Pranesh Santikellur

Personal Information

phone:	(91) 9886949575
Web page:	https://praneshss.github.io/profile
Google Scholar:	https://bit.ly/2LXi0u2
linkedin:	https://www.linkedin.com/in/praneshss
e-mail:	pranesh.santikellur@gmail.com, pranesh.sklr@iitkgp.ac.in

Profile

Currently, I am working as *Senior Embedded Security Researcher* at *Technology Innovation Institute*, Abu Dhabi, UAE. Prior to this, I pursued a Doctor of Philosophy (Ph.D.) at the Department of Computer Science, Indian Institute of Technology, Kharagpur under the supervision of Professor Rajat Subhra Chakraborty. **My dissertation focuses on the design and analysis of machine learning-based model building attacks on physically unclonable functions.** I'm yet to defend my PhD. Prior to joining IIT Kharagpur to pursue my PhD, I worked as an embedded Linux developer at Bengaluru, India for nearly 6 years.

Education

July 2017 - Dec 2021	*Ph.D. Research Scholar, Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur*
August 2006 - May 2010	*Bachelor of Engineering, Department of Computer Science , SDM College of Engineering and Technology, Dharwad* Percentage : 73.76
July 2004 - March 2006	*Higher Secondary (+2), Karnataka State Board* Percentage : 83.6
July 2003 - March 2004	*Class X, Karnataka State Board* Percentage : 86.88

Work Experience

Jan 2022 - Present — *Senior Embedded Security Researcher*

At *Technology Innovation Institute*(TII), My role included understanding and evaluating the Trusted Execution Environment landscape as part of the decision-making process of whether to develop or include existing TEEs as part of our product. In addition to an extensive review of existing literature on Intel SGX, I implemented SGX based applications and replicated page-fault and interrupt based attacks on Intel SGX. Furthermore, I have proposed two potential ideas which I am currently pursuing:

- An Evaluation of Machine Learning based Model-Stealing Attacks on Intel SGX.
- Malware Detection in a Trusted Execution Environment.

Sep 2016 - Apr 2020 *Senior Research Fellow (SRF)*.
I was part of a research project sponsored by Intel USA, entitled "Verification Challenges in Compression and Cryptographic Stacks in QuickAssist Technology" and worked under the guidance of Dr. Rajat Subhra Chakraborty. This included analysis of data compression efficiency on QAT hardware.

Dec 2012 - Sep 2016 *Firmware Engineer*
I was part of firmware design team at *Horner Engineering Automation Group*, Bengaluru, India. My responsibilities were:

- Ported the PLC product code-base from Linux Target Image Builder (LTIB) to Yocto for the new product.
- Developed the touch driver and implemented 3-point calibration rule to it.
- Involved in board bringing up of PLC products with embedded Linux OS.

Sep 2010 - Dec 2012 *Design Engineer*
I was part of embedded software team at *Processor Systems Pvt Ltd*, Bengaluru, India. The project was to build the control card for medical application. The tool used for the project were Nios-II Embedded processor. My responsibilities were

- Build the interactive terminal between soft-core MCU unit present inside Nios-II and computer through serial communication. This was also mainly used to download the firmware to flash.

Publications

Book **P. Santikellur** and R. S. Chakraborty, "Deep Learning for Computational Problems in Hardware Security: Modeling Attacks on Strong Physically Unclonable Function Circuits", Springer (forthcoming)

Journal Papers

P. Santikellur and R.S Chakraborty, "Intrinsic Dimension: A Deep Learning Assisted Empirical Metric to Estimate the Robustness of Physically Unclonable Functions to Modeling Attacks", minor revision version submitted to *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*.

S. Chattaopadhyay, **P. Santikellur**, R. S. Chakraborty, J. Mathew and M. Ottavi, "A Conditionally Chaotic Physically Unclonable Function Design Framework with High Reliability", in *ACM Transactions on Design Automation of Electronic Systems*, 26, 6, Article 41 (November 2021), pp. 1-24.DOI:https://doi.org/10.1145/3460004

P. Santikellur and R. S. Chakraborty, "A Computationally Efficient Tensor Regression Network based Modeling Attack on XOR Arbiter PUF and its Variants" in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems.*, vol. 40, no. 6, pp. 1197-1206, June 2021, doi: 10.1109/TCAD.2020.3032624.

V. Govindan, R. S. Chakraborty, **P. Santikellur**., A.K Chaudhary, "A Hardware Trojan Attack on FPGA based Cryptographic Key Generation: Impact and Detection", *Journal of Hardware and Systems Security* (Springer), vol. 2, no. 3, pp. 225-239, Sep. 2018.

