Acknowledgments

> . . . very little do we have and inclose which we can call our own in the deep sense of the word. We all have to accept and learn, either from our predecessors or from our contemporaries. Even the greatest genius would not have achieved much if he had wished to extract everything from inside himself. But there are many good people, who do not understand this, and spend half their lives wondering in darkness with their dreams of originality. I have known artists who were proud of not having followed any teacher and of owing everything only to their own genius. Such fools!
>
> Goethe, *Conversations with Eckermann*, 17.2.1832

First of all, I would like to thank three remarkable people who had a tremendous influence on my professional development: Shimon Even introduced me to theoretical computer science and closely guided my first steps. Silvio Micali and Shafi Goldwasser led my way in the evolving foundations of cryptography and shared with me their constant efforts for further developing these foundations.

I have collaborated with many researchers, yet I feel that my collaboration with Benny Chor and Avi Wigderson had the most important impact on my professional development and career. I would like to thank them both for their indispensable contribution to our joint research and for the excitement and pleasure I had when collaborating with them.

Leonid Levin deserves special thanks as well. I had many interesting discussions with Leonid over the years, and sometimes it took me too long to realize how helpful these discussions were.

Special thanks also to four of my former students, from whom I have learned a lot (especially regarding the contents of this volume): to Boaz Barak for discovering the unexpected power of non-black-box simulations, to Ran Canetti for developing definitions and composition theorems for secure multi-party protocols, to Hugo Krawczyk for educating me about message authentication codes, and to Yehuda Lindell for significant simplification of the construction of a posteriori CCA (which enables a feasible presentation).

Downloaded from https://www.cambridge.org/core. ETH-Bibliothek, on 22 Mar 2017 at 13:37:56, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511721656

Next, I'd like to thank a few colleagues and friends with whom I had significant interaction regarding Cryptography and related topics. These include Noga Alon, Hagit Attiya, Mihir Bellare, Ivan Damgard, Uri Feige, Shai Halevi, Johan Hastad, Amir Herzberg, Russell Impagliazzo, Jonathan Katz, Joe Kilian, Eyal Kushilevitz, Yoad Lustig, Mike Luby, Daniele Micciancio, Moni Naor, Noam Nisan, Andrew Odlyzko, Yair Oren, Rafail Ostrovsky, Erez Petrank, Birgit Pfitzmann, Omer Reingold, Ron Rivest, Alon Rosen, Amit Sahai, Claus Schnorr, Adi Shamir, Victor Shoup, Madhu Sudan, Luca Trevisan, Salil Vadhan, Ronen Vainish, Yacob Yacobi, and David Zuckerman.

Even assuming I did not forget people with whom I had significant interaction on topics touching upon this book, the list of people I'm indebted to is far more extensive. It certainly includes the authors of many papers mentioned in the reference list. It also includes the authors of many Cryptography-related papers that I forgot to mention, and the authors of many papers regarding the Theory of Computation at large (a theory taken for granted in the current book).

Finally, I would like to thank Boaz Barak, Alex Healy, Vlad Kolesnikov, Yehuda Lindell, and Minh-Huyen Nguyen for reading parts of this manuscript and pointing out various difficulties and errors.

Downloaded from https://www.cambridge.org/core. ETH-Bibliothek, on 22 Mar 2017 at 13:37:56, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/CBO9780511721656