Patanjali SLPSK
Assistant Professor
School of Computer and Cybersciences, Augusta University, Georgia
100 Grace Hopper Lane, Augusta, Georgia, 30904
patanjali.sristi@augusta.edu

RESEARCH INTEREST

My research focuses on addressing a fundamental question: "How can we ensure affordable security assurances for a given hardware design in the context of an untrusted supply chain while respecting the design constraints at each level of abstraction?" These themes are crucial in the design of hardware for IoT, AI, and data-centre applications, where security resources are often scarce. In this context, I have explored applying statistical learning techniques to tackle various aspects of system design. My research primarily focuses on building Machine learning (ML) models to tackle the security challenges in different design abstractions and also in different stages of the hardware supply chain. I have also worked on using machine learning techniques for designing energy-efficient systems and applying AI techniques for network security. I wish to continue contributing to the following research areas:

- **AI for System Design:** Data modelling and developing AI-models for designing the next generation of hardware systems
- **AI for Hardware Security:** Data modelling and AI-models for efficient countermeasure evaluation, vulnerability detection and AI-assisted countermeasures for mitigating higher-order supply chain threats
- **Cybersecurity for AI:** Developing metrics and algorithms for secure development, depolyment and operations of AI-systems

ACADEMIC BACKGROUND

Ph.D. Computer Science and Engineering 2020
Indian Institute of Technology Madras, Chennai, India

- Ph.D. in Computer Science under the guidance of prof. Kamakoti Veezhinathan.
- CGPA: 8.29
- Dissertation title: Gate Sizing For Energy Efficient and Secure Digital Design.

M.S. Computer Science 2014
Indian Institute of Technology, Madras , Chennai, India

- Focus areas: CAD for Low Power VLSI. (**Converted to PhD in 2014**).
- CGPA: 8.6

B.Tech. Electronics and Communication Engineering 2011
Pondicherry Engineering College , Puducherry, India

- CGPA: 8.32

EMPLOYMENT HISTORY

Postdoctoral Researcher Nov 2019 - Present
Warren B. Nelms Institute for the Connected World, University of Florida, Gainesville, FL, USA.

Research and Teaching Assistant June 2012 - Nov 2019
Indian Institute of Technology Madras, Chennai, India.

Research Intern June 2015 - Dec 2015
IBM Integrated Systems Development Lab, Bangalore

RESEARCH ARTICLES (Under Review)

2. Christopher Vega, **Patanjali SLPSK**, Shubhra Deb Paul, Swarup Bhunia (2022). FlexPUF:A Flexible Physical Unclonable Function Design Using Configurable Templates. ACM Journal on Emerging Technologies in Computing Systems (JETC).
1. Kshitij Raj, Atri Chatterjee, **Patanjali SLPSK**, Sandip Ray, Swarup Bhunia. SENTRY: Protecting System-on-Chip designs against Supply Chain attacks. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD).

JOURNAL ARTICLES (Published)

∗ - denotes work done during Postdoc. | - denotes work done during Ph.D.
See also my google scholar page.

10. ∗ Christopher Vega, **Patanjali SLPSK**, Swarup Bhunia. IOLock: An Input/Output Locking Scheme for Protection Against Reverse Engineering Attacks. IEEE Transactions on Very Large Scale Integration (VLSI) Systems (2023). **accepted. to appear.**
9. ∗ Jonathan Cruz, **Patanjali SLPSK**, Pravin Gaikwad, Swarup Bhunia. TVF: A Metric for Quantifying Vulnerability against Hardware Trojan Attacks. IEEE Transactions on VLSI (TVLSI), 31 (7), pp. 969-979.
8. ∗ **Patanjali SLPSK**, Sandip Ray, Swarup Bhunia (2022). TREEHOUSE: A Secure Asset Management Infrastructure For Protecting 3DIC Designs. IEEE Transactions on Computers, 72(8), pp. 2306-2320.
7. ∗**Patanjali SLPSK**, Abhishek Anil Nair, Chester Rebeiro, Swarup Bhunia (2022). SIGNED: A Challenge-Response Scheme for Electronic Hardware Watermarking. IEEE Transactions on Computers, 72(6), pp. 1763-1777.
6. ∗ Shubhra Deb Paul, Fengchao Zhang, **Patanjali SLPSK**, Amit Ranjan Trivedi, Swarup Bhunia (2022). RIHANN: Remote IoT Hardware Authentication with Intrinsic Identifiers. IEEE Internet of Things Journal, 9(24), 24615-24627.
5. ∗ Fengchao Zhang, Shubhra Deb Paul, **Patanjali SLPSK**, Amit Ranjan Trivedi, Swarup Bhunia. (2020). On database-free authentication of microelectronic components. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 29(1), 149-161.
4. ∗ Tamzidul Hoque, **Patanjali SLPSK**, Swarup Bhunia (2020). Trust issues in microelectronics: The concerns and the countermeasures. IEEE Consumer Electronics Magazine, 9(6), 72-83.
3. | Rahul Bodduna, Vinod Ganesan, **Patanjali SLPSK**, Kamakoti Veezhinathan, Chester Rebeiro. (2020). Brutus: Refuting the security claims of the cache timing randomization countermeasure proposed in ceaser. IEEE Computer Architecture Letters, 19(1), 9-12.
2. | **Patanjali SLPSK**, Milan Patnaik, Seetal Potluri, Kamakoti Veezhinathan (2018). Mltimer: Leakage power minimization in digital circuits using machine learning and adaptive lazy timing analysis. Journal of Low Power Electronics, 14(2), 285-301.
1. | Gnanambikai Krishnakumar, **Patanjali SLPSK**, Prasanna Karthik Vairam, Chester Rebeiro, Kamakoti Veezhinathan (2018). GANDALF: A Fine-Grained Hardware–Software Co-Design for Preventing Memory Attacks. IEEE Embedded Systems Letters, 10(3), 83-86.

