

# Contents

## Part I Financial Networks

<b>1</b>	<b>Mathematical Modeling of Systemic Risk .....</b>	<b>3</b>
	Hamed Amini and Andreea Minca	
1.1	Introduction .....	3
1.2	Financial Linkages and Contagion .....	5
1.2.1	Financial Networks .....	7
1.2.2	Insolvency Cascades .....	8
1.2.3	Illiquidity Cascades .....	11
1.2.4	Liquidation and Price Feedback Effects .....	15
1.3	Random Financial Network Models .....	16
1.4	Asymptotic Analysis of Default Cascades .....	20
	References .....	24
<b>2</b>	<b>Systemic Risk in Banking Networks Without Monte Carlo Simulation .....</b>	<b>27</b>
	James P. Gleeson, T.R. Hurd, Sergey Melnik, and Adam Hackett	
2.1	Introduction .....	27
2.2	Models of Contagion in Banking Networks .....	29
2.2.1	Generating Model Networks .....	30
2.2.2	Contagion Mechanisms .....	32
2.2.3	Liquidity Risk .....	34
2.2.4	Monte Carlo Simulations .....	35
2.3	Theory .....	35
2.3.1	Thresholds for Default .....	35
2.3.2	General Theory .....	37
2.4	Simplified Theory .....	39
2.4.1	Simplified Theory for GK .....	39
2.4.2	Frequency of Contagion Events .....	42

2.5	Results .....	42
2.5.1	GK Model .....	42
2.5.2	NYYA Benchmark Case .....	43
2.5.3	Networks with Fat-Tailed Degree Distributions.....	45
2.6	Discussion .....	48
	References.....	55
<b>3</b>	<b>Systemic Valuation of Banks: Interbank Equilibrium and Contagion</b>	<b>57</b>
	Grzegorz Hałaj	
3.1	Introduction.....	58
3.2	The Model .....	61
3.2.1	Valuation Fundamentals .....	61
3.2.2	Interbank Liquidity and Funding .....	62
3.2.3	Transfer of Credit Risk .....	63
3.2.4	The Equilibrium .....	64
3.2.5	Secondary Defaults: Domino Effect .....	66
3.3	Existence of Equilibrium and Numerical Procedure.....	67
3.3.1	How Does the Equilibrium Work? An Example .....	67
3.4	Back to Bank Valuation Formula .....	69
3.5	Valuation of US Banks .....	70
3.5.1	Data .....	71
3.5.2	Simulation .....	73
3.5.3	Discussion .....	74
3.6	Conclusions.....	79
3.7	Isotone $\Psi$ : The Proof.....	80
	References.....	82
<b>4</b>	<b>An Open Problem</b> .....	<b>85</b>
	John B. Walsh	

## Part II Network Security

<b>5</b>	<b>Dynamic Trust Management: Network Profiling for High Assurance Resilience</b> .....	<b>91</b>
	Mike Burmester and W. Owen Redwood	
5.1	Introduction.....	91
5.2	Overview of Related Work.....	92
5.2.1	Access Control and Trust Management .....	92
5.2.2	Intrusion Detection/Prevention Systems.....	93
5.2.3	Signature Detection Systems.....	94
5.2.4	Anomaly Detection Systems .....	95
5.2.5	Binary Versus Graduated Response Mechanisms .....	96
5.3	Threat Management .....	96
5.3.1	A Dynamic Trust Management Infrastructure .....	96
5.3.2	How the Threat Level Changes .....	98
5.3.3	Feature Selection .....	99

