London Mathematical Society
Lecture Note Series 317

Advances in Elliptic Curve Cryptography

Edited by
Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart

London Mathematical Society

CAMBRIDGE
UNIVERSITY PRESS

London Mathematical Society Lecture Note Series. 317

Advances in Elliptic Curve Cryptography

Edited by

Ian F. Blake
University of Toronto

Gadiel Seroussi
Hewlett-Packard Laboratories

Nigel P. Smart
University of Bristol

CAMBRIDGE
UNIVERSITY PRESS

PUBLISHED BY THE PRESS SYNDICATE OF THE UNIVERSITY OF CAMBRIDGE
The Pitt Building, Trumpington Street, Cambridge, United Kingdom

CAMBRIDGE UNIVERSITY PRESS
The Edinburgh Building, Cambridge CB2 2RU, UK
40 West 20th Street, New York, NY 10011-4211, USA
477 Williamstown Road, Port Melbourne, VIC 3207, Australia
Ruiz de Alarcón 13, 28014 Madrid, Spain
Dock House, The Waterfront, Cape Town 8001, South Africa

http://www.cambridge.org

First published 2005

Printed in the United Kingdom at the University Press, Cambridge

Typeface Times 10/12 pt. *System* LaTeX 2_ε [AU]

A catalog record for this book is available from the British Library.

Library of Congress Cataloging in Publication Data

Advances in elliptic curve cryptography / edited by Ian F. Blake, Gadiel Seroussi, Nigel P. Smart.
p. cm. – (London Mathematical Society lecture note series ; 317)
Includes bibliographical references and index.
ISBN 0-521-60415-X (alk. paper)
1. Computer security. 2. Public key cryptography. I. Blake, Ian F.
II. Seroussi, G. (Gadiel), 1955– III. Smart, Nigel P. (Nigel Paul), 1967– IV. Series.
QA76.9.A25A375 2004
005.8–dc22 2004054519

ISBN 0 521 60415 X paperback

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 from Cambridge University Press at www.cambridge.org

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
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
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 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. GOUVÉA & 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 *et al*
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 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)
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*
262 Analysis and logic, C.W. HENSON, J. IOVINO, A.S. KECHRIS & E. ODELL
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. ALBEVERIO & P. KURASOV
272 Character theory for the odd order theorem, T. PETERFALVI
273 Spectral theory and geometry, E.B. DAVIES & Y. SAFAROV (eds)
274 The Mandlebrot set, theme and variations, TAN LEI (ed)
275 Descriptive set theory and dynamical systems, M. FOREMAN *et al*
276 Singularities of plane curves, E. CASAS-ALVERO
277 Computational and geometric aspects of modern algebra, M.D. ATKINSON *et al*
278 Global attractors in abstract parabolic problems, J.W. CHOLEWA & T. DLOTKO
279 Topics in symbolic dynamics and applications, F. BLANCHARD, A. MAASS & A. NOGUEIRA (eds)
280 Characters and automorphism groups of compact Riemann surfaces, THOMAS BREUER
281 Explicit birational geometry of 3-folds, ALESSIO CORTI & MILES REID (eds)
282 Auslander-Buchweitz approximations of equivariant modules, M. HASHIMOTO
283 Nonlinear elasticity, Y. FU & R.W. OGDEN (eds)
284 Foundations of computational mathematics, R. DEVORE, A. ISERLES & E. SÜLI (eds)
285 Rational points on curves over finite fields, H. NIEDERREITER & C. XING
286 Clifford algebras and spinors 2ed, P. LOUNESTO
287 Topics on Riemann surfaces and Fuchsian groups, E. BUJALANCE, A.F. COSTA & E. MARTÌNEZ (eds)
288 Surveys in combinatorics, 2001, J. HIRSCHFELD (ed)
289 Aspects of Sobolev-type inequalities, L. SALOFF-COSTE
290 Quantum groups and Lie theory, A. PRESSLEY (ed)
291 Tits buildings and the model theory of groups, K. TENT (ed)
292 A quantum groups primer, S. MAJID
293 Second order partial differential equations in Hilbert spaces, G. DA PRATO & J. ZABCZYK
294 Introduction to the theory of operator spaces, G. PISIER
295 Geometry and integrability, LIONEL MASON & YAVUZ NUTKU (eds)
296 Lectures on invariant theory, IGOR DOLGACHEV
297 The homotopy category of simply connected 4-manifolds, H.-J. BAUES
299 Kleinian groups and hyperbolic 3-manifolds, Y. KOMORI, V. MARKOVIC, & C. SERIES (eds)
300 Introduction to Möbius differential geometry, UDO HERTRICH-JEROMIN
301 Stable modules and the D(2)-problem, F.E.A. JOHNSON
302 Discrete and continuous nonlinear Schrödinger systems, M.J. ABLOWITZ, B. PRINARI, & A.D. TRUBATCH
303 Number theory and algebraic geometry, MILES REID & ALEXEI SKOROBOGATOV (eds)
304 Groups St Andrews 2001 in Oxford Vol. 1, COLIN CAMPBELL, EDMUND ROBERTSON & GEOFF SMITH (eds)
305 Groups St Andrews 2001 in Oxford Vol. 2, C.M. CAMPBELL, E.F. ROBERTSON & G.C. SMITH (eds)
307 Surveys in combinatorics 2003, C.D. WENSLEY (ed)
309 Corings and comodules, TOMASZ BRZEZINSKI & ROBERT WISBAUER
310 Topics in dynamics and ergodic theory, SERGEY BEZUGLYI & SERGIY KOLYADA (eds)
312 Foundations of computational mathematics, Minneapolis 2002, FELIPE CUCKER *et al* (eds)

