipoor. Springer-Verlag, January 2017.
- "Boolean Satisfiability: Solvers and Extensions", Georg Weissenbacher, Pramod Subramanyan and Sharad Malik. *Software Systems Safety*, IOS Press, May 2014.

Journal Papers

- "Instruction-Level Abstraction (ILA): A Uniform Specification for System-on-Chip (SoC) Verification", Bo-Yuan Huang, Hongce Zhang, Pramod Subramanyan, Yakir Vizel, Aarti Gupta, and Sharad Malik. *ACM Transactions on Design Automation of Electronic Systems* ***(TOADES)***, 2018.
- "Template-based Parameterized Synthesis of Uniform Instruction-Level Abstractions for SoC Verification", Pramod Subramanyan, Bo-Yuan Huang, Yakir Vizel, Aarti Gupta and Sharad Malik. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* ***(TCAD)***, 2018.
- "Reverse Engineering Digital Circuits Using Structural and Functional Analyses", Pramod Subramanyan, Nestan Tsiskaridze, Wenchao Li, Adria Gascon, Wei Yang Tan, Ashish Tiwari, Natarajan Shankar, Sanjit A. Seshia and Sharad Malik. *IEEE Transactions on Emerging Topics in Computing: Special Issue on Nanoscale Architectures for Hardware Security, Trust and Reliability* ***(TETC)***, March 2014.

Conference Publications

- (**Invited**) "Towards Verifiably Secure Systems-on-Chip Platforms", Sujit Kumar Muduli and Pramod Subramanyan. To Appear in the Proceedings of the 28th IEEE Asian Test Symposium. **(ATS 2019)**. Kolkata, India. December 2019.
- "Verification of Authenticated Firmware Loaders", Sujit Kumar Muduli, Pramod Subramanyan and Sayak Ray. To Appear the Proceedings of 19th Conference on Formal Methods in Computer-Aided Design. **(FMCAD 2019)**. San Jose, CA. October 2019.
- "A Formal Approach to Secure Speculation", Kevin Cheang, Cameron Rasmussen, Sanjit A. Seshia and Pramod Subramanyan. Proceedings of the IEEE Computer Security Foundations Symposium. **(CSF 2019)**. Hoboken, NJ. June 2019.
- "Functional Analysis Attacks on Logic Locking", Deepak Sirone and Pramod Subramanyan. *Proceedings of Design Automation and Test in Europe.* ***(DATE 2019)***. Florence, Italy. March 2019.
- (**Invited**) "UCLID5: Integrating Modeling, Verification, Synthesis and Learning", Sanjit A. Seshia and Pramod Subramanyan. *Proceedings of the 16th ACM-IEEE International Conference on Formal Methods and Models for System Design* ***(MEMOCODE 2018)***, October 2018.
- "Lazy Self-Composition for Security Verification", Weikun Yang, Yakir Vizel, Pramod Subramanyan, Aarti Gupta and Sharad Malik. *Proceedings of the 30th International Conference on Computer Aided Verification.* ***(CAV 2018)***. Oxford, UK. July 2018.
- (**Best Paper**) "A Formal Foundation for Secure Remote Execution of Enclaves", Pramod Subramanyan, Rohit Sinha, Ilia Lebedev, Srinivas Devadas and Sanjit A. Seshia. *Proceedings of the ACM Conference on Computer and Communications Security* ***(CCS 2017)***. Dallas, TX. October 2017.
- "Malware Detection using Machine Learning Based Analysis of Virtual Memory Access Patterns", Zhixing Xu, Sayak Ray, Pramod Subramanyan and Sharad Malik. *Proceedings of Design Automation and Test in Europe.* ***(DATE 2017)***. Lausanne, Switzerland. March 2017.
- (**Invited**) "Specification and Modeling for Systems-on-Chip Security Verification", Sharad Malik and Pramod Subramanyan. *Proceedings of the Design Automation Conference (****DAC 2016****)*, June 2016, Austin, TX.
- "Verifying Information Flow Properties of Firmware using Symbolic Execution", Pramod Subramanyan, Sharad Malik, Hareesh Khattri, Abhranil Maiti and Jason Fung. *Proceedings of Design Automation and Test in Europe (****DATE 2016****)*, March 2016, Dresden, Germany.
- "Template-based Synthesis of Instruction-Level Abstractions for SoC Verification", Pramod Subramanyan, Yakir Vizel, Sayak Ray and Sharad Malik. *Proceedings of 15th Conference on Formal Methods in Computer-Aided Design. (****FMCAD 2015****)*, September 2015, Austin, TX.

