Acknowledgments

My graduate school experience spanned a little over five years across five cities. I am extremely fortunate to have Luca Trevisan as an advisor and a friend throughout the entire experience, getting me started on research and sticking with me even as I abandoned extractors. Luca taught me fairly early on that good coffee, good food, and a good time are imperative to doing research, and he never faulted me when I picked fun over work. His insight and advice on navigating research, the academic community, and the world beyond helped me mature as a researcher, an academic and a young adult. I aspire to be like Luca when I grow up — to work hard and play hard in a big city and to go through life with uncharacteristic humor and lots of sleep.

The general consensus is that there are only two excellent places to study cryptography and I gave up one to go to Berkeley. I was very lucky to meet Salil Vadhan before leaving Boston and I am extremely grateful for the many illuminating and inspiring discussions we had over the years. Salil and Luca generously gave of their time to help me develop my own research agenda, to instill in me the creativity and confidence to be a good researcher, and to engage me in a relentless pursuit of rigor in my research along with clarity in writing and in talks.

When I started out in graduate school, I would settle for a high-level understanding while reading papers and built-in templates while designing slides. Talking to and working with Andrej changed both of that. I have since learnt to reproduce quite a few proofs from scratch; I also wish and do believe some of Andrej’s impeccable taste in colors, typography and layout had rubbed off on me. His excellent penmanship, however, remains elusive.

I spent two lovely and very productive summers in New York, one at IBM T.J. Watson and another at Columbia, thanks to my mentors and hosts Ran Canetti, Rosario Gennaro, Tal Rabin, Tal Malkin and Rocco Servedio. Special thanks to Ran for getting me to think more like a cryptographer and a New Yorker! Apart from New York, I spent a summer at Microsoft Silicon Valley, a year at Tsinghua University in Beijing, and a semester at IPAM, all of which were wonderful learning experiences. I thank Cynthia Dwork, Andy Yao and my hosts at IBM and Columbia for their hospitality and for remaining such dedicated mentors since.
I wish to thank my co-authors for the collaboration, particularly Seung Geol Choi, Dana Dachman-Soled and Tal Malkin for the result in this thesis, as well as Daniel Jackson, Madhu Sudan and Silvio Micali for initiating my passage into research, theory and cryptography. In addition to the afore-mentioned, I have had many delightful and enjoyable discussions with Iftach Haitner, Rafael Pass, Alon Rosen, Guy Rothblum, David Woodruff, Vinod Vaikuntanathan, Emanuele Viola and Ke Yang on subjects technical and otherwise, and I look forward to many more.

I express my gratitude towards Christos Papadimitriou, Elchanan Mossel and Alistair Sinclair for serving on my thesis and quals committees, and for being so accommodating of my faults and my requests. I also thank Henry Lin and Guy for delivering a talk and my thesis in my absence and La Shana Polaris and Chang Su for making administration less of a nightmare.

I could not have made it this far if not for the amazing people I met along the way, who always regarded with unfailingly good humor my inexplicable idiosyncrasies ranging from an inaptitude for driving to a ban on broccoli and burrito. I refer to the occupants and affiliates of 587 Soda, FIT 1-280 and IPAM as well as all my friends from home, college and graduate school. Amongst these people, I would like to single out Andrej, Kamalika Chaudhuri, Ioannis Kerenidis, Kenji Obata, Ranjit Jhala, Kunal Talwar and David Ratajczak, who took on the various roles of little sister, big sibling, room-mate, caretakers of a man on crutches, and companions on numerous culinary expeditions, and also Robert Kessell, Ben Myers, Richard Tran and Kim Truong, who made sure I never got lost in America. I hope everyone will keep trying to make me eat green stuff.

Cafes have been an indispensable part of my life in graduate school, notably Brewed Awakening, Cafe Strada and S.I.T. Cafe. They are more than a place where coffee and ideas are brewed; they also keep me from brooding.

Finally, I thank my family for their unconditional support, even though I never tell them what exactly I do and where exactly I am going.

DEC 1, 2007