CONFERENCE PUBLICATIONS

11. * Christopher Vega, **Patanjali SLPSK**, Shubhra Deb Paul, Atri Chatterjee, Swarup Bhunia. MeLPUF: Memory-in-Logic PUF Structures for Low-Overhead IC Authentication. In 2023 IEEE Physical Assurance and Inspection of Electronics (PAINE), Huntsville, AL, USA, 2023, pp. 1-7.
10. * Pravin Gaikwad, **Patanjali SLPSK**, Swarup Bhunia. Invisible Scan for Protecting Against Scan-Based Attacks: You Can't Attack What You Can't See. In 2023 IEEE International Test Conference India (ITC India)(pp. 1-6).
9. * **Patanjali SLPSK**, Jonathan Cruz, Sandip Ray, Swarup Bhunia. PROTECTS: Secure Provisioning of System-on-Chip Assets in Untrusted Testing Facility. In 2023 IEEE International Test Conference India (ITC India) (pp. 1-6).
8. * Pritwish Basu Roy, **Patanjali SLPSK**, Chester Rebeiro (2022, January). Avatar: Reinforcing Fault Attack Countermeasures in EDA with Fault Transformations. In 2022 27th Asia and South Pacific Design Automation Conference (ASP-DAC) (pp. 417-422).
7. * Shuo Yang, Prabuddha Chakraborty, **Patanjali SLPSK**, Swarup Bhunia (2021, April). Trusted electronic systems with untrusted cots. In 2021 22nd International Symposium on Quality Electronic Design (ISQED) (pp. 198-203).
6. * Tamzidul Hoque, **Patanjali SLPSK**, Swarup Bhunia (2020, September). Trust issues in cots: The challenges and emerging solution. In Proceedings of the 2020 on Great Lakes Symposium on VLSI (pp. 211-216).
5. | Gargi Mitra, Prasanna Karthik Vairam, **Patanjali SLPSK**, Nitin Chandrachoodan, Kamakoti Veezhinathan (2020, June). Depending on HTTP/2 for Privacy? Good Luck!. In 2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) (pp. 278-285).
4. | Milind Srivastava, **Patanjali SLPSK**, Indrani Roy, Chester Rebeiro, Aritra Hazra, Swarup Bhunia. (2020, March). SOLOMON: An automated framework for detecting fault attack vulnerabilities in hardware. In 2020 Design, Automation & Test in Europe Conference & Exhibition (DATE) (pp. 310-313).
3. | **Patanjali SLPSK**, Prasanna Karthik Vairam, Chester Rebeiro, Kamakoti Veezhinathan (2019, November). Karna: A gate-sizing based security aware EDA flow for improved power side-channel attack protection. In 2019 IEEE/ACM International Conference on Computer-Aided Design (ICCAD) (pp. 1-8).
2. | Gargi Mitra, Prasanna Karthik Vairam, **Patanjali SLPSK**, Nitin Chandrachoodan , Kamakoti Veezhinathan (2019, August). White mirror: Leaking sensitive information from interactive Netflix movies using encrypted traffic analysis. In Proceedings of the ACM SIGCOMM 2019 Conference Posters and Demos (pp. 122-124).
1. | Gautham, Ashok, Kunal Korgaonkar, **Patanjali SLPSK**, Shankar Balachandran, Kamakoti Veezhinathan (2012, October). The Implications of Shared Data Synchronization Techniques on Multi-Core Energy Efficiency. In 2012 Workshop on Power-Aware Computing and Systems (HotPower 12).