Preface

It is now more than five years since we started working on the book *Elliptic Curves in Cryptography* and more than four years since it was published. We therefore thought it was time to update the book since a lot has happened in the intervening years. However, it soon became apparent that a simple update would not be sufficient since so much has been developed in this area. We therefore decided to develop a second volume by inviting leading experts to discuss issues which have arisen.

Highlights in the intervening years which we cover in this volume include:

Provable Security. There has been considerable work in the last few years on proving various practical encryption and signature schemes secure. In this new volume we will examine the proofs for the ECDSA signature scheme and the ECIES encryption scheme.

Side-Channel Analysis. The use of power and timing analysis against cryptographic tokens, such as smart cards, is particularly relevant to elliptic curves since elliptic curves are meant to be particularly suited to the constrained environment of smart cards. We shall describe what side-channel analysis is and how one can use properties of elliptic curves to defend against it.

Point Counting. In 1999 the only method for computing the group order of an elliptic curve was the Schoof-Elkies-Atkin algorithm. However, for curves over fields of small characteristic we now have the far more efficient Satoh method, which in characteristic two can be further simplified into the AGM-based method of Mestre. We shall describe these improvements in this book.

Weil Descent. Following a talk by Frey in 1999, there has been considerable work on showing how Weil descent can be used to break certain elliptic curve systems defined over "composite fields" of characteristic two.

Pairing-Based Cryptography. The use of the Weil and Tate pairings was until recently confined to breaking elliptic curve protocols. But since the advent of Joux's tripartite Diffie–Hellman protocol there has been an interest in using pairings on elliptic curves to construct protocols which cannot be implemented in another way. The most spectacular example of this is the identity-based encryption algorithm of Boneh and Franklin. We describe not only these protocols but how these pairings can be efficiently implemented.

As one can see once again, the breadth of subjects we cover will be of interest to a wide audience, including mathematicians, computer scientists and engineers. Once again we also do not try to make the entire book relevant to all audiences at once but trust that, whatever your interests, you can find something of relevance within these pages.

The overall style and notation of the first book is retained, and we have tried to ensure that our experts have coordinated what they write to ensure a coherent account across chapters.

Ian Blake
Gadiel Seroussi
Nigel Smart

Abbreviations and Standard Notation

Abbreviations

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

AES	Advanced Encryption Standard
AGM	Arithmetic Geometric Mean
BDH	Bilinear Diffie–Hellman problem
BSGS	Baby Step/Giant Step method
CA	Certification Authority
CCA	Chosen Ciphertext Attack
CDH	Computational Diffie–Hellman problem
CM	Complex Multiplication
CPA	Chosen Plaintext Attack
DBDH	Decision Bilinear Diffie–Hellman problem
DDH	Decision Diffie–Hellman problem
DEM	Data Encapsulation Mechanism
DHAES	Diffie–Hellman Augmented Encryption Scheme
DHIES	Diffie–Hellman Integrated Encryption Scheme
DHP	Diffie–Hellman Problem
DLP	Discrete Logarithm Problem
DPA	Differential Power Analysis
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECDDH	Elliptic Curve Decision Diffie–Hellman problem
ECDH	Elliptic Curve Diffie–Hellman protocol
ECDHP	Elliptic Curve Diffie–Hellman Problem
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Scheme
ECMQV	Elliptic Curve Menezes–Qu–Vanstone protocol
GHS	Gaudry–Hess–Smart attack
GRH	Generalized Riemann Hypothesis
HCDLP	Hyperelliptic Curve Discrete Logarithm Problem
HIBE	Hierarchical Identity-Based Encryption

