London Mathematical Society
Lecture Note Series 265

Elliptic Curves in Cryptography

Ian Blake, Gadiel Seroussi & Nigel Smart

London Mathematical Society

CAMBRIDGE
UNIVERSITY PRESS

LONDON MATHEMATICAL SOCIETY LECTURE NOTE SERIES

Managing Editor: Professor N.J. Hitchin, Mathematical Institute,
University of Oxford, 24–29 St Giles, Oxford OX1 3LB, United Kingdom

The titles below are available from booksellers, or, in case of difficulty, from Cambridge University Press.

46 p-adic Analysis: a short course on recent work, N. KOBLITZ
59 Applicable differential geometry, M. CRAMPIN & F.A.E. PIRANI
66 Several complex variables and complex manifolds II, M.J. FIELD
86 Topological topics, I.M. JAMES (ed)
87 Surveys in set theory, A.R.D. MATHIAS (ed)
88 FPF ring theory, C. FAITH & S. PAGE
90 Polytopes and symmetry, S.A. ROBERTSON
92 Representations of rings over skew fields, A.H. SCHOFIELD
93 Aspects of topology, I.M. JAMES & E.H. KRONHEIMER (eds)
96 Diophantine equations over function fields, R.C. MASON
97 Varieties of constructive mathematics, D.S. BRIDGES & F. RICHMAN
99 Methods of differential geometry in algebraic topology, M. KAROUBI & C. LERUSTE
100 Stopping time techniques for analysts and probabilists, L. EGGHE
104 Elliptic structures on 3-manifolds, C.B. THOMAS
105 A local spectral theory for closed operators, I. ERDELYI & WANG SHENGWANG
107 Compactification of Siegel moduli schemes, C.-L. CHAI
109 Diophantine analysis, J. LOXTON & A. VAN DER POORTEN (eds)
113 Lectures on the asymptotic theory of ideals, D. REES
114 Lectures on Bochner-Riesz means, K.M. DAVIS & Y.-C. CHANG
116 Representations of algebras, P.J. WEBB (ed)
119 Triangulated categories in the representation theory of finite-dimensional algebras, D. HAPPEL
121 Proceedings of *Groups - St Andrews 1985*, E. ROBERTSON & C. CAMPBELL (eds)
128 Descriptive set theory and the structure of sets of uniqueness, A.S. KECHRIS & A. LOUVEAU
130 Model theory and modules, M. PREST
131 Algebraic, extremal & metric combinatorics, M.-M. DEZA, P. FRANKL & I.G. ROSENBERG (eds)
132 Whitehead groups of finite groups, ROBERT OLIVER
138 Analysis at Urbana, II, E. BERKSON, T. PECK, & J. UHL (eds)
139 Advances in homotopy theory, S. SALAMON, B. STEER & W. SUTHERLAND (eds)
140 Geometric aspects of Banach spaces, E.M. PEINADOR & A. RODES (eds)
141 Surveys in combinatorics 1989, J. SIEMONS (ed)
144 Introduction to uniform spaces, I.M. JAMES
146 Cohen-Macaulay modules over Cohen-Macaulay rings, Y. YOSHINO
148 Helices and vector bundles, A.N. RUDAKOV *et al*
149 Solitons, nonlinear evolution equations and inverse scattering, M. ABLOWITZ & P. CLARKSON
150 Geometry of low-dimensional manifolds 1, S. DONALDSON & C.B. THOMAS (eds)
151 Geometry of low-dimensional manifolds 2, S. DONALDSON & C.B. THOMAS (eds)
152 Oligomorphic permutation groups, P. CAMERON
153 L-functions and arithmetic, J. COATES & M.J. TAYLOR (eds)
155 Classification theories of polarized varieties, TAKAO FUJITA
156 Twistors in mathematics and physics, T.N. BAILEY & R.J. BASTON (eds)
158 Geometry of Banach spaces, P.F.X. MÜLLER & W. SCHACHERMAYER (eds)
159 Groups St Andrews 1989 volume 1, C.M. CAMPBELL & E.F. ROBERTSON (eds)
160 Groups St Andrews 1989 volume 2, C.M. CAMPBELL & E.F. ROBERTSON (eds)
161 Lectures on block theory, BURKHARD KÜLSHAMMER
162 Harmonic analysis and representation theory, A. FIGA-TALAMANCA & C. NEBBIA
163 Topics in varieties of group representations, S.M. VOVSI
164 Quasi-symmetric designs, M.S. SHRIKANDE & S.S. SANE
166 Surveys in combinatorics, 1991, A.D. KEEDWELL (ed)
168 Representations of algebras, H. TACHIKAWA & S. BRENNER (eds)
169 Boolean function complexity, M.S. PATERSON (ed)
170 Manifolds with singularities and the Adams-Novikov spectral sequence, B. BOTVINNIK
171 Squares, A.R. RAJWADE
172 Algebraic varieties, GEORGE R. KEMPF
173 Discrete groups and geometry, W.J. HARVEY & C. MACLACHLAN (eds)
174 Lectures on mechanics, J.E. MARSDEN
175 Adams memorial symposium on algebraic topology 1, N. RAY & G. WALKER (eds)
176 Adams memorial symposium on algebraic topology 2, N. RAY & G. WALKER (eds)
177 Applications of categories in computer science, M. FOURMAN, P. JOHNSTONE & A. PITTS (eds)
178 Lower K- and L-theory, A. RANICKI
179 Complex projective geometry, G. ELLINGSRUD *et al*
180 Lectures on ergodic theory and Pesin theory on compact manifolds, M. POLLICOTT
181 Geometric group theory I, G.A. NIBLO & M.A. ROLLER (eds)
182 Geometric group theory II, G.A. NIBLO & M.A. ROLLER (eds)
183 Shintani zeta functions, A. YUKIE
184 Arithmetical functions, W. SCHWARZ & J. SPILKER
185 Representations of solvable groups, O. MANZ & T.R. WOLF
186 Complexity: knots, colourings and counting, D.J.A. WELSH
187 Surveys in combinatorics, 1993, K. WALKER (ed)
188 Local analysis for the odd order theorem, H. BENDER & G. GLAUBERMAN
189 Locally presentable and accessible categories, J. ADAMEK & J. ROSICKY
190 Polynomial invariants of finite groups, D.J. BENSON

