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

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