Anirudh Srikant Iyengar

Security Researcher
Intel Product Assurance and Security (IPAS)
Ph: 813-992-2296 E-mail: anirudh.s.iyengar@intel.com
Website: https://anirudhiyengar.github.io

Summary:

A recent Intel hire with experience in device, circuit, and micro-architecture design with an emphasis on emerging memory technologies, looking to pursue a career in design and security.

Education:

- **Ph.D. in EECS,** University of South Florida continued at Pennsylvania State University (Aug 2018-Completed), GPA of 3.85/4.0.
- **M.S.E.E**, University of South Florida. (May 2013), GPA of 3.70/4.0.
- **B.E in Instrumentation and Control,** Manipal Institute of Technology, India, (June 2010). GPA 7.76/10.

Employment:

- Security Researcher, Intel Product Assurance and Security (IPAS) Intel Corp. (present).
  - → Analyzing and evaluating security concerns surrounding the Intel server platform.
  - → Researching upcoming threats that can compromise Intel products.
- Research Assistant, School of Electrical Engineering and Computer Science, PSU (fall 2017 – spring 2018).
- Student Intern at Security Center of Excellence (SeCoE) Intel Corp. (summer 2017).
  - → Working on a security validation framework/tool for writing tests centered on IP security validation.
- Research Assistant, School of Electrical Engineering and Computer Science, PSU (fall 2016 – spring 2017).
- Student Intern at Security Center of Excellence (SeCoE) Intel Corp – *focus on 3DXpoint security***.** (summer 2016).
  - → Worked on realizing the 3DXpoint memory as a Physically Unclonnable Function (PUF).
- Teaching Assistant, Department of Computer Science and Engineering, USF (spring 2015 – fall 2015).
  - → Taught Logic Design and assisted with the Introduction to FPGA and CMOS-VLSI course.
- Research Assistant, Department of Computer Science and Engineering, USF (fall 2013 – spring 2016).
- Tutor at the athletics department for, USF (spring 2012).
  - → Taught basic Chemistry and Physics to student athletes.
- Assistant Software Engineer, Accenture, India (August 2010).

Technical Skills:

- Languages: Verilog HDL, VerilogA HDL, PERL, Python, C, C++, VHDL.
- Design: Cadence Virtuoso (layout & schematic), L-edit, Xilinx ISE, Circuit-maker.
- Simulation: Matlab, Hspice, Spectre, LT-Spice, Simple scalar, Model SIM, Questa SIM, PSpice.

Research:

My research is focused towards emerging spintronic devices for low-power and enhanced security. In particular, I am interested in the following topics:

- **Security using spintronics:** In this project, I investigate the prospects and challenges of spintronic devices towards hardware security.
  - → Investigating the emerging threat models, detection and protection mechanisms associated with spintronic memories. [J4, J5, C4, C7, C9].
  - → Exploit the randomness in Domain Wall dynamics for security primitives such as Physically Unclonable Functions. (**An inter/intra die Hamming distance of ~50%/5% was achieved**) [J1, J4, C2].
  - → Additionally, I have explored the side channel vulnerabilities of STTRAM memory and have provided some low-overhead countermeasures [C8].

- **Application of spintronics [sponsored by SRC]:** In this project, I investigate the state retentive sequentials and non-volatile cache. [J3]

  → Modeling, circuit design and micro-architectures for robust, low-power and energy efficient Domain wall memories (DWM). (**3-33% performance and 1.2X-14.4X power improvement achieved**) [J1, J2, C1, C3].

- **Reliability and retention analysis of spin transfer torque RAM (STTRAM) memory:** In this project I am modeling the STTRAM lifetime and retention and developing algorithms for test time improvement. [J5, J9, J10, C7, C10]

- **Camouflaging of circuit design using threshold defined switches [sponsored by DARPA]:** In this project, I investigate the potential security application of threshold voltage defined switches in circuit camouflaging.

  → Investigate the tradeoff between area and performance overhead against reverse engineering effort [C5, C6].

  → Look at the best-case implementation of camouflage gates, quantified over circuit node's observability and controllability metrics [P6].

  → Investigate a Charge-trap based camouflage circuit that allows dynamic selection of camouflage gates [C11].

