Review of the book

"Identity-Based Encryption"

by Sanjit Chatterjee and Palash Sarkar

Springer, 2011

ISBN: 978-1-4419-9382-3

Lorena Ronquillo
IT University of Copenhagen (Denmark)

October 20, 2014

1 Summary of the review

Identity-Based Encryption is a kind of public key encryption scheme where the public key of a user can be any arbitrary string (typically the e-mail address), thus greatly simplifying certificate management. Quoting Shamir, who first posed this challenge to the cryptographic community: "*It makes the cryptographic aspects of the communication almost transparent to the user, and it can be used effectively even by laymen who know nothing about keys or protocols.*"

The book "Identity-Based Encryption" by Sanjit Chatterjee and Palash Sarkar tries to serve as a single comprehensive source of information on Identity-Based Encryption. Different aspects and schemes are presented and discussed in its twelve chapters, with a strong emphasis on their security proofs.

In general, the book provides a good and rather complete survey of the relevant literature on (Hierarchical) Identity-Based Encryption schemes, at least to the date the book was written. The authors do a good job in relating and comparing the schemes to each other, and also describing each one of them with simpler words.

2 Summary of the book

The volume is divided into eleven medium-sized chapters, plus a short final chapter summarizing some of the commercial products and drafts standards related to Identity-Based Encryption schemes implemented to the date.

Chapter 1: Introduction.

This chapter provides a brief overview of public and symmetric key cryptography, and also introduces Identity-Based Encryption in the context of public-key cryptography.

Chapter 2: Definitions and Notations.

This chapter presents some definitions and notation that will be used throughout the remaining chapters of the book. This includes a more formal definition of public key encryption schemes and the security models usually employed, namely IND-CPA, IND-CCA, and IND-CCA2 security. This chapter also provides a formal definition of Identity-Based Encryption (IBE) schemes and its extension to the so-called Hierarchical Identity-Based Encryption (HIBE) schemes, as well as introducing the security models that apply to this area: IND-ID-CCA security, IND-ID-CPA security, and IND-sID-CCA security (selective-ID security model). The chapter ends by giving an intuition of the structure of reductionist security proofs in cryptography, and also mentioning the issues related to random oracles.

Chapter 3: A Brief Background on Elliptic Curves and Pairings.

This chapter gives an informal description of the algebra involved in IBE schemes. According to the authors, it is not meant to be an exhaustive review, but it seems to cover most of the background necessary to understand the rest of the book, and also points to some other references for those willing to know more. This chapter introduces bilinear pairings, cyclic groups, finite fields and some of the basics of elliptic curves. Then, a Tate Pairing over elliptic curve groups is defined, the three different types of pairings are introduced, and it ends by describing the most common hardness assumptions over pairing groups. It is worth to mention that this chapter does a big emphasis on the efficiency and other practical issues of algebraic computations, although the different techniques to speed-up pairing computations have been considered by the authors out of the scope of the book and are therefore not explained.

Chapter 4: Boneh-Franklin IBE and its Variants.

This chapter is devoted to the first practical IBE scheme using bilinear pairing, by Boneh and Franklin (BF-IBE), which spurred further research in the area. The chapter also includes the corresponding security proofs of both the CPA-secure version and the CCA-secure version, assuming the hardness of the Bilinear Diffie-Hellman problem (BDH). It also presents some generalizations of IBE schemes to HIBE schemes, like the one given by Gentry and Silverberg, in this case with a rather intuitive version of its security proof.

Chapter 5: Selective-Identity Model.

This chapter describes the construction and provides the security proof of the schemes due to Boneh and Boyen (BB-HIBE) and Boneh, Boyen and Goh (BBG-HIBE) in the selective-identity model, that is, the weaker notion of security in which the adversary commits to a target identity before the system is set up. The authors also point to some of the algebraic techniques used in the construction and security proof of these schemes, as they have been widely used later on, specially when constructing IBE schemes which are secure against adaptive-identity attacks.

Chapter 6: Security Against Adaptive Chosen Ciphertext Attacks.

