Seetal Potluri

Assistant Professor
University at Albany, SUNY
Website: seetalpotluri.com

Phone: +1 (919) 601-2719
E-mail: spotluri@albany.edu
ETEC, Washington Avenue, Albany, NY 12226.

Research Interests

Security, Reliability, Computer Architecture, and Machine Learning.

Education

Post-Doc, Department of ECE, **North Carolina State University** 2019 – Present

Ph.D., Department of EE, **Indian Institute of Technology Madras** 2009 – 2015
Thesis: *Power: Its Manifestations in Digital Systems Testing*

M.Tech., Department of EE, **Indian Institute of Technology Madras** 2007 – 2009
Thesis: *Cell-aware UDFM for Deep Submicron Process Nodes*

B.Tech., Department of ECE, **Amrita School of Engineering** 2003 – 2007
Thesis: *Implementation of Adaptive Viterbi Decoder on FPGA*

Honors and Awards

Best Paper Recognition Award - IEEE HOST Symposium 2021
Best Doctoral Thesis Runner-Up in Asia - IEEE TTTC Doctoral Thesis Contest 2015
Academic Recognition - Class topper with highest Cumulative G.P.A. in M.Tech. 2009
Academic Recognition - Class topper with highest Cumulative G.P.A. in B.Tech. 2007

Grant Writing Experience as Co-PI

National Science Foundation Secure and Trustworthy Cyberspace (SaTC), $500K 2021
LockedNet: A Holistic Solution for Neural Network Hardware and Model IP Protection
(Will be resubmitted)

Semiconductor Research Corporation Hardware Security (HWS), $210K 2020
Scan Infrastructure Security for Neural Networks: Analyzing and Countering Advanced Model Stealing Attacks (Phase-I Success; Invited for Full Proposal)

Research Experience

Postdoctoral Scholar, NC State University. 2019 – Present

- Secure virtualization in multi-tenant FPGAs.
- Secure Non-Volatile Memory on FPGAs.
- Exposed scan-chain vulnerability for neural network hardware accelerators.
- Exposed power side-channel vulnerability of Microsoft's SEAL encryption library.
- Exposed power side-channel vulnerability of lattice-based key exchange.
- Cache timing side-channel attacks on Apple's iPhone.

Postdoctoral Scholar, TU Dresden. 2018 – 2019

- Secure DFT scheme that is resilient to 9 different state-of-the-art attacks.

Senior DFT Engineer, Xilinx Asia Pacific, Singapore. 2016 – 2018

- DFT, and post-silicon validation for high-bandwidth memory project.
- Top-off cell-aware ATPG: currently in production on Zynq SoCs.
- Delta-IDDq to catch test escapes: currently in production on Zynq SoCs.

Postdoctoral Scholar, TU Denmark. 2015 – 2016

- Physical design, DFT, and logic design for on-chip control in biochips.
- Fault-tolerant execution in biochips through cost-effective redundancy.

Research Assistant, IIT Madras. 2008 – 2015

- Power and IR drop reduction during the structural at-speed test.
- Exploiting power measurements to improve fault diagnostic resolution.
- Cell-aware UDFM creation for an entire standard library.

Teaching Experience

North Carolina State University

- ECE 592 Cryptographic Engineering and Hardware Security (6 lectures) 2019 – 2022
- ECE 212 Fundamentals of Logic Design (6 lectures) 2019 – 2020

Technical University of Denmark

- 02228 Fault-Tolerant Systems (3 lectures) 2015 – 2016

Indian Institute of Technology Madras

- CS 6330 Digital Systems Testing and Testable Design (25 lectures) 2011 – 2015
- CS 6230 CAD for VLSI (3 lectures) 2012
- EE 5311 Digital IC Design (3 lectures) 2010 – 2012

