MR2162716 (2007f:14020) 14G50 (11G05 11G07 11T71 94-00 94A60)

★**Handbook of elliptic and hyperelliptic curve cryptography.**

Edited by Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen and Frederik Vercauteren.

Discrete Mathematics and its Applications (Boca Raton).

Chapman & Hall/CRC, Boca Raton, FL, 2006. *xxxiv*+808 *pp*. $99.95.

ISBN 978-1-58488-518-4; 1-58488-518-1

Contents: Roberto M. Avanzi and Tanja Lange, Introduction to public-key cryptography (1–15) MR2162717; Christophe Doche and David Lubicz, Algebraic background (19–37) MR2162718; David Lubicz, Background on p-adic numbers (39–44) MR2162719; Gerhard Frey and Tanja Lange, Background on curves and Jacobians (45–85) MR2162720; Gerhard Frey and Tanja Lange, Varieties over special fields (87–113) MR2162721; Sylvain Duquesne and Gerhard Frey, Background on pairings (115–124) MR2162722; Gerhard Frey and Tanja Lange, Background on Weil descent (125–132) MR2162723; David Lubicz and Frederik Vercauteren, Cohomological background on point counting (133–141) MR2162724; Christophe Doche, Exponentiation (145–168) MR2162725; Christophe Doche, Integer arithmetic (169–199) MR2162726; Christophe Doche, Finite field arithmetic (201–237) MR2162727; Frederik Vercauteren, Arithmetic of p-adic numbers (239–263) MR2162728; Christophe Doche and Tanja Lange, Arithmetic of elliptic curves (267–302) MR2162729; Sylvain Duquesne and Tanja Lange, Arithmetic of hyperelliptic curves (303–353) MR2162730; Christophe Doche and Tanja Lange, Arithmetic of special curves (355–387) MR2162731; Sylvain Duquesne and Gerhard Frey, Implementation of pairings (389–404) MR2162732; Reynald Lercier, David Lubicz and Frederik Vercauteren, Point counting on elliptic and hyperelliptic curves (407–453) MR2162733; Gerhard Frey and Tanja Lange, Complex multiplication (455–473) MR2162734; Roberto M. Avanzi, Generic algorithms for computing discrete logarithms Avanzi and Nicolas Thériault, Index calculus (495–509) MR2162736; Roberto M. Avanzi and Nicolas Thériault, Index calculus for hyperelliptic curves (511–527) MR2162737; Gerhard Frey and Tanja Lange, Transfer of discrete logarithms (529–543) MR2162738; Gerhard Frey and Tanja Lange, Algebraic realizations of DL systems (547–572) MR2162739; Sylvain Duquesne and Tanja Lange, Pairing-based cryptography (573–590) MR2162740; Roberto M. Avanzi and Henri Cohen, Compositeness and primality testing factoring (591–614) MR2162741; Kim Nguyen and Andrew Weigl, Fast arithmetic in hardware (617–646) MR2162742; Bertrand Byramjee and Andrew Weigl, Smart cards (647–667) MR2162743; Bertrand Byramjee, Jean-Christophe Courrège and Benoît Feix, Practical attacks on smart cards (669–685) MR2163784; Tanja Lange, Mathematical countermeasures against side-channel attacks (687–714) MR2163785; Tanja Lange, David Lubicz and Andrew Weigl, Random numbers generation and testing (715–735) MR2167252.

Let G be a finite abelian group and let $g \in G$. The discrete logarithm problem (DLP) is the computational problem: given a randomly chosen element h in the subgroup generated by g, compute an integer n such that $h = g^n$. The first example of a group for which the DLP seems to

be hard is the multiplicative group of a finite field. Public key cryptosystems have been developed whose security relies on the hardness of the discrete logarithm problem. Hence, there is great interest in groups for which the discrete logarithm problem seems to be hard.