POSTER PRESENTATIONS

3. | **Patanjali SLPSK**, Prasanna Karthik Vairam, Chester Rebeiro, Kamakoti Veezhinathan (2019, June). Karna: A Security Aware EDA Flow for Improved Side-Channel Attack Protection. In Proceedings of the 2019 Design Automation Conference (DAC 2019) under the Work-In-Progress section.
2. | **Patanjali SLPSK**, Seetal Potluri, Kamakoti Veezhinathan (2015, June). HALTimer: A Fast Vt Replacement Heuristic for Leakage Power Minimization.

In Proceedings of 2015 Design Automation conference (DAC'15) under Work-In-Progress section

1. | **Patanjali SLPSK**, Seetal Potluri, Kamakoti Veezhinathan (2014, June). FastReplace: Efficient Vt Replacement Technique for Leakage Power Minimization. In Proceedings of the 2014 Design Automation Conference (DAC 2014)under Work-In-Progress section.

PATENTS

6. * Swarup Bhunia, Christopher Vega, Reiner Dizon, Rohan Reddy Kalavakonda, **Patanjali SLPSK** . "Reconfigurable jtag architecture for implementation of programmable hardware security features in digital designs." U.S. Patent Application 17/661,232.
5. * Swarup Bhunia, Atul Prasad Deb Nath, Kshitij Raj, Sandip Ray, **Patanjali SLPSK** Sriramakumara. "Establishing trust in untrusted ic testing and provisioning environment." U.S. Patent Application 17/662,399.
4. * Swarup Bhunia, Prabuddha Chakraborty, Reiner Dizon-Paradis, Parker Difuntorum, Christopher Vega, **Patanjali SLPSK** (2022). Drone-based administration of remotely located instruments and gadgets. U.S. Patent Application 17/467,823.
3. * Prabuddha Chakraborty, Reiner Dizon-Paradis, Christopher Vega, Joel B. Harley, Sandip Ray, Swarup Bhunia, **Patanjali SLPSK** (2022). Smart Infrastructures and First-Responder Network for Security and Safety Hazards. U.S. Patent Application 17/392,376.
2. * Swarup Bhunia, Christopher Vega, Shubhra Deb Paul,Parker Difuntorum, Reiner Dizon-Paradis, **Patanjali SLPSK** (2021). DEFENSE OF JTAG I/O NETWORK. U.S. Patent Application 17/303,648.
1. * Swarup Bhunia, Tamzidul Hoque, Abhishek Anil Nair, **Patanjali SLPSK** (2021). Framework for obfuscation based watermarking. U.S. Patent Application 17/224,559.

SPECIAL ACHIEVEMENTS

Awards

- **Finalist** AI-vs-Humans Security Challenge, CSAW 2022.
- **Finalist** Logic Locking Contest, CSAW 2022.
- **One of the Seven Finalists** SIGDA PHD Forum, DAC 2020.
- **Winner and Runner-up** in Applied Research Competition in CSAW 2020. (Along with Gargi Mitra and Prasanna Karthik Vairam).
- **Runner-up** in Student Hardware Demo in the NELMS Annual IoT Conference.
- **Winner** in Applied Research contest Shaastra 2019, IIT Madras.
- One of the top-100 (rank:40) of the technical writing challenge conducted by Department of Science and Technology, India.
- **First Place** in Embedded Systems Challenge in CSAW 2016.
- Second Place in HackU 2013 at IIT Madras.
- STAR Teaching Assistant Award, Computer Science Department, IIT Madras 2018.

In the Media

- Our work on System-on-Chip Security was featured in the news.
- Our work on Memory-In-Logic PUF was featured in the news.

- Our article on Privacy issues on Video Streaming Applications was featured in wired Magazine
- Our work on the CSAW 2016 challenge was featured in Business Insider.

Invited Lectures and Talk

- Delivered a Webinar on AI-guided heuristics for Trojan Attacks at IEEE CEDA/HSTTC organized Webinar on CAD for Assurance.
- Delivered a demonstration on Secure SoC Architectures at Northrop Grumman. Jan 2023.
- Delivered a talk on Cybersecurity and System Design at Sony Finishing School. IITM Pravaratak. June 2024.