5.3.4	Threat Level Policies .....	99
5.3.5	Rollback Access .....	100
5.3.6	Equivocated Sanitization .....	101
5.4	Mathematical Background .....	103
5.4.1	An Introduction to Markov Chains .....	103
5.4.2	Properties of Markov Chains.....	104
5.4.3	Markov Chains of Order $m$ .....	104
5.4.4	The Markov Evolution Function .....	105
5.4.5	Hidden Markov Models .....	106
5.4.6	Bayesian Inference .....	106
5.4.7	Principal Component Analysis.....	107
5.5	Understanding Network Profiling .....	109
5.5.1	Scenario A: Defending an Enterprise Network Against Insider Privacy Attacks.....	109
5.5.2	Scenario B: Defending an Open Network Against Insider Privacy Attacks.....	111
5.6	Conclusion .....	114
	References .....	114
<b>6</b>	<b>Security Issues in Link State Routing Protocols for MANETs .....</b>	<b>117</b>
	Gimer Cervera, Michel Barbeau, Joaquin Garcia-Alfaro, and Evangelos Kranakis	
6.1	Introduction .....	117
6.2	Optimized Link State Routing (OLSR) .....	120
6.2.1	Related Work .....	123
6.2.2	Security Issues in OLSR Networks .....	126
6.2.3	Countermeasures .....	130
6.3	Hierarchical OLSR .....	131
6.3.1	Related Work .....	134
6.3.2	Security Issues in HOLSR Networks .....	138
6.3.3	Countermeasures .....	139
6.4	Multipath OLSR-Based Routing .....	140
6.4.1	Related Work .....	142
6.4.2	Security Issues in Multipath OLSR-Based Networks.....	143
6.4.3	Countermeasures .....	144
6.5	Conclusion and Future Work .....	145
6.5.1	Future Work.....	145
	References .....	146
<b>7</b>	<b>TCHo: A Code-Based Cryptosystem .....</b>	<b>149</b>
	Alexandre Duc and Serge Vaudenay	
7.1	Introduction .....	149
7.1.1	Code-Based Cryptosystems .....	150
7.1.2	Lattice-Based Cryptosystems .....	151
7.1.3	TCHo .....	152
7.1.4	Structure of This Paper .....	153

7.2	Notations and Definitions .....	153
7.3	Computational Problems .....	157
7.3.1	Low Weight Polynomial Multiple Problem .....	157
7.3.2	The Noisy LFSR Decoding Problem .....	160
7.3.3	The Noisy LFSR Distinguishing Problem .....	162
7.4	Presentation of the TCHo Cryptosystem .....	163
7.4.1	Parameters .....	163
7.4.2	Key Generation .....	164
7.4.3	Encryption .....	165
7.4.4	Decryption .....	165
7.4.5	TCHo Is a Cryptosystem .....	167
7.5	Security of TCHo .....	168
7.5.1	TCHo Is IND-CPA-Secure .....	168
7.5.2	TCHo Is Not OW-CCA Secure .....	169
7.5.3	The Herrmann-Leander Attack .....	169
7.5.4	Achieving IND-CCA Security .....	171
7.6	Implementation Results .....	172
7.6.1	Parameter Selection .....	172
7.6.2	Heuristic Assumption for the Key Generation Algorithm .....	173
7.6.3	Software Implementation .....	174
7.6.4	Hardware Implementation.....	175
7.7	Conclusion.....	175
	References.....	176
<b>8</b>	<b>Formal Model for (k)-Neighborhood Discovery Protocols .....</b>	<b>181</b>
	Raphaël Jamet and Pascal Lafourcade	
8.1	Introduction .....	181
8.1.1	Motivational Scenario .....	183
8.1.2	Contributions .....	184
8.1.3	Related Works .....	185
8.1.4	Outline .....	186
8.2	Timed Model .....	186
8.2.1	Networks and Nodes .....	187
8.2.2	Events .....	188
8.2.3	Rules and Traces.....	189
8.2.4	Intruder Rules .....	192
8.2.5	Mobility .....	194
8.3	Neighborhood and (k)-Neighborhoods.....	195
8.3.1	Neighborhood .....	195
8.3.2	(k)-Neighborhood .....	197
8.4	Example: Authenticated Ranging Protocol .....	198
8.4.1	Description of the Protocol.....	199
8.4.2	Protocol Modelling .....	199
8.4.3	Authenticated Ranging Protocol Satisfies the Neighborhood Property .....	199

