Preface

The first International Workshop on Post-Quantum Cryptography took place at the Katholieke Universiteit Leuven in 2006. Scientists from all over the world gave talks on the state of the art of quantum computers and on cryptographic schemes that may be able to resist attacks by quantum computers. The speakers and the audience agreed that post-quantum cryptography is a fascinating research challenge and that, if large quantum computers are built, post-quantum cryptography will be critical for the future of the Internet. So, during one of the coffee breaks, we decided to edit a book on this subject. Springer-Verlag promptly agreed to publish such a volume. We approached leading scientists in the respective fields and received favorable answers from all of them. We are now very happy to present this book. We hope that it serves as an introduction to the field, as an overview of the state of the art, and as an encouragement for many more scientists to join us in investigating post-quantum cryptography.

We would like to thank the contributors to this volume for their smooth collaboration. We would also like to thank Springer-Verlag, and in particular Ruth Allewelt and Martin Peters, for their support. The first editor would like to additionally thank Tanja Lange for many illuminating discussions regarding post-quantum cryptography and for initiating the Post-Quantum Cryptography workshop series in the first place.

Chicago and Darmstadt,
December 2008

Daniel J. Bernstein
Johannes A. Buchmann
Erik Dahmen

http://www.springer.com/978-3-540-88701-0

Post-Quantum Cryptography
Bernstein, D.J.; Buchmann, J.; Dahmen, E. (Eds.)
2009, X, 246 p., Hardcover
ISBN: 978-3-540-88701-0