Professional Activities (Selected)

- Conducted a workshop on Hardware Security"Hardware-based Attacks and Defenses" at IITM Pravartak. $7-8^{th}$ March 2024.
- Technical Program Committee (TPC) Member for IEEE/ACM International Conference on Computer-Aided Design (ICCAD), 2020, 2021, 2022.
- Artefact Reviewer for Eurosys 2021.
- Shadow PC Member for Eurosys 2021.
- *Reviewing Experience*
  Reviewer for journals: HASS, JETC, IEEE IOT Journal, TIFS, TECS, TCAD, TVLSI, TC, and Embedded System Letters.
  Reviewer of Conferences: DAC 2020 and DAC 2019.

RESEARCH EXPERIENCE

- **Automatic Implementation of Secure Silicon (Feb 2021-Current)**
  Project Lead
  The primary goal of the DARPA AISS project is to develop secure System on Chips (SoCs) that can be widely used by designers with varying range of security expertise. However, it is also crucial to ensure that the security architectures are compliant with the power, performance, and area requirements.
  Critical Outcomes produced
  1. Developed and demonstrated a proof-of-concept implementation a complete SoC implementation with hardware and firmware support for integrating PUF, Logic Locking protocols, and IP watermarking techniques.
  2. Developed AI-models for identifying vulnerable locations in the SoC.
  3. Developed a secure boot methodology for provisioning critical assets during boot time.
  4. Developed a security specification language for describing security requirements at the user-level.
- **Lightweight Authentication Protocols for securing IoT Devices (June 2020- Current)**
  Counterfeit integrated circuits (ICs) have become a significant security concern in the semiconductor industry as a result of the increasingly complex and distributed nature of the supply chain. These counterfeit chips may result in performance degradation, profit reduction, and reputation risk for the manufacturer. Therefore, developing effective countermeasures against such malpractices is becoming severely crucial. As a part of our research effort we develop lightweight authentication techniques using Physically Unclonable Functions (PUFs) and watermarks for detecting counterfeit ICs.

Critical Outcomes:

1. Developed a challenge-vector free authentication technique using delay variations in boundary scan-chains.
2. Developed a hybrid PUF protocol that combines the benefits of strong and weak PUFs by integrating bistable elements in design logic.
3. Developed a lightweight watermarking technique for verifying IP provenance.
4. Developed ML-models for demonstrating the efficiency of the watermark and PUF signatures.

- **RTL-level Security estimation of digital designs (Jan 2018-Dec 2018)**
  Embedded devices have started playing an increasing role in our day-to-day lives, due to the emergence of IoT, leading to the question "Can these devices be trusted?". The emergence of side-channel attacks in the recent years has shown that the underlying hardware too has to be secured. This quest for quantifying the resilience of the device to the side channels has led researchers to develop several statistical metrics. However, these metrics i) quantify the security of a **manufactured** device, thereby functioning only in a preventive capacity ii) they do not explore or identify the root cause of the vulnerability. Our works seeks to address these two problems by
  - Identifying the optimizations/changes made to the device during the transition from a High level language (eg: Verilog) to actual hardware and quantifying its impact to the security of the device.
  - Propose a security aware power optimization scheme that takes in to account the security metric along with the other design constraints.

  Critical Outcomes:

  1. Developed an RTL-level framework that would help designers map the vulnerable RTL-code to their corresponding gate-level or layout-level counterpart (SOLOMON DATE'2018).
  2. Developed a gate-sizing framework for optimization gates to meet both security and power objectives (AVATAR ASPDAC'2022).

- **Hardware-Software codesign framework for preventing memory attacks on embedded systems (June 2016-Dec 2016)**
  Embedded Systems operate in resource-constrained settings and often operate on sensitive data. Thus their security is important but any security protocol that is deployed must not incur significant overheads. It is also important to ensure that the security countermeasure be lightweight so as to not become the focal point of novel attack vectors in the field.
  Critical Outcomes:
  - **Won first place in Embededd systems challenge in CSAW 2016**.
  - Developed a **lightweight** full-stack architecture to prevent memory attacks on OpenRISC processors.
  - Our framework allows legacy code and protected to co-exist without any additional overheads.We demonstrate this by running Linux and execute the protected code on top of it.
  - We achieve complete temporal safety with only 1% delay overhead 0% area overhead, 60% code size increase.

