

Preface

One of the main reasons for writing this monograph is the curiosity to know more. Identity-based encryption is a fascinating area of modern cryptography. We have done some work in this area and wanted to explore the area in some depth. This motivation, however, was not sufficient for us to take up the job. The catalytic effect is due to Peter Wild, who suggested us to take up this work and very kindly referred us to Springer.

Determining the focus of a monograph is difficult. More specifically, it is difficult to determine who would benefit from the text. Within a decade or so, identity-based encryption has emerged as a distinct area of research starting, virtually, from scratch. Naturally, IBE now attracts many research students from across the world. For a beginner, it might be a little difficult to get a unified account of the evolution of this research area from the scattered literature. It is precisely this gap that we try to fill through this monograph.

Starting from the basic ideas, the monograph attempts to cover all the important IBE schemes that have been proposed till date. Among these are included the more recently proposed lattice-based IBE schemes. A major thrust of the research in IBE is the so-called security proof. Proofs of the security reductions of most of the important schemes are provided in details. Our guiding principle in selecting the proofs for inclusion is that they highlight some novel techniques. Many more schemes are described without any formal proof and in some cases an intuitive description of the security reduction is provided. Hopefully, going through the book will help a research student to grasp the central ideas involved in constructing IBE schemes. If this is indeed achieved, then our efforts will have succeeded. We also hope that the book may be useful to experts as reference for quickly looking up a particular topic.

The actual writing of the monograph took several months (and included missing a deadline). We are thankful to Springer, especially Susan Lagerstrom-Fife for her enthusiasm and support to the project. Jennifer Maurer looked over the manuscript several times and provided useful feedback.

Technical feedback on the contents of the monograph were provided by several of our colleagues and students. In fact, they formed the test cases for the judging the usefulness of the monograph. We gratefully acknowledge the comments and

feedback received from Rana Barua, Sanjay Bhattacharjee, Sherman S. M. Chow, M. Prem Laxman Das, Kishan C. Gupta, Koray Karabina and Somindu C. Ramanna. Without their feedbacks, there would surely been many more mistakes present in the book than there is now. Needless to say, any errors that do remain are entirely our own responsibility.

Kolkata, India,
November 2010

Sanjit Chatterjee
Palash Sarkar



<http://www.springer.com/978-1-4419-9382-3>

Identity-Based Encryption

Chatterjee, S.; Sarkar, P.

2011, XI, 180 p., Hardcover

ISBN: 978-1-4419-9382-3