Sanjay Deshpande

✉ sanjay.deshpande1@northwestern.edu www.sanjaydeshpande.phd
in linkedin.com/in/sanjaydeshpandephd

Education

Yale University — *New Haven, CT*
Doctor of Philosophy in Electrical Engineering (GPA: 4.0) — *Aug. 2021 – Dec 2025*

George Mason University — *Fairfax, VA*
Master of Science in Computer Engineering (GPA: 3.83) — *Aug. 2014 – Dec 2016*

Jawaharlal Nehru Technological University — *Hyderabad, India*
Bachelor of Technology in Electronics & Communication Engineering (GPA: 4.0) — *Sep. 2010 – May 2014*

Work Experience

Postdoctoral Scholar — *Jun 2025 - current*
Northwestern University — *Remote*

- Conducted research on side channel attacks on post-quantum cryptographic algorithms.
- Proposed countermeasures to secure post-quantum cryptographic algorithms from side-channel attacks.
- Conducted research on accelerating fully homomorphic encryption schemes in hardware.

PQC Research Scientist Resident — *Nov 2024 - May 2025*
SandboxAQ — *Remote*

- Designed and implemented modular hardware (RTL) architecture for NIST proposed Rjindael 256 algorithm.
- Hardware design and implementation of Vole-in-the-head variant of Syndrome Decoding in the Head signature scheme from ongoing on-ramp NIST Post-quantum digital signature schemes standardization process.

Research Intern — *Jun 2024 - Aug 2024*
Microsoft Research — *Remote*

- Designed and implemented a modular hardware (RTL) architecture for an ISO-standardized Post-Quantum Cryptographic scheme (targeting ASIC). The implemented design supports run-time switching between different security levels the scheme offers. Additionally, it also has synthesis-time reconfigurability for different performance trade-offs.
- The design was further extended with a capability to protect against power side-channel attacks.

Research Assistant — *Aug 2021 - May 2025*
Yale University — *New Haven, CT*

- Conducted research on primitives of Post-Quantum Cryptosystems and designed and implemented secure and efficient hardware (RTL) designs of Key Encapsulation Mechanism and Digital Signature Algorithm for multiple candidates from ongoing NIST PQC competition.
- Conducted research on secure hardware architectures for cloud-based quantum computers and proposed and implemented novel software and hardware-based solutions.

PQC Research Scientist Resident — *Apr 2023 - Dec 2023*
SandboxAQ — *Remote*

- Evaluated the submissions from the NIST's Post Quantum Digital Signature Schemes standardization competition.
- Implemented a hardware (RTL) design for the Syndrome Decoding in the Head (SDitH) algorithm from the NIST PQC Digital signature scheme competition.

Associate Researcher II — *Oct 2020 - Aug 2021*
Yale University — *New Haven, CT*

- Conducted research and developed hardware implementations of key components in Public Key Cryptography, and Post Quantum Cryptography targeting FPGAs.
- Analyzed timing and optimized the design area of the RTL implementations.
- Conducted research on hardware accelerators compatible with RISC V CPU architecture.

Sr. Security Researcher (formerly Sr. Cryptography Hardware Engineer, DarkMatter LLC) — *Apr 2019 -Jul 2020*
Technology Innovation Institute — *Abu Dhabi, UAE*

- Research and implementation of hardware accelerators (RTL targeting FPGA) for Post Quantum Cryptography primitives.

- Platform independent RTL implementations of cryptographic algorithms and protocols targeting FPGAs and ASICs. Development process right from customer requirement to production-ready IP.
- Optimized RTL designs for performance in terms of Power, Timing, Frequency, and Area. Drew test plans for verification and validation of the IP.
- Took Ownership of the Hardware Accelerators for FPGA based design and assisted in the Integration process.
- Analyzed the RTL implementations for side-channel attacks and developed side-channel resistant RTL implementations of cryptographic algorithms.