Amrita School of Engineering

- EC 302 Digital Communication (1 lecture) 2006

Mentoring Experience

Emre Karabulut – Ph.D. at NC State	2021 – Present
Furkan Aydin – Ph.D. at NC State	2019 – 2021
Priyank Kashyap – Ph.D. at NC State	2019 – 2021
Gregor Haas – M.S. at NC State	2019 – 2021
Shamik Kundu – Ph.D. at UT Dallas	2020
Yitong Zhou (BUPT, China) – GEARS exchange student	2020
Qinhan Tan (Zhejiang University, China) – GEARS exchange student	2019
Huili Chen – Ph.D. at UC, San Diego	2016 – 2017
Morten Chabert Eskesen – M.Sc. at DTU	2015
Satya Trinadh Adireddy – Ph.D. at IIT Hyderabad	2012 – 2015
Patanjali SLPSK – Ph.D. at IIT Madras	2013 – 2015
Roopashree Baskaran – B.Tech. at NIT Trichy	2013
Ramakumar Pasumarthi – B.Tech. at IIT Madras	2011 – 2012

Publication List

Google Scholar Profile: https://scholar.google.com.sg/citations?user=TG9epCwAAAAJ&hl=en

13 journal articles, **20** conference proceedings, **3** theses, and **1** patent.

Journal Articles

[1] S. Potluri, S. Kundu, A. Kumar, K. Basu, and A. Aysu, "SeqL+: Secure Scan-Obfuscation with Theoretical and Empirical Validation", IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Vol. 42, No. 5, 2023, pp. 1406-1410.

[2] P. Kashyap, F. Aydin, **S. Potluri,** P. Franzon, and A. Aysu, "2Deep: Enhancing Side-Channel Attacks on Lattice-Based Key-Exchange via 2D Deep Learning"**,** IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Vol. 40, No. 6, 2021, pp. 1217-1229.

[3] H. Chen, **S. Potluri,** and F. Koushanfar, "Security of Microfluidic Biochip: Practical Attacks and Countermeasures", ACM Transactions on Design Automation of Electronic Systems (TODAES) 2020, 27:1-27:29.

[4] **S. Potluri,** P. Pop, and J. Madsen, "Design-for-Testability of On-Chip Control in mVLSI Biochips", IEEE Design & Test, Vol. 36, No. 1, 2019, pp. 48-56.

[5] **S. Potluri**, A. Satya Trinadh, Ch. Sobhan Babu, V. Kamakoti, and N. Chandrachoodan, "DFT Assisted Techniques for Peak Power Reduction during Scan Tests", ACM Transactions On Design Automation of Electronic Systems (TODAES), Vol. 21, No. 1, 2015, 21(1): 14:1-14:25.

[6] A. S. Trinadh, **S. Poturi,** Ch. Sobhan Babu, S. G. Singh, and V. Kamakoti, "Optimal Don't Care Filling for Minimizing Peak Toggles During At-Speed Stuck-At Testing", ACM Transactions On Design Automation of Electronic Systems (TODAES), Vol. 5, No. 1, 2017, 23(1): 5:1-5:26.

[7] G. V. Krishnan, V. Kamakoti, N. Chandrachoodan, and **S. Potluri**, "A Scalable Pseudo-Exhaustive Methodology for Testing and Diagnosis in Flow-based Microfluidic Biochips", IET Computers and Digital Techniques, Vol. 14, No. 3, 2020, pp. 122-131.

[8] S. L. P. S. K. Patanjali, M. Patnaik, **S. Potluri,** and V. Kamakoti, "MLTimer: Leakage Power Minimization in Digital Circuits Using Machine Learning and Adaptive Lazy Timing Analysis", Journal of Low Power Electronics, Vol. 14, No. 2, 2018, pp. 285-301.

[9] S. Burman, **S. Potluri,** D. Mukhopadhyay, and V. Kamakoti, "Power Consumption Vs. Hardware Security: Feasibility Study of Differential Power Attack on Linear Feedback Shift Register Based Stream Ciphers and Its Countermeasures", Journal of Low Power Electronics, Vol. 12, No. 2, 2016, pp. 99-106.

