

# Contents

<i>Preface</i>	vii
<i>Acknowledgments</i>	ix
<i>List of Figures</i>	xv
<i>List of Tables</i>	xvii
1. Introduction	1
1.1 Overview of Trusted Collaborative Computing . . . . .	1
1.2 Basic Concepts in Terms of Security . . . . .	3
1.3 Basic Concepts in Terms of Reliability . . . . .	9
1.4 Abbreviations and Notations . . . . .	13
1.5 Outline . . . . .	14
2. Secure Group Communication (SGC)	17
2.1 Overview of Secure Group Communication (SGC) . . . . .	17
2.2 Typical Group Key Management Schemes for SGC . . . . .	19
2.2.1 Centralized Group Key Distribution . . . . .	20
2.2.2 De-centralized Group Key Management . . . . .	26
2.2.3 (Distributed) Contributory Group Key Agreement	29
2.2.4 Distributed Group Key Distribution . . . . .	32
2.3 Enhanced Group Key Management for SGC . . . . .	35
2.3.1 SGC for Wireless and Mobile Ad Hoc Networks .	35
2.3.2 Authenticated Key Exchange (AKE) . . . . .	38
2.3.3 Self-Healing Key Distribution . . . . .	44
2.3.4 Block-free Group Key Management . . . . .	48
2.3.5 Secure Dynamic Conferencing . . . . .	52

2.4	Conclusion . . . . .	56
3.	Cryptography based Access Control . . . . .	59
3.1	Overview of Access Control in Collaborative Computing . . . . .	59
3.2	An Efficient Differential Access Control (DIF-AC) Scheme . . . . .	64
3.2.1	System Description and Initialization . . . . .	64
3.2.2	System Dynamics and Maintenance . . . . .	67
3.2.3	Discussion . . . . .	68
3.3	Cryptographic Hierarchical Access Control (CHAC) Schemes . . . . .	71
3.3.1	HAC Model . . . . .	71
3.3.2	Directly Dependent Key Schemes . . . . .	73
3.3.3	Indirectly Dependent Key Schemes . . . . .	75
3.3.4	Polynomial and Interpolation based Schemes . . . . .	75
3.3.5	An Efficient CHAC Scheme with Locality . . . . .	77
3.4	A Uniform CHAC Scheme Based on Access Polynomials . . . . .	79
3.4.1	Principle . . . . .	80
3.4.2	Key Computation/Derivation . . . . .	80
3.4.3	Node/Vertex Level Dynamics . . . . .	81
3.4.4	User Level Dynamics . . . . .	82
3.4.5	Security and Performance Analysis . . . . .	83
3.4.6	An Illustrative Example and Experiment Results . . . . .	87
3.4.7	Discussion . . . . .	90
3.5	Conclusion . . . . .	94
4.	Intrusion Detection and Defense . . . . .	95
4.1	Overview of Intrusion Detection and Defense . . . . .	95
4.2	Intruding Attacks . . . . .	96
4.3	Intrusion Detection Models . . . . .	98
4.3.1	Anomaly Modeling . . . . .	100
4.3.2	Misuse Modeling . . . . .	101
4.3.3	Specification Modeling . . . . .	102
4.4	Intrusion Response . . . . .	104
4.5	DoS/DDoS Attacks . . . . .	105
4.5.1	Typical DoS Attacks . . . . .	105
4.5.2	Distributed Denial of Service (DDoS) Attacks . . . . .	110
4.6	Typical DoS/DDoS Defense Mechanisms . . . . .	115
4.6.1	Single-node Defending Method . . . . .	115

4.6.2	Multiple-node Defending Methods . . . . .	116
4.6.3	Honeygot . . . . .	118
4.7	Defending against DoS/DDoS Attacks–Traceback . . . . .	119
4.7.1	ICMP Traceback . . . . .	121
4.7.2	(Probabilistic) IP Packet Marking . . . . .	122
4.7.3	Hash Based Traceback . . . . .	123
4.7.4	Hybrid Approach . . . . .	124
4.7.5	Intrusion Detection and Traceback in Wireless Networks . . . . .	126
4.7.6	Pushback . . . . .	127
4.8	Exemplary DoS/DDoS Defense Research Projects and Systems . . . . .	128
4.8.1	Best Practice Methods . . . . .	128
4.8.2	D-Ward . . . . .	130
4.8.3	Netbouncer . . . . .	130
4.8.4	DefCom . . . . .	131
4.8.5	SIFF . . . . .	131
4.8.6	Hop-Count Filtering . . . . .	132
4.8.7	PacketScore . . . . .	132
4.8.8	Speak-Up . . . . .	133
4.9	Secure Overlay Service (SOS) . . . . .	134
4.10	Conclusion . . . . .	136
5.	Reliability in Grid Computing . . . . .	137
5.1	Overview of Reliability in Grid Computing . . . . .	137
5.2	Grid Service Reliability and Performance . . . . .	139
5.2.1	Description of the Grid Computing . . . . .	139
5.2.2	Failure Analysis of Grid Service . . . . .	141
5.2.3	Grid Service Reliability and Performance . . . . .	142
5.2.4	Grid Service Time Distribution and Indices . . . . .	144
5.3	Star Topology Grid Architecture . . . . .	147
5.3.1	Universal Generating Function . . . . .	147
5.3.2	Illustrative Example . . . . .	151
5.4	Tree Topology Grid Architecture . . . . .	155
5.4.1	Algorithms for Determining the pmf of the Task Execution Time . . . . .	156
5.4.2	Illustrative Example . . . . .	159
5.4.3	Parameterization and Monitoring . . . . .	163
5.5	Conclusion . . . . .	165

6.	Security in Grid Computing	167
6.1	Overview of Security in Grid Computing . . . . .	167
6.2	Existing Research on Grid Computing Security . . . . .	169
6.3	Secure Grid Communication and Controlled Resource Sharing in Grid Computing . . . . .	173
6.4	Dual-Level Key Management (DLKM) . . . . .	175
6.4.1	First Level . . . . .	175
6.4.2	Second Level . . . . .	177
6.4.3	Combination of Two Levels . . . . .	177
6.4.4	Security and Algorithm Analysis . . . . .	178
6.5	Secure Grid Computing by DLKM . . . . .	184
6.5.1	Access Local Resources . . . . .	185
6.5.2	Access Remote Resources . . . . .	186
6.5.3	Data Grid . . . . .	186
6.5.4	Non-Monitored Grid Service . . . . .	188
6.5.5	An Illustrative Example . . . . .	188
6.6	Conclusion . . . . .	192
7.	Trusted and Seamless Medical Information Systems	193
7.1	Overview of Trusted and Seamless Medical Information Systems . . . . .	193
7.2	Health Information Technology and Medical Information System . . . . .	195
7.3	Architecture of the Proposed Secure MIS . . . . .	197
7.3.1	System Architecture . . . . .	198
7.3.2	Security Functions Supported by ACP . . . . .	199
7.3.3	Tele-medicine Service . . . . .	201
7.3.4	Additional Features Resulting from the ACP Mechanism . . . . .	202
7.4	Dependable MIS based on Grid Computing Technology .	203
7.5	Conclusion . . . . .	205
	<i>Bibliography</i>	207
	<i>Index</i>	225