- (**Best Student Paper**) "Evaluating the Security of Logic Encryption Algorithms", Pramod Subramanyan, Sayak Ray and Sharad Malik. *Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust (**HOST 2015**)*, May 2015, McLean, VA.

- "Template-based circuit understanding", Adria Gascon, Pramod Subramanyan, Bruno Dutertre, Ashish Tiwari, Dejan Jovanovic and Sharad Malik. *Proceedings of 14th Conference on Formal Methods in Computer-Aided Design. (**FMCAD 2014**)*, October 2014, Lausanne, Switzerland.

- "Formal Verification of Taint-propagation Security Properties in a Commercial SoC Design", Pramod Subramanyan and Divya Arora. *Proceedings of Design Automation and Test in Europe (**DATE 2014**)*, March 2014, Dresden, Germany.

- "All-SAT using Minimal Blocking Clauses", Yinlei Yu, Pramod Subramanyan, Nestan Tsiskaridze and Sharad Malik. *Proceedings of the 27th International Conference on VLSI Design (**VLSID 2014**)*, January 2014, Mumbai, India.

- "WordRev: Finding Word-Level Structures in a Sea of Bit-Level Gates", Wenchao Li, Adria Gascon, Pramod Subramanyan, Wei Yang Tan, Ashish Tiwari, Sharad Malik, Natarajan Shankar and Sanjit A. Seshia. *Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust **(HOST 2013)***, June 2013, Austin, TX.

- "Reverse Engineering Digital Circuits Using Functional Analysis", Pramod Subramanyan, Nestan Tsiskaridze, Kanika Pasricha, Dillon Reisman, Adriana Susnea and Sharad Malik, *Proceedings of Design Automation and Test In Europe (**DATE 2013**)*, March 2013, Grenoble, France.

- "Adaptive Execution Assistance for Multiplexed Fault-Tolerant Chip Multiprocessors", Pramod Subramanyan, Virendra Singh, Kewal Saluja and Erik Larsson, *Proceedings of the 29th IEEE International Conference on Computer Design, (**ICCD 2011**)*, October 2011, Amherst, MA.

- "Energy-Efficient Fault Tolerance in Chip Multiprocessors Using Critical Value Forwarding", Pramod Subramanyan, Virendra Singh, Kewal Saluja and Erik Larsson, *Proceedings of the 40th IEEE/IFIP International Conference on Dependable Systems and Networks (**DSN 2010**)*, June 2010, Chicago, IL.

- "Energy-Efficient Fault Tolerance in Chip Multiprocessors", Pramod Subramanyan, Virendra Singh, Kewal Saluja and Erik Larsson, *Proceedings in the 20th ACM Great Lakes Symposium on VLSI (**GLSVLSI 2010**)*, May 2010, Providence, RI.

- "Multiplexed Redundant Execution: A Technique for Efficient Fault Tolerance in Chip Multiprocessors", Pramod Subramanyan, Virendra Singh, Kewal Saluja and Erik Larsson. *Proceedings of Design Automation and Test In Europe (**DATE 2010**)*, March 2010, Dresden, Germany.

Other Publications

- "Generation of Minimal Leakage Input Vectors with Constrained NBTI Degradation", Pramod Subramanyan, Ram Rakesh Jangir, Jaynarayan Tudu, Erik Larsson and Virendra Singh. *Proceedings of the 7th East-West Design and Test Workshop (**EWDTS 2009**)*, September, Moscow, Russia.
- "Power-Efficient Redundant Execution for Chip Multiprocessors", Pramod Subramanyan, Virendra Singh, Kewal Saluja and Erik Larsson. *Proceedings of the 3rd Workshop on Dependable and Secure Nanocomputing (**WDSN 2009**) held in conjunction with DSN 2009*, June 2009, Lisbon, Portugal.
- "Accelerating Signal Processing Applications Using Graphics Processors", Ashwin Prasad and Pramod Subramanyan. *Proceedings of the 14th National Conference on Communications, (**NCC 2008**)*, February 2008, Mumbai, India.