Hardware Security Researcher *Mar 2017 -Apr 2019*
DarkMatter LLC *Abu Dhabi, UAE*

- Conducted research and implemented Hardware accelerators (RTL targeting FPGA) for Elliptic Curve Cryptography primitives.
- Reverse Engineering and hardware hacking of various devices.
- Tested and Provided mitigations for security threats related to hardware for various devices.

Research and Teaching Assistant *Aug 2015 – Dec 2016*
Cryptographic Engineering Research Group (CERG), George Mason University *Fairfax, VA*

- Hardware Implementations (VHDL and Verilog) of the Cryptographic Algorithms targeting FPGAs: Virtex 6, Virtex 7, and Zynq 7000 FPGA/SoC families.
- Analyzed performance bottlenecks of authenticated ciphers on hardware (Xilinx Virtex 7), and designed and implemented methods to overcome the bottlenecks.
- Assisted students in Digital Systems Design using VHDL course and FPGA and ASIC Design with VHDL lab. Conducted Linear Electronics lab for undergraduate students.

Junior Electrical Engineer *May 2015 – Aug 2015*
Rysc Corp. *Manassas, VA*

- Designed and Prototyped electronic hardware.
- Conducted PCB Design using Eagle CAD and Tested and Evaluated PCBs.
- Developed ARM Firmware in C.

Lab Assistant *Aug 2014 – Aug 2015*
George Mason University *Fairfax, VA*

- Assisted students in experiments based on Electrical and Computer Engineering.
- Verified the quality of the components used in Lab Experiments.

Teaching Experience

Yale University *New Haven, CT*
Teaching Fellow

- CPSC415/CPSC515: Law, Security, and Logic — Fall 2022
- EENG201: Introduction to Computer Engineering — Spring 2023, Spring 2024

George Mason University *Fairfax, VA*
Teaching Assistant

- ECE334: Linear Electronics Lab — Fall 2015, Fall 2016
- ECE545: Digital System Design with VHDL — Fall 2015, Fall 2016
- ECE448: FPGA Design with VHDL Lab — Spring 2016
- ECE232: Digital System Design Lab — Summer 2016

Academic Activities

Visiting Scholar *Nov 2025*
Academia Sinica *Taipei, Taiwan*

- Built a methodology that standardizes hardware evaluation practices and ensures consistent design assessment.

Academic Reviewing Service

- International Symposium on Circuits and Systems (ISCAS) 2026 — *Nov 2025*
- Journal of Systems Architecture — *Oct 2025*
- IEEE Transactions on Computers — *Oct 2025*
- CHIPS Journal — *Jul 2025*

- IEEE Computer Architecture Letters *Jun 2024*
- International Symposium on Circuits and Systems (ISCAS) 2024 *Dec 2023*

Program Committee Member

- IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS) 2026 *Dec 2025*
- Hardware and Architectural Support for Security and Privacy (HASP) 2025 *Sept 2025*
- ACM QSec: Quantum Security and Privacy Workshop (Co-located with ACM CCS 2025) *Oct 2025*

Invited Talks

- Academia Sinica, Taipei, Taiwan *Nov 2025*
- New York University, New York, USA *Oct 2025*
- Indian Institute of Technology, Kanpur, India *Aug 2025*
- Department of Electrical and Computer Engineering, Northwestern University, Evanston, USA *May 2025*
- Security Group, Qualcomm, Valbonne, France *Nov 2023*

Podcasts

- Boardwalk Bytes, Atlantic City, New Jersey, USA *Jul 2025*
- SandboxAQ, Palo Alto, California, USA *Jun 2024*

Awards

- Best of IEEE CAL award for a paper on Quantum Computer Security, IEEE CAL *Dec 2023*
- Best Project Award, Cyber-physical Systems Summer School, Sardegna, Italy *Sept 2025*
- Outstanding Academic Achievement Award, ECE Department at George Mason University, Fairfax, USA *May 2015*
- Best project award in Cryptography and Computer Network Security course at GMU, Fairfax, USA. *Jul 2014*
- Certificate of Excellence in Academics, Jawaharlal Nehru Technological University, India *Jul 2014*
- First Prize in Robocup 2k14, a zonal event, Jawaharlal Nehru Technological University, India *Oct 2013*