191 Finite geometry and combinatorics, F. DE CLERCK *et al*
192 Symplectic geometry, D. SALAMON (ed)
194 Independent random variables and rearrangement invariant spaces, M. BRAVERMAN
195 Arithmetic of blowup algebras, WOLMER VASCONCELOS
196 Microlocal analysis for differential operators, A. GRIGIS & J. SJÖSTRAND
197 Two-dimensional homotopy and combinatorial group theory, C. HOG-ANGELONI *et al*
198 The algebraic characterization of geometric 4-manifolds, J.A. HILLMAN
199 Invariant potential theory in the unit ball of $\mathbf{C}^n$, MANFRED STOLL
200 The Grothendieck theory of dessins d'enfant, L. SCHNEPS (ed)
201 Singularities, JEAN-PAUL BRASSELET (ed)
202 The technique of pseudodifferential operators, H.O. CORDES
203 Hochschild cohomology of von Neumann algebras, A. SINCLAIR & R. SMITH
204 Combinatorial and geometric group theory, A.J. DUNCAN, N.D. GILBERT & J. HOWIE (eds)
205 Ergodic theory and its connections with harmonic analysis, K. PETERSEN & I. SALAMA (eds)
207 Groups of Lie type and their geometries, W.M. KANTOR & L. DI MARTINO (eds)
208 Vector bundles in algebraic geometry, N.J. HITCHIN, P. NEWSTEAD & W.M. OXBURY (eds)
209 Arithmetic of diagonal hypersurfaces over finite fields, F.Q. GOUVÊA & N. YUI
210 Hilbert C*-modules, E.C. LANCE
211 Groups 93 Galway / St Andrews I, C.M. CAMPBELL *et al* (eds)
212 Groups 93 Galway / St Andrews II, C.M. CAMPBELL *et al* (eds)
214 Generalised Euler-Jacobi inversion formula and asymptotics beyond all orders, V. KOWALENKO *et al*
215 Number theory 1992–93, S. DAVID (ed)
216 Stochastic partial differential equations, A. ETHERIDGE (ed)
217 Quadratic forms with applications to algebraic geometry and topology, A. PFISTER
218 Surveys in combinatorics, 1995, PETER ROWLINSON (ed)
220 Algebraic set theory, A. JOYAL & I. MOERDIJK
221 Harmonic approximation, S.J. GARDINER
222 Advances in linear logic, J.-Y. GIRARD, Y. LAFONT & L. REGNIER (eds)
223 Analytic semigroups and semilinear initial boundary value problems, KAZUAKI TAIRA
224 Computability, enumerability, unsolvability, S.B. COOPER, T.A. SLAMAN & S.S. WAINER (eds)
225 A mathematical introduction to string theory, S. ALBEVERIO, J. JOST, S. PAYCHA, S. SCARLATTI
226 Novikov conjectures, index theorems and rigidity I, S. FERRY, A. RANICKI & J. ROSENBERG (eds)
227 Novikov conjectures, index theorems and rigidity II, S. FERRY, A. RANICKI & J. ROSENBERG (eds)
228 Ergodic theory of $\mathbf{Z}^d$ actions, M. POLLICOTT & K. SCHMIDT (eds)
229 Ergodicity for infinite dimensional systems, G. DA PRATO & J. ZABCZYK
230 Prolegomena to a middlebrow arithmetic of curves of genus 2, J.W.S. CASSELS & E.V. FLYNN
231 Semigroup theory and its applications, K.H. HOFMANN & M.W. MISLOVE (eds)
