

Table of Contents

Foreword	VII
Preface	XI
1. Introduction	1
1.1 Secure Multi-party Computation	1
1.2 Protocol Composition	8
1.2.1 Types of Protocol Composition	8
1.2.2 Feasibility of Security under Composition	10
1.3 Our Results	15
1.3.1 The Composition of Authenticated Byzantine Agreement	16
1.3.2 Secure Computation without Agreement	18
1.3.3 Universally Composable Multi-party Computation	18
2. The Composition of Authenticated Byzantine Agreement .	21
2.1 Introduction	21
2.2 Definitions	25
2.2.1 Computational Model	25
2.2.2 Byzantine Generals/Agreement	26
2.2.3 Composition of Protocols	27
2.3 Impossibility for Parallel Composition	29
2.4 Sequential Composition of Deterministic Protocols	35
2.5 Authenticated Byzantine Agreement Using Unique Identifiers	38
3. Secure Computation without Agreement	45
3.1 Introduction	46
3.1.1 Byzantine Agreement and Secure Multi-party Computation	46
3.1.2 Our Results	47
3.1.3 Related Work	51
3.2 Definitions – Secure Computation	53
3.2.1 Execution in the Ideal Model	54
3.2.2 Execution in the Real Model	58

3.2.3	Security as Emulation of a Real Execution in the Ideal Model.....	60
3.3	Broadcast with Abort.....	61
3.3.1	Strengthening Broadcast with Abort.....	62
3.4	Secure Computation with Abort and No Fairness.....	62
3.5	Secure Computation with Abort and Partial Fairness.....	72
3.6	Obtaining Security under Self Composition.....	77
4.	Universally Composable Multi-party Computation.....	81
4.1	Introduction.....	81
4.2	Overview.....	84
4.2.1	The Model.....	84
4.2.2	An Outline of the Results and Techniques.....	86
4.3	Preliminaries.....	93
4.3.1	Universally Composable Security: The General Framework.....	93
4.3.2	Universal Composition with Joint State.....	102
4.3.3	Well-Formed Functionalities.....	106
4.4	Two-Party Secure Computation for Semi-honest Adversaries ..	108
4.4.1	Universally Composable Oblivious Transfer.....	108
4.4.2	The General Construction.....	116
4.5	Universally Composable Commitments.....	128
4.6	Universally Composable Zero-Knowledge.....	141
4.7	The Commit-and-Prove Functionality $\mathcal{F}_{\text{CP}}$	143
4.7.1	UC Realizing $\mathcal{F}_{\text{CP}}$ for Static Adversaries.....	144
4.7.2	UC Realizing $\mathcal{F}_{\text{CP}}$ for Adaptive Adversaries.....	149
4.8	Two-Party Secure Computation for Malicious Adversaries ...	155
4.8.1	The Protocol Compiler.....	155
4.8.2	Conclusions.....	161
4.9	Multi-party Secure Computation.....	162
4.9.1	Multi-party Secure Computation for Semi-honest Adversaries.....	163
4.9.2	Authenticated Broadcast.....	169
4.9.3	One-to-Many Extensions of $\mathcal{F}_{\text{MCOM}}$, $\mathcal{F}_{\text{ZK}}$, and $\mathcal{F}_{\text{CP}}$	172
4.9.4	Multi-party Secure Computation for Malicious Adversaries.....	179
	References.....	185
	Index.....	191