[10] A. S. Trinadh, **S. Potluri**, S. Balachandran, Ch. Sobhan Babu, and V. Kamakoti, **"**XStat: Statistical X-Filling Algorithm for Peak Capture Power Reduction in Scan Tests", Journal of Low Power Electronics, Vol. 10, No. 1, 2013, pp. 107-115.

[11] A. S. Trinadh, **S. Potluri,** Ch. Sobhan Babu, and V. Kamakoti, **"**An Efficient Heuristic for Peak Capture Power Minimization During Scan-Based Test", Journal of Low Power Electronics, Vol. 9, No. 2, 2013, pp. 264-274.

[12] **S. Potluri,** N. Chandrachoodan, and V. Kamakoti, "Interconnect Aware Test Power Reduction", Journal of Low Power Electronics, Vol. 8, No. 4, 2012, pp. 516-525.

[13] R. Pasumarthi, V. R. Devanathan, V. Vishvanathan, **S. Potluri,** and V. Kamakoti, "Thermal-Safe Dynamic Test Scheduling Method Using On-Chip Temperature Sensors for 3D MPSoCs", Journal of Low Power Electronics, Vol. 8, No. 5, 2012, pp. 684-695.

Peer-Reviewed Conference Publications

[14] S. Jiang, **S. Potluri**, and T. Y. Ho, "Scalable Scan-chain-based Extraction of Neural Network Models", IEEE/ACM Design Automation and Test in Europe (DATE), 2023 (Accepted).

[15] F. Aydin, E. Karabulut, **S. Potluri,** E. Alkim, and A. Aysu, "RevEAL: Single-Trace Side-Channel Leakage of the SEAL Homomorphic Encryption Library", IEEE/ACM Design Automation and Test in Europe (DATE), 2022, pp. 1527-1532.

[16] E. Karabulut, C. Yuvarajappa, M. I. Shaikh, **S. Potluri**, A. Awad, and A. Aysu, "PR Crisis: Analyzing and Fixing Partial Reconfiguration in Multi-Tenant Cloud FPGAs", ACM Workshop on Attacks and Solutions in Hardware Security (ASHES), 2022 (Accepted).

[17] F. Aydin, **S. Potluri**, and A. Aysu, "Machine Learning for Side-Channel Assessment of Next Generation Cryptosystems", IEEE International Symposium on On-Line Testing and Robust System Design (IOLTS), 2022 (Invited).

[18] **S. Potluri,** and A. Aysu, "Stealing Neural Network Models through the Scan-Chain: A New Threat for ML Hardware", IEEE International Conference on Computer Aided Design (ICCAD), 2021, pp. 1-8.

[19] G. Haas, **S. Potluri,** and A. Aysu, "iTimed: Cache Attacks on the Apple A10 Fusion SoC", IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2021, pp. 80-90 (**Best Paper Recognition Award**).

[20] S. Potluri, A. Aysu, and A. Kumar, "SeqL: Secure Scan-Locking for IP Protection", IEEE International Symposium on Quality Electronic Design (ISQED), 2020, pp. 7-13.

[21] F. Aydin, P. Kashyap, **S. Potluri,** P. Franzon, and A. Aysu, "DeePar-SCA: Breaking Parallel Architectures of Lattice Cryptography via Learning Based Side-Channel Attacks", International Conference on Embedded Computer Systems: Architectures, Modeling and Simulation (SAMOS), 2020, pp. 262-280.

[22] F. Aydin, P. Kashyap, **S. Potluri,** P. Franzon, and A. Aysu, "Breaking Side-Channel Countermeasures through Deep Learning", IEEE International Conference on Computer Aided Design (ICCAD), 2020 (Invited).

[23] Q. Tan, **S. Potluri,** and A. Aysu, "Efficacy of SAT-based Attacks in the Presence of Circuit Reverse-Engineering Errors", IEEE International Symposium on Circuits and Systems (ISCAS), 2020, pp. 1-5.

[24] H. Chen, **S. Potluri,** and F. Koushanfar, "FlowTrojan: Insertion and Detection of Hardware Trojans on Flow-Based Microfluidic Biochips", IEEE International New Circuits and Systems Conference (NEWCAS), 2020, pp. 158-161.

