Acknowledgements

The book grew out of my lecture notes from the Masters course "Public key cryptography" at Royal Holloway. I thank the students who took that course for asking questions and doing their homework in unexpected ways.

The staff at Cambridge University Press have been very helpful during the preparation of this book.

I also thank the following people for answering my questions, pointing out errors in drafts of the book, helping with latex, examples, proofs, exercises etc: José de Jesús Angel Angel, Olivier Bernard, Nicolas Bonifas, Nils Bruin, Ilya Chevyrev, Bart Coppens, Alex Dent, Claus Diem, Marion Duporté, Andreas Enge, Victor Flynn, David Freeman, Pierrick Gaudry, Takuya Hayashi, Nadia Heninger, Florian Hess, Mark Holmes, Everett Howe, David Jao, Jonathan Katz, Eike Kiltz, Kitae Kim, David Kohel, Cong Ling, Alexander May, Esmaeil Mehrabi, Ciaran Mullan, Mats Näslund, Francisco Monteiro, James McKee, James Nelson, Samuel Neves, Phong Nguyen, TaeHun Oh, Chris Peikert, Michael Phillips, John Pollard, Francesco Pretto, Oded Regev, Christophe Ritzenthaler, Karl Rubin, Raminder Ruprai, Takakazu Satoh, Leanne Scheepers, Davide Schipani, Michael Schneider, Peter Schwabe, Reza Sepahi, Victor Shoup, Igor Shparlinski, Andrew Shallue, Francesco Sica, Alice Silverberg, Benjamin Smith, Martijn Stam, Damien Stehlé, Anton Stolbunov, Drew Sutherland, Garry Tee, Emmanuel Thomé, Frederik Vercauteren, Timothy Vogel, Anastasia Zaytseva, Chang-An Zhao, Paul Zimmermann.

The remaining errors and omissions are the authors responsibility.

Note added October 2018: Thanks to all the people who have pointed out errors. They are thanked in the errata list on my webpage.