

Table of Contents

1. Classic and Quantum Computation	1
1.1 Classical Computability Theory	1
1.2 Classical Complexity Theory	7
1.3 Quantum Information and Computation	15
1.4 Quantum Computability and Complexity	21
1.5 Conclusions, Notes, and Further Reading	26
References	28
2. Quantum Attacks on IFP-Based Cryptosystems	31
2.1 IFP and Classical Solutions to IFP	31
2.2 IFP-Based Cryptography	52
2.3 Quantum Attacks on IFP and IFP-Based Cryptography	72
2.4 Conclusions, Notes, and Further Reading	86
References	86
3. Quantum Attacks on DLP-Based Cryptosystems	93
3.1 DLP and Classic Solutions to DLP	93
3.2 DLP-Based Cryptography	109
3.3 Quantum Attack on DLP and DLP-Based Cryptography	122
3.4 Conclusions, Notes, and Further Reading	131
References	132
4. Quantum Attacks on ECDLP-Based Cryptosystems	137
4.1 ECDLP and Classical Solutions	137
4.2 ECDLP-Based Cryptography	151
4.3 Quantum Attack on ECDLP-Based Cryptography	173
4.4 Conclusions, Notes, and Further Reading	184
References	185
5. Quantum Resistant Cryptosystems	189
5.1 Quantum-Computing Attack Resistant	189
5.2 Coding-Based Cryptosystems	190
5.3 Lattice-Based Cryptosystems	192
5.4 Quantum Cryptosystems	194

5.5	DNA Biological Cryptography	196
5.6	Conclusions, Notes, and Further Reading	199
	References	200
Index		205
About the Author		207



<http://www.springer.com/978-1-4419-7721-2>

Quantum Attacks on Public-Key Cryptosystems

Yan, S.Y.

2013, VIII, 207 p., Hardcover

ISBN: 978-1-4419-7721-2