I am very interested to work in cryptography. I want to apply my Mathematics knowledge to develop more and more secure cryptographic primitives and the project “Cryptographic Protocols and Blockchains – Overcoming multiparty computation impossibilities using a distributed ledger” is the best opportunity for me to achieve my aim as this is the combination of two very interesting technologies blockchain and secure MPC which are going to play a major role to shape the future of our society.

For the past few years, I have been working in the area of cryptography with Prof. Mridul Nandi at ISI Kolkata, India, with Prof. Sourav Mukhopadhyay at IIT Kharagpur, India, and with Prof. Sudip Misra at IIT Kharagpur, India. With Prof. Mridul Nandi at RC Bose Centre (ISI), I was working in Symmetric Cryptography. In our project, we are doing cryptanalysis on some classical ciphers like substitution ciphers, ADFGVX ciphers, etc. We have chunks of ciphers and we are analyzing those based on some of our implementations.

In multi-party computation (MPC) protocols, a set of users have their private information interact with each other and compute a joint function. Computation in a secure and efficient manner is a challenging task in MPC. In cloud computing, due to the dynamic nature of data, the cloud is unable to provide precisely what information is leaked if a component is compromised. To minimize and deal with such challenges, I have worked on a project to develop an MPC protocol as an aid to cloud computing with Prof. Sourav Mukhopadhyay at IIT KGP Math-Crypto Research Lab.

When we plan for implementation in a closed environment, Public-key cryptography may not necessarily be the only solution for confidentiality, authentication, integrity, and non-repudiation. PKI is computationally expensive and uses known algorithms at each stage which is not safe for defence applications as these might be vulnerable or compromised and not reported. Hence we proposed a new indigenous framework with models and methods to ensure authentication, integrity, and non-repudiation of data communication in general and provide these features for a defence network in particular. With Prof. Sudip Misra at SWAN Lab (IIT Kharagpur), I have worked on this project. We used the concept of WOTS+ and proposed a hyper-tree based framework to ensure non-repudiation in the data communication.

I have more than four years of research experience. Though my MS work was not related to cryptography, but I got a deep interest in cryptography during my coursework. My MS Thesis title is "Controller Placement in SDN: Energy- and Mobility-aware perspectives". In my MS research works, I have studied the Controller Placement Problem (CPP) in SDN under the guidance of Prof. Sudip Misra and Prof. Sourav Mukhopadhyay. I have presented two schemes for energy-aware and mobility-aware controller placement in that work. In the first scheme EnPlace, I have presented a game theory-based network partitioning approach for energy-aware controller placements considering in-band control plane and dynamic data traffic of IoT devices. This work is under review in IEEE Transactions on Green Communications and Networking. In the second scheme MobiPlace, I placed local controllers at the selected Road Side Units (RSUs) to reduce the operation delay experienced in traditional SDVN architecture, where controllers are placed in the cloud. The controller placement module applies a simulated annealing-based algorithm to select potential RSUs that can serve as local controllers. This work has been led to a manuscript that has been published in IEEE Transactions on Vehicular Technology, vol. 70, no. 1, pp. 957-966, Jan. 2021.

As a graduate student, I would like to teach and mentor other students as well as continue my research. While at IIT Kharagpur I have been a teaching assistant for Dr. Sandip Chakraborty's course Programming and Data Structure. As a TA, I conducted tutorials, discussed some topics, conducted and evaluated the assessment. I also reviewed some cryptographic manuscripts with Prof. Sourav Mukhopadhyay at IIT Kharagpur. I also taught Mathematics to six high school students as a home tutor.

Working closely with professors and students in this way cemented my desire to continue as a graduate student. I am excited by the opportunity to begin in this project. In particular, I have enjoyed following some work of Dr. Satrajit Ghosh at IIT Kharagpur and found the area very interesting in which he worked. Dr. Ghosh at IIT Kgp and Prof. Magri at UoM do the exciting research and continuing my education there would provide an excellent opportunity to learn from them and contribute to this project. With such broad prospects of work possible, I am confident of my objective of becoming a professional researcher with a deep understanding of both theoretical and practical aspects in Cryptography and thus, pursuing a doctoral degree is the next natural step for me. It will expose me to a deeper, more thorough, and practically relevant understanding of the present and prospective problems in my field of interest.

I am aware of the hard work and perseverance required to pursue research as a discipline and a career, and of the high standard of intellect and application that are required at IIT Kharagpur and University of Manchester. However, based on my consistent academic performance, my experience in researches, and the acclamation I have received from my peers and superiors, I feel confident of being able to meet and indeed, go beyond these requirements and expectations. In closing, I would like to thank the admissions committee for considering my application to this Ph.D. program. I am looking forward to continuing my studies as a graduate student and am excited by the prospect of working with the professors and students of IIT Kharagpur and University of Manchester.