- **Integrity and authentication of Printed Circuit Boards [PCB]:** In this project, I investigate some countermeasures to mitigate PCB cloning, and put forth benchmarks to test PCB security [B1, P5].

  → I have also worked on PCB based PUFs for board authentication. [C9, P9]

Publications:

Journals:

J1. **A. Iyengar**, S. Ghosh, K. Ramclam, "Domain Wall Magnets for Embedded Memory and Hardware Security"**, JETCAS**, 2014.

J2. S. Motaman, **Anirudh Iyengar**, and S. Ghosh, "Domain Wall Memory—layout, circuits and synergistic systems", **TNANO**, 2014. **Impact Factor: 1.62.**

J3. **A. Iyengar**, S. Ghosh, and J. Jang. "MTJ-Based State Retentive Flip-Flop with Enhanced-Scan Capability to Sustain Sudden Power Failure." **TCAS-I** (2015).

J4. **A. Iyengar**, S. Ghosh, K. Ramclam, J. Jang and C. Lin, "Spintronic PUFs for Security, Trust and Authentication" **JETC** (Special Issue on Secure and Trustworthy Computing), 2015.

J5. **A. Iyengar**, S. Srinivasan and S. Ghosh, "Retention Testing Methodology for STTRAM" **IEEE Design & Test**, 2016.

J6. S. Ghosh, **A. Iyengar** et. al, "Circuits, Systems and Applications of Spintronics" **JETCAS**, 2017.

J7. S. Ghosh, RV Joshi, D Somasekhar, X Li, **A. Iyengar** et. al, "EMERGING MEMORIES—TECHNOLOGY, ARCHITECTURE, AND APPLICATIONS—SECOND ISSUE" **JETCAS,** 2017**.**

J8. S. Ghosh, R. Jha, **A. Iyengar,** and R. Govindaraj. "Design Space Exploration for Selector Diode-STTRAM Crossbar Arrays." IEEE Transactions on Magnetics **(TMAG)** 54, no. 6 (2018): 1-5.

J9. **A. Iyengar**, S. Ghosh, & N. Rathi, (2018). Magnetic Tunnel Junction Reliability Assessment under Process Variations and Activity Factors and Mitigation Techniques. Journal of Low Power Electronics **(JOLPE)**, 14(2), 217-226.

J10. N. I. Khan, **A. Iyengar** & S. Ghosh "Novel Magnetic Burn-In for Retention and Magnetic Tolerance Testing of STTRAM" IEEE Transactions on Very Large Scale Integration (VLSI) Systems **(TVLSI),** 2018**.**

J11. **A. Iyengar**, F. Zhang, S. Bhunia & S. Ghosh "Split-Manufacturing of Printed Circuit Boards", **MDPI Cybersecurity (submitted)**.

J12. JW. Jang, A. De, D. Vontela, I. Nirmala, S. Ghosh **& A. Iyengar**, S. Ghosh, "Threshold-defined Logic and Interconnect for Protection against Reverse Engineering" IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (**TCAD**), 2018.

Conferences:

C1. **A. Iyengar** and S. Ghosh, "Modeling and analysis of domain wall dynamics for robust and low-power embedded memory." In Design Automation Conference **(DAC)**, 2014 51st ACM/EDAC/IEEE, pp. 1-6. IEEE, 2014.

C2. **A. Iyengar,** K. Ramclam, S. Ghosh, "DWM-PUF: A Low-overhead, Memory-based Security Primitive." In Hardware-Oriented Security and Trust **(HOST)**, 2014 IEEE International Symposium on, pp. 154-159. IEEE, 2014.

C3. S. Motaman, **A. Iyengar**, and S. Ghosh. "Synergistic circuit and system design for energy-efficient and robust domain wall caches." In Proceedings of the 2014 international symposium on Low power electronics and design **(ISLPED)**, pp. 195-200. ACM, 2014.

C4. N. Rathi, S. Ghosh, **A. Iyengar** and H. Naeimi, "Data Privacy in Non-Volatile Cache: Challenges, Attack Models and Solutions." In Design Automation Conference **(ASP-DAC),** 2016 21st Asia and South Pacific, pp. 348-353. IEEE, 2016.

