Review of "Elliptic Curves in Cryptography" by Ian Blake, Gadiel Seroussi, Nigel Smart Cambridge University Press ISBN: 0-521-65374-6

Avradip Mandal
Microsoft Corp, USA

1 What the book is about

This book is about the mathematics behind elliptic curve cryptography. Elliptic curves offer smaller key sizes and efficient implementations compared to traditional public key cryptographic schemes over integers. The book consists of twelve chapters. In the first couple of chapters the book gives a short introduction to group based Public Key cryptography and finite field arithmetic. In the later chapters, it provides a thorough mathematical analysis of various aspects pertaining to efficient implementation of elliptic curve cryptography, as well as well-known attacks.

Chapter I - Introduction

This chapter gives a short introduction to various group based cryptosystems like Diffie-Hellman key exchange, El Gamal encryption, Digital Signature Algorithm (DSA), etc. This chapter also includes a short discussion on how elliptic curve cryptography compares to conventional cryptography in terms of security and key size.

Chapter II - Finite Field Arithmetic

In any elliptic curve implementation, the underlying finite field arithmetic plays an important role. This chapter discusses various issues related to that. In particular, pros and cons of odd and even characteristic fields, and special fields that might help implementation.

Chapter III - Arithmetic on an Elliptic Curve

This chapter provides the fundamentals about elliptic curves. Starting with the definition of elliptic curves and the group law, this chapter goes into ellip-

tic curves over certain kind of finite fields of cryptographic importance. This also gives a brief introduction on various other elliptic curve terminologies like division polynomials, isogenies, Weil Pairing, etc.

Chapter IV - Efficient Implementation of Elliptic Curves

This chapter describes the mathematics behind efficient point addition and multiplication. It also describes techniques for point compression (representing an elliptic curve point using minimum number of bits).

Chapter V - The Elliptic Curve Discrete Logarithm Problem

This chapter discusses various attacks on the elliptic curve version of the well-known discrete logarithm problem. Six different methods are covered.

- a simplification of Pohling and Hellman's method
- the MOV attack
- the anomalous attack
- Baby-step Giant-step method
- random walks-based method
- Index calculus method

Chapter VI - Determining the Group Order

The problem of determining the order of the group of rational points on an elliptic curve over a finite field - the *point counting problem* - is of critical importance in applications such as primality proving and cryptography. For cryptographic purposes one needs non-supersingular curves, whose group orders are divisible by a large prime factor. This chapter discusses some general methods to find group orders of finite groups.

Chapter VII - Schoof's Algorithm and Extensions

This chapter discusses Schoof's algorithm, which forms the bases of all current efficient schemes for point counting on elliptic curves. It also covers various improvements of Schoof's algorithms due to Elkies and Atkins.

Chapter VIII - Generating Curves using Complex Multiplication

This chapter provides a brief outline of the theory of complex multiplication. Then it discusses the CM (complex multiplication) method of generating elliptic curves of desirable group orders.

Chapter IX - Other Applications of Elliptic Curves

This chapter briefly discusses some additional applications of elliptic curves in cryptography.

- Factoring using elliptic curves
- Primality testing using elliptic curves
- Showing equivalence between Discrete Logarithm Problem and Diffie Hellman Problem for some special classes of groups.

Chapter X - Hyperelliptic Cryptosystems

The final chapter gives a brief introduction to hyperelliptic curves and its application to cryptography. It discusses the arithmetic on hyperelliptic curves, methods to generate hyperelliptic curves suitable to cryptography and the discrete logarithm problem on hyperelliptic curves.

2 What is the book like (style)?

This is a dense and small book. Only within about two hundred pages it covers almost everything about elliptic curve cryptography. Due to that reason, at times it almost feels like a survey paper, rather than a book. This book does not expect the reader to be familiar with mathematics elliptic curves or cryptography (even though, that would definitely be a big plus to follow the book). However, the reader must be well versed in basic modern algebra (group and field theory). In most of the chapters, the authors nicely captured the high level ideas and mentioned various pitfalls important for implementation. However, in many cases they skipped the detailed mathematical proofs and referred the readers to original papers.

3 Would you recommend this book?

This is not a self-sustaining book that one can read from start to end. For a novice but dedicated reader, it would take months (or years) to look up the references and assimilate everything. Which is not surprising, because this book covers almost everything about elliptic curve cryptography that was known when the book was first published (1999). However the book, still can be immensely useful for the following category of readers: Anybody who has basic understanding of modern algebra and wants to get a quick overview about elliptic curve cryptography, especially from an implementation perspective. For researchers, who are familiar with elliptic curve cryptography this book can act as an excellent starting point to quickly find out anything that he/she is not sure of.

The reviewer works at Microsoft Corp., USA.