

Contents

1	Introduction	5
1.1	Outsourced Computation	6
1.2	Multi-Party Computation	7
1.3	MPC Applications	8
1.4	Overview	14
2	Defining Multi-Party Computation	15
2.1	Notations and Conventions	15
2.2	Basic Primitives	17
2.3	Security of Multi-Party Computation	19
2.4	Specific Functionalities of Interest	28
2.5	Further Reading	31
3	Fundamental MPC Protocols	32
3.1	Yao's Garbled Circuits Protocol	33
3.2	Goldreich-Micali-Wigderson (GMW) Protocol	37
3.3	BGW protocol	42
3.4	MPC From Preprocessed Multiplication Triples	44
3.5	Constant-Round Multi-Party Computation: BMR	47
3.6	Information-Theoretic Garbled Circuits	50

3.7	Oblivious Transfer	54
3.8	Custom Protocols	59
3.9	Further Reading	63
4	Implementation Techniques	65
4.1	Less Expensive Garbling	66
4.2	Optimizing Circuits	74
4.3	Protocol Execution	79
4.4	Programming Tools	83
4.5	Further Reading	85
5	Oblivious Data Structures	88
5.1	Tailored Oblivious Data Structures	89
5.2	RAM-Based MPC	93
5.3	Tree-Based RAM-MPC	94
5.4	Square-Root RAM-MPC	97
5.5	Floram	99
5.6	Further Reading	102
6	Malicious Security	103
6.1	Cut-and-Choose	103
6.2	Input Recovery Technique	108
6.3	Batched Cut-and-Choose	110
6.4	Gate-level Cut-and-Choose: LEGO	111
6.5	Zero-Knowledge Proofs	114
6.6	Authenticated Secret Sharing: BDOZ and SPDZ	117
6.7	Authenticated Garbling	122
6.8	Further Reading	125
7	Alternative Threat Models	127
7.1	Honest Majority	128
7.2	Asymmetric Trust	132
7.3	Covert Security	134
7.4	Publicly Verifiable Covert (PVC) Security	138