C5. **A. Iyengar** and S. Ghosh, "Threshold Voltage-Defined Switches for Programmable Gates", **GOMACTech**, 2015.

C6. I. Nirmala, D. Vontela, S. Ghosh, **A. Iyengar** "A novel threshold voltage defined switch for circuit camouflaging." In Test Symposium **(ETS),** 2016 21th IEEE European, pp. 1-2. IEEE, 2016.

C7. **A. Iyengar,** "Retention Testing Methodology for STTRAM" **TECHCON 2016**.

C8. **A. Iyengar,** S. Ghosh, N. Rathi & H. Naeimi "Side channel attacks on STTRAM and low-overhead countermeasures." In 2016 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems **(DFT),** pp. 141-146. IEEE, 2016**.**

C9. **A. Iyengar,** N. Vobilisetti & S. Ghosh, "Authentication of Printed Circuit Boards." In 42nd International Symposium for Testing and Failure Analysis, (**ISTFA)** 2016. ASM International, 2016.

C10. N.I.Khan, **A. Iyengar** & S. Ghosh "Novel Magnetic Burn-In for Retention Testing of STTRAM." In 2017 Design, Automation & Test in Europe Conference & Exhibition **(DATE**), pp. 666-669. IEEE, 2017**.**

C11. A. De, **A. Iyengar** et. al, "CTCG: Charge-Trap Based Camouflaged Gates for Reverse Engineering Prevention." In 2018 IEEE International Symposium on Hardware Oriented Security and Trust **(HOST)**, pp. 103-110. IEEE, 2018.

C12. **A. Iyengar,** et. al "Threshold Defined Camouflaged Gates in 65nm Technology for Reverse Engineering Protection." In Proceedings of the International Symposium on Low Power Electronics and Design (**ISLPED)**, p. 6. ACM, 2018.

Poster Presentations:

P1. **A. Iyengar**, K. Ramclam, Jae-Won Jang & C. W. Lin, "Spintronic PUFs for Security, Trust and Authentication", Cyber Security Awareness Week Conference (**CSAW**), 2014.

P2. **A. Iyengar**, N. Rathi, S. Ghosh, "Static and Dynamic Current Throttling for Improved Oxide Lifetime of STTRAM Arrays", IEEE Design Automation Conference (***DAC***), 2015.

P3. **A. Iyengar**, S. Ghosh, D. Vontela & I. R. Nirmala "Threshold Defined Logic Engines and Applications", Florida Institute for Cybersecurity Research (**FICS**), 2016.

P4. **A. Iyengar** & S. Ghosh, "Threshold Voltage-Defined Switches for Programmable Gates", Government Microcircuit Applications & Critical Technology Conference (**GOMACTech**), 2016.

P5. **A. Iyengar**, F. Zhang, S. Ghosh & S. Bhunia, "Split-Manufacturing of Printed Circuit Boards", IEEE Design Automation Conference (**DAC**), 2016.

P6. **A. Iyengar**, D. Vontela, I. Reddy Nirmala & S. Ghosh, "A Novel Threshold Voltage Defined Switch for Circuit Camouflaging", IEEE European Test Symposium (**ETS**), 2016.

P7. **A. Iyengar,** "Spintronic memory towards Secure and Energy-Efficient Computing" **PhD Forum at DAC** 2016.

P8. **A. Iyengar**, "Retention Testing Methodology for STTRAM" abstract accepted for a full paper & poster presentation in **TECHCON 2016**.

P9. **A. Iyengar,** S. Ghosh "Side Channel Attacks on STTRAM and Low-Overhead Countermeasures" **GOMACTech 2017.**

P10. **A.Iyengar,** S. Ghosh "Protecting Sensitive Intellectual Property Even Under Full Reverse Engineering of Functionality" **GOMACTech 2018.**

P11. **A. Iyengar,** "Spintronic memory towards Secure and Low-Power Computing" **PhD Forum at DATE 2018**.

Book Chapters:

B1. **A. Iyengar** & S. Ghosh, "Hardware Trojans and Piracy of PCBs." In The Hardware Trojan War, pp. 125-145. Springer, Cham, 2018. Springer International.

