Sanjay Deshpande

Personal Website: https://sanjaydeshpande.netlify.app/
Linkedin: https://www.linkedin.com/in/sanjay-deshpande-6036b5a2/
New Haven, CT | Email: sanjay.deshpande@yale.edu | Mobile: (703) 678 1894

Summary

I am a third-year Ph.D. student from Yale University, advised by Prof. Jakub Szefer. My research focuses on the efficient and secure hardware implementations of post-quantum cryptographic algorithms and quantum computer security. I have 4+ years of experience in micro-architecture (RTL) design targeting FPGAs, designing Hardware IP cores for symmetric, asymmetric, and post-quantum cryptography algorithms. I have 1+ year of experience with quantum circuits and quantum computer security. In my previous roles, I have taken ownership of the hardware IPs and assisted in the integration process. I am actively looking for a Summer Internship (2024).

Education

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

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

Research Assistant — *Aug 2021 - Present*
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 Crosstalk-based attacks on Quantum Computers and developed Antivirus to scan and detect malicious quantum circuits.
- Ongoing research on performing side channel analysis and attacks on candidates from ongoing Post Quantum and Lightweight Crypto competitions.
- Ongoing research on circuit splitting and circuit obfuscation techniques for quantum circuits.

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.
- Conducted the Linear Electronics Lab for undergraduate students.
- Assisted students in Digital Systems Design using VHDL course and FPGA and ASIC Design with VHDL lab.

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.

Peer-Reviewed Publications

Cryptography and Hardware Research

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

2. Sanjay Deshpande, Yongseok Lee, Cansu Karakuzu, Jakub Szefer, and Yunheung Paek. SPHINCSLET - A LightWeight Implementation of SPHINCS$^+$. Under review

3. 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

4. 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

5. 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

6. 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

7. 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

8. 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

9. 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

10. Theodoros Trochatos, Sanjay Deshpande, Chuanqi Xu, Yao Lu, Yongshan Ding, and Jakub Szefer. CASQUE: Confidential Computing Architecture for Superconducting Quantum Computers. Under review

11. 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

12. 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

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.

RTL implementation of an authenticated cipher | *FPGA, VHDL, Cryptography* *Aug 2014 – Dec 2014*

Designed an RTL implementation for CAESAR competition Round 2 authenticated block cipher candidate – Minalpher targeting FPGAs.

Motion Detection Camera | *Embedded Hardware* *Aug 2014 – Dec 2014*

Assembled hardware and designed a system that senses motion and captures images.

Technical Skills

Languages: Verilog, VHDL, TCL, C, Python, Qiskit, Assembly.
Operating Systems: Windows, Linux, OSX.
Programmable Hardware: Xilinx – Spartan 6, Artix 7, Spartan 3E, Zynq 7000, Virtex 7, Zynq UltraScale+
Tools: Xilinx Vivado, Xilinx ISE, Xilinx ISim, Mentor Graphics Modelsim, Aldec Active-HDL, Intel Quartus prime, GHDL, Xilinx SDK, GMU ATHENa, Code Composer Studio, Cadsoft Eagle, Matlab, Cryptool, GnuPG, Synopsys Tools: Design Compiler, PrimeTime, IC compiler.
Communication Interface: UART, SPI, I2C, AXI.
Word Processing Tools: LaTeX, Microsoft Word, PowerPoint, Excel.
Version Control Tools: Git, TortoiseSVN.
Graphic Design Tools: Omnigraffle, Microsoft Visio.
Microcontrollers worked on: 8051, MSP430, Arduino.
Experience with lab tools: Logic Analyzers, Oscilloscopes, Soldering.

Achievements

- *Dec. 2023* – Won Best of IEEE CAL award for a paper on Quantum Computer Security, IEEE CAL.
- *Sept. 2023* – Won Best Project Award, Cyber-physical Systems Summer School, Sardegna, Italy.
- *May 2017* – Won Outstanding Academic Achievement Award, Electrical and Computer Engineering Department at George Mason University, Virginia, USA.

- *Dec. 2015* – Won third place in the Contest for the Best Project in the Cryptography and Computer Network Security course –at George Mason University, Virginia, USA.
- *Jul. 2014* – Received Certificate of Excellence in Academics, Jawaharlal Nehru Technological University, India.
- *Oct. 2013* – Won First Prize in Robocup 2k14, a zonal event, Jawaharlal Nehru Technological University, India.

Invited Talks

- *Nov 2023* – Security Group, Qualcomm, France – Presentation on the Hardware Implementation of NIST PQC candidate, HQC.

Program Committee Member

- *Dec 2023* – International Symposium on Circuits and Systems (ISCAS) 2024.