

# Contents

<b>1</b>	<b>Introduction</b>	1
1.1	Background	1
1.2	Identity-Based Encryption	8
1.3	Plan of the Book	9
<b>2</b>	<b>Definitions and Notations</b>	13
2.1	Public Key Encryption	13
2.2	Identity-Based Encryption	16
2.2.1	Hierarchical Identity-Based Encryption	17
2.3	Security Model for (H)IBE	19
2.3.1	Chosen Ciphertext Attack	20
2.3.2	Chosen Plaintext Attack	22
2.3.3	Selective-ID Model	23
2.3.4	Anonymous (H)IBE	24
2.3.5	Use of Random Oracles	25
2.4	Structure of Security Proofs	26
2.5	Conclusion	28
<b>3</b>	<b>A Brief Background on Elliptic Curves and Pairings</b>	29
3.1	Finite Fields, Elliptic Curves and Tate Pairing	30
3.1.1	Exponentiation in General Cyclic Groups	30
3.1.2	Finite Fields	32
3.1.3	Elliptic Curves	33
3.1.4	Tate Pairing	39
3.1.5	Types of Pairings	43
3.2	Hardness Assumptions	44
3.3	Conclusion	48
<b>4</b>	<b>Boneh-Franklin IBE and its Variants</b>	49
4.1	Boneh-Franklin IBE	49
4.1.1	Security Against Chosen Ciphertext Attacks	54

4.2	Hierarchical Identity-Based Encryption .....	57
4.3	Boneh-Katz-Wang CPA-Secure IBE .....	59
4.4	Attrapadung et al's CCA-Secure IBE .....	60
4.5	Conclusion .....	61
<b>5</b>	<b>Selective-Identity Model .....</b>	<b>63</b>
5.1	Boneh-Boyen HIBE .....	64
5.1.1	Security .....	65
5.2	Constant Size Ciphertext HIBE .....	67
5.3	Interpreting Security Models .....	69
5.4	Conclusion .....	70
<b>6</b>	<b>Security Against Adaptive Chosen Ciphertext Attacks .....</b>	<b>71</b>
6.1	A High Level Description .....	72
6.2	Canetti-Halevi-Katz Transformation .....	72
6.2.1	One-Time Signatures .....	73
6.2.2	The Transformation .....	73
6.2.3	Security .....	74
6.3	The Boyen-Mei-Waters Transformation .....	76
6.4	Conclusion .....	80
<b>7</b>	<b>IBE in Adaptive-Identity Model Without Random Oracles .....</b>	<b>81</b>
7.1	Boneh-Boyen IBE .....	82
7.2	Waters IBE .....	83
7.2.1	Security .....	84
7.3	Generalisation of Waters IBE .....	93
7.4	Adaptive-Identity Secure HIBE .....	93
7.5	Converting to a CCA-Secure HIBE .....	94
7.6	Further Applications of Waters Technique .....	97
7.7	Conclusion .....	98
<b>8</b>	<b>Further IBE Constructions .....</b>	<b>99</b>
8.1	Gentry's IBE .....	100
8.1.1	CPA-Secure Construction .....	101
8.1.2	CCA-Secure Construction .....	105
8.1.3	Previous and Further Work .....	106
8.2	Dual System Encryption .....	107
8.2.1	Extensions .....	119
8.3	Conclusion .....	120
<b>9</b>	<b>IBE Without Pairing .....</b>	<b>121</b>
9.1	IBE Based on Number Theory .....	122
9.1.1	Cocks' IBE .....	122
9.1.2	Boneh-Gentry-Hamburg IBE .....	123
9.2	IBE From Lattices .....	125
9.2.1	Background on Lattices .....	125

9.2.2	Pre-Image Sampling . . . . .	127
9.2.3	Gentry-Peikert-Vaikuntanathan IBE . . . . .	128
9.2.4	Generalized Pre-Image Sampling . . . . .	130
9.2.5	Agrawal-Boneh-Boyer IBE . . . . .	131
9.3	Conclusion . . . . .	134
<b>10</b>	<b>Applications, Extensions and Related Primitives . . . . .</b>	<b>137</b>
10.1	Signature Schemes . . . . .	137
10.1.1	Boneh-Lynn-Shacham Short Signature . . . . .	137
10.1.2	A Hierarchical Identity-Based Signature . . . . .	139
10.2	Identity-Based Key Agreement . . . . .	143
10.3	Broadcast Encryption . . . . .	145
10.4	Fuzzy Identity-Based Encryption . . . . .	148
10.5	Public Key Encryption with Keyword Search . . . . .	149
10.6	Other Applications . . . . .	151
10.7	Conclusion . . . . .	153
<b>11</b>	<b>Avoiding Key Escrow . . . . .</b>	<b>155</b>
11.1	Distributed PKG . . . . .	155
11.2	Certificate-Less Encryption . . . . .	156
11.3	Certificate-Based Encryption . . . . .	158
11.4	Other Approaches . . . . .	160
11.5	Conclusion . . . . .	161
<b>12</b>	<b>Products and Standards . . . . .</b>	<b>163</b>
12.1	Voltage Security . . . . .	163
12.2	Trend-Micro . . . . .	164
12.3	IEEE P1363.3/D1 Draft Standard . . . . .	164
12.4	IETF Memo . . . . .	165
12.5	Conclusion . . . . .	165
<b>13</b>	<b>Bibliography . . . . .</b>	<b>167</b>
	References . . . . .	167
	<b>Index . . . . .</b>	<b>177</b>



<http://www.springer.com/978-1-4419-9382-3>

Identity-Based Encryption

Chatterjee, S.; Sarkar, P.

2011, XI, 180 p., Hardcover

ISBN: 978-1-4419-9382-3