

Contents

1	Introduction	1
1.1	Classical Ciphers	1
1.1.1	Substitution Ciphers	2
1.1.2	Transposition Ciphers	3
1.1.3	Product Ciphers	5
1.2	Secret Key Encryption	7
1.2.1	Secret Key Encryption Model	7
1.2.2	Data Encryption Standard	8
1.2.3	Advanced Encryption Standard	11
1.3	Public-Key Encryption	14
1.3.1	Public-Key Encryption Model	14
1.3.2	RSA	16
1.3.3	Rabin Public-Key Encryption	20
1.3.4	Public-Key Cryptography Standards	22
	References	24
2	Homomorphic Encryption	27
2.1	Homomorphic Encryption Definition	27
2.2	Goldwasser–Micali Encryption Scheme	29
2.3	ElGamal Encryption Scheme	32
2.4	Paillier Encryption Scheme	36
2.5	Boneh–Goh–Nissim Encryption Scheme	41
	References	46
3	Fully Homomorphic Encryption	47
3.1	Fully Homomorphic Encryption Definition	47
3.2	Overview of Fully Homomorphic Encryption Schemes	49
3.3	Somewhat Homomorphic Encryption Scheme over Integers	50
3.3.1	Secret Key Somewhat Homomorphic Encryption	50
3.3.2	Public-Key Somewhat Homomorphic Encryption	54
3.4	Fully Homomorphic Encryption Scheme over Integers	58
3.4.1	Squashed Encryption	58

3.4.2	Bootstrappable Encryption	63
3.4.3	Implementation	64
References	65
4	Remote End-to-End Voting Scheme	67
4.1	Introduction	67
4.2	Remote End-to-End Voting	70
4.2.1	Participating Parties	70
4.2.2	Basic Remote Voting Scheme	70
4.2.3	General Remote Voting Scheme	74
4.2.4	Voter Reference Refresh	76
4.3	Conclusion and Discussion	78
References	78
5	Nearest Neighbor Queries with Location Privacy	81
5.1	Introduction	81
5.2	Private k Nearest Neighbor Queries	84
5.2.1	Security Model	84
5.2.2	Private kNN Queries Without Data Privacy	87
5.2.3	Private kNN Queries with Data Privacy	89
5.2.4	Private kNN Queries Based on POI Type	91
5.2.5	Private Cloaking Region	94
5.3	Performance Analysis	96
5.3.1	Protocol Performance	96
5.3.2	Performance Comparison	97
5.4	Conclusion and Discussion	97
References	98
6	Private Searching on Streaming Data	101
6.1	Introduction	101
6.2	Overview of Private Searching on Streaming Data	103
6.3	Preliminaries	106
6.3.1	Integer Addition with FHE	106
6.3.2	Integer Comparison with FHE	107
6.3.3	Binary Linear Codes	107
6.4	Definitions	108
6.5	Private Threshold Query Based on Keyword Frequency	111
6.5.1	Disjunctive Threshold Query	111
6.5.2	Conjunctive Threshold Query	115
6.5.3	Complement Threshold Query	118
6.5.4	Generic Threshold Query	121
6.6	Performance Analysis	122
6.7	Conclusion and Discussion	124
References	125

Homomorphic Encryption and Applications

Yi, X.; Paulet, R.; Bertino, E.

2014, XII, 126 p. 23 illus., 14 illus. in color., Softcover

ISBN: 978-3-319-12228-1