Review of the book

"*Handbook of Elliptic and Hyperelliptic Curve Cryptography*"
by Henri Cohen and Gerhard Frey,
also Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren

Chapman & Hall/CRC, Taylor & Francis Group, 2006
ISBN 978-1-58488-518-4

review by Thierry Moreau
June 6, 2011

This book could have been titled "*Mathematics and Mathematical Algorithms for Elliptic and Hyperelliptic Curves, with a Focus on Cryptography*." With this clarification, it offers a very comprehensive coverage of this vast subject area, by a total of 16 authors and contributors. Overall a useful and essential treaty for anyone involved in elliptic curve algorithms, *except* if someone looks for definitive technical guidance as in a cookbook.

The elliptic curve cryptography owes a lot more to mathematical advances than integer factorization based systems, and this may be shocking if one uses this book as an introduction. Indeed, the book chapters on mathematical background (from chapter 2) were kind of hopeless to me but, as the preface suggests, the rest of the book attempts at self-contained exposition of relevant mathematical algorithms (chapter 9 onwards). Actually, some of the later chapters are also very mathematical-intensive, but fortunately it is less so for algorithms that are likely to find industrial applications. In a sense, cryptography and elliptic curves are not different from computer algorithms in general, that is very dependent on the works of mathematicians. This book, in trying to explain its subject area in the perspective of implementations, goes very far in providing mathematical support.

The systematic dedication to the implementation of elliptic curve and support algorithms provides a lot of value to the reader. Simple pseudo-code is complemented by remarks covering error-prone details, alternative strategies, and other practical advice. Each algorithm running time estimate is indicated, using uniform notation from the science of computational complexity. Maybe because I have previous experience in implementing some of the algorithm starting from academic publications, I am very pleased with such systematic presentation of a large collection of cryptography related algorithms.

Somehow surprisingly, cryptography is covered to a limited extent in this book (essentially chapters 1 and 23). The first thing I did with the book was to search for HMQV (a key establishment protocol based on the discrete logarithm problem) in the index, to find out it is not even mentioned. Only the ECDSA signature scheme is covered, as an example of discrete log cryptosystems, furthermore in a variant using hyperelliptic curve arithmetic (not mainstream from an industrial perspective). While the influence of cryptographic applications is adequately reflected in the exposition of mathematics and mathematical algorithms (I paid special attention to this specific point), the book provides no explicit coverage of debatable aspects of ECC, such as complexity theory proofs of equivalence between a cryptosystem and the discrete log problem, actual key sizes recommendations, basis of trust for ECC parameters selection by a third party, intellectual property issues, and the very comparative analysis between ECC and RSA. But in the end analysis, the reader may be better equipped with factual information instead of debatable arguments.

A downside of the book is the counterpart of its systematic approach to algorithm explanations without compromise in mathematical foundations: the book does not address a readily identified audience. The reader has a homework to do depending on the next step after having learned something. An implementer would need to double-check an algorithm against academic publications or related reference or open source implementations. A cryptosystem designer will need to translate the relevant details from the mathematical exposition while mounting a security analysis. And obviously, the publication date being 2006, the more recent developments are to be investigated by the reader based on other sources. I am not able to tell exactly how a pure mathematician may benefit from this book, but if mathematical advances have potential applications, this book can certainly be used as a methodology model for reporting results with some attention paid to implementers.

The contents comprehensiveness is astounding. Within its scope and approach, the book covers many facets and ramifications. The arithmetic is covered in two sections, respectively 4 chapters for generic arithmetic and 4 chapters for specialized curve arithmetic. Somehow boringly, this establishes the algorithmic foundations for the next three sections that, together, sets the elliptic curve technology for cryptography. First, the choice of a curve requires point counting algorithms, maybe the book section where the mathematical intensiveness is most disturbing from an industrial deployment perspective. Then, ECC being secure to the extend it is hard to compute discrete logarithms, a section of 4 chapters is devoted to algorithms that might crack ECC. Finally, the culmination of the book is the section on applications, and specifically chapter 23. This forms a structured body of knowledge with ramifications, such as hyperelliptic curves, present at each layer.

After reading the preface and introduction, you may either read from chapter 2 (theory), chapter 9 (arithmetic), or jump directly to chapter 23 (integration into applications). The ECC mathematical intensiveness is such that none of these strategies allow you to ignore your limitations (if any) in mastering the theoretical foundations. Personally, I don't blame the book for ECC mathematical intensiveness. As mentioned before, if you look for a cookbook, you should look elsewhere.

The later chapters of the book contain significant additional material, the value of which would depend on specific reader interests. A secure hardware designer may find invaluable information about fast arithmetic in hardware. The two chapters on smart card attacks and countermeasures are also noteworthy. Other chapters look like survey publications, but they nicely complete the global picture of the ECC technology.

If the fascination for the ECC techniques operates on you and if you accept to be exposed to scientific knowledge that you don't master, I would recommend this book without hesitation. If one devotes the time and effort to learn, this book offers the opportunity to grasp the ECC technology with a diversified and comprehensive perspective. I took this opportunity with the book review and I now got a much clearer idea of my ignorance. This book will remain on my shelf for a long time and will land on my desk on many occasions, if only because the coverage of the issues common to factoring and discrete log cryptosystems is excellent.

The reviewer is the founder of CONNOTECH, a consulting and R&D firm specialized in information security and payment systems.