

Cambridge University Press

978-1-107-04305-3 - Secure Multiparty Computation and Secret Sharing

Ronald Cramer, Ivan Bjerre Damgård and Jesper Buus Nielsen

Table of Contents

[More information](#)

Contents

*Preface**page ix***Part I Secure Multiparty Computation**

1	Introduction	3
1.1	Private Information, Uses and Misuses	3
1.2	Do We Have to Trust Someone?	5
1.3	Multiparty Computation	6
2	Preliminaries	14
2.1	Basic Notation	14
2.2	Algorithms	16
2.3	Families of Random Variables	20
2.4	Interactive Systems	24
2.5	Public-Key Cryptosystems	30
3	MPC Protocols with Passive Security	32
3.1	Introduction	32
3.2	Secret Sharing	32
3.3	A Passively Secure Protocol	36
3.4	Optimality of the Corruption Bound	47
4	Models	51
4.1	Introduction	51
4.2	The UC Model	59
4.3	Adversaries and Their Powers	79
4.4	Some Ideal Functionalities	85
4.5	Adaptive versus Static Security Revisited	93
4.6	Notes	102
5	Information-Theoretic Robust MPC Protocols	104
5.1	Introduction	104

Cambridge University Press

978-1-107-04305-3 - Secure Multiparty Computation and Secret Sharing

Ronald Cramer, Ivan Bjerre Damgård and Jesper Buus Nielsen

Table of Contents

[More information](#)

vi

Contents

5.2	Model for Homomorphic Commitments and Some Auxiliary Protocols	104
5.3	A Secure Function–Evaluation Protocol for Active Adversaries	113
5.4	Realization of Homomorphic Commitments	120
5.5	Final Results and Optimality of Corruption Bounds	133
5.6	Notes	137
6	MPC from General Linear Secret-Sharing Schemes	139
6.1	Introduction	139
6.2	General Adversary Structures	139
6.3	Linear Secret Sharing	141
6.4	A Passively Secure Protocol	148
6.5	Actively Secure Protocols	149
6.6	Notes	157
7	Cryptographic MPC Protocols	159
7.1	Introduction	159
7.2	The Case of Honest Majority	159
7.3	The Case of Dishonest Majority	161
8	Some Techniques for Efficiency Improvements	163
8.1	Introduction	163
8.2	Circuit Randomization	163
8.3	Hyperinvertible Matrices	165
8.4	Packed Secret Sharing	171
8.5	Information-Theoretic Protocols in the Preprocessing Model	173
8.6	Open Problems in Complexity of MPC	179
8.7	Notes	180
9	Applications of MPC	182
9.1	A Double Auction	182
9.2	Zero-Knowledge Proofs via MPC in the Head	191
9.3	Notes	199
Part II Secret Sharing		
10	Algebraic Preliminaries	203
10.1	Introduction	203
10.2	Groups, Rings, Fields	204
10.3	Modules and Vector Spaces	209
10.4	Quotients	212
10.5	Direct Products and Direct Sums	213
10.6	Basic Field Theory	215

Cambridge University Press

978-1-107-04305-3 - Secure Multiparty Computation and Secret Sharing

Ronald Cramer, Ivan Bjerre Damgård and Jesper Buus Nielsen

Table of Contents

[More information](#)

<i>Contents</i>		vii
10.7	Algebraic Number Fields	220
10.8	Algebras	224
10.9	Tensor Products	229
11	Secret Sharing	236
11.1	Introduction	236
11.2	Notation	237
11.3	Interpolation Codes	238
11.4	Secret Sharing from Interpolation Codes	239
11.5	Existence of Interpolation Codes	242
11.6	Alternative Proofs of Lagrange's Theorem	245
11.7	Using the Point at Infinity	247
11.8	Secret Recovery in the Presence of Corruptions	249
11.9	Formal Definition of Secret Sharing	253
11.10	Linear Secret-Sharing Schemes	260
11.11	Generalizations of Linear Secret Sharing	267
11.12	Bounds for Secret Sharing	273
11.13	Interpolation over Algebraic Number Fields and Black Box Secret Sharing	282
12	Arithmetic Codices	299
12.1	Introduction	299
12.2	The Codex Definition	299
12.3	Equivalent Definitions	306
12.4	Basic Constructions	311
12.5	Applications	314
12.6	Basic Limitations on Codices	320
12.7	Towers of Algebraic Function Fields	327
12.8	Asymptotically Good Arithmetic Secret-Sharing Schemes	342
12.9	The Torsion Limit and Its Applications	348
12.10	Outlook	352
	<i>List of Algorithms</i>	355
	<i>List of Exercises</i>	357
	<i>References</i>	359
	<i>Index</i>	369