232 The descriptive set theory of Polish group actions, H. BECKER & A.S. KECHRIS
233 Finite fields and applications, S. COHEN & H. NIEDERREITER (eds)
234 Introduction to subfactors, V. JONES & V.S. SUNDER
235 Number theory 1993–94, S. DAVID (ed)
236 The James forest, H. FETTER & B. GAMBOA DE BUEN
237 Sieve methods, exponential sums, and their applications in number theory, G.R.H. GREAVES *et al*
238 Representation theory and algebraic geometry, A. MARTSINKOVSKY & G. TODOROV (eds)
239 Clifford algebras and spinors, P. LOUNESTO
240 Stable groups, FRANK O. WAGNER
241 Surveys in combinatorics, 1997, R.A. BAILEY (ed)
242 Geometric Galois actions I, L. SCHNEPS & P. LOCHAK (eds)
243 Geometric Galois actions II, L. SCHNEPS & P. LOCHAK (eds)
244 Model theory of groups and automorphism groups, D. EVANS (ed)
245 Geometry, combinatorial designs and related structures, J.W.P. HIRSCHFELD *et al*
246 p-Automorphisms of finite p-groups, E.I. KHUKHRO
247 Analytic number theory, Y. MOTOHASHI (ed)
248 Tame topology and o-minimal structures, LOU VAN DEN DRIES
249 The atlas of finite groups: ten years on, ROBERT CURTIS & ROBERT WILSON (eds)
250 Characters and blocks of finite groups, G. NAVARRO
251 Gröbner bases and applications, B. BUCHBERGER & F. WINKLER (eds)
252 Geometry and cohomology in group theory, P. KROPHOLLER, G. NIBLO, R. STÖHR (eds)
253 The q-Schur algebra, S. DONKIN
254 Galois representations in arithmetic algebraic geometry, A.J. SCHOLL & R.L. TAYLOR (eds)
255 Symmetries and integrability of difference equations, P.A. CLARKSON & F.W. NIJHOFF (eds)
256 Aspects of Galois theory, HELMUT VÖLKLEIN *et al*
257 An introduction to noncommutative differential geometry and its physical applications 2ed, J. MADORE
258 Sets and proofs, S.B. COOPER & J. TRUSS (eds)
259 Models and computability, S.B. COOPER & J. TRUSS (eds)
260 Groups St Andrews 1997 in Bath, I, C.M. CAMPBELL *et al*
261 Groups St Andrews 1997 in Bath, II, C.M. CAMPBELL *et al*
263 Singularity theory, BILL BRUCE & DAVID MOND (eds)
264 New trends in algebraic geometry, K. HULEK, F. CATANESE, C. PETERS & M. REID (eds)
265 Elliptic curves in cryptography, I. BLAKE, G. SEROUSSI & N. SMART
267 Surveys in combinatorics, 1999, J.D. LAMB & D.A. PREECE (eds)
268 Spectral asymptotics in the semi-classical limit, M. DIMASSI & J. SJÖSTRAND
269 Ergodic theory and topological dynamics, M. B. BEKKA & M. MAYER
270 Analysis on Lie Groups, N. T. VAROPOULOS & S. MUSTAPHA
271 Singular perturbations of differential operators, S. ALBERVERIO & P. KURASOV
272 Character theory for the odd order function, T. PETERFALVI
273 Spectral theory and geometry, E. B. DAVIES & Y. SAFAROV (eds)
274 The Mandlebrot set: theme and variation, TAN LEI (ed)