- **AI-guided heurisitics for Leakage Power Minimzation in Digital Circuits. (Jan 2016-Dec 2017)**

  Power optimization techniques in a VLSI flow typically end up being the performance bottlenecks leading to a large turn around time for the following reasons 1. **Scalability**: The design typically spans millions and millions of gates with different operating conditions leading to a large search space. 2. **Portability**: The constraints vary across technology nodes hindering reusability of solutions. ML models are inherently trained to operate on large datasets and navigate a complex search space. The contributions of our work are as follows.

  Critical Outcomes:

  1. We propose a novel learning (Support Vector Machine) based classifier, which provides a good initial design configuration that guarantees leakage optimal solution.
  2. We use a Lazy Timing Analysis procedure that postpones the timing validation step as much as possible.
  3. We show the efficiency of our technique on large scale benchmark datasets (25K - 1million gates). Our technique performs 23% better in terms of solution quality when compared with the state-of-the art technique and 50% better in terms of runtime.

- **A distributed EDA framework for scalable design management IBM System Development Labs India (June-December 2015)**

  In a typical design flow, multiple tools and scripts are used. Each tool reads the input, its associated constraints, processes and generates data as output. At present there is no mechanism to represent this data in a database which limits the possibility of live query on the data and get a useful information and value add out of it. For example: to find a timing critical path it requires to load a timer which in turn processes the input and eventually writes out report. Instead, it can be easily queried if the database is annotated with relevant information. The project produced the following outcomes:

  Critical Outcomes: Developed a distributed logic simulation framework in Scala that can:

  – Handle Hierarchical design data

  – Distribution over multiple clusters (as design is developed over multiple sites and multiple people and partitioned)

  – Extensible as data can be annotated with any information on top of the base structure.

TEACHING EXPERIENCE

As Instructor

- Co-taught a course on VLSI Circuits and Technology (EEE 6323), Spring 2022 at UF.

As Teaching Assistant

- Computer Organization and Architecture: 2013, 2014 and 2015
- Operating Systems: 2015, 2016.
- Digital Systems Testing and Testable Design: 2014, 2015, 2016, 2017, 2018, and 2019.
- CAD for VLSI: 2016, 2017, and 2018.
- Digital Design Verification: 2016, 2017.
- Secure Systems Engineering: 2016, 2017, 2018, and 2019

- GPU Programming: 2018
- **Labs** Set up CTF for Secure Systems Engineering courses in the years 2016-2019.
- Set up an X86 lab using Intel Atom and Galileo Boards for the years 2013-2015.

STUDENTS MENTORED

7. **Milind Srivatsava**
   Dual Degree, IIT Madras.
   Project Title: SOLOMON: An Automated Framework for Detecting Fault Attack Vulnerabilities in Hardware.
6. **Harish Reddy**
   Dual Degree, IIT Madras.
   Project Title: Privacy in Deep Learning.
5. **Pritwish Basu Roy**
   MS, IIT Madras.
   Project Title: Fault attack countermeasures using EDA transformations.
4. **Reiner Dizon**
   Ph.D. student, University of Florida.
   Project Title: Autonomous navigation of Drones for emergency applications
3. **Christopher Vega**
   Ph.D., University of Florida.
   Project Title: A fully synthesizable and configurable random number generator for low-power IoT applications
2. **Abhishek Anil Nair**
   Dual Degree, IIT Madras.
   Project Title: A low-overhead challenge-response based watermarking framework for IP protection.
1. **Archit Jaiswal**
   Research Intern, University of Florida.
   Project Title: A low-overhead watermarking framework for preventing software piracy

TECHNICAL SKILLS

- **Programming Languages:** C, C++, Python, MATLAB, Scala, Bluespec, VHDL and Verilog
- **Simulation Platforms** Xilinx, Altera, Cadence and Synopsys.

COURSEWORK

- **Machine Learning**: Machine Learning
- **VLSI**: CAD for VLSI, Digital Design Verification, Digital Systems Testing and Testable Design, Mapping Signal Processing algorithms to DSP architecures.
- **System Design**: Computer Architecture, Concurrent Programming
- **Security**: Foundations of Cryptography, Mathematical concepts in Computer science.

REFERENCES **Contact Information will be provided upon request.**

- Dr. V. Kamakoti, IIT Madras.
- Dr. Swarup Bhunia, University of Florida.
- Dr. Sandip Ray, University of Florida.
- Dr. Chester Rebeiro, IIT Madras.