[25] S. Potluri, A. Schneider, M. Horslev-Petersen, P. Pop, and J. Madsen, "Synthesis of On-chip Control Circuits for mVLSI Biochips", IEEE/ACM Design Automation and Test in Europe (DATE), 2017, pp. 1799-1804.

[26] S. Potluri, A. Mathew, R. Nerukonda, I. Hartanto, and S. Toutounchi, "Cell-aware ATPG to improve defect coverage for FPGA IPs and next generation MPSoCs", IEEE Asian Test Symposium (ATS), 2017, pp. 157-162.

[27] M. C. Ekesen, P. Pop, and **S. Potluri**, "Architecture Synthesis of Cost Constrained Fault Tolerant Flow-based Biochips", IEEE/ACM Design Automation and Test in Europe (DATE), 2016, pp. 618-623.

[28] A. Satya Trinadh, S. G. Singh, Ch. Sobhan Babu, **S. Potluri,** and V. Kamakoti, "DP- fill : A dynamic programming approach to X- filling for minimizing peak test power in scan tests", IEEE/ACM Design Automation and Test in Europe (DATE), 2015, pp. 836-841.

[29] H.Chen, **S. Potluri,** and Farinaz Koushanfar, "BioChipWork: Reverse Engineering of Microfluidic Biochips"**,** IEEE International Conference of Computer Design (ICCD), 2017, pp. 9-16.

[30] S. Potluri, A. S. Trinadh, C. Rajamanikkam, and S. Balachandran, "LPScan : An algorithm for supply scaling and switching activity minimization during test", IEEE International Conference on Computer Design (ICCD), 2013, pp. 463-466.

[31] S. Potluri, A. S. Trinadh, S. Saraf, and V. Kamakoti, "Component fault localization using switching current measurements", IEEE European Test Symposium (ETS), 2016, pp. 1-2.

[32] S. Potluri, A. S. Trinadh, R. Baskaran, N. Chandrachoodan, and V. Kamakoti, "PinPoint: An algorithm for enhancing diagnostic resolution using capture cycle power information", IEEE European Test Symposium (ETS), 2013, pp. 1.

[33] S. Potluri, N. Chandrachoodan, and V. Kamakoti, "Post-Synthesis Circuit Techniques for Runtime Leakage Reduction", IEEE International Symposium on VLSI (ISVLSI), 2011, pp. 319-320.

Patent

[33] S. Potluri, P. Pop, and J. Madsen, "Complementary pneumatic digital logic for on-chip control of lab-on-chip devices", World Intellectual Property Organization (WIPO) 2018, Pub. No. WO/2018/104516.
Link: https://patentscope.wipo.int/search/en/detail.jsf?docId=WO2018104516

Theses

[34] S. Potluri, "Power: Its Manifestations in Digital Systems Testing", Doctoral Dissertation, Indian Institute of Technology Madras, 2015.

[35] S. Potluri, "Cell-Aware UDFM for Deep Submicron Process Nodes", Masters Dissertation, Indian Institute of Technology Madras, 2009.

[36] S. Potluri, "Implementation of Adaptive Viterbi Decoder on FPGA", Bachelors Dissertation, Amrita School of Engineering, Coimbatore, 2007.

News Coverage of Research

DATE 2022: RevEAL: Single-Trace Side-Channel Leakage of the SEAL Homomorphic Encryption Library.

My DATE 2022 research paper has been publicized through an NC State news release and has subsequently been featured on Hacker News, CSO Online, and The Digital Hacker among other places. This was covered by the cybersecurity news site Dark Reading and the interview was published online along with the news coverage.

HOST 2021: iTimed: Cache Attacks on the Apple A10 Fusion SoC.

My HOST 2021 research paper has been publicized through an NC State news release and has subsequently been featured in several news agencies including The Register and WRAL TechWire. This was covered by CBS Raleigh and the interview was published on live TV (CBS 17) as part of Wake County News.