London Mathematical Society Lecture Note Series. 265

Elliptic Curves in Cryptography

I. F. Blake
Hewlett-Packard Laboratories, Palo Alto

G. Seroussi
Hewlett-Packard Laboratories, Palo Alto

N. P. Smart
Hewlett-Packard Laboratories, Bristol

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo

Cambridge University Press
The Edinburgh Building, Cambridge CB2 2RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521653749

First published 1999
Reprinted 2000 (three times), 2001, 2002, 2004

A catalogue record for this publication is available from the British Library

Library of Congress Cataloguing in Publication data
Blake Ian F.
Elliptic Curves in Cryptography / I.F. Blake, G. Seroussi, N.P. Smart
p. cm. – (London Mathematical Society Lecture Note Series; 265)
Includes bibliographical references and index.
ISBN 0 521 65374 6 (pbk.)
1. Computer security. 2. Cryptography. 3. Curves, Elliptic–Data processing.
I. Seroussi, G. (Gadiel), 1955 - II. Smart, Nigel P. (Nigel Paul), 1967 -.
III. Title. IV. Series.
QA76.9.A25.B27 1999
005.8′.2–dc21 99–19696 CIP

ISBN-13 978-0-521-65374-9 paperback
ISBN-10 0-521-65374-6 paperback

Transferred to digital printing 2006

To

Elizabeth, Lauren and Michael,

Lidia, Ariel and Dahlia,

Maggie, Ellie and Oliver.

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, [illegible]

[illegible]
The Edinburgh Building, Cambridge [illegible]

Published in the United States of America by Cambridge University Press, [illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

Contents

Preface

Much attention has recently been focused on the use of elliptic curves in public key cryptography, first proposed in the work of Koblitz [**62**] and Miller [**103**]. The motivation for this is the fact that there is no known sub-exponential algorithm to solve the discrete logarithm problem on a general elliptic curve. In addition, as will be discussed in Chapter I, the standard protocols in cryptography which make use of the discrete logarithm problem in finite fields, such as Diffie–Hellman key exchange, ElGamal encryption and digital signature, Massey–Omura encryption and the Digital Signature Algorithm (DSA), all have analogues in the elliptic curve case.

Cryptosystems based on elliptic curves are an exciting technology because for the same level of security as systems such as RSA [**134**], using the current knowledge of algorithms in the two cases, they offer the benefits of smaller key sizes and hence of smaller memory and processor requirements. This makes them ideal for use in smart cards and other environments where resources such as storage, time, or power are at a premium.

Some researchers have expressed concern that the basic problem on which elliptic curve systems are based has not been looked at in as much detail as, say, the factoring problem, on which systems such as RSA are based. However, all such systems based on the perceived difficulty of a mathematical problem live in fear of a dramatic breakthrough to some extent, and this issue is not addressed further in this work.

This book discusses various issues surrounding the use of elliptic curves in cryptography, including:

- The basic arithmetic operations, not only on the curves but also over finite fields.
- Ways of efficiently implementing the basic operation of adding a point to itself a large number of times (point multiplication).
- Known attacks on systems based on elliptic curves.
- A large section devoted to computing the number of rational points on elliptic curves over finite fields.
- A discussion on the generalization of elliptic curve systems to hyperelliptic systems.

The book is written for a wide audience ranging from the mathematician who knows about elliptic curves (or has been acquainted with them) and who wants a quick survey of the main results pertaining to cryptography, to an implementer who requires some knowledge of elliptic curve mathematics for use in a practical cryptosystem. Clearly, aiming for such diverse audiences is hard, and not all parts of the book will be of the same level of interest to all readers. However, most of the important points such as implementation issues, security issues and point counting issues can be acquired with only a moderate understanding of the underlying mathematics.

We try and give a flavour of the mathematics involved for those who are interested. We decided however not to include most proofs since that not only would dramatically increase the size of the book but also would not serve its main purpose. It is hoped that the numerous references cited and the extensive bibliography provided will direct the interested reader to appropriate sources for all the missing details. In fact, much of the necessary mathematical background can be found in the books by Silverman, [**147**] and [**148**].

Some of the topics covered in the book by Menezes [**97**] are expanded upon. In particular the improvements made to the algorithm of Schoof [**141**] for determining the number of rational points on an elliptic curve are explained, and the method of finding curves using the theory of complex multiplication is discussed. This latter method has other applications when one uses elliptic curves to construct proofs of primality. We also give the first treatment in book form of such methods as point compression (including x-coordinate compression), the attack on anomalous curves and the generalization of the MOV attack to curves such as those with the trace of Frobenius equal to two. Two chapters are devoted to implementation issues. One covers finite fields while the second covers the various techniques available for point multiplication. In addition, the chapter on Schoof's algorithm and its improvements provides algorithmic summaries intended to facilitate the implementation of these point counting techniques.