Book Chapter

P. Santikellur, R. S. Chakraborty, and J. Mathew, "Hardware Security in the Context of Internet of Things: Challenges and Opportunities." *Internet of Things and Secure Smart Environments: Successes and Pitfalls*, 2020, p.64.

P. Santikellur, R. S. Chakraborty, S. Bhunia, (2022). Hardware IP Protection Using Register Transfer Level Locking and Obfuscation of Control and Data Flow. In: Katkoori, S., Islam, S.A. (eds) Behavioral Synthesis for Hardware Security. Springer, Cham. https://doi.org/10.1007/978-3-030-78841-4$_4$

Conference Papers

P. Santikellur, R. Mukherjee, and R. S. Chakraborty. "APUF-BNN: An Automated Framework for Efficient Combinational Logic Based Implementation of Arbiter PUF through Binarized Neural Network". In *Proceedings of the 2021 on Great Lakes Symposium on VLSI (GLSVLSI '21)*. Association for Computing Machinery, New York, NY, USA, 89–94. **(Best Paper Nominated)**

P. Santikellur, Lakshya, S. R. Prakash and R. S. Chakraborty, "A Computationally Efficient Tensor Regression Network based Modeling Attack on XOR Arbiter PUF", *IEEE Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*, 2019, pp. 1-6.

V. S. Balijabudda, D. Thapar, **P. Santikellur**, R. S. Chakraborty and I. Chakrabarti, "Design of a Chaotic Oscillator based Model Building Attack Resistant Arbiter PUF", *IEEE Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*, 2019, pp. 1-6.

U. Chatterjee, **P. Santikellur**, R. Sadhukhan, V. Govindan, D. Mukhopadhyay and R. S. Chakraborty, "United We Stand: A Threshold Signature Scheme for Identifying Outliers in PLCs (poster with 2 page short-paper)", Late Breaking Results (LBR) track of *IEEE/ACM Design Automation Conference (DAC)*, Las Vegas, Nevada, USA, 2019.

P. Santikellur, R. Mukherjee, and R. S. Chakraborty: Logic Synthesis of Arbiter PUF using Binarized Neural Networks (poster)", *International Conference on Security, Privacy and Applied Cryptographic Engineering* (SPACE), Gandhinagar, India, 2019.

Student Project

P. Santikellur, T. Haque, M. Al-Zewairi and R. S. Chakraborty, "Optimized Multi-Layer Hierarchical Network Intrusion Detection System with Genetic Algorithms," *IEEE International Conference on new Trends in Computing Sciences (ICTCS)*, Amman, Jordan, 2019.

Achievements

- Intel AI Student Ambassador from IIT Kharagpur, India.
- Intel's one of the first Certified Instructors for oneAPI and DPC++ Essentials.
- Secured Second Prize in CSAW'17 Embedded Security Challenge held at IIT Kanpur, 2017.

Invited Talks

- Invited for webinar at "cadforassurance.org" for the topic on our tool "Deep Feed Forward Neural Network Based PUF Attack Tool".
- Invited for talk at IIEST, Shibpur on for the topic "Recent Advances in Machine Learning based Modeling Attacks on PUF".
- Invited for talk at IEEE TENCON 2019 for the topic "Physically Unclonable Functions: Design, Applications, Threats".

Teaching Assistance

- Machine learning (CS60050)
- MIPS assembly language (CS39001, CS31007)
- Programming and Data Structures Laboratory (CS11001)

Technical Skill

- Languages: C, C++, MATLAB, Python, Verilog
- ML frameworks: TensorFlow(+Keras), H2O, Scikit-Learn
- Tools: LTIB, Yocto, GDB, QtSpim

Professional activities

- Co-Chair of ISQED 2021 (Session Title: Application of AI/ML in Hardware Security)
- A member of TCHES 2021 artifact review committee.
- External Reviewer: TCHES, IEEE TCAD, IEEE TCAS, ACM CSUR, DSD, GLSVLSI, VDAT, Sadhana

References

- **Prof. Rajat Subhra Chakraborty**
  Associate Professor,
  Dept of Computer Science and Engg, IIT Kharagpur, India.
  Email: rschakraborty@cse.iitkgp.ac.in
- **Varsha Chakraborty**
  Operations Head, Horner Engineering India,
  Bengaluru, India.
  Email: varsha.chakraborty@india.horner-apg.com