8.5	$(k)$ -or-Less-Neighbors Discovery Protocol .....	202
8.5.1	Description of the Protocol.....	202
8.5.2	Rules of Sharek Protocol .....	203
8.5.3	Security of Sharek .....	204
8.6	Conclusion .....	205
	References .....	205
<b>9</b>	<b>A Tutorial on White-Box AES</b> .....	209
	James A. Muir	
9.1	Introduction.....	210
9.2	Barak et al.'s Impossibility Theorem .....	211
9.3	Table-Based Implementation .....	212
9.3.1	AES-128 .....	212
9.3.2	T-Boxes .....	215
9.3.3	$Ty_i$ Tables .....	215
9.3.4	XOR Tables .....	216
9.3.5	Table Composition.....	216
9.3.6	Summary .....	216
9.4	Protected Implementation.....	217
9.4.1	Encodings .....	218
9.4.2	Mixing Bijections.....	220
9.4.3	External Encodings .....	222
9.4.4	Summary .....	224
9.5	Cryptanalysis .....	225
9.5.1	The BGE Attack .....	225
9.6	Remarks.....	228
	References.....	229
<b>10</b>	<b>Efficient 1-Round Almost-Perfect Secure Message Transmission Protocols with Flexible Connectivity</b> .....	231
	Reihaneh Safavi-Naini and Mohammed Ashraful Alam Tuhin	
10.1	Introduction .....	232
10.1.1	Motivation of Our Work .....	233
10.1.2	Our Results .....	234
10.2	Background .....	236
10.3	1-Round $(0, \delta)$ -SMT Protocol Using Wire Virtualization .....	238
10.3.1	Virtualization Method .....	238
10.3.2	The Implementation of Protocols $\pi_1$ and $\pi_2$ .....	241
10.3.3	Security and Efficiency Analysis .....	242
10.4	Modular Construction of a 1-Round Optimal APSMT Protocol for $n = 2t + k$ .....	242
10.4.1	Main Idea .....	242
10.4.2	$(n, t, \delta)$ -Send .....	243
10.4.3	Non-interactive Privacy Amplification for SMT .....	246
10.4.4	Description of the Protocol.....	247

10.5	Modular Construction of a 1-Round Optimal APSMT Protocol for $n = (2 + c)t$ .....	248
10.6	Conclusion and Future Work .....	250
	References .....	252

### Part III Social Networks

<b>11</b>	<b>Mathematical Modelling to Evaluate Measures and Control the Spread of Illicit Drug Use</b> .....	257
	Afsaneh Bakhtiari and Alexander Rutherford	
11.1	Introduction .....	258
11.2	Model .....	259
11.3	Degree Distribution in the Scale Free Network Model .....	260
11.4	Mean Field Approximation of the Model .....	260
11.4.1	Fixed Points of the System of Equations .....	262
11.5	Bifurcation When $b$ Varies .....	263
11.6	Simulation Result .....	263
11.7	Comparison Between Analytical Result and Simulation Result ...	264
11.8	Conclusions .....	265
	References .....	267
<b>12</b>	<b>Complex Networks and Social Networks</b> .....	269
	Anthony Bonato and Yanhua Tian	
12.1	Introduction .....	269
12.2	Properties of Complex Networks .....	270
12.3	Models of Complex Networks .....	272
12.3.1	Kronecker Graphs .....	272
12.3.2	The ILT Model .....	273
12.3.3	Affiliation Networks .....	275
12.3.4	The MAG Model .....	276
12.3.5	The GEO-P Model .....	277
12.4	Open Problems .....	284
	References .....	285
<b>13</b>	<b>NAVEL Gazing: Studying a Networked Scholarly Organization</b> .....	287
	Dimitrina Dimitrova, Barry Wellman, Anatoliy Gruzd, Zack Hayat, Guang Ying Mo, Diana Mok, Thomas Robbins, and Xiaolin Zhuo	
13.1	Introduction: Networked Work in Networked Organizations .....	288
13.2	Literature Review .....	289
13.2.1	The Turn to Networked Organizations .....	289
13.2.2	Benefits and Costs of Networked Organizations .....	291
13.2.3	Organization of Work and Collaborative Practices .....	293
13.3	The GRAND Network of Centres of Excellence .....	294
13.4	Methods .....	296

