Statement of Purpose

VLSI has come a long way from its inception in the 1970s when integrated chips were used for computing purposes only to the present day where they have become omnipresent, from personal computers to many critical computing infrastructures such as financial systems, smart grids, sensitive government organizations, etc. These critical computing platforms are threatened by the recent advancement in the side and covert channel attack models in the past three decades. Additionally, the rapid development in the field of Quantum computers has shown signs that there is a dire need for the quantum secure cryptographic protocol implementations. I am fascinated with the design challenges inherent in this domain and want to contribute to meeting these challenges through my graduate studies. In graduate school, I would like to focus on developing efficient architecture and algorithms for secure cryptographic protocols and computer architecture concerning various attack methodologies.

My foray in the domain of Hardware Security began under the supervision of Prof. Mrigank Sharad working on analog current mirror-based Physically Unclonable Functions (PUF) circuits. We were looking for an area-efficient low power SRAM topology-based analog PUF circuit with the bit cells consisting of the cascode current mirrors. In our pursuit to seek improvements across various levels in the design hierarchy to meet our final goal, we proposed an adaptive multi-bit response of the PUF after inferences from the Monte Carlo Simulation and a power gating technique to achieve zero static power. My work initially involved extensive use of the Cadence Virtuoso tool to design the schematics and layout using the 180 nm scl CMOS library. The project helped me understand the Analog VLSI design flow starting from schematic design to I/O design for the chip also I learned about various power optimization techniques, ADC, and statistical modeling algorithms. This work, Adaptive Multi-bit SRAM Topology Based Analog PUF is under review at Journal.

A further opportunity to delve deeper into this field of VLSI Design took a definite shape when I was selected for an internship at The University of Tokyo, VLSI Design and Education Centre under the guidance of Prof. Masahiro Fujita working on Logic Synthesis using Discrete Neural Networks (DiNN). I began with the study of various binarized and ternary neural network models and addressing the question how the logic functions can be represented using these models?, I used the And Inverted Graphs (AIG's) to devise the network architecture of the logic functions. Furthermore, I devised a CAD tool to solve the partial logic synthesis problem by updating the weight of only the small section of the network designed form the logic function instead of the existing Satisfiability based solutions. This thrilling journey comprising of a literature review to proposing a solution in such a short period in a new country with a different environment instilled in me the belief of tackling a complicated and difficult problem. Presently, this project is under a remote collaboration with one of the Master Students at the FUJITA Lab, The University of Tokyo.

With the great foundation of the Digital VLSI Design through the internship and keen interest in Hardware Security through the PUF project. I decided to pursue my Bachelor Thesis under the guidance of Prof. Debdeep Mukhopadhyay working on Side-Channel Attacks on Block cipher gift. Before this, I possessed very little knowledge about the attack models and the techniques of secure Implementations. During my Bachelor Thesis, first I designed the cipher on Artix-7 FPGA and performed correlation power analysis attacks exploiting the property of the inherent bit permutation unit. Additionally, I also explored the attack possibility on the Threshold Implementation and the masking strategies to mitigate such attacks. The project helped me realize the importance of the secure digital design of the cipher as I can understand from the attacker as well as the designer's perspective. This culminating step in my undergraduate research career taught me some of the essential skills required in the life of a successful researcher – independent thinking, determination, and learning from failure. Since then, I have delved deep into the domain of secure cryptographic protocol design and its evaluation. Currently, in my senior year, I am working on the design of Homomorphic Encryption Scheme primitives under the supervision of Prof. Debdeep Mukhopadhyay and Prof. Indrajit Chakrabarti. I am working on a secure design of a Ring Learning with Error (RLWE) cryptography protocol which incorporates a Gaussian Sampler, Modular Arithmetic, and Number Theoretic Transform modules. This project has enabled me to work on the state of the art post-quantum cryptographic protocols considering the attack perspective in mind. While designing the framework, I learned about the various optimization schemes, security metrics and the Digital Design Flow on Xilinx FPGAs using the basic building blocks of FPGA like LUTs, carry chains and flops, and by the end of my graduation, I hope to design the secure, efficient architecture of one of the recent Fast Fully Homomorphic Encryption scheme.

I realized industrial experience is an indispensable supplement to technical education when I spent the summers of 2019 at Qualcomm India Private Limited, Bangalore. I worked with the Memory Design Team on the development of a CAD tool to detect Electromigration (EM) prone structures from the IC layout. I was able to devise a modular library using Calibre SVRF and python to detect EM likely structures during the layout designing phase instead of the post-layout EM verification. My brief stint at the company taught me to deliver under tight deadlines and successfully culminated in a standing job offer. The industrial experience at one of the leaders in the semiconductor industry has helped me concretize my career goals and ambitions and made me realize that I can fulfill my desire to obtain comprehensive knowledge and pursue innovative research only through my graduate studies.

IIT Kharagpur presented me with a plethora of opportunities, and I tried my level best to make the most of every opportunity that knocked at my doorstep. I have helped inculcate thriving research culture in my college and share my passion for technology through the Kharagpur RoboSoccer Students' Group under the supervision of Prof. Jayanta Mukhopadhyay– a research group aims at developing autonomous soccer-playing robots. The knowledge, exposure, and experience I gained from the group empowered me to push my horizons further. I also represented IIT Kharagpur as an undergraduate representative at Small Sized League of RoboCup-2017 held in Nagoya, Japan. Presently, I am the student coordinator of the group and the experience throughout my tenure as the head gave me the conviction that I have the potential to lead an organization from the front, boosting it to reach new heights. As a consequence of my involvement in Robotics system design, I was selected to represent IIT Kharagpur for the 6th and 8th Inter IIT Tech Meets. This bestowed upon me a tremendous learning opportunity, not only concerning the technicality of the products developed but also in the subtler aspects like leadership and team-building skills.

Having worked on all the broad aspects of Hardware Security with a focus on design, secure implementation and computer architecture based security come as a natural choice to me for my PhD research. My experiences in analog/digital VLSI circuit design, embedded systems, and machine learning through various projects have given me a comprehensive view of the field. I believe I shall be able to hone on this tenacious attitude and diverse undergraduate research to come up with a valuable contribution to the world of Hardware Security, which would simultaneously help me in achieving my future goals as a research scientist, educationist, as well as a probable entrepreneur.

I am applying to (School) because (research interests of Profs) have been accorded a major focus in the current research scenario here. Given my keen interest to pursue research in this domain, my contribution could add substantial value here. I feel that I would be able to learn a great deal if given the opportunity to work with (Prof.XX). His paper on the (paper motivation and correlation 2 lines). In addition, I'm very interested in the work done by (Prof.YY) on (topic). I found his paper on (paper motivation and correlation 2 lines).

Being a part of a world-class institution, I am confident that the exemplary faculty, diverse peer group, premier research facilities, and rich learning environment will help me achieve my goals and prepare me for the challenges of research, in academia or industry, thorough understanding of the subject at an advanced level, and sharpening my analytical skills to provide novel solutions for real-life problems. As a young man starting a new page of the next chapter in his life, with tremendous faith and confidence in his capabilities, I submit my candidature for the PhD program in (Course Name) Engineering at the (School Name).