We would like to thank D. Boneh, S. Galbraith, A.J. Menezes, K. Paterson, M. Rubinstein, E. Scheafer, R. Schoof and S. Zaba who have looked over various portions of the manuscript and given us their comments. All of the remaining mistakes and problems are our own and we apologize in advance for any you may find. The authors would also like to thank Dan Boneh, Johannes Buchmann, Markus Maurer and Volker Müller for many discussions on elliptic curves, their assistance with the implementation of point counting algorithms and the prompt answering of many queries. Thanks are due also to John Cremona for his LaTeX algorithm template which we modified to produce the algorithms in this book.

Finally thanks are due to Hewlett–Packard Company and our colleagues and managers there for their support, assistance and encouragement during the writing of this book.

Abbreviations and Standard Notation

Abbreviations

The following abbreviations of standard phrases are used throughout the book:

AES	Advanced Encryption Standard
BSGS	baby step/giant step method
CM	Complex multiplication
CRT	Chinese Remainder Theorem
DES	Data Encryption Standard
DHP	Diffie–Hellman problem
DLP	Discrete logarithm problem
DSA	Digital Signature Algorithm
ECDLP	Elliptic curve discrete logarithm problem
ECM	Elliptic curve factoring method
ECPP	Elliptic curve primality proving method
GCD	Greatest common divisor
LCM	Least common multiple
MOV	Menezes–Okamoto–Vanstone attack
NAF	Non-adjacent form
NFS	Number field sieve
ONB	Optimal normal basis
RNS	Residue number system
RSA	Rivest–Shamir–Adleman encryption scheme
SD	Signed digit
SEA	Schoof–Elkies–Atkin algorithm

Standard notation

The following standard notation is used throughout the book, often without further definition. Other notation is defined locally near its first use.

$K^{\bullet}$, K^{+}, $\overline{K}$	for a field K, the multiplicative group, additive group, and algebraic closure, respectively
$\mathrm{Gal}(K/F)$	Galois group of K over F
$\mathrm{Aut}(G)$	Automorphism group of G
$\mathrm{char}(K)$	characteristic of K
$\gcd(f,g), \mathrm{lcm}(f,g)$	GCD, LCM of f and g
$\deg(f)$	degree of a polynomial f
$\mathrm{ord}(g)$	order of an element g in a group
$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$	integers, rationals, reals and complex numbers
$\mathbb{Z}_{>k}$	integers greater than k; similarly for $\geq, <, \leq$
$\mathbb{Z}/n\mathbb{Z}$	integers modulo n
$\mathbb{Z}_p$, $\mathbb{Q}_p$	p-adic integers and numbers, respectively
$\mathbb{F}_q$	finite field with q elements
$\mathrm{Tr}_{q\mid p}(x)$	trace of $x \in \mathbb{F}_q$ over $\mathbb{F}_p$, $q = p^n$
$\langle g \rangle$	cyclic group generated by g
$\#S$	cardinality of the set S
E	elliptic curve (equation)
$E(K)$	group of K-rational points on E
$[m]P$	multiplication-by-m map applied to the point P
$E[m]$	group of m-torsion points on the elliptic curve E
$\mathrm{End}(E)$	Endormorphism ring of E
$\mathcal{O}$	point at infinity (on an elliptic curve)
$\wp$	Weierstrass 'pay' function
φ	Frobenius map
ϕ_{Eul}	Euler totient function
$GL_2(R)$	general linear group over the ring R: 2×2 matrices over R with determinant a unit in R
$PGL_2(K)$	projective general linear group over the field K, with scalar multiples identified
$SL_2(\mathbb{Z})$	special linear group of 2×2 matrices over $\mathbb{Z}$ with determinant one
$\left(\frac{\cdot}{p}\right)$	Legendre symbol
$\mathrm{Re}(z), \mathrm{Im}(z)$	real and imaginary parts of $z \in \mathbb{C}$, respectively
$\mathcal{H}$	Poincaré half-plane $\mathrm{Im}(z) > 0$
$O(f(n))$	function $g(n)$ such that $\lvert g(n)\rvert \leq c\lvert f(n)\rvert$ for some constant $c > 0$ and all sufficiently large n
$o(f(n))$	function $g(n)$ such that $\lim_{n\to\infty}(g(n)/f(n)) = 0$
$\log_b x$	logarithm to base b of x; natural log if b omitted

