



## *Preface*

The study of elliptic curves by algebraists, algebraic geometers and number theorists dates back to the middle of the nineteenth century. There now exists an extensive literature that describes the beautiful and elegant properties of these marvelous objects. In 1984, Hendrik Lenstra described an ingenious algorithm for factoring integers that relies on properties of elliptic curves. This discovery prompted researchers to investigate other applications of elliptic curves in cryptography and computational number theory.

Public-key cryptography was conceived in 1976 by Whitfield Diffie and Martin Hellman. The first practical realization followed in 1977 when Ron Rivest, Adi Shamir and Len Adleman proposed their now well-known RSA cryptosystem, in which security is based on the intractability of the integer factorization problem. Elliptic curve cryptography (ECC) was discovered in 1985 by Neal Koblitz and Victor Miller. Elliptic curve cryptographic schemes are public-key mechanisms that provide the same functionality as RSA schemes. However, their security is based on the hardness of a different problem, namely the elliptic curve discrete logarithm problem (ECDLP). Currently the best algorithms known to solve the ECDLP have fully exponential running time, in contrast to the subexponential-time algorithms known for the integer factorization problem. This means that a desired security level can be attained with significantly smaller keys in elliptic curve systems than is possible with their RSA counterparts. For example, it is generally accepted that a 160-bit elliptic curve key provides the same level of security as a 1024-bit RSA key. The advantages that can be gained from smaller key sizes include speed and efficient use of power, bandwidth, and storage.

**Audience** This book is intended as a guide for security professionals, developers, and those interested in learning how elliptic curve cryptography can be deployed to secure applications. The presentation is targeted to a diverse audience, and generally assumes no more than an undergraduate degree in computer science, engineering, or mathematics. The book was not written for theoreticians as is evident from the lack of proofs for mathematical statements. However, the breadth of coverage and the extensive surveys of the literature at the end of each chapter should make it a useful resource for the researcher.

**Overview** The book has a strong focus on efficient methods for finite field arithmetic (Chapter 2) and elliptic curve arithmetic (Chapter 3). Next, Chapter 4 surveys the known attacks on the ECDLP, and describes the generation and validation of domain parameters and key pairs, and selected elliptic curve protocols for digital signature, public-key encryption and key establishment. We chose not to include the mathematical details of the attacks on the ECDLP, or descriptions of algorithms for counting the points on an elliptic curve, because the relevant mathematics is quite sophisticated. (Presenting these topics in a readable and concise form is a formidable challenge postponed for another day.) The choice of material in Chapters 2, 3 and 4 was heavily influenced by the contents of ECC standards that have been developed by accredited standards bodies, in particular the FIPS 186-2 standard for the Elliptic Curve Digital Signature Algorithm (ECDSA) developed by the U.S. government’s National Institute for Standards and Technology (NIST). Chapter 5 details selected aspects of efficient implementations in software and hardware, and also gives an introduction to side-channel attacks and their countermeasures. Although the coverage in Chapter 5 is admittedly narrow, we hope that the treatment provides a glimpse of engineering considerations faced by software developers and hardware designers.

**Acknowledgements** We gratefully acknowledge the following people who provided valuable comments and advice: Mike Brown, Eric Fung, John Goyo, Rick Hite, Rob Lambert, Laurie Law, James Muir, Arash Reyhani-Masoleh, Paul Schellenberg, Adrian Tang, Edlyn Teske, and Christof Zalka. A special thanks goes to Helen D’Souza, whose artwork graces several pages of this book. Thanks also to Cindy Hankerson and Sherry Shannon-Vanstone for suggestions on the general theme of “curves in nature” represented in the illustrations. Finally, we would like to thank our editors at Springer, Wayne Wheeler and Wayne Yuhasz, for their continued encouragement and support.

Updates, errata, and our contact information are available at our web site: <http://www.cacr.math.uwaterloo.ca/ecc/>. We would greatly appreciate that readers inform us of the inevitable errors and omissions they may find.

Darrel R. Hankerson, Alfred J. Menezes, Scott A. Vanstone  
Auburn & Waterloo  
July 2003



<http://www.springer.com/978-0-387-95273-4>

Guide to Elliptic Curve Cryptography

Hankerson, D.; Menezes, A.J.; Vanstone, S.

2004, XX, 312 p., Hardcover

ISBN: 978-0-387-95273-4