

# Contents

## Part I Introduction and Definitions

<b>1</b>	<b>Introduction</b>	3
1.1	Secure Multiparty Computation – Background	3
1.2	The GMW Protocol for Secure Computation	11
1.3	A Roadmap to the Book	13
1.3.1	Part I – Introduction and Definitions	13
1.3.2	Part II – General Constructions	15
1.3.3	Part III – Specific Constructions	17
<b>2</b>	<b>Definitions</b>	19
2.1	Preliminaries	19
2.2	Security in the Presence of Semi-honest Adversaries	20
2.3	Security in the Presence of Malicious Adversaries	23
2.3.1	The Definition	24
2.3.2	Extension to Reactive Functionalities	25
2.3.3	Malicious Versus Semi-honest Adversaries	26
2.4	Security in the Presence of Covert Adversaries	30
2.4.1	Motivation	30
2.4.2	The Actual Definition	33
2.4.3	Cheating and Aborting	35
2.4.4	Relations Between Security Models	36
2.5	Restricted Versus General Functionalities	38
2.5.1	Deterministic Functionalities	39
2.5.2	Single-Output Functionalities	39
2.5.3	Non-reactive Functionalities	41
2.6	Non-simulation-Based Definitions	42
2.6.1	Privacy Only	42
2.6.2	One-Sided Simulatability	45
2.7	Sequential Composition – Simulation-Based Definitions	46

## Part II General Constructions

<b>3</b>	<b>Semi-honest Adversaries</b> .....	53
3.1	An Overview of the Protocol .....	53
3.2	Tools .....	57
3.2.1	“Special” Private-Key Encryption .....	57
3.2.2	Oblivious Transfer .....	61
3.3	The Garbled-Circuit Construction .....	63
3.4	Yao’s Two-Party Protocol .....	66
3.5	Efficiency of the Protocol .....	78
<b>4</b>	<b>Malicious Adversaries</b> .....	81
4.1	An Overview of the Protocol .....	81
4.1.1	High-Level Protocol Description .....	82
4.1.2	Checks for Correctness and Consistency .....	84
4.2	The Protocol .....	89
4.3	Proof of Security .....	93
4.3.1	Security Against a Malicious $P_1$ .....	93
4.3.2	Security Against a Malicious $P_2$ .....	99
4.4	Efficient Implementation of the Different Primitives .....	105
4.5	Efficiency of the Protocol .....	106
4.6	Suggestions for Further Reading .....	107
<b>5</b>	<b>Covert Adversaries</b> .....	109
5.1	Oblivious Transfer .....	109
5.1.1	The Basic Protocol .....	111
5.1.2	Extensions .....	119
5.2	Secure Two-Party Computation .....	121
5.2.1	Overview of the Protocol .....	122
5.2.2	The Protocol for Two-Party Computation .....	124
5.2.3	Non-halting Detection Accuracy .....	141
5.3	Efficiency of the Protocol .....	143

## Part III Specific Constructions

<b>6</b>	<b>Sigma Protocols and Efficient Zero-Knowledge</b> .....	147
6.1	An Example .....	147
6.2	Definitions and Properties .....	149
6.3	Proofs of Knowledge .....	153
6.4	Proving Compound Statements .....	158
6.5	Zero-Knowledge from $\Sigma$ -Protocols .....	160
6.5.1	The Basic Zero-Knowledge Construction .....	161
6.5.2	Zero-Knowledge Proofs of Knowledge .....	164
6.5.3	The ZKPOK Ideal Functionality .....	167
6.6	Efficient Commitment Schemes from $\Sigma$ -Protocols .....	173
6.7	Summary .....	175

<b>7</b>	<b>Oblivious Transfer and Applications</b>	177
7.1	Notational Conventions for Protocols	178
7.2	Oblivious Transfer – Privacy Only	178
7.2.1	A Protocol Based on the DDH Assumption	178
7.2.2	A Protocol from Homomorphic Encryption	182
7.3	Oblivious Transfer – One-Sided Simulation	185
7.4	Oblivious Transfer – Full Simulation	188
7.4.1	1-out-of-2 Oblivious Transfer	188
7.4.2	Batch Oblivious Transfer	196
7.5	Another Oblivious Transfer – Full Simulation	201
7.6	Secure Pseudorandom Function Evaluation	202
7.6.1	Pseudorandom Function – Privacy Only	203
7.6.2	Pseudorandom Function – Full Simulation	209
7.6.3	Covert and One-Sided Simulation	211
7.6.4	Batch Pseudorandom Function Evaluation	212
<b>8</b>	<b>The <math>k</math>th-Ranked Element</b>	213
8.1	Background	213
8.1.1	A Protocol for Finding the Median	214
8.1.2	Reducing the $k$ th-Ranked Element to the Median	216
8.2	Computing the Median – Semi-honest	218
8.3	Computing the Median – Malicious	221
8.3.1	The Reactive Greater-Than Functionality	221
8.3.2	The Protocol	223
<b>9</b>	<b>Search Problems</b>	227
9.1	Background	228
9.2	Secure Database Search	229
9.2.1	Securely Realizing Basic Database Search	231
9.2.2	Securely Realizing Full Database Search	236
9.2.3	Covert and One-Sided Simulation	237
9.3	Secure Document Search	238
9.4	Implementing Functionality $\mathcal{F}_{\text{CPRP}}$ with Smartcards	242
9.4.1	Standard Smartcard Functionality and Security	243
9.4.2	Implementing $\mathcal{F}_{\text{CPRP}}$ with Smartcards	246
9.5	Secure Text Search (Pattern Matching)	248
9.5.1	Indexed Implementation for Naor-Reingold	249
9.5.2	The Protocol for Secure Text Search	252
	<b>References</b>	255
	<b>Index</b>	261



<http://www.springer.com/978-3-642-14302-1>

Efficient Secure Two-Party Protocols  
Techniques and Constructions

Hazay, C.; Lindell, Y.

2010, XIII, 263 p., Hardcover

ISBN: 978-3-642-14302-1