Membership

Member IEEE – Institute of Electrical and Electronics Engineers

Member ACM – Association for Computing Machinery

Invited Talks and Presentations

Stealing Neural Network Models through the Scan-Chain: A New Threat for ML Hardware

- Second Workshop on Machine Learning & Hardware Security 2021

SeqL: Secure Scan-Locking for IP Protection

- IEEE CEDA CAD for Assurance 2021
- Indian Institute of Technology Madras 2019
- North Carolina State University, ECE 592 Guest Lecture 2019

Design automation for Microfluidic Biochips

- École Polytechnique Fédérale de Lausanne 2016
- University of Cambridge 2016

Power: Its Manifestations in Digital Systems Testing

- Rice University 2013
- Purdue University 2013
- University of California at Berkeley 2014
- Technical University of Denmark 2015
- Indian Institute of Technology Kharagpur 2015
- Indian Statistical Institute Kolkata 2015

Workshops Attended

Side Channel Analysis and Fault Injection 2021
S. Bhasin et al, Singapore.

Side Channel Analysis and Fault Injection 2019
R. B. Carpi, Raleigh, North Carolina.

Riscure User Workshop 2019
M. Witteman et al, Fort Meade, Maryland.

3D Workshop at DATE Conference 2015
P. Vivet et al, Grenoble, France.

International Workshop on Reliability Aware Design and Test 2011
A. Singh et al, Chennai, India.

Academic Service

Technical Program Committee Member

IEEE Design Automation Conference (DAC) 2022, 2023
IEEE International Conference on Computer-Aided Design (ICCAD) 2023
IEEE Asia South Pacific Design Automation Conference (ASP-DAC) 2018 – 2022
IEEE European Test Symposium (ETS) 2016 – 2018
IEEE Asian Test Symposium (ATS) 2017, 2022, 2023
IEEE International Test Conference Asia (ITC-Asia) 2017
IEEE International Conference on VLSI Design (VLSID) 2022, 2023
IEEE International Symposium on VLSI (ISVLSI) 2022, 2023
IEEE International Conference on Computer Design (ICCD) 2022, 2023
ACM Hot Topics in the Science of Security (HotSoS) 2023
ACM Hardware and Architectural Support for Security and Privacy (HASP) 2023
ACM Workshop on Attacks and Solutions in Hardware Security (ASHES) 2023

Session Co-Chair

IEEE Design Automation Conference (DAC) 2022
IEEE International Symposium on Circuits and Systems (ISCAS) 2020
IEEE Design, Automation and Test in Europe (DATE) 2017
IEEE Asian Test Symposium (ATS) 2017

Journal Reviewer

IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)
IEEE Transactions on Computers (TC)
IEEE Transactions on Very Large Integrated Systems (TVLSI)
IEEE Design & Test (D&T)
ACM Transactions on Design Automation of Electronic Systems (TODAES)
ACM Transactions on Embedded Computing Systems (TECS)
Springer Journal of Cryptographic Engineering (JCEN)
Springer Journal of Electronic Testing: Theory and Applications (JETTA)
IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)
IEEE Security and Privacy Magazine
IET Computers & Digital Techniques
Elsevier Microelectronics Journal
Elsevier Microprocessors and Microsystems (MICPRO)

Conference Reviewer

IEEE Design Automation Conference (DAC) 2020, 2021
IEEE Design Automation & Test in Europe (DATE) 2020 – 2022
IEEE International Conference on Computer-Aided Design (ICCAD) 2019
ACM International Symposium on Field-Programmable Gate Arrays (FPGA) 2020, 2021
IEEE International Symposium on Hardware Oriented Security and Trust (HOST) 2020, 2021
IACR Cryptographic Hardware and Embedded Systems (CHES) 2022
IEEE International Conference on Computer Design (ICCD) 2020, 2021
IEEE International Conference on VLSI Design (VLSID) 2022, 2013
ACM Workshop on Attacks and Solutions in Hardware Security (ASHES) 2019 – 2021