

Contents

Part I Introduction and Fundamentals

1	Introduction	3
1.1	Introduction to E-commerce	3
1.2	Security Issues in E-commerce	6
1.3	Security Services and Protocols	8
1.4	The Non-repudiation Service	10
1.5	Challenges and Goals of this Book	12
	Appendix	14
2	Fundamentals of Non-repudiation	17
2.1	Specific Non-repudiation Services	17
2.2	Evidence	19
2.3	Roles of the TTP	21
2.4	Non-repudiation Phases	23
2.5	Non-repudiation Requirements	25
2.6	Analysis of Standards	27
2.7	Supporting Legal Framework	29

Part II Multi-Party Non-repudiation

3	Multi-Party Non-repudiation: Analysis	35
3.1	General MPNR Problem	35
3.1.1	Definitions	35
3.1.2	State of the Art Analysis	40
3.2	1-N MPNR Problem and State of the Art	47
3.3	General Contribution to Multi-Party Problem	50
3.3.1	Model Definition	53
3.3.2	Cryptographic Primitives	54
3.4	Summary of MPNR Protocol Properties	57

4	New Design Approaches for MPNR	59
4.1	MPNR Protocol for Different Messages	60
4.1.1	On-line MPNR Protocol for Distribution of Several Messages	60
4.1.2	Optimistic MPNR Protocol for Exchange of Different Messages	64
4.1.3	Fairness vs. Collusion	71
4.1.4	Further Discussions	71
4.2	Agent-Mediated Non-repudiation Protocols	74
4.2.1	Model	75
4.2.2	First Solution	75
4.2.3	Simple Agent-Mediated Protocol	77
4.2.4	Extension to Multiple Recipients	80
4.2.5	Further Extension to Multiple Messages	84
4.2.6	Applications	87
4.2.7	Requirements Fulfillment	88
4.3	Event-Oriented Simulation	89
4.3.1	Protocol	89
4.3.2	Simulation Model	90
4.3.3	Main Model Simulation Events	94
4.3.4	Output Analysis	98

Part III Applications

5	Multi-Party Non-repudiation Applications	109
5.1	Multi-Party Optimistic Fair CEM	109
5.1.1	A Protocol for Fair CEM with Deadline Time	110
5.1.2	Extension to Fair CEM with Asynchronous Timeliness	111
5.1.3	Extension to Multi-Party Fair CEM	113
5.1.4	Requirements Fulfillment	116
5.2	Multi-Party Contract Signing	119
5.2.1	A New Synchronous MPCS Protocol	120
5.2.2	Requirements Fulfillment	123
5.2.3	Achieving Abuse-Freeness	125
5.2.4	Achieving Timeliness	127
6	Scenarios Supported by MPNR Services	131
6.1	Extension of an OMA-based DRM Framework	132
6.1.1	Protocol	135
6.1.2	Design and Implementation	140
6.1.3	Requirements Fulfillment	142
6.2	Practical Service Charge for P2P Content Distribution	145
6.2.1	Scenario and Requirements	145
6.2.2	P2P Payment Protocol	147
6.2.3	A New Approach	148

- 6.2.4 Requirements Fulfillment 152
 - 6.2.5 Practical View 155
- 6.3 Free Roaming Agent Result-Truncation Defense 157
 - 6.3.1 Security Requirements 158
 - 6.3.2 Cheng-Wei Protocol 159
 - 6.3.3 Security Analysis 162
 - 6.3.4 Amendments 164
 - 6.3.5 Security Requirements Analysis 166

Part IV

- 7 Conclusions 171**
- References 177**
- Index 183**

List of Figures

1.1	Conglomerate of Applications	5
1.2	Security Architectural Elements in X.805 ITU-T Recommendation ..	9
2.1	Models of Message Transfer	18
3.1	n2n Scenario	36
3.2	Non-repudiation Service.....	38
3.3	Ferrer et al. Solution for Multi-party Certified Email	49
3.4	E-commerce Scenario	50
3.5	Layered Architecture of Non-repudiation Protocols	54
4.1	Protocol for Distribution of Different Messages	61
4.2	Optimistic Protocol with Different Messages.....	66
4.3	E-commerce Scenario with an Active Intermediary Agent.....	75
4.4	An Intuitive Solution to Non-repudiation	76
4.5	Virtual Shopping	87
4.6	Simulation Events	91
5.1	Deadline Time Intervals	111
5.2	CEM-ZOL Protocol	114
6.1	Content Distribution	133
6.2	DRM	134
6.3	Right Object Acquisition	135
6.4	HTTP Communication Flow	140
6.5	P2P Service and Payment Scenario.....	146
6.6	Application Scenario.....	156
6.7	Agent Transmission	162
6.8	Attack Scenario	163
6.9	Amended Agent Transmission.....	166

List of Tables

3.1	Multi-party Protocols' Properties Summary	58
3.2	New Solutions' Properties Summary	58
4.1	O's Computation Complexity	64
4.2	R_i 's Computation Complexity	64
4.3	TTP's Computation Complexity	64
4.4	General Off-line Solution Comparison	70
4.5	Public Key Operations Comparison	70
4.6	Simulator Entity	93
4.7	Message Entity	93
4.8	Originator Entity	94
4.9	Recipient Entity	94
4.10	TTP Entity	95
4.11	Input Test for P1	101
4.12	Output Results for P1	101
4.13	Input Test for P2	104
4.14	Output Results for P2	105
6.1	Model Notation	160
6.2	Cryptographic Notation	160