Acknowledgement

The path toward this thesis has been serpentine. Having a background in Mathematics, I found it challenging to pursue the degree at the Department of Computer Science and Engineering. To complete this endeavour, I am very much thankful to some special persons who challenged, supported, and stuck with me along the way.

This journey is not possible without the constant motivation and endless support of my parents. I need to thanks them for ensuring the freedom to choose my career. My mother Nandita Ganguly has been my backbone. I would also like to thank my relatives who supported me when my mother got hospitalized. I especially acknowledge the support of my sister Gopa and her husband Tanmoy in my life. Without their help, it is not possible to dream about higher studies.

It is a great pleasure and acknowledge my deepest thank and gratitude to Prof. Abhijit Das and Prof. Dipanwita Roy Chowdhury from the Department of Computer Science and Engineering, IIT Kharagpur, for suggesting the topic and for their kind supervision. Their immense knowledge and plentiful experience have encouraged me all the time during my academic research and daily life. I have been extremely lucky to have supervisors who cared so much about my work and who responded to my questions and queries so promptly.

Having the guidance of Prof. Das is a blessing of God. At many stages in the course of this research work, I benefited from his advice, particularly when exploring new ideas. His positive outlook and confidence in my research work inspired me and gave me confidence. His excellent teaching style encourages me to learn a lot of subjects from the very basics. His courses "Computational Number Theory" and "Foundations of Cryptography" helped me to understand the basics of the research topic. His careful editing contributed enormously to the production of the thesis. Apart from a great supervisor, he is an unparalleled human being. He supports and motivates me a lot during the up and down in the research life. I have learned a lot of things from him apart from academic research. Nights spent at B-217 along with lab members are the most beautiful memories in my life. I am always indebted to Prof. Roy Chowdhury for her treasured support which is influential in shaping my concepts.

I would like to thank my Departmental Academic Committee Members Prof. Soumya Kanti Ghosh, Prof. Shamik Sural, Prof. Pabitra Mitra from the Department of Computer Science and Engineering, IIT Kharagpur. Their valuable suggestions played a crucial role in the entire research work. A special thank to the Faculty advisor (for MS) Prof. Chittaranjan Mondal. I would like to extend my sincere thank to the former HOD Prof. Sudeshna Sarkar and the current HOD Prof. Dipanwita Roy Chowdhury for providing an outstanding research environment and endless facility in the department. I would also like to thank all professors and staff of our department who helped me in various ways during the research journey.

I am thankful to SAC-ISRO, Ahmedabad, and DST SERB for funding the research grant throughout the journey. It is an honor to me to collaborate with Mr. Deval Mehta from Space Application Center, ISRO, Ahmedabad.

I would like to express my deepest gratitude to Prof. Sourav Mukhopadhyay (from the Department of Mathematics, IIT Kharagpur), who introduced me to the field of cryptography, especially public-key cryptography. Besides, I am extremely grateful to Prof. Ramkrishna Nanduri and Prof. Mousumi Mondal (both from the Department of Mathematics, IIT Kharagpur) for clearing doubts related to Algebraic Geometry. It helped me to write the chapter on mathematical backgrounds in the thesis.

My seniors played a key role in the journey of research. I would like to thank Dr. Bidhan Chandra Sardar (IIT Ropar), Dr. Dhiman Saha (IIT Bhilai), Dr. Raju Hazari (NIT Kalikat), and Dr. Sabyasachi Karati (NISER Bhubaneswar) for motivating me in the research journey. I am indebted to Karati-da for helping me in the field of curve-based cryptography.

I also take this opportunity to express my thanks to my lab seniors Swapan-da, Souvik-da, Debranjan-da, Ghosal-da, and Amit-da for constant helping and encouraging throughout the journey. Souvik-da and Pritam helped me a lot when I got stuck with long codes. Special thank also go to Bijoy, Rashid, and Rahul for helping me in the critical time.

Life at KGP is colouful with a strong friend circle. I am lucky to have friends like Ashok, Bubai, Mainak, Nitin, Prem, Ravi, Sudipta, Tapas, Punit, and many others. We all together spent a lot of good times in KGP. I connected myself with societies like Druheen and Boikalik. I would also like to thank all the members of both the societies for a positive mindset. Thanks to the entire KGP community too for providing a fabulous environment.

Last but not least, I would like to thank IIT Kharagpur for the studentship that allows me to conduct the thesis.