

Contents

1	Introduction	1
1.1	Privacy-Enhancing Technologies	1
1.2	Outline	3
2	Basics of Efficient Secure Function Evaluation	5
2.1	Common Notation and Definitions	5
2.1.1	Notation	5
2.1.2	Cryptographic Primitives	6
2.1.3	Function Representations	6
2.1.4	Adversary Model	8
2.1.5	Random Oracle Model	9
2.2	Cryptographic Primitives for Secure Two-Party Computation	9
2.2.1	Homomorphic Encryption	9
2.2.2	Garbled Circuit Constructions	12
2.2.3	Oblivious Transfer	19
2.3	Garbled Circuit Protocols	22
2.3.1	Two-Party Secure Function Evaluation	22
2.3.2	Garbled Circuit Protocols with Multiple Parties	25
3	Circuit Optimizations and Constructions	29
3.1	Introduction	29
3.1.1	Protocols with Free XOR	29
3.1.2	Related Work	30
3.1.3	Preliminaries and Notation	31
3.2	Circuit Optimizations	32
3.2.1	Minimizing Circuits	32
3.2.2	Minimizing Circuits with Free XOR	36

3.3	Efficient Circuit Constructions	38
3.3.1	Addition and Subtraction	39
3.3.2	Multiplication	40
3.3.3	Comparison, Minima and Maxima	42
3.4	Applications: Secure Comparison and Auctions.	45
3.4.1	Comparison (Millionaires Problem).	45
3.4.2	Auctions	47
4	Hardware-Assisted Garbled Circuit Protocols	51
4.1	Creating Garbled Circuits with Hardware Token	51
4.1.1	Motivation and Setting	51
4.1.2	Related Work	52
4.1.3	Architecture, System and Trust Model.	54
4.1.4	Token-Assisted SFE	55
4.2	One-Time Programs.	61
4.2.1	Motivation	61
4.2.2	Non-Interactive GCs and One-Time Programs	63
4.2.3	Evaluating GCs in HW	69
4.3	Application: Privacy-Preserving Cloud Computing	75
4.3.1	Motivation	76
4.3.2	Model for Privacy-Preserving Cloud Computing.	78
4.3.3	Architectures for Privacy-Preserving Cloud Computing	80
4.3.4	Performance Comparison	83
5	Modular Design of Efficient SFE Protocols	85
5.1	Framework for Modular SFE Protocols	85
5.1.1	Function Representations	86
5.1.2	Modular SFE	86
5.1.3	Conversion Between Encrypted Values	88
5.2	Compiling Modular SFE Protocols	90
5.2.1	Introduction	90
5.2.2	Tool for Automating Secure Two-Party Computations. . .	95
5.2.3	TASTY Input Language.	96
5.2.4	Primitives and Optimizations	100
5.2.5	Performance Measurements	101
5.3	Application: Privacy-Preserving Face Recognition.	105
5.3.1	Motivation	105
5.3.2	Face Recognition Using Eigenfaces.	107
5.3.3	Privacy-Preserving Face Recognition.	109
5.3.4	A Further Improved Hybrid Minimum Protocol	114

Contents	xiii
6 Conclusion	121
6.1 Guidelines for Constructing Efficient SFE Protocols	121
6.2 Directions for Future Research	122
6.2.1 SFE of Large Functionalities	122
6.2.2 Automatic Partitioning into Hybrid SFE Protocols	124
References	125
Index	137