Contents

Preface *page* ix

1 Introduction to Privacy-preserving Computing 1
1.1 Definition and Background 1
1.2 Main Technologies of Privacy-preserving Computing 9
1.3 Privacy-preserving Computing Platforms and Cases 11
1.4 Challenges and Opportunities in Privacy-preserving Computing 12

2 Secret Sharing 13
2.1 Problem and Definition 14
2.2 Principle and Implementations 19
2.3 Advantages and Disadvantages 29
2.4 Application Scenarios 29

3 Homomorphic Encryption 36
3.1 Definition 36
3.2 Principle and Implementation 42
3.3 Advantages and Disadvantages 55
3.4 Applications 57

4 Oblivious Transfer 63
4.1 Definition 63
4.2 Implementation 64
4.3 Applications 67

5 Garbled Circuit 69
5.1 Definition 69
5.2 Implementation 71

5.3 Advantages and Disadvantages 77
5.4 Applications 77

6 Differential Privacy 80
6.1 Introduction 80
6.2 Problem Definition 82
6.3 Mechanisms for DP 89
6.4 Properties of DP 93
6.5 Applications 96
6.6 Advantages and Disadvantages 103

7 Trusted Execution Environment 105
7.1 Introduction 105
7.2 Principles and Implementations 107
7.3 Advantages and Disadvantages of TEE 113
7.4 Application Scenarios 116

8 Federated Learning 121
8.1 Background, Definition, and Categorization 121
8.2 Horizontal Federated Learning 126
8.3 Vertical Federated Learning 134
8.4 Federated Transfer Learning 139
8.5 Applications of Federated Learning 144
8.6 Future Prospectives 147

9 Privacy-preserving Computing Platforms 150
9.1 Introduction to Privacy-preserving Computing Platforms 150
9.2 FATE Secure Computing Platform 151
9.3 CryptDB Encrypted Database System 158
9.4 MesaTEE Secure Computing Platform (Teaclave) 164
9.5 Conclave Query System 172
9.6 PrivPy Privacy-preserving Computing Platform 178
9.7 Efficiency Issues and Acceleration Strategies 184

10 Case Studies of Privacy-preserving Computing 194
10.1 Financial Marketing and Risk Control 194
10.2 Advertising Billing 200
10.3 Advertisement Recommendation 204
10.4 Data Query 206
10.5 Genetic Research 209
10.6 Pharmaceutical Research 214

10.7 Speech Recognition 216
10.8 Privacy-preserving Computing in Governments 218
10.9 User Data Statistics 226

11 Future of Privacy-preserving Computing 233

References 238
Index 253