The set of points on an elliptic curve (e.g., $y^2 = x^3 + Ax + B$ where $4A^3 + 27B^2 \neq 0$) over a finite field is a finite abelian group. In 1985 Miller and Koblitz independently proposed using elliptic curves for public key cryptography based on the DLP. Miller noted that elliptic curves are attractive because, unlike the case of the multiplicative group of a finite field, there is no known index calculus algorithm for the DLP.

Koblitz later suggested using the divisor class group of a hyperelliptic curve of genus g (e.g., $y^2 = f(x)$ where $\deg(f(x)) = 2g + 1$ and $f(x)$ has no repeated root). The discrete logarithm problem in such groups also seems to be hard, though as the genus grows then index calculus algorithms become available.

In the years since these proposals were made, there has been a significant research effort to understand the difficulty of the DLP on elliptic and hyperelliptic curves, and to make public key cryptography practical in this setting. This book aims to give a thorough review of the current state-of-the-art of elliptic and hyperelliptic curve public key cryptography.

There are five main research themes which arise in this area:

1. Determining the difficulty of the DLP for elliptic and hyperelliptic curves.
2. Constructing/choosing curves suitable for practical applications.
3. Efficient and secure implementation of the basic computational operations.
4. Special properties/features of these curves.
5. Cryptographic protocols.

The first theme is clearly of great importance if these systems are to be trusted in practice. One characteristic of public key cryptography (indeed, of complexity theory) is that there is no proof that the underlying computational problems such as the DLP are hard. The only tools available are to obtain reductions between computational problems and to try to find algorithms to solve problems. For the computational problems arising in public key cryptography, a given problem is deemed to be hard if it resists efforts by a large number of researchers over a long period of time to find efficient algorithms to solve it.

The handbook thoroughly presents the state-of-the-art in algorithms for the DLP (including the Pollard methods, 'transfer attacks' such as the MOV/Frey-Rück method, Weil descent and index calculus algorithms). Despite all this algorithmic research, the best method for solving the DLP on a randomly chosen elliptic curve over a finite field is the parallel Pollard method, which has exponential complexity. This gives confidence that elliptic curves are secure for cryptography. Surprisingly, the handbook does not discuss why there do not seem to be any effective index calculus algorithms for the elliptic curve DLP.

Once it is decided what is required for a given DLP to be considered secure, it is necessary to generate examples. This leads to the fascinating computational problem of counting points on curves over finite fields. The results on this problem are also of interest outside the cryptographic community, and the handbook provides a good presentation of the background theory (without proofs) and the various algorithms (both l-adic and p-adic).

The third theme is efficient and secure implementation. The handbook details numerous tech-

niques for obtaining fast implementation of the group law on elliptic and hyperelliptic curves. All aspects are covered (arithmetic in the ground field, the group law itself, and efficient methods for exponentiation). The chapters on this topic require the least mathematical background and can be read more-or-less independently of the rest of the book. Most of the methods are presented with explicit algorithms and this is the only part of the book where the promise that the reader can "implement the algorithms directly as they are written" is completely satisfied.

The security of cryptosystems is not just a problem of mathematics: there are also attacks (called side-channel attacks) on cryptosystems which exploit properties of the actual implementation and computational environment. The handbook gives a discussion of the ways these attacks can be mounted, together with some techniques to render such attacks less effective.

The fourth theme, special properties, includes a discussion of pairing-based cryptography. This relatively recent development has allowed the solution of long-standing open problems such as efficient identity-based encryption.

The fifth theme is essentially not covered in the book. There are many good references for modern cryptographic protocols based on the DLP, so it is reasonable that the focus of the handbook is on the other four themes. However, it is disappointing to see ElGamal signatures and encryption presented without any discussion of security goals or attack models.

This is not a textbook. It has very few examples and proofs, and does not contain exercises. Instead, the book is designed for people who are working in the area and want to learn more about a specific issue. The chapters are written to be relatively independent so that readers can focus on the part of interest for them. Such readers will be grateful for the excellent index and extensive bibliography.

To conclude, the handbook covers a wide range of topics and will be a valuable reference for researchers in curve-based cryptography.

Reviewed by *Steven D. Galbraith*