Peer-Reviewed Publications and Research

Cryptography and Hardware Research

1. **Sanjay Deshpande**, Patrick Longa, , and Jakub Szefer. Accelerating FrodoKEM in Hardware. Under review

2. **Sanjay Deshpande**, Yongseok Lee, Mamuri Nawan, Kashif Nawaz, Ruben Niederhagen, Yunheung Paek, and Jakub Szefer. Unified MEDS Accelerator. SAC, August 2025

3. **Sanjay Deshpande**, Yongseok Lee, Cansu Karakuzu, Jakub Szefer, and Yunheung Paek. SPHINCSLET: An Area-Efficient Accelerator for the Full SPHINCS+ Digital Signature Algorithm. *ACM Trans. Embed. Comput. Syst.*, April 2025

4. **Sanjay Deshpande**, James Howe, Dongze Yue, and Jakub Szefer. SDitH in Hardware. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2023(2), Sept. 2024

5. **Sanjay Deshpande** and Chuanqi Xu and Mamuri Nawan and Kashif Nawaz and Jakub Szefer. Fast and Efficient Hardware Implementation of HQC. In *Proceedings of the Selected Areas in Cryptography*, SAC, Aug. 2023

6. Po-Jen Chen, Tung Chou, **Sanjay Deshpande**, Norman Lahr, Ruben Niederhagen, Jakub Szefer, and Wen Wang. Complete and improved FPGA Implementation of Classic Mceliece. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2022(3):71–113, Jun. 2022

7. **Sanjay Deshpande**, Santos Merino del Pozo, Victor Mateu, Marc Manzano, Najwa Aaraj, and Jakub Szefer. Modular Inverse for Integers using Fast Constant Time GCD Algorithm and its Applications. In *Proceedings of the International Conference on Field Programmable Logic and Applications*, FPL, Aug. 2021

8. **Sanjay Deshpande** and Kris Gaj. Analysis and Inner-Round Pipelined Implementation of Selected Parallelizable CAESAR Competition Candidates. In *2017 Euromicro Conference on Digital System Design (DSD)*, pages 274–282, 2017

Quantum Computer Security Research

9. Barbora Hrdá, **Sanjay Deshpande**, Theodoros Trochatos, and Jakub Szefer. CHEQ: Towards Enabling Circuit Integrity Checking in Quantum Controllers. In *Proceedings of the Great Lakes Symposium on VLSI 2025*, GLSVLSI, pages 265–272, June 2025

10. Theodoros Trochatos, Chuanqi Xu, **Sanjay Deshpande**, Yao Lu, Yongshan Ding, and Jakub Szefer. Trusted Execution Environments for Quantum Computers. *Frontiers in Computer Science*, 7, 2025

11. Theodoros Trochatos, Chuanqi Xu, **Sanjay Deshpande**, Yao Lu, Yongshan Ding, and Jakub Szefer. Protecting Quantum Computers with a Trusted Controller. In *International Conference on Quantum Computing and Engineering*, QCE, September 2024

12. Theodoros Trochatos, **Sanjay Deshpande**, Chuanqi Xu, Yao Lu, Yongshan Ding, and Jakub Szefer. Dynamic Pulse Switching for Protection of Quantum Computation on Untrusted Clouds. In *International Symposium on Hardware Oriented Security and Trust*, HOST, May 2024

13. Theodoros Trochatos, Chuanqi Xu, **Sanjay Deshpande**, Yao Lu, Yongshan Ding, and Jakub Szefer. A Quantum Computer Trusted Execution Environment. *IEEE Computer Architecture Letters*, (01):1–4, Oct. 2023

14. **Sanjay Deshpande**, Chuanqi Xu, Theodoros Trochatos, Hanrui Wang, Ferhat Erata, Song Han, Yongshan Ding, and Jakub Szefer. Design of Quantum Computer Antivirus. In *Proceedings of the International Symposium on Hardware Oriented Security and Trust*, HOST, May 2023