This chapter focuses on several techniques to obtain CCA-security for (H)IBE schemes, from CPA-secure (H)IBE schemes. It describes the method by Canetti, Halevi and Katz (CHK), whose efficiency was later improved by Boneh and Katz.

Chapter 7: IBE in Adaptive-Identity Model Without Random Oracles.

This chapter describes some important (H)IBE schemes in the Adaptive-Identity Model, such as the one by Waters and its generalisations, as relevant constructions first providing a practical (H)IBE in the standard model, that is, not using random oracles in its security reduction. Most of the schemes discussed in this chapter are proved secured under the Decisional Bilinear Diffie-Hellman (DBDH) assumption.

Chapter 8: Further IBE Constructions.

This chapter provides two techniques useful to construct IBE schemes in the adaptive-ID model without random oracle, with the aim of obtaining a tighter reduction for IBE. The first technique discussed is due to Gentry, while the second one is due to Waters and seems to be of particular relevance because it introduces a novel paradigm to argue the security of cryptographic schemes.

Chapter 9: IBE Without Pairing.

This chapter describes other constructions of IBE schemes not based on bilinear pairings, but on lattices and on elementary number theory, like quadratic residues. This chapter also provides a brief background on lattices. The efficiency of these new methods is roughly compared, although the authors do mention that there is currently no comparative study of the speed of actual implementations of lattice based IBE schemes and pairing based IBE schemes (and they don't provide it, either).

Chapter 10: Applications, Extensions and Related Primitives.

This chapter briefly describes some of the techniques that were used to construct IBE schemes and which had been later used to construct other cryptographic primitives, such as signature, key agreement, and broadcast encryption schemes, among others.

Chapter 11: Avoiding Key Escrow.

This chapter focuses on the methods existing in the literature in order to avoid or mitigate the power and influence of the private key generator (PKG) in IBE schemes. One of the techniques presented consists of distributing the PKG by means of threshold cryptography, or using double encryption.

Chapter 12: Products and Standards.

This last chapter provides a very brief summary of some of the products and drafts standards related to Identity-Based cryptography existing to the date, as a result of more than a decade of research in cryptographic applications of bilinear pairings.

3 What is the book like (style)?

Almost every chapter in the book includes an intuitive explanation of the security of the (H)IBE schemes explained, followed by a formal and quite detailed argument in the form of a security reduction.

The book is mainly addressed to researchers already having a solid background in cryptography and basic algebra. Although the writing is very clear and comprehensible, I would not consider this book as a textbook, mainly because of the lack of examples and exercises, and also because it is not self-contained. Indeed, concepts like cyclic groups or hash functions are only very vaguely defined and therefore assumed to be known by the reader. The reader is even assumed to be familiar with some notation related to cyclic groups, like denoting a multiplicative group by $\langle g \rangle$, when neither the operation $\langle \cdot \rangle$ nor the element g have been explicitly defined whatsoever. Of course, any reader familiar with the area will soon realize what the authors actually mean by this.

As in any book, it also contains a few typos without importance that are repeated in several places all over the book, like the words "residuacity" or "distingushability", but I guess they will soon be fixed in newer editions of the book.

In general, the book provides a good and rather complete survey, and whenever a scheme is not included in the book, the authors properly argue the reasons why they decided not to include it, showing that they were aware of it and not just forgot it. Even though the authors do not seem to include much more information than what it is already included in the schemes they mention and describe, they do a good job in gathering all the information, relating the schemes to each other, and explaining them with simpler words.

4 Would you recommend this book?

I would recommend this book to any researcher having a background in basic algebra and public-key cryptography, willing to start exploring the area of Identity-Based cryptography. The book gives a very good picture of the progress done in the area, and it also describes clearly the remaining and challenging open problems.
As an introduction in the area this is an excellent book. However, readers considering to acquire this book should also keep in mind that the IBE schemes described here are summarized and thus necessarily lack some details that can otherwise be found in the original papers.

The reviewer is a post-doc at the DemTech research group, at the IT University of Copenhagen, Denmark.