Often we will need to present binary, hexadecimal or decimal numbers which are too long to fit on one line. We shall use the standard convention of breaking the number into multiple lines, with a backslash at the end of a line indicating that the number is continued in the next line. For example

$$
\begin{aligned}
p &= 2^{230} + 67 \\
&= 1725436586697640946858688965569256363112777243042 5\backslash \\
& 96638790631055949891.
\end{aligned}
$$

CHAPTER I

Introduction

We introduce the three main characters in public key cryptography. As in many books on the subject, it is assumed that Alice and Bob wish to perform some form of communication whilst Eve is an eavesdropper who wishes to spy on (or tamper with) the communications between Alice and Bob. Of course there is no assumption that Alice and Bob (or Eve) are actually human. They may (and probably will) be computers on some network such as the Internet.

Modern cryptography, as applied in the commercial world, is concerned with a number of problems. The most important of these are:

1. **Confidentiality:** A message sent from Alice to Bob cannot be read by anyone else.
2. **Authenticity:** Bob knows that only Alice could have sent the message he has just received.
3. **Integrity:** Bob knows that the message from Alice has not been tampered with in transit.
4. **Non-repudiation:** It is impossible for Alice to turn around later and say she did not send the message.

To see why all four properties are important consider the following scenario. Alice wishes to buy some item over the Internet from Bob. She sends her instruction to Bob which contains her credit card number and payment details. She requires that this communication be confidential, since she wants other people to know neither her credit card details nor what she is buying. Bob needs to know that the message is authentic in that it came from Alice and not some impostor. Both Alice and Bob need to be certain that the message's integrity is preserved, for example the amount cannot be altered by some third party whilst it is in transit. Finally Bob requires the non-repudiation property, meaning that Alice should not be able to say she did not send the instruction.

In other words, we require transactions to take place between two mutually distrusting parties over a public network. This is different from conventional private networks, such as those used in banking, where there are key hierarchies and tamper proof hardware which can store symmetric keys.

It is common in the literature to introduce public key techniques in the area of confidentiality protection. Public key techniques are, however, usually infeasible to use directly in this context, being orders of magnitude slower than symmetric techniques. Their use in confidentiality is often limited to the transmission of symmetric cipher keys. On the other hand *digital signatures*, which give the user the authentication, integrity and non-repudiation properties required in electronic commerce, seem to require the use of public key cryptography.

A computer which is processing payments for a bank or a business may need to verify or create thousands of digital signatures every second. This has led to the demand for public key digital signature schemes which are very efficient. Whilst many schemes are based on the discrete logarithm problem in a finite abelian group, there is some debate as to what type of groups to use. One choice is the group of points on an elliptic curve over a finite field. This choice is becoming increasingly popular, precisely because of efficiency considerations. In this book, we attempt to summarize the latest knowledge available on both theoretical and practical issues related to elliptic curve cryptosystems.

I.1. Cryptography Based on Groups

In this section, some of the standard protocols of public key cryptography are surveyed. A more detailed discussion of all of these protocols and other related areas of cryptography can be found in the books by Menezes, van Oorschot and Vanstone **[99]** and Schneier **[139]**, although neither of these books covers the use of elliptic curves in cryptography. The protocols discussed here only require the use of a finite abelian group G, of order $\#G$, which is assumed to be cyclic. The group of interest in this work is the *additive* group of points on an elliptic curve. However, it is convenient for the remainder of this chapter to assume the group is *multiplicative*, with generator g, and that the order, $\#G$, is a prime. If this is not the case, we can always take a prime order subgroup of G as our group, with no loss of security. The additive vs. multiplicative issue is, of course, just one of notation. We will revert to additive notation later on, when the discussion focuses on the elliptic curve groups.

The group G should be presented in such a way as to make multiplication and exponentiation easy, whilst computing discrete logarithms is hard. The reason for this will become clearer below. It should also be possible to generate random elements from the group with an almost uniform distribution.

By the *discrete logarithm problem* (DLP) we mean the problem of determining the least positive integer, x, if it exists, which satisfies the equation

$$h = g^x$$

for two, given, elements h and g in the group G. Note that a common feature of all of the following schemes is that if there is a fast way to solve the DLP in G, then they are all insecure for the group G. Since we have assumed that G is of prime order such a discrete logarithm always exists.

I.1.1. Diffie–Hellman key exchange. Alice and Bob wish to agree on a secret random element in the group, which could be of use as a key for a