Acknowledgment

Md. Al-Amin Khandaker

November 13, 2018

The last 3 and a half year was one of the best time of my life that I will cherish forever. I'm immensely blessed throughout this period for which I have many people to thank. I'm grateful to many people who have directly and indirectly helped me finish this work.

This work would not be possible without the unceasing supervision, innumerable counselling and unrelenting persuasion of my Ph.D. advisor Professor Yasuyuki Nogami. I am indebted to *Nogami Sensei* for having me in his lab *(Information Security Lab.)* as a doctoral student and mentoring me on this work. He taught me how to analyze complex problems from different perspectives and express the ideas from pen and papers to a fully publishable article. I enjoyed his insightful comments on the research topics during our discussions. Sometimes his in-depth queries bewildered me and influenced my ideas in this thesis. He guided me in different ways to approach a problem and the need to be persistent to accomplish my goal. His presence and off-work discussion make the lab more than a workplace.

I'm also very grateful for to my doctoral course co-supervisors Professor Nobuo Funabiki (*Distributed Systems Design Lab.*) and Professor Satoshi Denno (*Multimedia Radio Systems Lab*) for having their time to read my thesis draft. Their insightful comments and helpful advice helped to shape the thesis into this state. I must recall my experience of taking the "Theory of Distributed Algorithm" course taught by Professor Nobuo Funabiki. His strong passion for algorithmic problem solving during the lectures was not only inspiring but also contagious.

I reminisce my encounters with Professor Satoshi Denno during my days at *Secure Wireless System lab.* He provided me with the deep-seated idea of the research works and Japan life. His questions and suggestions for the time of half yearly progress meetings were very intuitive.

I am very grateful to Associate Professor Nobumoto Yamane of *Information Transmission Lab.* for provided important comments at progress meetings.

I would like to express my gratitude to Senior Assistant Professor Takuya Kusaka of *(Information Security Lab.)* for the in-depth discussion of scientific topics. His strong work ethic and passion for research helped us to publish some of the remarkable collaborative works. He was always there to help while any difficulty arose from attending a conference to publishing a paper.

I express my gratitude to Senior Assistant Professor Hiroto Kagotani of *Information System Design Lab* for employing me as a research assistant for a

quarter. Since *Information System Design Lab* and *(Information Security Lab.)* share space, we had encountered more often and share of research discussions. His comments during the progress report were enlightening.

I am also grateful to Assistant Professor Kengo Iokibe (*Optical and Electromagnetic Waves Laboratory*) for the collaborative work we had on side-channel analysis of raspberry pi.

I would like to express my deep gratitude of Professor Sylvain Duquesne of Univ Rennes, France for having me at IRMAR as a short-term researcher and allowing me to present my work in front of some brightest audiences. Professor Duquesne's in-depth reviews on my works were not only helpful towards to final acceptability but also intriguing. My sincere gratitude to post-doctoral fellow Dr. Loubna Ghammam at Normandie University, France for her persistent guidance. Our collaboration with Professor Duquesne and Dr. Loubna helps me to work on the diverse area of mathematical aspects of cryptography.

I am also thankful to Professor Howon Kim of Pusan National University, South Korea and his Ph.D. student Taehwan Park for a great research collaboration on IoT security. My gratitude to one of the great IoT security expert Professor Hwajeong Seo of Hansung University, South Korea for being a co-author in my first major conference paper.

Thanks to MEXT, Japan for the scholarship which fulfilled my dream to pursue the doctoral study in Japan possible. I sincere acknowledge all the funds that afforded me to join several international conferences and conduct research activities.

I am also grateful to all administrative officer of the Faculty of Engineering who directly or indirectly made an impact in my doctoral course studies. My special thanks to Ms. Yumiko Kurooka for her kind support in administrative works.

Special thanks also to my seniors, juniors, and friends in the laboratory for creating a great work atmosphere and their generous support. Thanks to pairing team members of my lab who are one of brightest minds I've worked with.

I can not thank enough to my wife for her sacrifices and generous supports to my bread and butter. I would like to take the opportunity to appreciate my parents Ms. Nasima Akter and Mr. Md. Ali-Azzam Khandaker for their understanding, and encouragements.

So far so general we all are standing on the shoulders of the giants for our works. My profound gratitude to all great cryptographer, cryptographic engineers and researchers whose works keep inspiring students like me. I'm indebted to all my research collaborator, co-authors and reviewers for making my doctoral voyage engaging.