13.5	Findings.....	297
13.5.1	Rationales for Participating .....	297
13.5.2	Relationships in the GRAND Network.....	299
13.5.3	Modes of Communication.....	301
13.5.4	Relationships Within Projects.....	302
13.5.5	GRAND as a Networked Organization?.....	304
13.6	Conclusions.....	308
	References.....	311
<b>14</b>	<b>How Al Qaeda Can Use Order Theory to Evade or Defeat U.S. Forces: The Case of Binary Posets .....</b>	<b>315</b>
	Jonathan David Farley	
14.1	Introduction.....	315
14.2	Proof that the Optimal Binary Terrorist Cell with One Leader Is a Pure Fishbone Poset.....	318
14.3	Conclusion.....	321
	References.....	322
<b>15</b>	<b>The ABCs of Designing Social Networks for Health Behaviour Change: The VivoSpace Social Network .....</b>	<b>323</b>
	Noreen Kamal, Sidney Fels, Mike Blackstock, and Kendall Ho	
15.1	Introduction.....	323
15.2	Related Work .....	324
15.2.1	Technologies for Health Behaviour Change.....	325
15.2.2	Use of Theoretical Models When Designing ICTs .....	325
15.2.3	Personal Informatics.....	326
15.3	Determinants from Theoretical Models .....	327
15.3.1	Motivation for the Use of Online Social Networks .....	327
15.3.2	Motivation for Health Behaviour Change .....	329
15.4	ABC Framework .....	331
15.4.1	Appeal.....	331
15.4.2	Belonging .....	333
15.4.3	Commitment .....	333
15.5	Evaluation .....	334
15.5.1	Questionnaire: Recruitment and Respondents .....	335
15.5.2	Questionnaire: Results.....	335
15.5.3	Interviews .....	337
15.5.4	Iteration of the Framework.....	340
15.6	Design Strategies .....	340
15.6.1	Appeal.....	340
15.6.2	Belonging .....	341
15.6.3	Commitment .....	342
15.7	Case Study: VivoSpace .....	342
15.8	Conclusions.....	346
	References.....	346

<b>16</b>	<b>Evolution of an Open Source Community Network</b> .....	349
	Nilesh Saraf, Andrew Seary, Deepa Chandrasekaran, and Peter Monge	
16.1	Introduction .....	350
16.2	Literature .....	351
16.2.1	Software Engineering and OSS Project Networks .....	351
16.2.2	Complex Networks of OSS Projects .....	352
16.3	Data and Exploratory Analysis .....	353
16.3.1	Sampling .....	354
16.3.2	Analysis of Network Degrees .....	355
16.3.3	Analysis of Non-random Network Formation Processes .	357
16.3.4	Analysis of Network Change .....	360
16.4	Contribution, Limitations and Future Research .....	366
	References .....	377
<b>17</b>	<b>SociQL: A Query Language for the SocialWeb</b> .....	381
	Diego Serrano, Eleni Stroulia, Denilson Barbosa, and Victor Guana	
17.1	Introduction .....	381
17.2	Background .....	384
17.2.1	Social Networking Theories .....	384
17.2.2	Web Query Languages .....	384
17.2.3	Social Networking Data Services .....	386
17.2.4	Special-Purpose Query Languages .....	386
17.3	The SociQL Conceptual Framework .....	387
17.3.1	“sameAs” Interlinks .....	389
17.4	The Query Language .....	389
17.4.1	Influence and Induction .....	390
17.4.2	Interlinking Predicates .....	392
17.4.3	Visualizing Query Results .....	392
17.5	Design and Implementation of the SociQL Service .....	394
17.5.1	The Visual Query Editor .....	395
17.5.2	Query Execution in the SociQL Service .....	396
17.5.3	The System Catalog .....	396
17.5.4	Visibility and Reputation .....	398
17.5.5	Query Execution .....	399
17.5.6	The Query Planer .....	399
17.5.7	Linking Across Social Networks .....	400
17.6	The SociQL Service as a Means for Social-Network Interoperability .....	401
17.7	Conclusions and Future Work .....	403
	References .....	405
	<b>Index</b> .....	407



Advances in Network Analysis and its Applications

Kranakis, E. (Ed.)

2013, XVI, 412 p., Hardcover

ISBN: 978-3-642-30903-8