Invention Disclosures (Patents):

D1. Physically unclonable function based on domain wall memory and method of use**,** Swaroop Ghosh, **Anirudh Iyengar**, and Kenneth Ramclam (US9859018B2).

D2. Non-Volatile Flip-Flop with Enhanced-Scan Capability to Sustain Sudden Power Failure**,** Swaroop Ghosh and **Anirudh Iyengar** (US9728241B2).

D3. Threshold Voltage Defined Switches for Programmable Camouflage Gates, **Anirudh Iyengar**, Swaroop Ghosh, Deepakreddy Vontela & Ithihasa Reddy Nirmala (US20180302095A1).

Projects:

- **Layout Design of the Memory controller**: Designed and tested (LVS, DRC) of a memory controller used in a STTRAM sensing circuit. (was a collaborative effort with my colleagues from our Lab)
- **Identifying Open-Research Problems:** Propose ideas to implement Control-flow Integrity in an effort to thwart ROP and JOP based attacks.
- **ROP Attack:** Deploy various flavors of ROP attacks (using buffer overflow) using shared library functions and ROP gadgets from the executable code to invoke more powerful and robust attacks.
- **Password Management:** Design a password management system which strengthens the user's passwords for the given domains dynamically using a master password to resist against brute force and guessing attacks.
- **Charge Trap-based Camouflage Gates (CTCG) for Reverse Engineering Prevention:** Propose a CTCG which are resilient towards various RE attacks, without requiring a process change in realizing them.
- **Robust & Energy-Efficient Domain Wall Caches:** Exploit the trade-off between power and performance by address-based and work-load based cache monitoring.
- **SPA-Based attack on DES Encryption:** Crack the encryption key through a Trojan based side channel attack.
- **Design of low-power ALU with wide operating range**: Optimizing circuit design to sustain high performance at low power
- **Safety System for a Semi-Automatic Robot (**January-May 2010**):** Create a safety device for a human controlled robot that is capable of working in an obstacle-filled terrain.
- **Huffman Encoder:** Characters were assigned a bit size depending on their frequency of occurrence, using Verilog HDL.
- **Micro- UART**: Design of the Universal Asynchronous Receiver and Transmitter in Verilog HDL.
- **AMBA APB Protocol:** Data management, control, transmission & reception using Sys Verilog.

Leadership and Awards:

- **Won** the **Best Poster prize** at the 2018 PhD Forum at DATE.
- **Won** the **Best Poster Presentation award** at the 2016 PhD Forum at DAC.
- **Third place** in **Embedded Security Challenge** at Cyber Security Awareness Week Conference (**CSAW**), 2014.
- An article in ***IEEE XPLORE Innovation Spotlight***, titled "Domain Wall Memory: The Next Big Thing in Hardware Security?" July 2015.
- Organized and moderated events in the Fifth National Control Instrumentation Conference (CISCON) held at MIT, Manipal during November 2008.The conference is a National Annual event with participation from all over India.

Certifications:

- Plasma Etch Seminar (January 2012), hosted by Plasma Therm LLC.
- VLSI and Advanced System Design and Verification from January-June 2011, Sandeepani School organized by Core EL technologies, an authorized training partner of XILINX corp.
- Industrial Distributed control systems using Centum CS3000 under the guidance of the organization head, Broadfield Solutions from August-November 2010 as a project intern.

References:

Dr. Swaroop Ghosh

Assistant Professor

School of Electrical Engineering and Computer Science

Office: 319 Electrical Engineering East

Email: szg212@psu.edu

Phone: 814-865-1298

Dr. Ram Krishnamurthy

Principal Engineer

NEW TECHNOLOGY SUPER GROUP

INTEL LABS

Email: ram.krishnamurthy@intel.com

Phone: 503-712-5548

Dr. Sumeet Gupta

Assistant Professor of ECE

School of Electrical Engineering and Computer Science

Office: Electrical Engineering Building, 465 Northwestern Ave.

Email: guptask@purdue.edu

Phone: 765-496-6371

Dr. Sachhidh Kannan

Storage Security Architect and Security Researcher

NONVOLATILE MEMORY SOLUTIONS GROUP

Intel Corporation

Email: sachhidh.kannan@intel.com