Patents

- US Patent 8,040,276, October 18, 2011. "*Generation of Multi-satellite GPS Signals in Software*", Sastry Vadlamani, Vrishti Agrawal, Sanjeev G. Dhumawad, Pramod Subramanyan and Abhay Samant.
- "*Cache System With Biased Cache Line Replacement Policy and Method Therefor*", William L. Walker, Robert F. Krick, Tarun Nakra and Pramod Subramanyan. (Pending)

Awards

- ACM SIGDA Outstanding Ph.D. Dissertation Award in Electronic Design Automation. (2018)
- Best Paper Award, ACM Conference on Computer and Communications Security. (2017)
- Bede Liu Award for the Best Doctoral Thesis, Department of Electrical Engineering, Princeton University. (2017)
- Honorable Mention, IEEE System Validation and Debug Technology Council (SVDTC) Student Research Award. (2016)
- Wu Prize for Excellence, School of Engineering and Applied Science, Princeton University. (2015)
- Best Student Paper Award, IEEE International Symposium on Hardware-Oriented Security and Trust. (2015)
- Teaching Assistant Award, Department of Electrical Engineering, Princeton University for the course Introduction to Logic Design. (2014)
- Subramaniam Rajalakshmi Medal for best M.Sc (Engg.) thesis at the Supercomputer Education and Research Center, Indian Institute of Science. (2012)

Teaching Experience

- Instructor for "Computer Systems Security" (CS 628A) at the Indian Institute of Technology – Kanpur, Autumn 2019.
- Instructor for "Computer Systems Security" (CS 628A) at the Indian Institute of Technology – Kanpur, Spring 2019. (*Received a citation from the Academic Senate, IIT Kanpur for exceptionally good teaching evaluations.*)
- Instructor for "Designing Verifiably Secure Systems" (CS 698K) at the Indian Institute of Technology – Kanpur, Autumn 2018.

- Lead Teaching Assistant for "Formal Methods: Specification, Verification, and Synthesis" (EECS 219C) taught by Professor Sanjit Seshia, University of California, Berkeley, Spring 2018.
- Assistant in Instruction for "Designing Secure Systems" (ELE 476) taught by Professor Prateek Mittal, Princeton University, Fall 2014.
- Assistant in Instruction for "Introduction to Logic Design" (ELE 206/COS 306) taught by Professor Sharad Malik, Princeton University, Fall 2013.

Professional Experience

Indian Institute of Technology, Kanpur. Kanpur, India.

Assistant Professor (May 2018-Present)

I am an assistant professor in the Department of Computer Science and Engineering at IIT Kanpur. My research interests lie at the intersection of formal methods, security and systems.

University of California, Berkeley. Berkeley, CA.

Postdoctoral Researcher (January 2017-May 2018)

I was a postdoctoral researcher in Electrical Engineering and Computer Sciences at UC Berkeley. I worked on applying formal verification to hardware and system security concerns. My mentor was Professor Sanjit Seshia.

Intel Corporation. Santa Clara, CA and Hillsboro, OR.

Graduate Student Intern (Summers of 2013/14/15)

I worked in the Security Center of Excellence (SeCoE) and used formal techniques to verify security properties of hardware and firmware in Intel designs.

Advanced Micro Devices. Bangalore, India.

Design Engineer II (July 2010 to August 2011)

I worked in AMD India's performance modeling team where I developed simulators for core modeling, studied hardware features and enhancements and worked on the correlation of simulator and hardware (RTL) performance.

National Instruments. Bangalore, India.

Staff Software Engineer (May 2008 to July 2008)

Software Engineer (July 2006 to April 2008)

I was part of the radio frequency (RF) software group where I developed high-performance signal processing algorithms.

SERVICE

- VLSID 2019 Tutorial, "Logic Locking: Current Trends, Attacks and Future Directions", with Ujjwal Guin.
- DAC 2017 Tutorial, "Security Validation in Modern Systems-on-Chip", with Jason Fung and Sharad Malik.
- Program committees: VLSI Design Conference 2019, Secure Knowledge Management (SKM) 2019, Design Automation Conference (DAC) 2018 and 2019, ICISS 2018, Top Picks in Hardware and Embedded Security (TopInHES) 2018, Design Automation for Understanding Hardware Designs (DUHDe) 2019.
- Journal Reviewing: ACM JETC, IEEE TCAD, IEEE TETC, IEEE TIFS, IEEE ToC, Springer JETTA.
- Conference Reviewing: CAV 2019, CAV 2018, DAC 2017, FMCAD 2016, SAT 2015, ICCAD 2015, ICCD 2011.

PROFESSIONAL MEMBERSHIPS

Member of the IEEE and ACM.