IBE	Identity-Based Encryption
IBSE	Identity-Based Sign and Encryption
ILA	Information Leakage Analysis
KDF	Key Derivation Function
KDS	Key Distribution System
KEM	Key Encapsulation Mechanism
MAC	Message Authentication Code
MOV	Menezes–Okamoto–Vanstone attack
NIKDS	Non-Interactive Key Distribution System
PKI	Public Key Infrastructure
RSA	Rivest–Shamir–Adleman encryption scheme
SCA	Side Channel Analysis
SEA	Schoof–Elkies–Atkin algorithm
SHA	Secure Hash Algorithm
SPA	Simple Power Analysis
SSCA	Simple Side-Channel Attack
TA	Trusted Authority

Standard notation

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

Basic Notation

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$	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
$\#S$	cardinality of the set S
$\gcd(f,g), \operatorname{lcm}(f,g)$	GCD, LCM of f and g
$\deg(f)$	degree of a polynomial f
ϕ_{Eul}	Euler totient function
$\left(\frac{\cdot}{p}\right)$	Legendre symbol
$\log_b x$	logarithm to base b of x; natural log if b omitted
$O(f(n))$	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 $\lim_{n\to\infty}(g(n)/f(n)) = 0$
$\mathbb{P}^n$	projective space

Group/Field Theoretic Notation

$\mathbb{F}_q$	finite field with q elements
K^*, K^+, $\overline{K}$	for a field K, the multiplicative group, additive group and algebraic closure, respectively
$\mathrm{char}(K)$	characteristic of K
$\langle g\rangle$	cyclic group generated by g
$\mathrm{ord}(g)$	order of an element g in a group
$\mathrm{Aut}(G)$	automorphism group of G
$\mathbb{Z}_p$, $\mathbb{Q}_p$	p-adic integers and numbers, respectively
$\mathrm{Tr}_{q\mid p}(x)$	trace of $x \in \mathbb{F}_q$ over $\mathbb{F}_p$, $q = p^n$
$\boldsymbol{\mu}_n$	nth roots of unity
$N_{L/K}$	norm map

Function Field Notation

$\deg(D)$	degree of a divisor
(f)	divisor of a function
$f(D)$	function evaluated at a divisor
$\sim$	equivalence of divisors
$\mathrm{ord}_P(f)$	multiplicity of a function at a point

Galois Theory Notation

$\mathrm{Gal}(K/F)$	Galois group of K over F
$\sigma(P)$	Galois conjugation of point P by σ
f^{σ}	Galois conjugation of coefficients of function f by σ

Curve Theoretic Notation

E	elliptic curve (equation)
(x_P, y_P)	coordinates of the point P
$x(P)$	the x-cordinate of the point P
$y(P)$	the y-cordinate of the point P
$E(K)$	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
$\langle P, Q\rangle_n$	Tate pairing of P and Q
$e_n(P, Q)$	Weil pairing of P and Q
$e(P, Q)$	pairing of P and Q
$\hat{e}(P, Q)$	modified pairing of P and Q
$\mathrm{Tr}(P)$	trace map
$\mathcal{T}$	trace zero subgroup

Authors

We would like to acknowledge the following people who contributed chapters to this book.

Dan Brown,
Certicom Corp.,
Mississauga,
Canada.

Alex Dent,
Mathematics Department,
Royal Holloway,
University of London,
United Kingdom.

Steven Galbraith,
Mathematics Department,
Royal Holloway,
University of London,
United Kingdom.

Pierrick Gaudry,
Laboratoire d'Informatique (LIX),
École Polytechnique ,
France.

Florian Hess,
Institut für Mathematik,
T.U. Berlin,
Germany.

Marc Joye,
Card Security Group,
Gemplus,
France.

Elisabeth Oswald,
Institute for Applied Information Processing and Communications,
Graz University of Technology,
Austria.

Kenneth G. Paterson,
Info. Sec. Group,
Royal Holloway,
University of London,
United Kingdom.

Nigel Smart,
Deptartment of Computer Science,
University of Bristol,
United Kingdom.

Frederik Vercauteren,
Department of Computer Science,
University of Bristol,
United Kingdom.

The editors would like to thank Marc Joye for various bits of LaTeX help and Georgina Cranshaw and Ian Holyer for organizing our system for exchanging various files and keeping things up to date. As always, Roger Astley of Cambridge University Press was very helpful throughout the whole process.

The authors of each chapter would like to thank the following for helping in checking and in the creation of their respective chapters:

- **Nigel Smart:** Alex Dent and Dan Brown.
- **Dan Brown:** Nigel Smart, Alex Dent, Kenneth Patterson and Ian Blake.
- **Alex Dent:** Bill and Jean Dent, Steven Galbraith, Becky George, Louis Granboulan, Victor Shoup, Andrew Spicer and Christine Swart (twice).
- **Steven Galbraith:** Paulo Barreto, Dan Boneh, Young-Ju Choie, Keith Harrison, Florian Hess, Neal Koblitz, Wenbo Mao, Kim Nguyen, Kenny Paterson, Maura Paterson, Hans-Georg Rück, Adam Saunders, Alice Silverberg, Lawrence Washington, Annegret Weng, Bill Williams and The Nuffield Foundation (Grant NUF-NAL 02).
- **Elisabeth Oswald:** The power traces presented in this chapter were made with the FPGA measurement-setup which was built by Sıddıka Berna Örs and has been presented in [**268**].
- **Marc Joye:** Benoît Chevallier-Mames and Tanja Lange.
- **Kenneth G. Paterson:** Sattam Al-Riyami, Alex Dent, Steven Galbraith, Caroline Kudla and The Nuffield Foundation (Grant NUF-NAL 02).