15. **Sanjay Deshpande**, Chuanqi Xu, Theodoros Trochatos, Yongshan Ding, and Jakub Szefer. Towards an Antivirus for Quantum Computers. In *Proceedings of the International Symposium on Hardware Oriented Security and Trust*, HOST, Jun. 2022

16. Theodoros Trochatos, Chuanqi Xu, **Sanjay Deshpande**, Yao Lu, Yongshan Ding, and Jakub Szefer. SoteriaQ: Hardware Architecture for a Quantum Computer Trusted Execution Environment. Under review

Other Research

17. **Sanjay Deshpande** and Jakub Szefer. Analyzing ChatGPT's Aptitude in an Introductory Computer Engineering Course. In *Proceedings of the International Conference on Frontiers in Education: Computer Science & Computer Engineering*, FECS, Jul. 2023

Demos

18. Theodoros Trochatos, **Sanjay Deshpande**, and Jakub Szefer. SoteriaQ: Securing Quantum Circuits Hardware Demo. In *International Symposium on Hardware Oriented Security and Trust*, HOST, May 2024

Book Chapters

19. Sanjay Deshpande. Design of quantum computer antivirus. In Prabhat Mishra, editor, *Design Automation for Quantum Computing*. January 2026. To appear

Projects

Optimized Decomposition of $U_{Heis3}(t)$ into Quantum Gates | *Qiskit, Python, IBMQ* *Mar 2022 – May 2022*

Participated in the IBM challenge and contributed in improving the fidelity of Heisenberg Hamiltonian H_{Heis3} circuit. Implemented a ‘`trotter`’ function using optimal two-qubit transformations and demonstrated a fidelity of 52% on `ibmq_jakarta`.

Antivirus for Quantum Computers | *Qiskit, Python, Quantum Computing* *Sep 2021 – Dec 2021*

Proposed a method to detect malicious circuits in quantum programs. Explored the possibility of modifying Qiskit, and added multi-layered protection – an Antivirus system to detect the malicious attacker circuits, which would prevent malicious users from performing attacks, proposed to run Qiskit programs inside a trusted execution environment, protecting it from malicious users.

Survey on Inference Acceleration for various NN models on cloud processors *Oct 2021 – Dec 2021*

Benchmarked results for inference acceleration of pre-trained DNN models – ResNet50 and MobileNetV1 on cloud FPGAs, cloud GPUs, and cloud CPUs. Built a common framework to track different performance metrics - Time, Accuracy, Throughput, and Energy. Provided a fair performance comparison for DNN inference based on the different performance metrics on cloud CPU versus cloud GPU versus cloud FPGA.

Complete ASIC Design Flow using Synopsys ASIC design tools | *ASIC, Verilog* *Aug 2015 – Dec 2015*

Implemented an ALU and carried out the complete ASIC design flow – used Design Compiler for floorplanning, place, and route, and PrimeTime for clock tree insertion and power estimation generated area, power, and timing reports and located the critical paths of the designs. Optimized false paths and maximum delay paths. Used IC Compiler to create back-end designs and generated the GDSII files.

High-Level Synthesis of an ALU | *FPGA, High Level Synthesis* *Jan 2015 – May 2015*

Designed an ALU using high-level synthesis, created an custom IP to Vivado and interfaced it with Zynq 7000 using AXI Lite and AXI Stream interfaces.

Languages

- English
- Hindi
- Telugu
- Marathi
- Kannada

Technical Skills

Languages: Verilog, VHDL, TCL, C, Python, Qiskit, Assembly.
Operating Systems: Windows, Linux, OSX.
Programmable Hardware: AMD and Intel FPGAs, Arduino.
Tools: AMD Vivado, Xilinx ISE, Intel Quartus prime, GHDL, Verilator, Cadsoft Eagle, Matlab, OpenLane, OpenRoad.
Version Control Tools: Git, TortoiseSVN.
Experience with lab tools: Logic Analyzers, Oscilloscopes, Soldering.