

Contents

Foreword	vii
Symbol Description	ix
1 Pairing-Based Cryptography Sébastien Canard and Jacques Traoré	1-1
2 Mathematical Background Jean-Luc Beuchat, Nadia El Mrabet, Laura Fuentes-Castañeda, and Francisco Rodríguez-Henríquez	2-1
3 Pairings Sorina Ionica and Damien Robert	3-1
4 Pairing-Friendly Elliptic Curves Safia Haloui and Edlyn Teske	4-1
5 Arithmetic of Finite Fields Jean Luc Beuchat, Luis J. Dominguez Perez, Sylvain Duquesne, Nadia El Mrabet, Laura Fuentes-Castañeda, and Francisco Rodríguez-Henríquez	5-1
6 Scalar Multiplication and Exponentiation in Pairing Groups Joppe Bos, Craig Costello, and Michael Naehrig	6-1
7 Final Exponentiation Jean-Luc Beuchat, Luis J. Dominguez Perez, Laura Fuentes-Castaneda, and Francisco Rodriguez-Henriquez	7-1
8 Hashing into Elliptic Curves Eduardo Ochoa-Jiménez, Francisco Rodríguez-Henríquez, and Mehdi Tibouchi	8-1
9 Discrete Logarithms Aurore Guillevic and François Morain	9-1
10 Choosing Parameters Sylvain Duquesne, Nadia El Mrabet, Safia Haloui, Damien Robert, and Franck Rondepierre	10-1
11 Software Implementation Diego F. Aranha, Luis J. Dominguez Perez, Amine Mrabet, and Peter Schwabe	11-1
12 Physical Attacks Nadia El Mrabet, Louis Goubin, Sylvain Guilley, Jacques Fournier, Damien Jauvart, Martin Moreau, Pablo Rauzy, and Franck Rondepierre	12-1
Bibliography	A-1
Index	I-1