Contents

Preface *page* ix

Abbreviations and Standard Notation xi

Authors xv

Part 1. Protocols

Chapter I. Elliptic Curve Based Protocols
N.P. Smart 3
I.1. Introduction 3
I.2. ECDSA 4
I.3. ECDH/ECMQV 8
I.4. ECIES 12
I.5. Other Considerations 18

Chapter II. On the Provable Security of ECDSA
D. Brown 21
II.1. Introduction 21
II.2. Definitions and Conditions 23
II.3. Provable Security Results 32
II.4. Proof Sketches 33
II.5. Further Discussion 36

Chapter III. Proofs of Security for ECIES
A.W. Dent 41
III.1. Definitions and Preliminaries 42
III.2. Security Proofs for ECIES 50
III.3. Other Attacks Against ECIES 58
III.4. ECIES-KEM 61

Part 2. Implementation Techniques

Chapter IV. Side-Channel Analysis
E. Oswald 69
IV.1. Cryptographic Hardware 70
IV.2. Active Attacks 71
IV.3. Passive Attacks 72
IV.4. Simple SCA Attacks on Point Multiplications 77
IV.5. Differential SCA Attacks on Point Multiplications 84

Chapter V. Defences Against Side-Channel Analysis
M. Joye 87
V.1. Introduction 87
V.2. Indistinguishable Point Addition Formulæ 88
V.3. Regular Point Multiplication Algorithms 93
V.4. Base-Point Randomization Techniques 97
V.5. Multiplier Randomization Techniques 98
V.6. Preventing Side-Channel Analysis 100

Part 3. Mathematical Foundations

Chapter VI. Advances in Point Counting
F. Vercauteren 103
VI.1. p-adic Fields and Extensions 104
VI.2. Satoh's Algorithm 105
VI.3. Arithmetic Geometric Mean 115
VI.4. Generalized Newton Iteration 121
VI.5. Norm Computation 128
VI.6. Concluding Remarks 132

Chapter VII. Hyperelliptic Curves and the HCDLP
P. Gaudry 133
VII.1. Generalities on Hyperelliptic Curves 133
VII.2. Algorithms for Computing the Group Law 136
VII.3. Classical Algorithms for HCDLP 140
VII.4. Smooth Divisors 142
VII.5. Index-Calculus Algorithm for Hyperelliptic Curves 144
VII.6. Complexity Analysis 146
VII.7. Practical Considerations 149

Chapter VIII. Weil Descent Attacks
F. Hess 151
VIII.1. Introduction – the Weil Descent Methodology 151
VIII.2. The GHS Attack 153
VIII.3. Extending the GHS Attack Using Isogenies 166

VIII.4. Summary of Practical Implications 173
VIII.5. Further Topics 175

Part 4. Pairing Based Techniques

Chapter IX. Pairings
S. Galbraith 183
IX.1. Bilinear Pairings 183
IX.2. Divisors and Weil Reciprocity 184
IX.3. Definition of the Tate Pairing 185
IX.4. Properties of the Tate Pairing 187
IX.5. The Tate Pairing over Finite Fields 189
IX.6. The Weil Pairing 191
IX.7. Non-degeneracy, Self-pairings and Distortion Maps 192
IX.8. Computing the Tate Pairing Using Miller's Algorithm 196
IX.9. The MOV/Frey–Rück Attack on the ECDLP 197
IX.10. Supersingular Elliptic Curves 198
IX.11. Applications and Computational Problems from Pairings 201
IX.12. Parameter Sizes and Implementation Considerations 203
IX.13. Suitable Supersingular Elliptic Curves 204
IX.14. Efficient Computation of the Tate Pairing 205
IX.15. Using Ordinary Curves 208
Appendix: Proof of Weil Reciprocity 212

Chapter X. Cryptography from Pairings
K.G. Paterson 215
X.1. Introduction 215
X.2. Key Distribution Schemes 218
X.3. Identity-Based Encryption 221
X.4. Signature Schemes 228
X.5. Hierarchical Identity-Based Cryptography and Related Topics 235
X.6. More Key Agreement Protocols 240
X.7. Applications and Infrastructures 242
X.8. Concluding Remarks 250

Bibliography 253
Summary of Major LNCS Proceedings 271

Author Index 273

Subject Index 277

Part 1

Protocols